



# Implementing a Zero Trust approach with Azure Active Directory

## An illustrated technical overview

Authors: Philippe Beraud, Jean-Yves Grasset, Arnaud Jumelet (Microsoft France)

June 2019

For the latest up-to-date information about Azure Active Directory, you can visit the site:

<https://azure.microsoft.com/en-us/services/active-directory/>

This page is intentionally left blank.

# Table of contents

<b>DISCLAIMER.....</b>	<b>1</b>
<b>INTRODUCTION .....</b>	<b>2</b>
FORETHOUGHT .....	2
OBJECTIVES OF THIS WHITE PAPER.....	6
NON-OBJECTIVES OF THIS WHITE PAPER.....	6
ORGANIZATION OF THIS WHITE PAPER.....	6
AUDIENCE OF THIS WHITE PAPER .....	6
<b>DID YOU SAY ZERO TRUST (NETWORKS)? .....</b>	<b>7</b>
A VISION AND ITS PRINCIPLES .....	7
FROM THEORY TO A FIRST PRACTICAL IMPLEMENTATION.....	8
A SECOND "ITERATION" .....	9
TOWARDS A VISION MORE ALIGNED WITH REALITY.....	10
<b>MICROSOFT'S ZERO TRUST APPROACH .....</b>	<b>11</b>
END-TO-END SECURITY .....	11
CONDITIONAL ACCESS IN AZURE AD AT THE HEART OF THE STRATEGY .....	17
<b>MICROSOFT ZERO TRUST APPROACH'S IMPLEMENTATION PRINCIPLES.....</b>	<b>24</b>
VERIFYING IDENTITY .....	24
MANAGING DEVICES.....	39
MANAGING APPLICATIONS .....	47
PROTECTING DATA.....	53
STOPPING CYBER-ATTACKS .....	58
<b>CONCLUSION .....</b>	<b>63</b>
<b>REFERENCES.....</b>	<b>64</b>



# Disclaimer

This white paper is a reflection on the term Zero Trust (Networks) – as perceived by Microsoft France as of the date of this document – along with an implementation approach through Azure Active Directory (Azure AD), the Microsoft cloud service that manages identities and access at scale, as well as other cloud-based services, products, or Microsoft security technologies.

This document is provided for informational purposes only.

MICROSOFT DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO THE INFORMATION CONTAINED IN THIS WHITE PAPER. The white paper is provided "as is" without warranty of any kind and cannot be construed as a commitment on the part of Microsoft.

Microsoft cannot guarantee the veracity of the information presented. The information in this white paper, including but not limited to internet website and URL references, is subject to change at any time without notice. Furthermore, the opinions expressed in this white paper represent the current vision of Microsoft France on the issues cited at the date of publication of this white paper and are subject to change at any time without notice.

All intellectual and industrial property rights (copyrights, patents, trademarks, logos), including exploitation rights, rights of reproduction, and extraction on any medium, of all or part of the data and all of the elements appearing in this paper, as well as the rights of representation, rights of modification, adaptation, or translation, are reserved exclusively to Microsoft France. This includes, in particular, downloadable documents, graphics, iconographic, photographic, digital, or audiovisual representations, subject to the pre-existing rights of third parties authorizing the digital reproduction and/or integration in this paper, by Microsoft France, of their works of any kind.

The partial or complete reproduction of the aforementioned elements and in general the reproduction of all or part of the work on any electronic medium is formally prohibited without the prior written consent of Microsoft France.

Published: June 2019

Version 1.0

© 2019 Microsoft France. All rights reserved

# Introduction

## Forethought

The perimeter approach is obsolete!

The perimeter protection approach consists of defining and then controlling a boundary to make it watertight against the outside, considered hostile, the interior being considered trusted.

The analogy with the defensive principles of the castle is often used: the castle is surrounded by high walls, the ramparts, which connect towers positioned in the corners. The entrance is made by a single portal controlled by a series of mechanisms: a bridge, a drawbridge and often even a barbican. The overall can be surrounded by moats, ditches often filled with water to limit the risk of attacks by a work of undermining.

This perimeter protection, however, suffers from an inherent weakness, which is to assume that all people inside the perimeter are trustworthy. A classic attack is to bribe a resident of the castle who will enable access by lowering defense systems. The enemy army will then be able to enter through the opening without having to work hard to try to destroy the external defense lines.

This example is transposable to the perimeter protection of information systems. The DMZ is the border between the hostile exterior (the Internet) and the internal network of the organization. Firewalls implement the mechanisms for filtering and controlling inbound and outbound flows. Through the network address translation (NAT) mechanism, hosts within the network can access external resources (websites, applications, or cloud services) without being directly visible: only the entry point controlled by the firewall is accessible and renders internal resources and hosts invisible.

The flaw in this protection system is that, even if filtered, there is a two-way communication between an internal host and an outside service: the computer located inside becomes highly vulnerable and can be compromised. If the user is incited to click a link triggering the download of a malware exploiting a security flaw, the device located in the internal trusted zone is compromised and now serves as the gateway for the attacker. It is as if we had used cunning to bribe a resident of the castle and then use him to access resources or make him open the gates of the fortress.

The next phase is for the attacker to remain in the place and continue his work of compromise by lateral movements, trying to acquire higher rights by privilege escalation. This will allow him to access more sensitive information and ultimately take full control of the information systems.

The example of the ransomware "WannaCry" is eloquent: even if the compromising vector is not confirmed – it is probably a phishing mail –, the "DoublePulsar" malware is injected and, running in kernel mode, encrypts the computer local disk. "WannaCry" then relies on a flaw in a SMB v1 Protocol older version (i.e. EternalBlue) to propagate to the organization internal network and infects all systems that have not yet received the security patch, even though it had been released more than two months earlier. The spread was lightspeed fast and, luckily, was stopped by the discovery of a "killswitch", but the result is damning, with an estimate of 300,000 to 400,000 victims in 174 countries.

In response to "WannaCry", organizations reacted quickly by updating security patches ; this limited the damage of "(not) Petya", which appeared a month and a half later, the effects of which being even more destructive.

This demonstrates the extreme vulnerability of a perimeter security model to new threats – creating a single entry point can cause the entire internal network to be infected – and advocates for a fundamental overhaul of the security model.

Recognizing the obsolescence of the perimeter protection model is not new, but it is necessary to design a new approach that can be broken down into solutions and not just remains conceptual.

In 2009, Forrester published a report acknowledging this reality and outlining some simple concepts.

The evocative title of this report [NO MORE CHEWY CENTERS: THE ZERO TRUST MODEL OF INFORMATION SECURITY](#) referred<sup>1</sup> to the fact that information system, like a crunchy candy, had to be protected by a hard shell – the boundary with external networks – while offering a soft interior to allow unhindered communication on the internal network.

In this report, Forrester coined the phrase "Zero Trust" in the context of a model that is summarized by the following quotation:

***In Zero Trust, all network traffic is untrusted. This means that security professionals must ensure that all resources are accessed securely regardless of location, adopt a least privilege strategy, strictly enforce access control, and inspect and log all traffic<sup>2</sup>.***

---

This synthesis remains very general and needs to be analyzed.

We find the same "motto" in the book [ZERO TRUST NETWORKS, BUILDING SECURE SYSTEMS IN UNTRUSTED NETWORKS](#)<sup>3</sup> by Doug Barth and Evan Gilman:

***The assumption that systems and traffic within a datacenter can be implicitly trusted is flawed. Modern networks and usage patterns no longer echo those that made the perimeter defense make sense many years ago. As a result, moving freely in a "secure" infrastructure is frequently trivial once a single host or link has been compromised.***

---

Even if the protection layer is composed of several layers in accordance with the concepts of defense in depth, the end result is the same: once the shell is pierced, the soft belly of the information system is exposed, i.e. "the soft interior of the confectionery".

## The world has changed

### Waves of change

To date, three huge waves of change have impacted organizations and contributed further to the obsolescence of the perimeter approach:

1. Rationalization and outsourcing of information technology (IT),
2. APIs economy,
3. Consumerization of IT.

These three "tsunamis" form the key industry trends and are now an integral part of the landscape of organizations, together with the Internet of Things (IoT) which is in full expansion. Technology and its

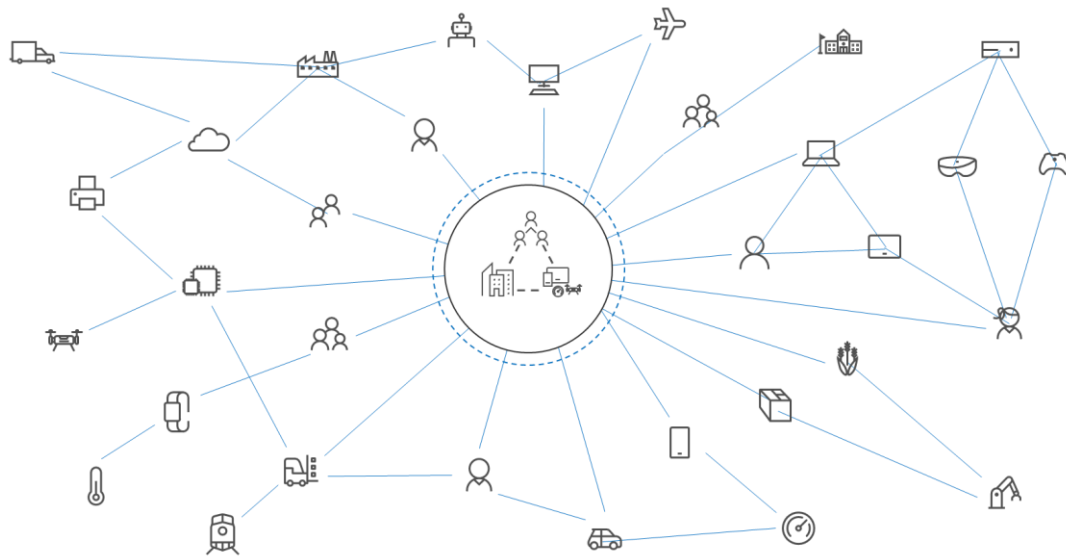
---

<sup>1</sup> NO MORE CHEWY CENTERS: THE ZERO TRUST MODEL OF INFORMATION SECURITY:  
<https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682>

<sup>2</sup> Ibid

<sup>3</sup> Zero Trust Networks, Building Secure Systems in Untrusted Networks: <http://shop.oreilly.com/product/0636920052265.do>

uses have triggered a change to the historical paradigm that blurred the boundaries: business versus personal world, physical versus digital world, inside versus outside the firewall, etc.



Rationalization and outsourcing of information technology (IT)

Organizations have no choice but to become "slimmer", better targeted and more responsive to their goals and missions. Under such conditions, organizations need decisive changes to survive and often have little choice but to carry out their digital transformation in one way or another (see next section).

Many organizations have started using the public cloud for their new applications (whether internal IT is in agreement or not, creating the "Shadow IT" phenomena, which we will discuss later), and many have already opted for the use of ready-to-use SaaS (Software-As-A-Service) solutions for generic activities (for example, Office/Microsoft 365, Salesforce.com, Workday, etc.).

APIs economy



As the components of the cloud ecosystem materialize, all organizations can create their own systems, applications or services (or part of them) in the form of cloud services that use these modules. As a result, organizations can expose their "specialized" services via simple RESTful APIs that can be consumed in turn, via appropriate API management, by other organizations, applications and services, through a so-called open innovation.

This allows organizations to focus on what they do best, avoid unnecessary developments, and maximize their competitiveness.

## Consumerization of IT

Another significant development is the fact that the devices including laptops, smartphones, tablets and hybrids have become more affordable in recent years and therefore, unsurprisingly, proliferate.

The same applies to cellular and wireless networks that have become ubiquitous. Social networks (Facebook, Instagram, LinkedIn, etc.) and their corporate counterparts or CSN (Yammer, etc.) change the way people get information and communicate.

Everyone wishes (and expects) the content to be accessible and services to operate transparently across all of these devices and environments. Everyone is becoming more and more connected: at home, at work and everywhere, to the point where personal and professional communications become indistinguishable from each other.

As technology plays an increasingly important role in everyone's personal life, expectations from professional technology solutions increase accordingly.

People have access to powerful and affordable computers, laptops and tablets, they are increasingly using mobile devices; they expect permanent connectivity and connect in new ways, using social (corporate) networks. Ultimately, they have more choices, more options and more flexibility in the technology that they use every day and, as this technology spreads in their professional lives, the boundary between personal time and professional time is fading. People want to be able to choose the technology they use at work and increasingly want to use the same technology in all aspects of their lives.

The "Consumerization of IT" is the current phenomenon by which consumer technologies and consumers' behavior are, in different ways, the drive for innovation in Information Technology within organizations. As people feel more comfortable with technological innovations in their personal lives, they expect the same experience in their professional lives. This translates, for example, in the concept of BYOS (Bring Your Own Software).

Employees undoubtedly expect access to everything from anywhere: i) from any location: at work, at home or when mobile, ii) from any device, whether or not managed, owned by them or by the company, and with a user interface that meets the high standards dictated by the consumption world.

## Digital transformation in motion

Most organizations are profoundly challenged by the emergence of all types and sizes of disruptive actors in their markets and are forced to transform to survive. Improving agility and developing a culture of continuous change to become able to continuously redefine what is possible and be able to deploy new optimized operating models, is vital for those organizations. Those are the indispensable foundations to become able to better understand the customer expectations, to improve existing and create new customer experiences, to invent new business models and, ultimately, to generate new sources of revenue.

Digital transformation is therefore a key factor of growth, innovation and differentiation in a market with heightened competition.

In this context, the increasing usage of the cloud by these organizations, the use of more and more varied types of device, and more and more mobility scenarios, present new challenges to provide adequate security, as parts of the processing and data, are now, de facto, outside the reassuring boundaries of the firewalls.

## Objectives of this white paper

In light of the above, this white paper first proposes i) to revisit the term "Zero Trust" and what it covers in its structuring principles, then ii) to describe how these principles apply to a computer environment to improve end-to-end security, and, finally, iii) to discuss how to translate these principles concretely with Azure Active Directory (Azure AD) and Microsoft security services, products and technologies.

## Non-objectives of this white paper

The purpose of this white paper is not to constitute an introduction to Azure AD, or a comprehensive description of all the security services, products and technologies offered by Microsoft or a step-by-step guide to implementing the services, products and technologies required for the implementation of a "Zero trust" vision.

Nor is it intended to replace the detailed online documentation available, but rather to provide an overview of the services, products and technologies that can be integrated in the implementation of a "Zero Trust" approach – it provides many links to the official documentation from Microsoft and blog posts that allow to deepening each of the covered topics.

## Organization of this white paper

To cover the objectives stated above, this document is organized according to the following sections:

- DID YOU SAY ZERO TRUST (NETWORKS)?
- MICROSOFT'S ZERO TRUST APPROACH;
- MICROSOFT ZERO TRUST APPROACH'S IMPLEMENTATION PRINCIPLES.

We hope that this structure allows for a progressive and clear approach to the various topics addressed, in order to help understand the key principles that support the adoption and implementation of a Zero Trust (networks) approach with Azure AD (and security services, products, and technologies) and Microsoft's associated strategy and investments in this area.

## Audience of this white paper

This document is intended for IT professionals, system architects, and all those interested in the concept of Zero Trust Networks (ZTN) and its realization and implementation principles based on Microsoft services and technologies, and in particular Azure Active Directory (Azure AD).

# Did you say Zero Trust (Networks)?

The protection based on the perimeter model has, for about ten years, largely demonstrated its ineffectiveness against the latest threats – we have shared some illustrations in the introduction. Throughout this period, threats have only increased: they culminated in the form of Advanced Persistent Threats (APTs) which aim to exfiltrate sensitive information – quite simply data theft –, or more recently, in the form of ransomwares such as “Wannacry”, or outright destructive malwares such as “(Not)Petya”.

It is unfortunately clear that with the digital transformation, the whole society is increasingly exposed. In the face of the explosion of the number of attacks, the awareness of the digital risk remains very inadequate today. In a context marked by the massive digitization of data and the increasing interconnectivity of networks, securing computer systems becomes an imperative and a crucial issue for our companies, now exposed to very real systemic risks.

Companies themselves lack of confidence in their resilience despite security solutions they put in place (more than 10 on average); this tends to demonstrate, if it were necessary, that the existing approach is probably no longer the right one.

Recently, the terms Zero Trust Networks and Zero Trust Model have made headlines again, but what exactly does it cover? How could security issues, which have increased with the necessary and inevitable opening of information systems to take into account the “new world” with its scenarios of mobility and numerical nomadism and its Cloud applications, be solved with a new “Zero Trust” approach?

To do this, we propose to start from the “ZERO trust” vision and the main principles that derive from it.

## A vision and its principles

It can be inferred from the reinterpretation of Forrester's vision discussed above, that the model is based on the following broad principles:

1. **All resources must be secure.** The term resources here is taken in a broad sense and encompasses the resources accessed (data, applications, services, etc.) as well as the resources accessing them (devices, services, etc.). The notion of managing resources according to their sensitivity, will only appear later.
2. **Communication flows must be considered unreliable unless proven otherwise.** All traffic must be inspected to detect suspicious behaviors and logged.
3. **The location or hosting model is irrelevant.** This means that, wherever the resource is accessed from or wherever the resource itself is located, access control must be the same. Clearly, this principle applies to applications and other resources hosted in the cloud, even if in 2009 hosting (outsourcing) was the dominant trend and the cloud was in its infancy.
4. Access to resources must be limited and significantly reinforced, with special consideration for privileged identities (power accounts). This implies that access control will be implemented in a holistic manner and that privileged accounts will be more particularly protected and scrutinized.

This relatively generic approach first appeared in 2009 and was initially translated in the form of a network-oriented implementation that was very logically called “Zero Trust Networks” or “ZTN”. This is the purpose of the next section.

# From theory to a first practical implementation

The first implementation from the Forrester theory was done by adapting the principles of "Zero Trust" to internal network architectures. The proposed solution is based on the following three pillars:

1. Segmentation of the network to isolate resources in different zones according to their sensitivity;
2. Access control to the different zones by a central gateway, in which access control strategies are defined according to the users and resources accessed;
3. A network flow control system.

In the presentation [5 STEPS TO A ZERO TRUST NETWORK-FROM THEORY TO PRACTICE](https://fr.slideshare.net/AlgoSec/5-steps-to-a-zero-trust-network-from-theory-to-practice)<sup>4</sup> dated 2015, Forrester details 5 steps to implement a ZTN solution, including the identification of sensitive data sources (referred to as "toxic" according to the chosen terminology), the transaction flow mapping, the segmentation architecture, access rules definition and updates based on traffic analysis.

Based on these principles, the leading network solution providers have proposed bricks for the implementation of ZTN solution components, by upgrading their firewall solution to more intelligent versions (Next Generation Firewall or NGFW) and adding a centralized control system. New solutions implementing a network micro-segmentation closest to resources have also emerged.

This approach is not new since Microsoft advocated and implemented it in the mid-2000, with a solution based on the generalized implementation of IPsec in transport mode and centralized control by Active Directory policies.<sup>5</sup>

But this approach is restrictive by the fact that it remains purely focused on the security of the **internal network** and neglects important elements in a modern approach to security, such as securing identities and devices, attack detection (and associated responses), etc. During this first evolution, "Zero Trust" came to be associated, in the words of Forrester, *"primarily with the network segmentation and the obvious vehicle for enforcing that segmentation, the next-generation firewall (NGFW)"*<sup>6</sup>.

**Note** According to Gartner, a Next-Generation Firewall (NGFW) is a "deep packet inspection firewall" that exceeds the inspection and blocking of port/protocol by adding an application-level inspection, intrusion prevention and intelligence gathering from outside the firewall".

---

<sup>4</sup> 5 STEPS TO A ZERO TRUST NETWORK - FROM THEORY TO PRACTICE: <https://fr.slideshare.net/AlgoSec/5-steps-to-a-zero-trust-network-from-theory-to-practice>

<sup>5</sup> DOMAIN ISOLATION POLICY DESIGN: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/domain-isolation-policy-design>

<sup>6</sup> FORRESTER, THE ZERO TRUST EXTENDED (ZTX) ECOSYSTEM JANUARY 19, 2018: <https://go.forrester.com/blogs/the-zero-trust-x-wave-ground-truth/>

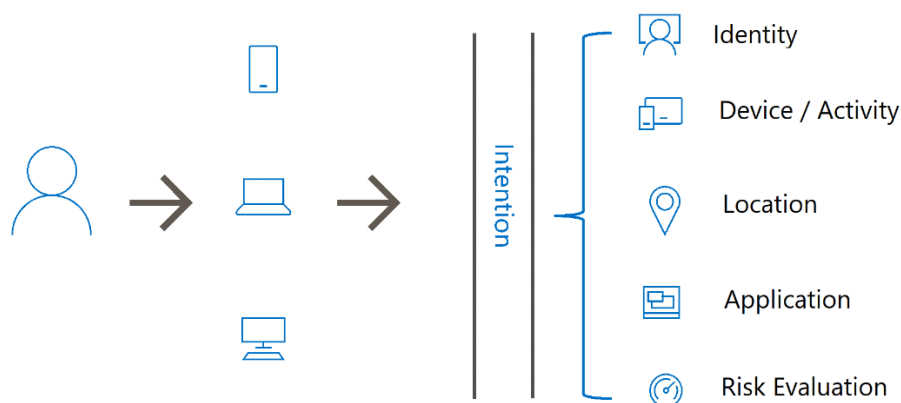
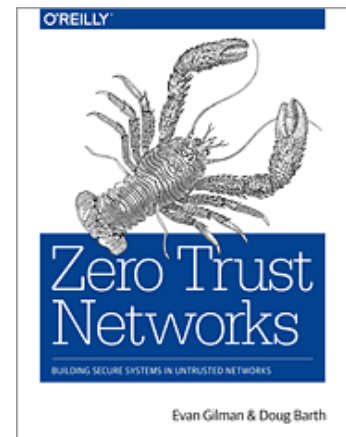
## A second "iteration"

The detailed vision in the book [ZERO TRUST NETWORKS, BUILDING SECURE SYSTEMS IN UNTRUSTED NETWORKS](http://shop.oreilly.com/product/0636920052265.do)<sup>7</sup> by Doug Barth and Evan Gilman revisits the previous principles and proves much more developed.

It carries through the essential role of the central control system (*control plane*) and defines all resources as part of the *data plane*. All access requests go through the central control system, which only accepts secure and authenticated connections from devices and users.

Access to the resource in the data plane will be allowed or declined, depending on the resource to be accessed and the access rules. Those can consider dynamic criteria such as user identity parameters (his/her role in the organization), the type of device, the access times, the physical location, etc. The user may be asked to provide a stronger authentication method like, for example, a multi-factor authentication. From a network point of view, the path to the resource in the data plane is dynamically configured to accept traffic from the client.

The first important element is the introduction of a conditional access control.



According to the authors:

***The basic idea is that an authoritative source, or trusted third party, is granted the ability to authenticate, authorize, and coordinate access in real time, based on a variety of inputs.***

This more recent and far more comprehensive approach introduces the new important element, which is the concept of identity for both the user and the device:

- The identity trust is based on scrupulous and robust identity management by the directory or directories that have the responsibility, authority and strength of authentication. The latter can be based on passwords whose complexity should be controlled, on authentication without password based on FIDO2<sup>8</sup> standards, biometrics, multi-factor authentication, etc.

---

<sup>7</sup> Zero Trust Networks, Building Secure Systems in Untrusted Networks: <http://shop.oreilly.com/product/0636920052265.do>

<sup>8</sup> FIDO2 WebAuthn & CTAP: <https://fidoalliance.org/fido2/>

- The security of the device is addressed with the use of the Trusted Platform Module (TPM) to secure the OS boot sequence (secured boot), the X.509 certificate authentication for secure connections, the presence of the device in the inventory or management tool, etc., which are additional confidence criteria for evaluation by the central control system.

Even though the reflection is starting to evolve towards a broader vision, it is still very much oriented towards internal networks. For example, access control remains at the network level on 802.1x and the central control system acts on the opening of the network flows. Moreover, the crucial game changer that is the cloud and its impact on organizations (federated) information systems, and the introduction and increased efficiency of artificial intelligence (AI) for detection and active threat protection, are however not yet taken into account.

## Towards a vision more aligned with reality

Since the introduction of the “Zero Trust” terminology in 2009, and the subsequent introduction in 2015, of a more practical implementation centered on network security, the Forrester’s 2018 vision has evolved significantly, to develop a more holistic approach including data (Zero Trust Data), identities (Zero Trust People), devices (Zero Trust Device), workloads and the threat detection portion and response automation<sup>9</sup>.

The concept is now far beyond the protection of the internal network – which is only one of the components of this latest vision – with a refocusing on the main security principles of data classification and protection (through encryption), identity management and protection, particularly privileged accounts control, application protection, and protection of all devices including the Internet of Things (IoT).

This broader approach is described in a new version of the Forrester’s white paper [FIVE STEPS TO A ZERO TRUST NETWORK, ROAD MAP: THE SECURITY ARCHITECTURE AND OPERATIONS PLAYBOOK \(OCTOBER 1, 2018\)](#)<sup>10</sup> which (at last) introduces the cloud in the equation (see section § THE WORLD HAS CHANGED).

Conditional access control remains an important and central element, but the emphasis is on the classification and protection of data by encryption, whose access, when internally hosted, is controlled and constrained by a micro-segmentation approach. Threat detection is introduced with the discussion of SOC (Security Operations Center) processes and their enhanced automation.

Finally, the consideration given to the new challenges created by mobility, device proliferation and the generalization of the cloud in its most diverse uses, opens the reflection beyond the previously network restricted vision.

---

<sup>9</sup> The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018: <https://go.forrester.com/blogs/the-zero-trust-x-wave-ground-truth/>

<sup>10</sup> Five Steps To A Zero Trust Network, Road Map: The Security Architecture And Operations Playbook: <https://www.forrester.com/report/Five+Steps+To+A+Zero+Trust+Network/-/E-RES120510>

# Microsoft's Zero Trust approach

## End-to-end security

For many years, Microsoft has been advocating for the adoption of end-to-end security best practices that the main principles in the "Zero Trust" approach encompass.

As such, the document published in 2013 [BRING YOUR OWN DEVICE: SECURITY VISION AND SOLUTIONS APPROACH](https://www.slideshare.net/ZDNet_France/microsoft-francebringyourowndevice)<sup>11</sup> already proposed evolution of the perimeter security model towards the concept of access context – device security, identity trust, authentication strength and location of connection – to adapt permissions based on the sensitivity level of the data.

Most of the principles underpinning the "Zero Trust" philosophy were already included, such as strong user identity verification, dynamic access control depending on the context, securing the devices used to access data, securing the transmission channels – for an end-to-end protection between data and data consumer guaranteeing data confidentiality and integrity in transit. Topics such as the classification and protection of data by encryption were also addressed, the data constituting the new "perimeter".

The evolution and proliferation of threats render necessary the adoption of an "assume breach" posture instead of a perimeter protection focused approach. Whether or not you have experienced a security incident in the past, you probably know that it is not a question of *whether* an attacker will succeed in compromising your enterprise resources, but *when*.

The major shift in the reflection is to consider that the digital defenses **in place are vulnerable at any given time**.

We live in a world where attacks and attack vectors can come from anywhere. Unfortunately, the news reports every day that the attacks are increasingly sophisticated and the attackers more and more organized. It is a world without a perimeter, dynamic and in perpetual evolution.

To accept such a posture does not mean to give up; it means that you have taken the first step towards mitigating the risks for data integrity in the digital age, as evidenced by the article [ASSUMPTION OF BREACH: HOW A NEW MINDSET CAN HELP PROTECT CRITICAL DATA](http://searchsecurity.techtarget.com/tip/Assumption-of-breach-How-a-new-mindset-can-help-protect-critical-data)<sup>12</sup>.

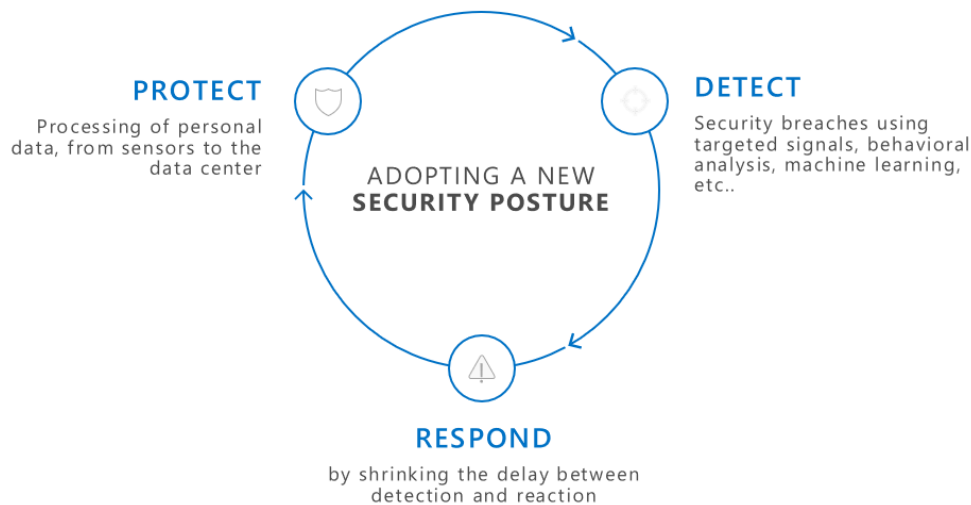
So, what is plan B? What is the plan to detect an intrusion? How do you react to this type of incident?

---

<sup>11</sup> BRING YOUR OWN DEVICE: SECURITY VISION AND SOLUTIONS APPROACH: [https://www.slideshare.net/ZDNet\\_France/microsoft-francebringyourowndevice](https://www.slideshare.net/ZDNet_France/microsoft-francebringyourowndevice)

<sup>12</sup> ASSUMPTION OF BREACH: HOW A NEW MINDSET CAN HELP PROTECT CRITICAL DATA: <http://searchsecurity.techtarget.com/tip/Assumption-of-breach-How-a-new-mindset-can-help-protect-critical-data>

This concept implies moving to a more holistic approach including at least the three pillars to address the following objectives:



Therefore, this modern protection strategy requires proactive threat prevention – what was so far referred to as “protection” – to which must be added early threat detection and fast response.

The functions Protect, Detect, and Respond are a continuum as illustrated above.

**Note** The NIST offers two additional components: Identify, protect, detect, respond, and recover. For more information, see document [FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY](#)<sup>13</sup>.

Such a modern approach to security is consistent with one of the "Zero Trust" principles that assumes that the internal network is not trusted.

The first pillar, developed previously, consists of proactively protecting data and resources, identities, devices and connections, by relying on dynamic and contextual access control. But protection cannot stop there, given the asymmetry of positions between the defenders and the attackers, in today's world.

Thus, the detection of an attack in progress can, for example, avoid the exfiltration of data and thereby a violation as defined by the European General Data Protection Regulation (GDPR) if it implies personal data. The sooner you discover an attacker and regain control, the less damage the attacker will be able to do; this not only saves time and money but it helps preserve your image and reputation.

In terms of detection, the aim is to move towards a behavioral approach where the violation detection is triggered by the behavior (of the attack vector, in the case of an intrusion) and the recognition of given patterns. As Gartner points out, "by understanding user behavior and following legitimate processes, companies can use the User and Entity Behavior Analytics (UEBA) to detect security vulnerabilities."<sup>14</sup>

This second pillar applies to the following:

- Devices: by studying their behavior to detect a compromise;

---

<sup>13</sup> FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY: <https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework>

<sup>14</sup> DETECT SECURITY BREACHES EARLY BY ANALYZING BEHAVIOR: <http://www.gartner.com/smarterwithgartner/detect-security-breaches-early-by-analyzing-behavior/>



- Identities: to identify suspicious attacks or behaviors that would be related to identity spoofing;
- Network traffic: to identify attacks with lateral movement attempts, data leaks, and so on.

Finally, the third pillar is the response. After the most effective detection possible, including detection of weak signals, a response mechanism must be able to react as quickly as possible to isolate the compromised elements and segment the compromised area, by containing its spread.

It requires therefore that the dynamic security controls can be activated in response to the behavior detection, to shrink the gap between discovery and reactive action. This requires a radical change in how to react.

Microsoft's end-to-end security vision includes a cloud dimension that is lacking in the initial "Zero Trust" approach, which was very focused on the internal network (on-premises).

Indeed, as highlighted earlier, organizations are increasingly using applications or services available in Software-as-a-Service (SaaS) mode; this implies being able to include them in a modern perimeter (at least) hybrid (see section § THE WORLD HAS CHANGED).

To do this, [Azure AD](#)<sup>15</sup>, the cloud-based Microsoft enterprise scale service that manages identities and access, is the focal point in the "Zero Trust" approach proposed in the continuation of this document to manage internal employee identities and control all accesses to the organization's resources.

For organizations that have a local environment with internal directory services (Active Directory), Azure AD provides a hybrid identity solution that works with existing on-premises IT solutions. Such a hybrid approach to Identity and Access Management (IAM) allows you to maintain and expand your existing IT systems while leveraging the capabilities of control, visibility and cloud-based identity security.

Azure AD enables your employees to connect and access the right business applications and enterprise data from their own devices – Azure AD supports iOS, Mac OS X, Android, and Windows devices. Azure AD integrates with the device management services (Mobile Device Management or MDM) like [Microsoft Intune](#)<sup>16</sup>. We will have the opportunity to come back to this later in the document.

Microsoft Azure AD is recognized as a leader in this domain in the latest Gartner "magic quadrants".



<sup>15</sup> Azure Active Directory: <https://Azure.microsoft.com/en-us/services/active-directory/>

<sup>16</sup> Microsoft Intune: <https://www.microsoft.com/en-us/cloud-platform/microsoft-intune>

**Note** For more information, see article [VISION + EXECUTION TICKET: MICROSOFT NAMED A LEADER AGAIN IN GARTNER MQ FOR ACCESS MANAGEMENT](#)<sup>17</sup> and latest [Gartner report](#)<sup>18</sup>.

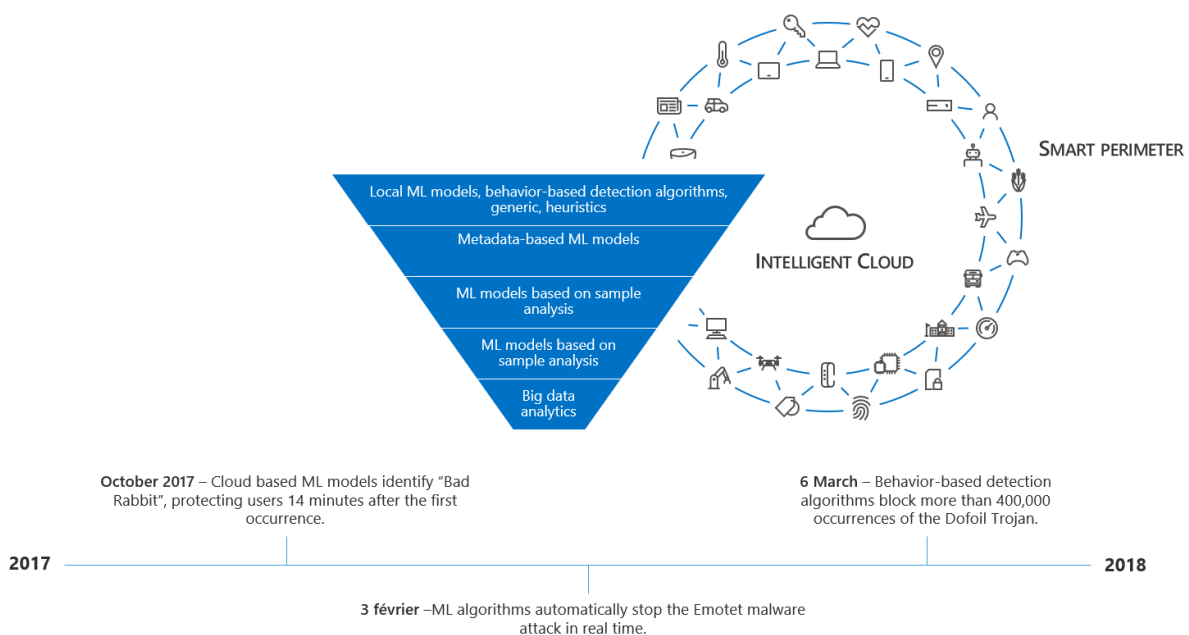
Azure AD also allows for management of access for partners or other external providers.

As for security related services, most of them are available in the cloud to take advantage of virtually limitless computing and storage capabilities and leverage artificial intelligence (AI) to provide more effective analysis and detection of cyber threats, relying on a wide range of signals from different data sources from the cloud and elsewhere. **It's all about using the cloud to master the cloud.**

As cyber-attacks continue to become increasingly sophisticated and automated, it is crucial to obtain real-time information and leverage predictive intelligence across all networks to keep one step ahead of cyber threats. This requires being able to correlate one's own security data with industry and partner intelligence to distinguish "good" from "bad" as broadly and comprehensively as possible.

This is now the foundation of any holistic and agile approach to security, "augmented" with the information from an intelligent security graph and with integration with partners and the industry.

Leveraging new, broader, and deeper security signals allows for earlier recognition and reaction to new and existing threats. Leveraging the immense volume of data and signals from the Cloud all the way to the endpoints, allows for building, through the integration of different services and related systems, an [intelligent security graph](#)<sup>19</sup>. This graph is formed by over 6.5 trillion of signals per day from billions of sources, that can learn from a given domain and apply the "learning" to all the services offered, combining artificial intelligence (AI) and behavioral recognition approaches, in order to profile the behaviors and to evaluate the activity of users and other entities, to identify trends and patterns of attack, and ultimately, to detect anomalies, suspicious activities and sophisticated attacks.



<sup>17</sup> VISION + EXECUTION: MICROSOFT NAMED A LEADER AGAIN IN GARTNER MQ FOR ACCESS MANAGEMENT: <https://www.microsoft.com/en-us/microsoft-365/blog/2018/06/25/vision-execution-microsoft-named-a-leader-again-in-gartner-mq-for-access-management/>

<sup>18</sup> Microsoft a leader in Gartner's Magic Quadrant for Access Management: <http://aka.ms/gartnermqam18>

<sup>19</sup> BILLIONS OF DATA POINTS MAKE A DIFFERENCE: <https://www.microsoft.com/en-us/security/intelligence>

Given the agility and scalability of the cloud, the ability to quickly analyze and determine responses to unprecedented volumes of data becomes crucial in detecting the malicious and abusive behaviors that otherwise could go unnoticed, and in providing the ability to break kill chains as soon as possible.

Extracting an attacker's signals from billions of log events in near real-time from a petabyte-wide storage is indeed a daunting task.

It is thus necessary to take advantage of Data Science, and in particular Machine Learning and its most recent fields of research such as Transfer Learning, for the prevention, detection and lastly, the investigation of the threats. Applying Machine Learning algorithms to MSRC (Microsoft Security Response Center), Microsoft Digital Crime Unit (DCU), Microsoft Malware Protection Center (MMPC), and Office 365 Advanced Threat Protection<sup>20</sup> data, and to other data sources (such as the vast amounts of data from the logs and telemetry collected by the various services), gives unprecedented knowledge and capability for anomaly detection, in order to identify malicious behaviors or entities, be it hackers, attackers, malwares, unwanted behaviors, and so on.

Machine Learning opens two main avenues to better understanding of identity based threats, reinforcing and evolving local and cloud systems, and increasing security standards: i) Next generation identity-based threat detection and response, and ii) simplified security, operations and protection strategies management. These provides the necessary elements to identify and understand the various identity-based threats, to strengthen and evolve cloud and on-premise systems, and to raise the bar in terms of security level:

The ultimate sophistication of cyber-attacks is that they also leverage Data Science, masquerading as noise and to quickly learning from errors. Machine learning helps services like Azure AD to address these recent developments by reinforcing traditional detections based on rules and heuristics.

For example, supervised Machine learning models are trained by presenting malicious and benign examples. The model then generalizes the examples into an algorithm. This greatly helps to reduce triage by prioritizing alerts (and making them at a human scale), combining independent alert flows and providing informed scores, with each alert combining multiple anomalies by nature: *is the call sequence (API) unusual for this account? Is the IP address unusual? Does the access time seem normal? and so on.*

Security expertise requires the development of highly adapted models, using a multitude of analyzed examples. This implies integrating the comments of security analysts (and users) to improve the signals to provide interpretable results. It also implies understanding why a Machine learning algorithm believes that such or such signal is abnormal. As attackers, once detected and blocked, will slightly tune their behavior in order to slip under the radar, the models developed must automatically adapt to these changes to quickly adjust to such "moving targets".

---

<sup>20</sup> EXCHANGE ONLINE ADVANCED THREAT PROTECTION SERVICE DESCRIPTION: <https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description>

**Note** For more information, watch following sessions [MACHINE LEARNING AND THE CLOUD: DISRUPTING THREAT DETECTION AND PREVENTION](#)<sup>21</sup>, [ADVANCES IN CLOUD-SCALE MACHINE LEARNING FOR CYBER-DEFENSE](#)<sup>22</sup> and [TRANSFER LEARNING: REPURPOSING ML ALGORITHMS FROM DIFFERENT DOMAINS TO CLOUD DEFENSE](#)<sup>23</sup> recorded during past RSA conferences.

These techniques based on cyber threat detection capabilities help identify attackers and their attacks more effectively than other software-driven approaches, dynamically elevate the defenses of attacked resources, etc. and of course, ensure that the organizations attacked are informed. Ultimately, it's about defending Microsoft's cloud services, infrastructure and customers, but also their local infrastructure and devices.

Examples include:

- [Microsoft Defender Advanced Threat Protection](#)<sup>24</sup>, the protection solution for Mac OS X and Windows 10 devices;
- [Azure Advanced Threat Protection \(ATP\)](#)<sup>25</sup>, a cloud security solution that analyzes signals from on-premises Active Directory directories to detect advanced threats, compromised identities, and actions of malicious internal users.

[Azure Sentinel](#)<sup>26</sup> (in public pre-release to date), is the recent Microsoft SIEM (Security Information and Event Manager) and SOAR (Security Orchestration and Automated Response) solution, which provides not only consolidation and analysis of internal events, from Microsoft clouds and from other clouds events, but also offers automatic orchestration and response capabilities.

In summary, even if Microsoft's approach had not highlighted the terminology "Zero Trust" as such, it declines all of its principles and takes into account the extended scope of modern organizations where the cloud is now fully present in one form or another.

Beyond this quick overview, let's see what the detail is about and start with the "foundation" that constitutes conditional access control in Azure AD.

---

<sup>21</sup> MACHINE LEARNING AND THE CLOUD: DISRUPTING THREAT DETECTION AND PREVENTION: <https://www.rsaconference.com/events/us16/agenda/sessions/2532/machine-learning-and-the-cloud-disrupting-threat>

<sup>22</sup> ADVANCES IN CLOUD-SCALE MACHINE LEARNING FOR CYBER-DEFENSE: <https://www.rsaconference.com/events/us17/agenda/sessions/7520-advances-in-cloud-scale-machine-learning-for-cyber>

<sup>23</sup> TRANSFER LEARNING: REPURPOSING ML ALGORITHMS FROM DIFFERENT DOMAINS TO CLOUD DEFENSE: <https://www.rsaconference.com/events/us18/agenda/sessions/11539-transfer-learning-repurposing-ml-algorithms-from>

<sup>24</sup> Microsoft Defender Advanced Threat Protection: <https://www.microsoft.com/en-us/WindowsForBusiness/windows-atp>

<sup>25</sup> Azure Advanced Threat Protection: <https://docs.microsoft.com/en-us/Azure-advanced-threat-protection/what-is-atp>

<sup>26</sup> Azure Sentinel: <https://azure.microsoft.com/en-us/services/azure-sentinel/>

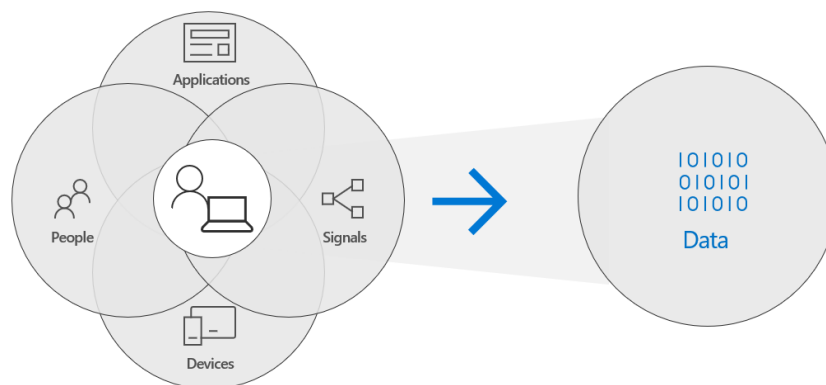
# Conditional access in Azure AD at the heart of the strategy

In today's work environment, we have seen that users can work on any device, whether using a laptop provided by the organization or using a personal smartphone, and from any location, working from home, at the office or on the move. Employees expect to have seamless access to what they need in order to do their jobs (see section § CONSUMERIZATION OF IT).

While the need for productivity does not change with circumstances of access, the level of risk of each connection does evolve. Not all devices, applications, or networks are as secure, and attackers are likely to exploit any vulnerabilities that will give them access to your users and/or resources. It is therefore essential to protect identities, but it is not enough.

Managing and verifying identities is the first step in protecting your environment. Provisioning user identities through Azure AD, and connecting your on-premises Active Directory service if necessary, allows you to centralize identities for each user, in order to then be able to establish policies based on devices, groups and applications. See section § CONNECTING ALL IDENTITIES.

As previously discussed, the "Zero Trust" approach requires flexible security policies that meet the requirements for user access to data and resources.



Moreover, one of the essential aspects of a "good" security is that it should be almost invisible to legitimate users. Excessive friction inhibits productivity, and legitimate users will find ways to circumvent provisions that block their productivity, thereby creating (additional) risks. Although you can enforce multi-factor authentication (MFA) for each user, maximizing productivity is ideally expected to allow legitimate users to do their jobs with minimal disruptions, while blocking malicious people.

Azure AD enables you to set conditional access policies for users in your organization to help secure your hybrid or cloud environment.

[Conditional access in Azure AD](#)<sup>27</sup> allows you to accomplish exactly that by defining a set of policies that specify conditions and controls. You can set access levels by employee, by device, or by group.

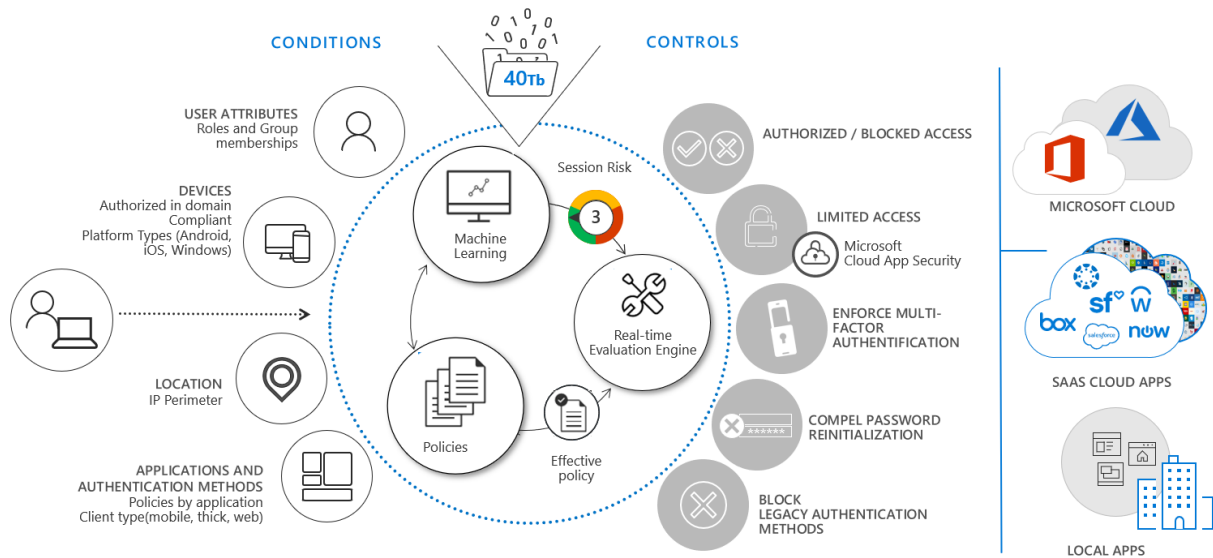
Conditional access in Azure AD is a hub of identity-based security policies.

Previously, you should have specified: "no access outside the corporate network" or "no access from a personal device"; today, the ability to block or authorize access is offered under conditions.

---

<sup>27</sup> CONDITIONAL ACCESS IN AZURE ACTIVE DIRECTORY: <https://docs.microsoft.com/en-us/Azure/active-directory/active-directory-conditional-access>

Conditional access in Azure AD allows enforcing security policies that are triggered automatically when certain conditions are met. You can block access if the context data suggests that the user has been compromised, or if it is very unlikely that the user should log in under these conditions. You can apply additional authentication requirements when the system detects a medium risk based on connection conditions.



**Note** Conditional access in Azure AD is an [Azure AD Premium feature \(P1 or P2\)](#)<sup>28</sup>. All users accessing an application or resource limited by conditional access policies must have an Azure AD Premium license.

## Configuring conditional access policies in Azure AD

We recommend that you apply appropriate policies to your organization for the following conditions:

- **Users and user groups:** to reduce the risk of sensitive data leakage, define which users or groups of users can access applications or resources, paying particular attention to the highly sensitive information sources such as human resources or financial data.
- **Connection risk:** Machine Learning algorithms in Azure AD evaluate each connection and give it a low, medium, or high risk score based on the probability that someone other than the legitimate owner of the account is attempting to connect. Anyone with a medium risk must be challenged with multi-factor authentication (MFA) when connecting. If the connection is high risk, access must be blocked. This condition requires Azure AD Identity Protection (see below).
- **Location:** a location can be risky if it is a country with limited security policies or if the wireless network is unsecured or simply because it is not a place where the organization usually has activities. You can change the access requirements for connections from locations that are not on a list of safe IP addresses or that are risky for other reasons. Users accessing a service when they are outside the corporate network must be forced to use multi-factor authentication.
- **Device platform:** for this condition, you can define a policy for each device platform that blocks access, requires for example compliance with Microsoft Intune, or requires that the device be joined to the domain.

<sup>28</sup> Azure AD Premium (P1 where P2): <http://www.microsoft.com/identity>

- **Device status:** you can use this condition to set policies for devices that are not managed by your organization.
- **Client applications:** users can access many applications using different client application types, such as Web applications, mobile applications, or office productivity applications. You can enforce security policies if an access attempt is made by using a client application type that causes known issues, or you can require that only managed devices access certain types of applications.
- **Cloud applications:** this condition specifies unique policies for sensitive applications. For example, you can require that HR applications such as Workday be blocked if Azure AD detects a risky connection or if a user tries to access it with an unmanaged device.

When a condition is met, you can choose the policy that Azure AD will enforce in terms of control:

- Require multi-factor authentication to prove identity;
- Modify the actions that the user can take in cloud applications;
- Restrict access to sensitive data, such as limiting downloads or sharing features;
- Require password reset;
- Block access.

New

×

Info

\* Name

Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ

Specific users included >

Cloud apps ⓘ

2 apps included >

Conditions ⓘ

1 condition selected >

Access controls

Grant ⓘ

0 controls selected >

Session ⓘ

0 controls selected >

Enable policy

On

Off

Grant

□ ×

Select the controls to be enforced.

○ Block access

● Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ  
[See list of approved client apps](#)

☐ Require app protection policy (preview) ⓘ  
[See list of policy protected client apps](#)

For multiple controls

● Require all the selected controls

○ Require one of the selected controls

Select

Implementing a Zero Trust approach with Azure Active Directory 19

**Note** For more information, see article [AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS SETTINGS REFERENCE](#)<sup>29</sup>.

Once defined, these policies will automatically apply without manual intervention.

**Note** You can use the [conditional access plan](#)<sup>30</sup> as a step-by-step guide to help you through implementation.

Also, in this context, [Azure AD Identity Protection](#)<sup>31</sup> will help quickly discover suspicious anomalies or incidents and configure policies that will automate a response. The sooner you discover an attacker and regain control, the less damage the attacker can do, helping to save time, money and preserve your image and reputation.

**Note** Azure AD Identity Protection is an Azure AD Premium P2 feature.

As mentioned above, Azure AD Identity Protection allows configuring policies to automate a response based on the conditions you define.

It is thus possible to integrate with the conditional access policies, the concept of risk profile in terms of either connections (access from an anonymizing browser, from improbable places, with several attempts of unsuccessful authentication, etc.) or users (credentials available on the " Darknet "):

- A [sign-in risk policy](#)<sup>32</sup> is a conditional access policy that can be configured based on the level of risk assigned to a connection.
- A [user risk policy](#)<sup>33</sup> is a conditional access policy that can be configured based on the likelihood that a person has been compromised.

These strategies are made possible by the Microsoft Intelligent Security Graph mentioned earlier. As stated, this is the accumulated intelligence Microsoft collects not only from all of our products, services, and internal teams but also from external sources, and used to stop cyber-attacks (see section § STOPPING CYBER-ATTACKS).

Azure AD Identity Protection applies Machine Learning algorithms to this data, to analyze each connection to detect anomalies or suspicious incidents. It then assigns a low, medium, or high level of risk to indicate the likelihood that the legitimate user did not execute the connection. This is called a risk event. Azure AD also analyzes risk events for each user and calculates a low, medium, or high level of risk to indicate the likelihood that a user has been compromised.

Azure AD Identity Protection notifies if it detects a suspicious behavior, assists in investigating the situation, and helps to take automated measures such as blocking a connection attempt (see section § BLOCKING OR UPDATING COMPROMISED IDENTITIES), mandating strong authentication (see section § PROPERLY

---

<sup>29</sup> AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS SETTINGS REFERENCE: <https://docs.microsoft.com/en-us/Azure/active-directory/conditional-access/technical-reference>

<sup>30</sup> Azure Active Directory Conditional Access Deployment Plan: <https://aka.ms/CADPDownload>

<sup>31</sup> AZURE ACTIVE DIRECTORY IDENTITY PROTECTION: <https://docs.microsoft.com/en-us/Azure/active-directory/active-directory-identityprotection>

<sup>32</sup> HOW TO: CONFIGURE THE SIGN-IN RISK POLICY: <https://docs.microsoft.com/en-us/Azure/active-directory/identity-protection/howto-sign-in-risk-policy>

<sup>33</sup> HOW TO: CONFIGURE THE USER RISK POLICY: <https://docs.microsoft.com/en-us/Azure/active-directory/identity-protection/howto-user-risk-policy>



ENFORCING MULTI-FACTOR AUTHENTICATION TO MITIGATE SESSION RISKS) or triggering a password reset as previously indicated.

For example, Azure AD Identity Protection allows defining conditional access policies to mitigate the risks of unsafe connections by blocking connections or by imposing multi-factor authentication.

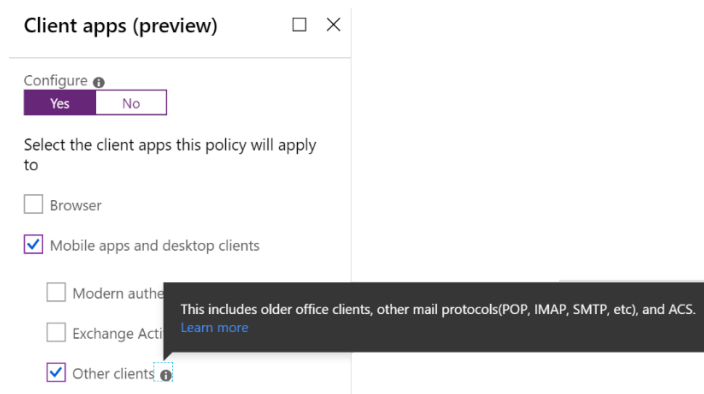
We recommend that you create a connection risk policy that requires all medium-risk connections to use the [multi-factor authentication](#)<sup>34</sup>. We also recommend that users with a high level of risk being forced to change their password securely after verifying their identity using multi-factor authentication. In both cases, these policies will be applied automatically without the intervention of an administrator.

To summarize, and in a more general way, Azure AD Identity protection allows for:

- Detecting potential vulnerabilities that affect organization identities;
- Configuring automatic responses to detected suspicious actions that are related to organization identities;
- Examining suspicious incidents and take appropriate actions to resolve them.

## Blocking inherited authentication and control access to high privileged accounts

Legacy applications that use an inherited authentication method, such as POP3, IMAP4, or SMTP clients, can increase your risk because they prevent Azure AD from performing an advanced security assessment and do not allow the use of more modern forms of authentication, such as multi-factor authentication. We recommend that you use these [client application conditional access rules](#)<sup>35</sup> to completely block such applications.



You can also use conditional access rules to reduce the risk that high-privileged user accounts or service accounts being compromised. For example, if your HR system uses a service account to access the email account, you can make sure that it can run only on the service from a specific IP address at the appropriate time of day.

---

<sup>34</sup> HOW IT WORKS: AZURE MULTI-FACTOR AUTHENTICATION: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

<sup>35</sup> WHAT ARE CONDITIONS IN AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS?: <https://docs.microsoft.com/en-us/Azure/active-directory/conditional-access/conditions#legacy-authentication>

## Improving conditional access with Intune and Microsoft Cloud App Security

As already mentioned, Azure AD integrates with [Microsoft Intune](#)<sup>36</sup> and other MDM (Mobile Device Management) solutions, so that conditional access policies can take into account the state of the device as part of the approach; this allows you to define access controls for devices that run legacy operating systems or other security vulnerabilities.

You can also use conditional access in Microsoft Intune to ensure that only Intune-managed applications can access corporate email or other Office 365 services. Azure AD will ensure that these rules are applied. See the section § ENFORCING SECURITY POLICIES.

In addition, if conditional access should apply for certain Office/Microsoft 365 services (see section § SHAREPOINT ONLINE/ONEDRIVE FOR BUSINESS AND EXCHANGE ONLINE), Microsoft Cloud App Security can extend this type of capabilities to other applications in the cloud or on-premises (via the [Azure AD application proxy](#)<sup>37</sup>) and ensure that the actions authorized within an application depend on the access context, once it has been granted.

Indeed, with the [Cloud App Security application conditional access control](#)<sup>38</sup>, you can block downloads from applications, restrict activities in the application, monitor users at risk or block access to the application entirely. This topic will be discussed later on in this document. See section § CONTROLLING SESSION WITH MICROSOFT CLOUD APP SECURITY.

Once policies are in place, we recommend that you use the [Azure AD What If](#)<sup>39</sup> to simulate possible connection scenarios that users may encounter. The "What if" tool allows to select a user, the application that the user is attempting to access, and the conditions of that connection, in order to determine which policies will apply.

---

<sup>36</sup> WHAT IS MICROSOFT INTUNE?: <https://docs.microsoft.com/en-us/intune/what-is-intune>

<sup>37</sup> Remote access to on-premises applications through Azure Active Directory's Application Proxy: <https://docs.microsoft.com/en-us/Azure/active-directory/manage-apps/application-proxy>

<sup>38</sup> MICROSOFT CLOUD APP SECURITY OVERVIEW: <https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security>

<sup>39</sup> WHAT IS THE WHAT IF TOOL IN AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS?: <https://docs.microsoft.com/en-us/Azure/active-directory/conditional-access/what-if-tool>

## What If

Policies

### Info

Test the impact of conditional access on a user when signing in under certain conditions.

[Learn more](#)

### \* User

0 users selected

### Cloud apps

Any cloud app

### IP address

Enter IP address (ex: 40.77.182.32)

### Country

Select country...

### Device platform

Select device platform...

### Client apps (preview)

Select a client app...

### Device state (preview)

Select device state...

What If

Reset

This step will give better visibility of how the strategies will impact users. You can also check policies that do not apply to a specific scenario.

We want to draw your attention to the final precaution: be sure to configure an exception group for each conditional access policy in Azure AD so that you do not lock yourself out.

Let us now look at the key principles underpinning the implementation of conditional access.

# Microsoft Zero Trust approach's implementation principles

The adoption and implementation of the Microsoft "Zero Trust" approach are based on five key principles:

1. Verifying identity;
2. Managing devices;
3. Managing applications;
4. Protecting data;
5. Stopping cyber-attacks.

The following sections describe each of these principles in order.

## Verifying identity

When it comes to cyber-attacks, attackers are often targeting accounts and their passwords. Most compromises begin with stolen or guessed user credentials. This is the best way to enter a corporate network without being detected. Hence, they work to steal these identity and credentials information.

Once the attackers are introduced, they try to elevate their privileges, or they exploit their access to discover and target users with administrative rights that have access to valuable data. The rapid detection of a compromised account, regardless of its level of access, is therefore essential.

Thus, identity verification must be the first line of defense in a "defense-in-depth" approach.

Because most cyber-security attacks originate from lost, weak, or compromised user credentials, it is necessary to have a security level that passwords alone cannot provide.

This section addresses the control and protection against compromised credentials and internal threats.

This requires to:

- Connect all identities;
- Use multi-factor authentication;
- Set up single sign-on for all applications and APIs;
- Reduce the number of administrator accounts and implement policies;
- Monitor user behavior locally.



**Note** For more information, see blog post [ZERO TRUST PART 1: IDENTITY AND ACCESS MANAGEMENT BLOG](#)<sup>40</sup>.

## Connecting all identities

Establishing a single and common identity for each user is the basic step in the implementation of a “Zero Trust” approach, to lay the foundations for a holistic conditional access strategy.

If you currently have a local footprint (on-premises) and are managing a hybrid environment, the first step is to create a unique common identity for all your users. This means connecting your Azure AD to your on-premises resources and establishing an identity bridge.

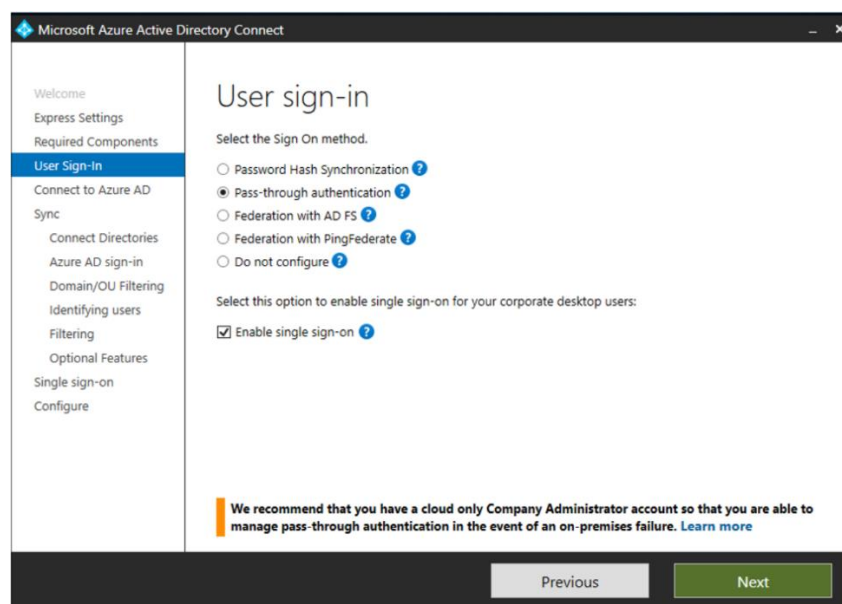
**Note** For more information, see whitepaper [ACTIVE DIRECTORY FROM ON-PREMISES TO THE CLOUD](#)<sup>41</sup>.

## Creating a single common identity for all identities

Creating a unique identity requires importing and synchronizing your local employees' identities to Azure AD, and then integrating your on-premises directories with Azure AD using [Azure AD Connect](#)<sup>42</sup>.

This allows you to provide a common and secure identity for users for Office/Microsoft 365, Azure, and thousands of other Software-As-A-Service (SaaS) applications integrated with Azure AD.

There are various requirements and circumstances that will influence the resulting hybrid identity and the authentication method you choose, but if you choose cloud authentication or federation -based authentication, each has important security implications that should be considered.



This section guides you through the recommended security practices for each hybrid identity method.

---

<sup>40</sup> ZERO TRUST PART 1: IDENTITY AND ACCESS MANAGEMENT: <https://www.microsoft.com/security/blog/2018/12/17/zero-trust-part-1-identity-and-access-management/>

<sup>41</sup> ACTIVE DIRECTORY FROM ON-PREMISES TO THE CLOUD: <https://www.microsoft.com/en-us/download/details.aspx?id=36391>

<sup>42</sup> WHAT IS HYBRID IDENTITY?: <https://docs.microsoft.com/en-us/Azure/active-directory/connect/active-directory-aadconnect>

**Note** For more information, see the series of whitepapers AZURE AD/OFFICE 365 SEAMLESS SIGN-IN whitepaper series available from the download [ACTIVE DIRECTORY FROM ON-PREMISES TO THE CLOUD – AZURE AD WHITEPAPERS](#)<sup>43</sup>.

When using Azure AD Connect, the wizard allows you to use your on-premises Active Directory as authority, so that you can use your own password policy. Azure AD Connect gives complete visibility into all types of applications and identities that access your enterprise resources.

Microsoft recommends enabling [Password Hash Synchronization](#)<sup>44</sup> (or PHS) as the main authentication method. PHS synchronizes the password hash value from the on-premises Active Directory to Azure AD. This allows authentication in the cloud without local dependency, thus simplifying the deployment process. This configuration also allows you to take advantage of Azure AD Identity Protection features, which will alert you if any of your organization's user names and passwords have been sold on the obscure part of the invisible Web, the "Dark Web".

If your authentication requirements are not natively supported by PHS, another option available through Azure AD Connect is [direct authentication](#)<sup>45</sup> (Pass-Through Authentication or PTA). PTA provides simple password validation for Azure AD authentication services, by using a software agent that runs on one or more on-premises servers. Because direct authentication relies solely on the on-premises infrastructure, users may lose access to cloud resources connected to Active Directory and local resources, if the on-premises environment becomes unavailable. To limit the impact on the users and the resulting loss of productivity, we recommend that PHS be configured as backup. This will allow your users to connect and access cloud resources in case of an on-premises outage occurs. This configuration also gives you access to advanced security features, such as Azure AD Identity Protection as already mentioned.

---

<sup>43</sup> Active Directory from on-premises to the cloud – Azure AD White papers: <https://www.microsoft.com/en-us/download/details.aspx?id=36391>

<sup>44</sup> IMPLEMENT PASSWORD HASH SYNCHRONIZATION WITH AZURE AD CONNECT SYNC: <https://docs.microsoft.com/en-us/Azure/active-directory/connect/active-directory-aadconnectsync-implement-password-hash-synchronization>

<sup>45</sup> USER SIGN-IN WITH AZURE ACTIVE DIRECTORY PASS-THROUGH AUTHENTICATION: <https://docs.microsoft.com/en-us/Azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication>

**Note** One of the main reasons why users choose weak or common passwords is that long passwords that require digits, letters, and special characters are difficult to remember, especially if they must be changed every few months. [Microsoft recommends that you disable these rules and prohibit users from choosing common passwords](#)<sup>46</sup>.

If you have a hybrid environment, you will need to deploy Azure AD password protection agents on-premises to enable this feature. [Azure AD password protection](#)<sup>47</sup> prevents users from choosing common passwords, as well as any passwords you specify. If you implement PHS as a primary or backup authentication method, you will have access to a report of all the leaked user credentials, which provides user names and password that have been disclosed on the obscure part of the invisible Web, the "Dark Web".

Custom smart logout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

Active Directory Federation Services (ADFS), a server role of Windows Server, may be the right choice (or any other supported local authentication provider solution) if your organization requires local authentication or if you have already invested in identity federation services. Identity federation services authenticate users and connect to the cloud using a local footprint that may require multiple servers. To ensure that your users and your data are as safe as possible, we recommend two additional steps if you are or want to be in this configuration.

First, we recommend that you enable PHS as a backup authentication method to benefit from Azure AD Identity Protection capabilities and to minimize interruptions if an on-premises server failure occurs. Then, if you rely on AD FS for federation services, we recommend that you implement the extranet lockout. Extranet Lockout protects against brute force attacks targeting AD FS, while preventing users from being locked out by Active Directory and thus receive a denial of service. If you are using AD FS in Windows Server 2016 or later, you should configure the [Extranet Smart Lockout](#)<sup>48</sup>. For AD FS in Windows Server 2012 R2, you should enable [extranet lockout protection](#)<sup>49</sup>.

---

<sup>46</sup> FIVE STEPS TO SECURING YOUR IDENTITY INFRASTRUCTURE: <https://docs.microsoft.com/en-us/Azure/security/Azure-ad-secure-steps>

<sup>47</sup> ELIMINATE BAD PASSWORDS IN YOUR ORGANIZATION: <https://docs.microsoft.com/en-us/Azure/active-directory/authentication/concept-password-ban-bad>

<sup>48</sup> DESCRIPTION OF THE EXTRANET SMART LOCKOUT FEATURE IN WINDOWS SERVER 2016: <https://support.microsoft.com/en-us/help/4096478/extranet-smart-lockout-feature-in-windows-server-2016>

<sup>49</sup> CONFIGURE AD FS EXTRANET LOCKOUT PROTECTION: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection>

**Note** You can use the [AD FS transfer authentication deployment plan](#)<sup>50</sup> as a step-by-step guide through the implementation process.

## Connecting your partner identities

[Azure AD B2B collaboration](#) capabilities<sup>51</sup> enable organizations using Azure AD to work securely with users in other organizations, regardless of their size.

Organizations using Azure AD can provide access to documents, resources, and applications to their partners while maintaining full control over their own business data.

B2B collaboration users (guest) can be added to your organization from the Azure portal. Developers can use the Azure AD B2B application programming interfaces (APIs) to manage invitations and/or write applications that enable organizations to collaborate more securely.

Partners can use their own credentials without having to use Azure AD: a simple email address is enough.

## Using multi-factor authentication

Balancing employee productivity needs with enterprise security begins with identity protection. As we pointed out in the introduction, the days when users accessed the organization's resources behind a firewall using devices belonging to the organization, are gone. Employees and partners use multiple devices and applications for their daily work (see section § THE WORLD HAS CHANGED). They share documents with other users via emails and productivity (cloud) applications, and switch between personal and work-related applications and devices throughout the day. This has created a world of opportunities for attackers with increasingly sophisticated techniques.

Attackers know that users often use the same (weak) password for all their application accounts (if single sign-on is NOT in place, see next section).

They employ several tactics to take advantage of these vulnerabilities:

1. Password spray is a method consisting in trying common passwords against known lists of accounts – it is, so to speak, the opposite approach to brute force;
2. In a compromised relay, a malicious actor steals an organization's password and then uses this password to try to access other networks.
3. Phishing campaigns encourage users to give their password directly to the attacker.

**Note** The access credentials in the form email addresses and passwords are the two most compromised data types, at 44.3% and 40%, respectively<sup>52</sup>.

Azure AD provides several features to reduce the likelihood of these three attack methods. You can:

- Using Azure MFA;
- Using other conditional access-compatible solutions in Azure AD;

---

<sup>50</sup> Azure Active Directory Migration from ADFS to Pass-Through Authentication Deployment Plan: <https://aka.ms/ADFSTOPTADPDownload>

<sup>51</sup> WHAT IS GUEST USER ACCESS IN AZURE ACTIVE DIRECTORY B2B?: <https://docs.microsoft.com/en-us/Azure/active-directory/b2b/what-is-b2b>

<sup>52</sup> DATA BREACH RECORD EXPOSURE UP 305% FROM 2016: <https://www.darkreading.com/vulnerabilities---threats/data-breach-record-exposure-up-305--from-2016/d/d-id/1330359>



- Using multi-factor authentication without password.

## Using Azure MFA

Given the frequency at which the credentials are stolen, guessed or phished, we recommend that [Azure MFA](#)<sup>53</sup> be enabled to add another layer of security to the accounts.

Multi-factor authentication is responsible for controlling access to resources under the unique identity system and significantly reduces the chances that a compromised identity will lead to a security breach.

Multi-factor authentication works by requiring two or more of the following authentication methods:

- Something you know (typically a password);
- Something you own (a trusted device that is not easily duplicated, such as a phone);
- Something you are (biometrics).

**Note** You can use the [MFA deployment plan](#)<sup>54</sup> as a step-by-step guide through the implementation process.

Multi-factor authentication can be applied statically to individual user accounts or through a conditional access policy, this second approach is preferable.

## Using other conditional access-compatible solutions in Azure AD

Conditional access in Azure AD integrates through custom controls with many third-party solutions such as [Duo Security](#)<sup>55</sup>, [Entrust Datacard](#)<sup>56</sup>, [Ping Identity](#)<sup>57</sup>, RSA, [Silverfort](#)<sup>58</sup>, [Symantec VIP](#)<sup>59</sup> or [Trusona](#)<sup>60</sup>.

So, if you use one of these providers to support multi-factor authentication, you can easily use it in the conditional access engine of Azure AD.

---

<sup>53</sup> HOW IT WORKS: AZURE MULTI-FACTOR AUTHENTICATION: <https://docs.microsoft.com/en-us/Azure/active-directory/authentication/concept-mfa-howitworks>

<sup>54</sup> Azure Active Directory Multi-Factor Authentication Deployment Plan: <https://aka.ms/MFADPDownload>

<sup>55</sup> Duo - Microsoft Azure Active Directory: <https://duo.com/docs/Azure-ca>

<sup>56</sup> IntelliTrust: <https://intellitrust.entrustdatacard.com/>

<sup>57</sup> Benches for Azure To:  
[https://documentation.pingidentity.com/pingid/pingidAdminGuide/index.shtml#pid\\_c\\_AzureADIntegration.html](https://documentation.pingidentity.com/pingid/pingidAdminGuide/index.shtml#pid_c_AzureADIntegration.html)

<sup>58</sup> AZURE AD CONDITIONAL ACCESS CUSTOM CONTROLS INTEGRATION GUIDE: <https://www.silverfort.io/company-2/using-silverfort-mfa-with-Azure-active-directory/>

<sup>59</sup> VIP INTEGRATION WITH MICROSOFT AZURE TO:  
[https://help.symantec.com/bucket/VIP\\_Integrate\\_with\\_Azure\\_AD/integrating\\_symantec\\_vip\\_with\\_microsoft\\_Azure\\_ad](https://help.symantec.com/bucket/VIP_Integrate_with_Azure_AD/integrating_symantec_vip_with_microsoft_Azure_ad)

<sup>60</sup> AZURE ACTIVE DIRECTORY INTEGRATION GUIDE: <https://www.trusona.com/docs/Azure-ad-integration-guide>

**Note** For more information, see blog post [AZURE AD + 3RD PARTY MFA = AZURE AD CUSTOM CONTROLS](#)<sup>61</sup> and article [WHAT ARE ACCESS CONTROLS IN AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS?](#)<sup>62</sup>.

## Using multi-factor authentication without password

A better method would be to get rid of passwords altogether and there are several alternatives some applicable today and others to come in the near. One of the reasons why passwords are often stolen is that they work from anywhere.

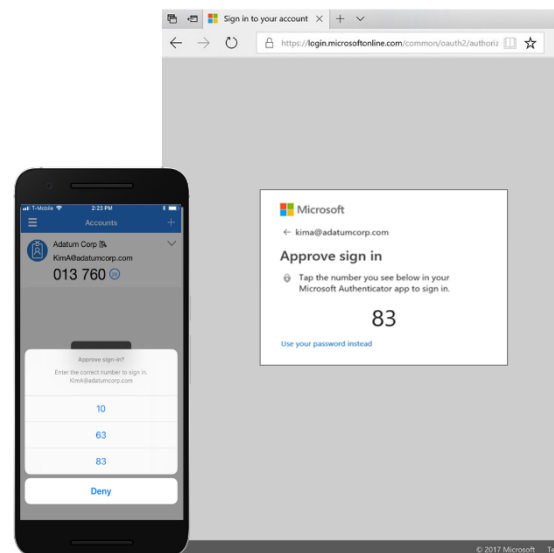
To reinforce employees sign-in from Windows 10 devices, you can deploy [Windows Hello for business](#)<sup>63</sup>, which replaces passwords with strong two-factor authentication on these devices. Windows Hello for business allows users to configure authentication using either PIN or biometrics, such as a fingerprint scanner or facial recognition. This form of authentication proves to be easier for users because they do not have to remember (complex) passwords, but it is also safer as the authentication method is linked to the considered device. An attacker would have to take possession of the device and the PIN or biometrics to compromise your network.

Usable with Android and iOS devices, the [Microsoft Authenticator](#) mobile app<sup>64</sup> can be used to connect to any Azure AD account without using a password.

Like Windows Hello for Business technology, Microsoft Authenticator uses key-based authentication to enable user credentials related to a device and uses PIN or biometrics.

**Note** To download the application and learn more, please access [Microsoft authenticator](#)<sup>65</sup>.

Windows Hello for Business and the Microsoft Authenticator mobile application are already in themselves powerful alternatives to passwords but creating a world without passwords requires an interoperable solution that works on all platforms and browsers in the industry.



<sup>61</sup> AZURE AD + 3RD PARTY MFA = AZURE AD CUSTOM CONTROLS: <https://blogs.technet.microsoft.com/cbernier/2017/10/16/Azure-ad-3rd-party-mfa-Azure-ad-custom-controls/>

<sup>62</sup> WHAT ARE ACCESS CONTROLS IN AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS?: <https://docs.microsoft.com/en-us/Azure/active-directory/conditional-access/controls#custom-controls>

<sup>63</sup> WINDOWS HELLO FOR BUSINESS: <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification>

<sup>64</sup> PASSWORD-LESS PHONE SIGN-IN WITH THE MICROSOFT AUTHENTICATOR APP (PUBLIC PREVIEW): <https://docs.microsoft.com/en-us/Azure/active-directory/authentication/howto-authentication-phone-sign-in>

<sup>65</sup> Microsoft Authenticator:  
[https://app.adjust.com/dku5qky\\_lzq8cok?fallback=https%3A%2F%2Fwww.microsoft.com%2Fauthenticator%3Fcmp%3Ddku5qky\\_lzq8cok](https://app.adjust.com/dku5qky_lzq8cok?fallback=https%3A%2F%2Fwww.microsoft.com%2Fauthenticator%3Fcmp%3Ddku5qky_lzq8cok)



Such an alternative to the password seems to be emerging through the Fido Alliance [FIDO2](#) initiative<sup>66</sup>.

FIDO2 is an open authentication standard for a simpler and more secure authentication experience, using public key cryptography. The "Standards" that FIDO2 relies on is the W3C [WEB AUTHENTICATION: AN API FOR ACCESSING PUBLIC KEY CREDENTIALS](#)<sup>67</sup> recommendation and the corresponding FIDO Alliance [CLIENT TO AUTHENTICATOR PROTOCOL \(CTAP\)](#)<sup>68</sup> specification.

With FIDO2, users manipulate an external security key, also known as the FIDO2 authenticator. FIDO2 security keys are portable and can be moved between devices, whether computers, tablets, or smartphones, to authenticate without a password.

The user experience is simple: users must unlock access to the security key locally by either typing their PIN code or using their fingerprint.

Now available for Microsoft Accounts (or MSA) for the general public, FIDO2 will soon be supported with Azure AD<sup>69</sup>.

**Note** For more information, see blog post [BUILDING A WORLD WITHOUT PASSWORDS](#)<sup>70</sup>.

## Setting up single sign-on for all applications and APIs

As already noted, corporate security compromise begins with a compromised user account which makes protecting these accounts a critical priority.

A huge advantage of hybrid deployment is that you can configure single sign-on (SSO). Users already connect to local resources using a username and password that they know. [Single sign-on \(SSO\) in Azure AD](#)<sup>71</sup> enables them to use the same set of credentials to access local resources but also to Azure, Dynamics 365, Office 365, and a large catalog of SaaS-based cloud applications connected to Azure AD such as ServiceNow, Workday, Google apps, and Salesforce.com - over 3100 to date - not to mention connecting to your own applications and APIs built into Azure AD.

---

<sup>66</sup> FIDO2: <https://fidoalliance.org/fido2/>

<sup>67</sup> Web Authentication: An API for accessing Public Key Credentials Level 1 W3C Recommendation, 4 March 2019: <https://www.w3.org/TR/webauthn-1/>

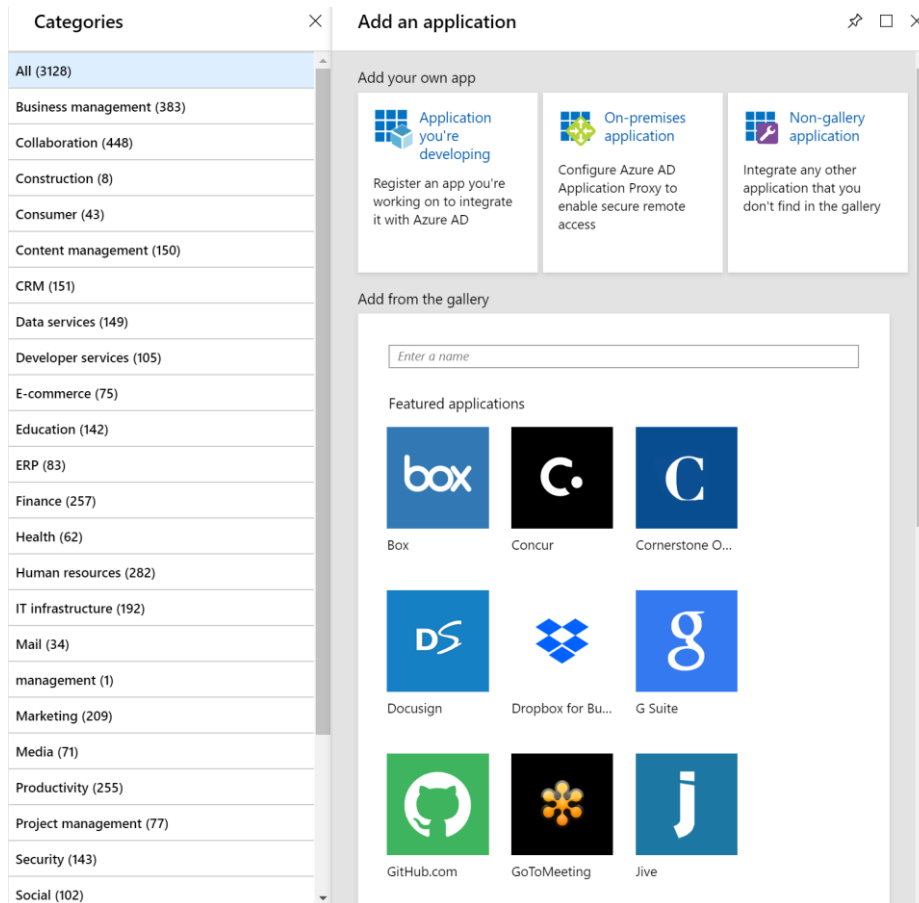
<sup>68</sup> CLIENT TO AUTHENTICATOR PROTOCOL (CTAP) PROPOSED STANDARD, JANUARY 30, 2019: <https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html>

<sup>69</sup> ANNOUNCING PASSWORD-LESS FIDO2 SUPPORT FOR MICROSOFT ACCOUNTS: <https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Announcing-password-less-FIDO2-support-for-Microsoft-accounts/ba-p/289034>

<sup>70</sup> BUILDING A WORLD WITHOUT PASSWORDS: <https://cloudblogs.microsoft.com/microsoftsecure/2018/05/01/building-a-world-without-passwords/>

<sup>71</sup> TUTORIAL: CONFIGURE SAML-BASED SINGLE SIGN-ON FOR AN APPLICATION WITH AZURE ACTIVE DIRECTORY: <https://docs.microsoft.com/en-us/Azure/active-directory/manage-apps/configure-single-sign-on-portal>

**Note** For more information about integrating applications and APIs with Azure AD, see article [INTEGRATING WITH AZURE ACTIVE DIRECTORY](#)<sup>72</sup>.



Single sign-on in Azure AD allows for management of authentication on devices, cloud applications, and on-premises applications. Once you enable single sign-on, employees can access resources in real time from any device while working remotely, including confidential or sensitive working documents.

Productivity can be increased by extending single sign-on to include more cloud applications and on-premises applications through [Azure AD application proxy](#)<sup>73</sup>.

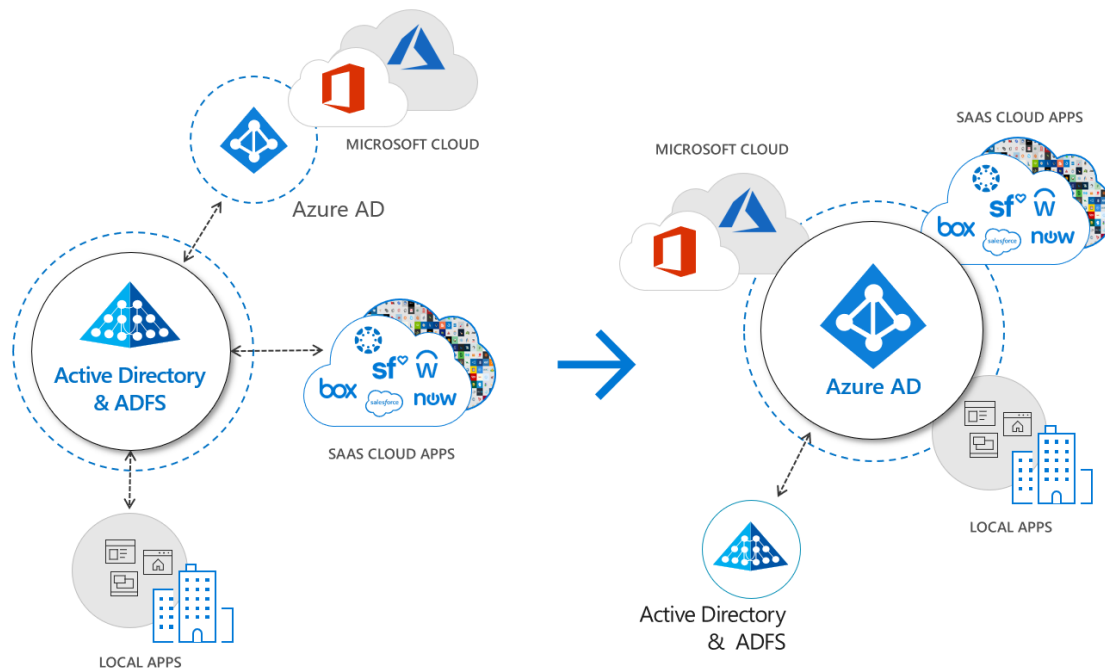
**Note** You can use the [application proxy plan](#)<sup>74</sup> as a step-by-step guide through the implementation.

The following figure illustrates this path.

<sup>72</sup> INTEGRATING WITH AZURE ACTIVE DIRECTORY: <https://docs.microsoft.com/en-us/Azure/active-directory/develop/app-types>

<sup>73</sup> Remote access to on-premises applications through Azure Active Directory's Application Proxy: <https://docs.microsoft.com/en-us/Azure/active-directory/manage-apps/application-proxy>

<sup>74</sup> Plan an Azure AD Application Proxy deployment: <https://aka.ms/deploymentplans/appproxy>



Various resources are available on [aka.ms/migrateapps](https://aka.ms/migrateapps) and in particular:

- [SOLUTION GUIDE: MIGRATING ACTIVE DIRECTORY FEDERATION SERVICES \(AD FS\) APPLICATIONS TO AZURE AD](#)<sup>75</sup>. This solution guide walks through the same four phases of planning and executing an application migration project. Please review this guide to apply these phases to the specific purpose of moving an application from AD FS to Azure AD.
- [Tool: The Active Directory Federation Services \(AD FS\) Migration Preparation Script](#)<sup>76</sup>. This script can be run on the on-premises AD FS environment to determine the application readiness status for migrating to Azure AD.

Needless to say, of course, customers who are only in the cloud get the same productivity benefits by configuring single sign-on between Azure AD, Office 365 and applications cloud connected/integrated to Azure AD.

**Note** You can use [SSO deployment plan](#)<sup>77</sup> as a step-by-step guide through the implementation process to add more applications to the scope of single sign-on in Azure AD.

And, in fact, if you're like most organizations today, you're probably somewhere on the way to adopting cloud applications and identities. You may be operational with Azure AD connect and Office/Microsoft 365. You may have configured SaaS cloud applications for some key workloads, but not all.

Having said that, many organizations do have SaaS applications or custom LOB applications federated directly to a local authentication service such as AD FS, alongside Office 365 and other applications integrated/connected to Azure AD.

<sup>75</sup> Solution Guide: migrating Active Directory Federation Services (AD FS) applications to Azure AD: <https://aka.ms/migrateapps/adfsolutionguide>

<sup>76</sup> Active Directory Federation Services (AD FS) migration preparation script: <https://aka.ms/migrateapps/adfstools>

<sup>77</sup> Azure Active Directory Single Sign-On Deployment Plan: <https://aka.ms/SSODPDownload>

For an organization that already uses AD FS (Ping Federate, or another supported local authentication provider), moving applications to Azure AD has the following benefits:

- **Safer access:**
  - Configure granular access control by application using conditional access in Azure AD (see section § [CONDITIONAL ACCESS IN AZURE AD AT THE HEART OF THE STRATEGY](#)). Conditional access policies can be applied to SaaS applications as well as custom applications in the same way as can be done for Office/Microsoft 365.
  - Benefit from Azure AD Identity Protection to detect threats and help protect authentication with machine learning and heuristics that identify risky traffic.
- **Secure collaboration through Azure AD B2B.** Once you connect to SaaS apps with Azure AD, you can give partners access to cloud resources with Azure AD B2B collaboration capabilities (see section § [CONNECTING YOUR PARTNER IDENTITIES](#)).
- **Simplified administration experience and additional features of Azure AD.** Azure AD, as an identity provider for SaaS applications, supports additional features such as:
  - Token signing certificates per application;
  - [Configurable certificates expiration dates](#)<sup>78</sup>;
  - [Automated provisioning](#)<sup>79</sup> of user accounts (in key applications on the market) based on Azure AD identities.
- **Maintain the benefits of a local identity provider.** While you are enjoying the benefits of Azure AD, you can continue to use your on-premises solution for authentication. In this way, requirements such as the use of a multi-factor authentication solution, logging and local auditing remain in place for compliance with your security policies or other regulatory frameworks.
- **Assist in removing the local identity provider.** For organizations that want to replace their local authentication solution, moving applications to Azure AD makes it easier to transition, as part of the work is done *de facto*.

**Note** For more information, see article [MOVE APPLICATIONS FROM AD FS TO AZURE AD](#)<sup>80</sup>.

## Reducing the number of administrator accounts and implementing policies

Even with good detection and response tools, there is still a risk that an attacker might get through your defenses. In these cases, you should minimize the likelihood that a compromised account can work with a privileged role.

---

<sup>78</sup> MANAGE CERTIFICATES FOR FEDERATED SINGLE SIGN-ON IN AZURE ACTIVE DIRECTORY: <https://docs.microsoft.com/en-us/Azure/active-directory/manage-apps/manage-certificates-for-federated-single-sign-on>

<sup>79</sup> Automate user provisioning and deprovisioning to SaaS applications with Azure Active Directory: <https://docs.microsoft.com/en-us/Azure/active-directory/manage-apps/user-provisioning>

<sup>80</sup> MOVE APPLICATIONS FROM AD FS TO AZURE TO: <https://docs.microsoft.com/en-us/Azure/active-directory/manage-apps/migrate-ads-apps-to-Azure>

[Azure AD Privileged Identity Management](#)<sup>81</sup> (PIM) gives visibility of the users assigned to administrative roles and allows to establish rules and policies that govern these accounts.

Azure AD roles - Roles

« + Add member Access reviews Export

Overview  
Quick start

Tasks

- My roles
- My requests
- Approve requests
- Review access

Manage

- Roles
- Members
- Alerts
- Access reviews
- Wizard
- Settings

Activity

- Directory roles audit history
- My audit history

Troubleshooting + Support

- Troubleshoot
- New support request


Your role: Security Administrator and 2 others

ROLE	DESCRIPTION
Application Administrator	Users with this role can create and manage all aspects of app registrations and...
Application Developer	Users with this role can create application registrations independent of the 'U...
Authentication Administrator	Can access to view, set and reset authentication method information for any ...
Billing Administrator	Makes purchases, manages subscriptions, manages support tickets, and moni...
Cloud Application Administrator	Users with this role can create and manage all aspects of app registrations an...
Cloud Device Administrator	Full access to manage devices in Azure AD.
Compliance Administrator	Users with this role have management permissions within in the Office 365 S...
Conditional Access Administrator	Users with this role have the ability to manage Azure Active Directory condi...
CRM Service Administrator	Users with this role have global permissions within Microsoft CRM Online
Customer LockBox Approver	Can approve Microsoft support requests to access customer organizational d...
Desktop Analytics Administrator	Users in this role will have access to manage Desktop Analytics and Office Cu...
Device Administrators	Users with this role become local machine administrators on all Windows 10 ...
Directory Readers	Allows access to various read only tasks in the directory.
Directory Writers	Allows access read tasks and a subset of write tasks in the directory.
Exchange Administrator	Users with this role have global permissions within Microsoft Exchange Online
Global Administrator	Users with this role have access to all administrative features in Azure Active ...
Guest Inviter	Users in this role can manage Azure Active Directory B2B guest user invitatio...
Information Protection Administrator	Users with this role have user rights only on the Azure Information Protection...

Once you have identified the users, you can remove those who do not need privileged access and move the remaining users' permissions from permanent to eligible.

<sup>81</sup> WHAT IS AZURE AD PRIVILEGED IDENTITY MANAGEMENT?: <https://Azure.microsoft.com/en-us/documentation/articles/active-directory-privileged-identity-management-configure/>

Convert members to eligible



Reducing the number of users in your organization who have permanent privileged role assignments will minimize your vulnerability to security breaches.  
To learn more, [click here for documentation of Azure AD Privileged Identity Management](#).

Select the members you want to make eligible to activate their roles

GLOBAL ADMINISTRATOR

☐ MOD Administrator  
admin@M365x585300.onmicrosoft.com

☐ Isaiah Langer  
IsaiahL@M365x585300.OnMicrosoft.com

☐ Lidia Holloway  
LidiaH@M365x585300.OnMicrosoft.com

☐ Megan Bowen  
MeganB@M365x585300.OnMicrosoft.com

☐ Nestor Wilke  
NestorW@M365x585300.OnMicrosoft.com

PRIVILEGED ROLE ADMINISTRATOR

☐ MOD Administrator  
admin@M365x585300.onmicrosoft.com

SECURITY ADMINISTRATOR

☐ MOD Administrator  
admin@M365x585300.onmicrosoft.com

Next

A user who is eligible for administrative access must request access every time he wants to perform a privileged task. We recommend that multi-factor authentication should be enabled for all privileged roles so their identities can be verified. We also recommend setting time limits for administrative access. Users must have access only long enough to accomplish the privileged task but not more. These steps will make it much more difficult for an attacker to access the most valuable data and resources.

Azure AD PIM can be configured from the Azure portal to trigger alerts when there is a suspicious or dangerous activity in your environment and then recommend mitigation strategies. The vulnerabilities identified and reported by Azure AD Identity Protection include risks such as the non-configured multi-factor authentication registration, unmanaged cloud applications, Azure AD PIM security alerts, assigned roles outside of Azure AD PIM or that are enabled too frequently. You need to address these vulnerabilities to enhance your organization's security posture and prevent attackers from exploiting them<sup>82</sup>.

**Note** You can use the [PIM plan](#)<sup>83</sup> as a step-by-step to guide through the implementation.

The higher the user privileges, the greater the potential for damage if such accounts are compromised. With the visibility of these privileged identities, [Azure AD PIM](#)<sup>84</sup> is a feature of the Azure AD Premium P2 Edition that helps reduce the risk associated with administrator access privileges through control, access management, and reporting on these critical administrator roles.

<sup>82</sup> VULNERABILITIES DETECTED BY AZURE ACTIVE DIRECTORY IDENTITY PROTECTION: <https://docs.microsoft.com/en-us/Azure/active-directory/identity-protection/vulnerabilities>

<sup>83</sup> DEPLOY AZURE AD PRIVILEGED IDENTITY MANAGEMENT (PIM): <https://docs.microsoft.com/en-us/Azure/active-directory/privileged-identity-management/pim-deployment-plan>

<sup>84</sup> WHAT IS AZURE PRIVILEGED IDENTITY AD MANAGEMENT?: <https://azure.microsoft.com/En-us/documentation/Articles/Active-Directory-Privileged-Identity-Management-configure/>



Thus, Azure AD PIM helps to bring welcome hygiene by enabling just-in-time and just-enough administration. It is a matter of ensuring that just-in-time privileged access or discontinuing permanent privileges become the norm.

This capability is also now coupled with Azure's role-based access control (RBAC) for resource management in Azure.

**Note** The [Privileged Access Manager \(PAM\)](#)<sup>85</sup> solution allows you to restrict privileged access within an existing AD environment. PAM fulfils two objectives: i) restoring control over a compromised AD environment by retaining a separate bastion environment known to be unaffected by malicious attacks and ii) isolation of privileged accounts used to reduce the risk of theft of these credentials. PAM is an instance of PIM implemented using Microsoft Identity Manager (MIM).

Also, Azure AD now allows you to govern the access of employees and business partners (external users) to enterprise-wide resources with powerful compliance and auditing controls.

[Azure AD Entitlement Management](#)<sup>86</sup> (recently announced and now available in public preview on the date of publication of this white paper) eliminates barriers to internal collaboration by automating access requests, approvals, audits and reviews of employees and partners for Office/Microsoft 365, for thousands of popular SaaS applications, as well as for any LOB application that is integrated with Azure AD.

**Note** For more information, see article [WHAT IS AZURE AD ENTITLEMENT MANAGEMENT? \(PREVIEW\)](#)<sup>87</sup> and blog post [ANNOUNCING A NEW AZURE AD IDENTITY GOVERNANCE PREVIEW — ENTITLEMENT MANAGEMENT](#)<sup>88</sup>.

Last year, at the Ignite Conference, Microsoft outlined its vision of governance and managing access to resources with Azure AD. Azure AD Entitlement Management is the fourth module of identity governance within Azure AD, the three other modules, Azure AD PIM addressed above, the [terms of use](#)<sup>89</sup> and the [revisions of access](#)<sup>90</sup> being already generally available.

## Monitoring user behavior locally

As already noted, Azure ATP enables the analysis of signals from on-premises Active Directory directories to detect advanced threats, compromised identities, and actions of malicious internal users.

---

<sup>85</sup> PRIVILEGED ACCESS MANAGEMENT FOR ACTIVE DIRECTORY DOMAIN SERVICES: <https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services>

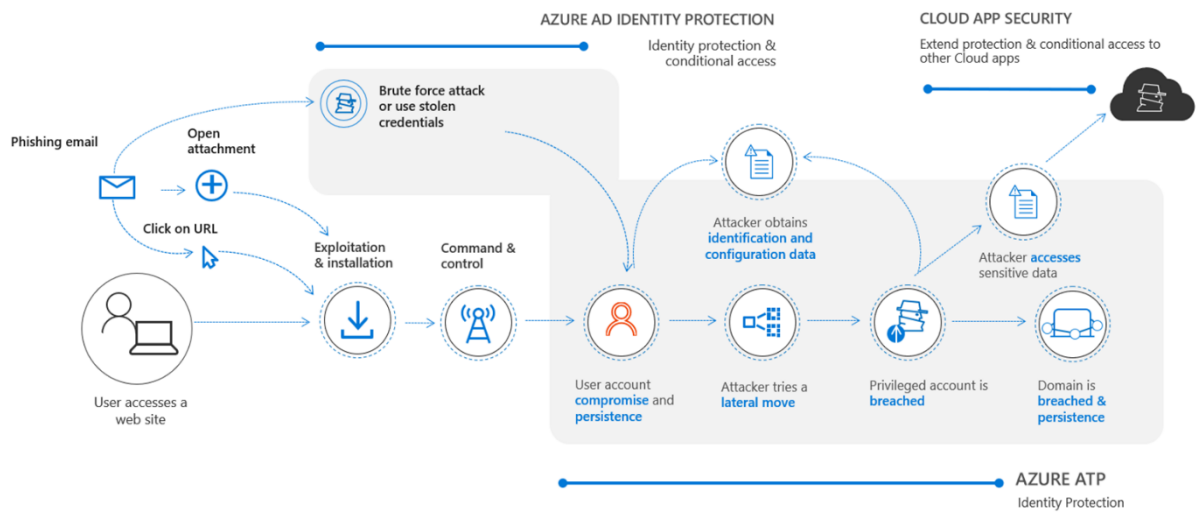
<sup>86</sup> WHAT IS AZURE AD ENTITLEMENT MANAGEMENT? (PREVIEW): <https://docs.microsoft.com/en-us/Azure/active-directory/governance/entitlement-management-overview>

<sup>87</sup> Ibid

<sup>88</sup> ANNOUNCING A NEW AZURE AD IDENTITY GOVERNANCE PREVIEW—ENTITLEMENT MANAGEMENT: <https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Announcing-a-new-Azure-AD-identity-governance-preview/ba-p/480864>

<sup>89</sup> AZURE ACTIVE DIRECTORY TERMS OF USE FEATURE: <https://docs.microsoft.com/en-us/Azure/active-directory/conditional-access/terms-of-use>

<sup>90</sup> WHAT ARE AZURE AD ACCESS REVIEWS?: <https://docs.microsoft.com/en-us/Azure/active-directory/governance/access-reviews-overview>



# Managing devices

With the generalization of the mobile workforce, using laptops, tablets, or smartphones, the device remains the main input vector of any attack. The simple click of a user on a phishing email link can install malware or retrieve the login credentials that will immediately give access to the applications or the corporate network.

According to the 2018 Verizon report,<sup>91</sup> targeted phishing (spear phishing) is responsible for **93%** of the leakage or violation of data, email being the most used in 96% of cases. Even though 78% of people will not take the bait, for others, in two third of cases, it leads to malware being installed on the device. In environment with only a perimeter protection, just one infected device connected to the network is enough for the spread of the malware to start or, for the attacker to gain a foothold in the case of a targeted attack.

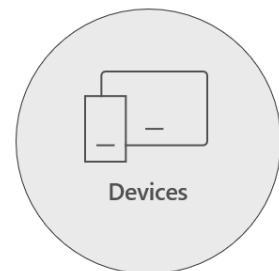
The Zero Trust approach addresses the intrinsic weakness of the perimetric model with these strong principles:

- Devices are not trusted and should be best protected against phishing (and other) attacks and be as resistant to malware as possible;
- Devices must be able to protect themselves, whether they are outside the company (the Internet) or connected to the internal network. The latter cannot be considered as trustworthy because of the high probability that it hosts compromised devices;
- Any abnormal behavior of a device must be identified at the earliest to detect the weak signals characteristic of a targeted attack, to avoid any propagation of a compromise or to try and minimize its impacts.

**Note** In the one-third of cases where phishing results in theft of identifiers, it is an attack on identity, that multi-factor authentication could help prevent. For more information, see previous section.

This section describes associated activities as follows:

- Authenticating devices;
- Ensuring that devices are healthy and ;
- Setting up threat detection on endpoints and anti-malware software on all devices.



## Authenticating devices

To ensure the security of any device that connects to the organization's resources, it must be known and referenced in a management tool to be controlled. The preferred tool for this is the MDM (Mobile Device Management) which allows you to manage mobile devices, smartphones, tablets (iOS and Android) as well as Windows devices.

The MDM provides many features that will bring a knowledge and a level of control on the device and increase the confidence accordingly. A device must first be registered to be referenced in the MDM and receive a certificate. This certificate will be used to authenticate the device with the MDM service and to ensure the confidentiality of communications. This enables a clear distinction between enterprise-

---

<sup>91</sup> 2018 DATA BREACH INVESTIGATIONS REPORT: [https://enterprise.verizon.com/resources/reports/DBIR\\_2018\\_Report.pdf](https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf)

managed devices and those that an employee (or an attacker) would attempt to use to access the company's applications.

**Note** For more information about registering devices, see article [WHAT IS DEVICE ENROLLMENT?](#)<sup>92</sup>.

In the Microsoft solution portfolio, the MDM functionality is provided by [Microsoft Intune](#)<sup>93</sup> that is accessible directly from the Azure portal. Microsoft Intune is integrated with Azure AD.

**Note** Other MDM solutions are integrated with Azure AD, such as AirWatch, Hexnode, MobileIron solutions. For more information about how to integrate an MDM with Azure AD, see article [AZURE ACTIVE DIRECTORY INTEGRATION WITH MDM](#)<sup>94</sup>.

Thanks to Microsoft Intune, the registration process provides a set of device configuration options, such as security policies and configuration options, through management profiles. It is possible to deploy Simple Certificate Enrollment Protocol (SCEP) authentication certificates to enable the connection to the company's Wi-Fi.

**Note** For more information about profile management capabilities for accessing enterprise resources, see [COMPANY RESOURCE ACCESS](#)<sup>95</sup>.

It should be noted that Microsoft Intune belongs to the broader category of Enterprise Mobile Management Systems (EMMS), combining MDM function, and that of Mobile Application Management, or MAM, that are addressed further on in this white paper (See section § LIMITING ACCESS TO ONLY TRUSTED MOBILE APPS AND CONFIGURATIONS). It also incorporates features that were previously found only in Client Management Tools (CMT), such as [Microsoft System Center Configuration Manager](#)<sup>96</sup> (SCCM).

In mid-2018, Microsoft Intune was positioned among the leaders in the Gartner Magic Quadrant in the EMM category<sup>97</sup>.

## Ensuring that devices are healthy and compliant

### Enforcing security policies

Once registered in the MDM, the device will be manageable from a security standpoint: security policies are set to impose chosen rules, for example, a PIN code with a level of complexity, a minimum OS version level, storage encryption, prohibiting the use of "jailbroken" devices, etc.

If at any given time, the device no longer complies with the security policy imposed, it will be considered non-compliant and may be denied access to certain resources of the company or, at least, have restricted access.

---

<sup>92</sup> WHAT IS DEVICE ENROLLMENT?: <https://docs.microsoft.com/en-us/intune/device-enrollment>

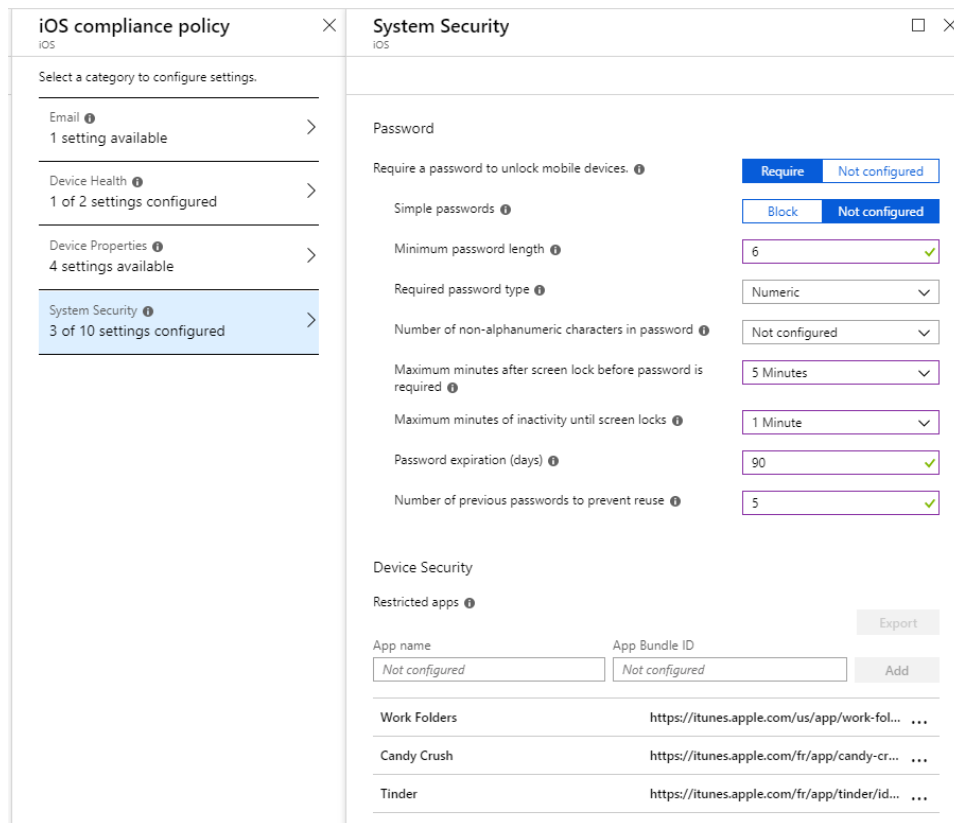
<sup>93</sup> Microsoft Intune : <https://www.microsoft.com/en-us/enterprise-mobility-security/microsoft-intune>

<sup>94</sup> AZURE ACTIVE DIRECTORY INTEGRATION WITH MDM: <https://docs.microsoft.com/en-us/windows/client-management/mdm/Azure-active-directory-integration-with-mdm>

<sup>95</sup> COMPANY RESOURCE ACCESS: <https://docs.microsoft.com/en-us/intune/device-management-capabilities#company-resource-access>

<sup>96</sup> Microsoft System Center Configuration Manager: <https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager>

<sup>97</sup> MICROSOFT EMERGES AS A LEADER IN GARTNER MQ FOR UNIFIED ENDPOINT MANAGEMENT (UEM): <https://www.microsoft.com/en-us/microsoft-365/blog/2018/07/25/microsoft-emerges-as-a-leader-in-gartner-mq-for-unified-endpoint-management-uem/>



In the policy defined in the above example for iOS, the use of a 6-character password (PIN code) is required. The administrator has, moreover, banned the use of certain applications through the **Restricted apps** option.

**Note** For more information about restricting and configuring security policies, see article [DEVICE CONFIGURATION AND SECURITY](#)<sup>98</sup>.

A key element of an end-to-end security solution vision is to know in near real-time the health status of a device, to detect whether the defenses are still active and to take appropriate measures accordingly.

Windows 10 devices as an illustration

The Windows 10 device health status can be determined and validated with "Windows Defender System Guard Runtime Attestation" and combined with Azure AD conditional access policies for a "Zero Trust" approach.

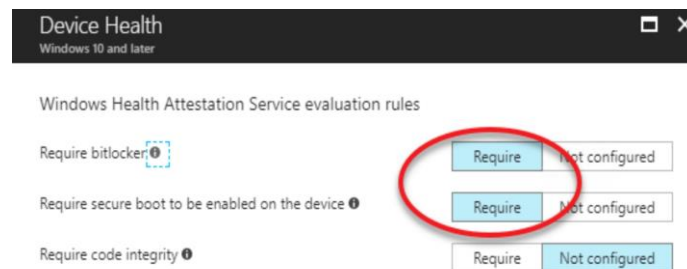
<sup>98</sup> DEVICE CONFIGURATION AND SECURITY: <https://docs.microsoft.com/en-us/intune/device-management-capabilities#device-security-and-configuration>

**Note** For more information, see articles [INTRODUCING WINDOWS DEFENDER SYSTEM GUARD RUNTIME ATTESTATION](#)<sup>99</sup> and [BUILDING ZERO TRUST NETWORKS WITH MICROSOFT 365](#)<sup>100</sup>.

The raw measures taken when starting Windows 10 are stored in the Platform Configuration Registers (PCR) of the Trusted Platform Module (TPM) while the details of all events (executable path, certification authority, etc.) are available in the TCG log.

Microsoft Defender ATP can determine whether the boot sequence contains signs of malware, such as a rootkit. It can also decide to send the boot log to a remote health attestation server to provide a separation between the measurement component and the verification component.

Microsoft Intune, or a third-party MDM, can also inspect the report generated by the health verification service and determine whether security defenses, such as BitLocker disk encryption or applications code integrity control, are active on the device.



## Reporting compliance information

We recommend taking advantage of MDM optional ability to be integrated with Azure AD to provide the device's compliance information. This information will then be available as an input criterion in the Azure AD conditional access control evaluation engine. For example, Microsoft Intune can report device compliance to Azure AD regardless of the OS.

The conditional access policies defined by the organization in Azure AD will then be able to enforce, for instance, that only compliant devices can access the more sensitive applications. For other applications, you can authorize access but in a restricted way, for instance, by allowing only reading but without the possibility of downloading information. Unregistered devices will be, by definition, considered non-compliant and will be constrained by the related policies.

---

<sup>99</sup> INTRODUCING WINDOWS DEFENDER SYSTEM GUARD RUNTIME ATTESTATION: <https://www.microsoft.com/security/blog/2018/04/19/introducing-windows-defender-system-guard-runtime-attestation/>

<sup>100</sup> BUILDING ZERO TRUST NETWORKS WITH MICROSOFT 365: <https://www.microsoft.com/security/blog/2018/06/14/building-zero-trust-networks-with-microsoft-365/>

**Note** At the time of writing this document, third-party MDMs are able to report compliance only for Windows 10 devices. For more information, see article [WHAT ARE ACCESS CONTROLS IN AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS](#)<sup>101</sup>.

## Updating devices and applications

**Updating the operating system** on all devices, regularly and whenever possible as soon as they are available, is a **necessity from a security point of view**. Windows 10 devices can be updated directly by the MDM while for other mobile OSs, a user action remains necessary.

Windows 10 provides MDM with the necessary APIs to drive device updates and specifically enforce an automatic update policy or specify a list of approved updates to ensure that only the latter are installed.

For other OSs, MDM has features to encourage and, if necessary, compel the user to update his device. For example, in the case of Microsoft Intune, the user will first be informed by a series of emails stating that he has *x* days left before having to update his device. Once this delay has passed, the device becoming *de facto* non-compliant, a conditional access control policy may prohibit access to certain applications. The application protection policies of the Microsoft Intune MAM features are also available to enforce a particular version of OS to continue using the MDM-protected applications.

**Note** For more information, please see articles [MOBILE DEVICE MANAGEMENT \(MDM\) FOR DEVICE UPDATES](#)<sup>102</sup> and [MANAGE OPERATING SYSTEM VERSIONS WITH INTUNE](#)<sup>103</sup>.

## Setting up threat detection on endpoints and anti-malware software on all devices

It is recommended that all devices be equipped with a malware protection solution. These solutions can also provide network protection against malicious Wi-Fi, verification of unpatched vulnerabilities, etc. and leverage cloud and Machine Learning to detect suspicious behaviors related to malicious applications. MDM can impose installation from the organization app store during the registration phase.

These solutions, known as the Mobile Threat Defense (MTD), can interface with MDM tools to feed alerts and information about the device's health status.

For Intune, several partner solutions integrate such as Lookout, Symantec Endpoint Protection Mobile, Check Point SandBlast Mobile, and more.

**Note** For the full list of partners, see article [MOBILE THREAT PROTECTION PARTNERS](#)<sup>104</sup>.

Depending on its analysis, the solution returns a threat level (low, medium or high), which Intune uses to indicate whether the device is compliant or not. This information may be leveraged by the conditional access policies to restrict access to certain applications or prohibit it.

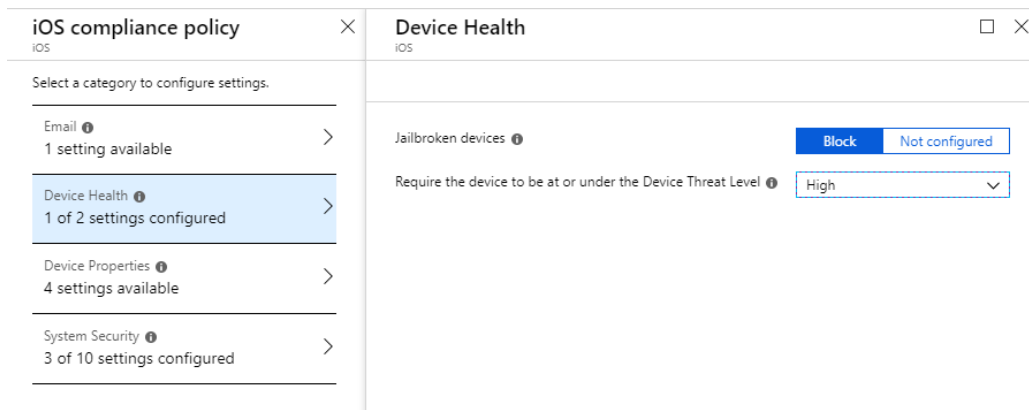
---

<sup>101</sup> WHAT ARE ACCESS CONTROLS IN AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS?: <https://docs.microsoft.com/en-us/Azure/active-directory/conditional-access/controls#compliant-device>

<sup>102</sup> MOBILE DEVICE MANAGEMENT (MDM) FOR DEVICE UPDATES: <https://docs.microsoft.com/en-us/windows/client-management/mdm/device-update-management>

<sup>103</sup> MANAGE OPERATING SYSTEM VERSIONS WITH INTUNE: <https://docs.microsoft.com/en-us/intune/manage-os-versions>

<sup>104</sup> MOBILE THREAT PROTECTION PARTNERS: <https://docs.microsoft.com/en-us/intune/mobile-threat-defense#mobile-threat-defense-partners>



In the example above, the iOS compliance policy allows adjusting the level below which the device is no longer considered compliant.

**Note** For more information, see articles [ADD AND ASSIGN MOBILE THREAT DEFENSE \(MTD\) APPS WITH INTUNE](https://docs.microsoft.com/en-us/intune/mtd-apps-ios-app-configuration-policy-add-assign)<sup>105</sup> and [CREATE A COMPLIANCE POLICY FOR MOBILE THREAT DEFENSE \(MTD\) DEVICES WITH INTUNE](https://docs.microsoft.com/en-us/intune/mtd-device-compliance-policy-create)<sup>106</sup>.

## Windows 10 devices (and Mac OS X) as an illustration

Maintaining the security of all devices including Windows 10 devices is one of the cornerstones of an end-to-end security as well as the Zero Trust vision.

Windows 10 devices have a set of protection mechanisms to reduce the attack surface:<sup>107</sup>

- [Windows Defender Exploit Protection](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/exploit-protection-exploit-guard)<sup>108</sup> ensures the protection of Windows 10 operating system against the different types of exploits by integrating all the protection mechanisms previously available with the "Enhanced Mitigation Experience Toolkit";
- [Windows Defender System Guard](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-system-guard/how-hardware-based-root-of-trust-helps-protect-windows)<sup>109</sup> ensures a secure boot of the OS while guaranteeing its integrity by anchoring the trusted root into the hardware through the UEFI BIOS and the TPM module. The ongoing system integrity checks are performed remotely through a certificate and are used as a criterion in access control;
- [Windows Defender Credential Guard](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-how-it-works)<sup>110</sup> isolates the Local Security Authority (LSA) subsystem and the secrets it manipulates in a container relying on Hyper-V virtualization. This helps to protect

<sup>105</sup> ADD AND ASSIGN MOBILE THREAT DEFENSE (MTD) APPS WITH INTUNE: <https://docs.microsoft.com/en-us/intune/mtd-apps-ios-app-configuration-policy-add-assign>

<sup>106</sup> CREATE A MOBILE THREAT DEFENSE (MTD) DEVICE COMPLIANCE POLICY WITH INTUNE: <https://docs.microsoft.com/en-us/intune/mtd-device-compliance-policy-create>

<sup>107</sup> OVERVIEW OF ATTACK SURFACE REDUCTION: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/overview-attack-surface-reduction>

<sup>108</sup> PROTECT DEVICES FROM EXPLOITS: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/exploit-protection-exploit-guard>

<sup>109</sup> WINDOWS DEFENDER SYSTEM GUARD: HOW A HARDWARE-BASED ROOT OF TRUST HELPS PROTECT WINDOWS 10: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-system-guard/how-hardware-based-root-of-trust-helps-protect-windows>

<sup>110</sup> HOW WINDOWS DEFENDER CREDENTIAL GUARD WORKS: <https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-how-it-works>



user identity-related secrets and to thwart pass-the-hash and pass-the-ticket types of attacks, which are used for lateral moves with privilege escalation;

- [Windows Defender Application Guard](#)<sup>111</sup> protects the OS and other applications when the user accesses untrusted Web sites via the Edge browser. The site is opened in an isolated Hyper-V container to avoid jeopardizing the host in case the site is malicious;
- [Windows Defender Application Control](#)<sup>112</sup> reduces the attack surface by limiting applications that users are allowed to run, as well as the code that can be run in the system kernel.

In addition, [Windows Defender Advanced Threat Protection](#)<sup>113</sup> (ATP) previously mentioned is an anti-malware solution that can be implemented on Windows 10 devices (and more recently on Mac) that offers functions related to detection, protection and response. The protection is ensured by the cloud-based anti-malware feature, that provides near-instantaneous detection and blocking against emerging threats.

**Note** Windows Defender Advanced Threat Protection has been renamed to Microsoft Defender Advanced Threat Protection (ATP) and is also available to date on a Mac platform. For more information, see blog post [ANNOUNCING MICROSOFT DEFENDER ATP FOR MAC](#)<sup>114</sup>.

The Endpoint Detection and Response (EDR) collects information about Windows 10 devices behavior and stores it in a cloud storage that is accessible only by the organization. The information from all your Windows 10 devices is analyzed and correlated, and the results made available through a security dashboard. When alerts are reported, the organization SOC analysts can carry out their investigation on the identities and machines identified at risk, to get full visibility on the compromise and take appropriate measures.

Finally, as illustrated by the following schema, Windows Defender Advanced Threat Protection (ATP) integrates with Microsoft Intune, which itself is integrated with Azure AD to transfer the status of Windows 10 devices.

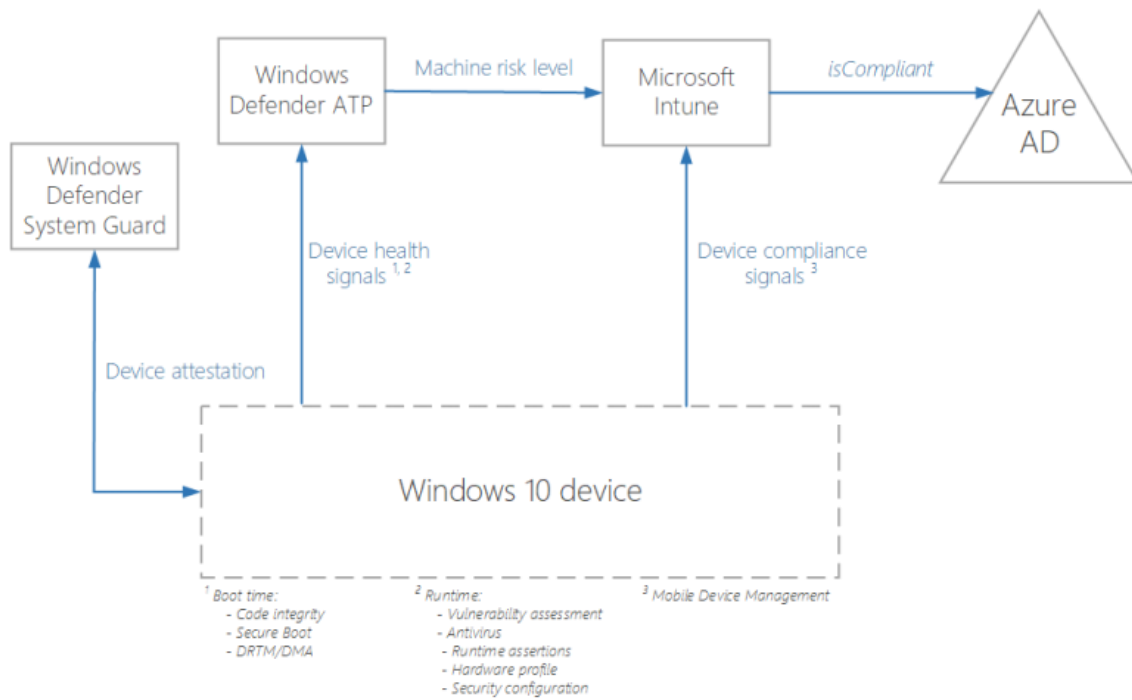
---

<sup>111</sup> WINDOWS DEFENDER APPLICATION GUARD: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview>

<sup>112</sup> WINDOWS DEFENDER APPLICATION CONTROL: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control>

<sup>113</sup> WINDOWS DEFENDER ADVANCED THREAT PROTECTION: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection>

<sup>114</sup> ANNOUNCING MICROSOFT DEFENDER ATP FOR MAC: <https://techcommunity.microsoft.com/t5/Windows-Defender-ATP/Announcing-Microsoft-Defender-ATP-for-Mac/ba-p/378010>



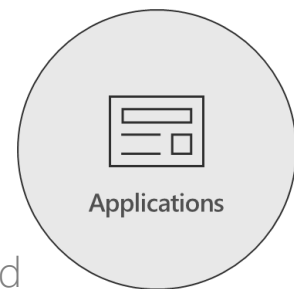
**Note** For more information, see blog post [BUILDING ZERO TRUST NETWORKS WITH MICROSOFT 365](https://cloudblogs.microsoft.com/microsoftsecure/2018/06/14/building-zero-trust-networks-with-microsoft-365/)<sup>115</sup>.

<sup>115</sup> BUILDING ZERO TRUST NETWORKS WITH MICROSOFT 365: <https://cloudblogs.microsoft.com/microsoftsecure/2018/06/14/building-zero-trust-networks-with-microsoft-365/>

# Managing applications

This section describes how to protect against risky applications as follows:

- Limiting access to only trusted mobile apps and configurations;
- Discovering the applications in use in the organization;
- Monitoring and managing application sessions.



## Limiting access to only trusted mobile apps and configurations

Beyond the "pure" device management that is detailed in the previous sections, mobile device management tools offer the ability to manage the enterprise applications that will be installed on the employee's devices.

Application management or Mobile Application Management (MAM) allows choosing which applications will be deployed on which mobile devices, targeting by user categories or groups. It is possible to configure settings specific to each application such as language, security, or company customization.

This application control is possible when the device is registered in the MDM, which is the most restrictive scenario where the device belongs to the company and is provided to the user. A second and more flexible type of scenario, BYOD (Bring-Your-Own-Device), is also possible when the employee uses his personal device for personal and professional use. In this case, **the device will not be registered in the MDM**, but the administrator will be able to assign applications to user groups, and to assign protection policies to given applications, etc. even if some functions will not be available such as, for instance, uninstalling applications.

In the case of Microsoft Intune, a second level of control applies to applications that incorporate their own protection policies, meaning that they have been adapted to provide an additional level of information protection for the data they process. For instance, it may be possible to mandate a PIN code to open an application in a business context, to control the sharing of data between applications or to prevent the copy of data from the company's applications to a personal storage location.

This additional level of protection is available for all Office mobile applications and can be implemented for enterprise applications by using a development kit.<sup>116</sup>

**Note** For more information, see articles [WHAT ARE APP PROTECTION POLICIES?](https://docs.microsoft.com/en-us/intune/app-protection-policy)<sup>117</sup>, [ASSIGN APPS TO GROUPS WITH MICROSOFT INTUNE](https://docs.microsoft.com/en-us/intune/apps-deploy)<sup>118</sup>, and [APPLICATION CONFIGURATION POLICIES FOR MICROSOFT INTUNE](https://docs.microsoft.com/en-us/intune/app-configuration-policies-overview)<sup>119</sup>.

## Discovering the applications in use in the organization

With the proliferation of applications in SaaS mode and the ease for the LOBs to subscribe to them, what has been referred to as "Shadow IT" can undermine the company's security policies. These applications are not controlled by the internal IT or by the security teams, and constitute a threat as there is no

---

<sup>116</sup> INTRODUCING THE MICROSOFT INTUNE APP SDK: <https://docs.microsoft.com/en-us/intune/app-sdk>

<sup>117</sup> WHAT ARE APPLICATION PROTECTION POLICIES?: <https://docs.microsoft.com/en-us/intune/app-protection-policy>

<sup>118</sup> ASSIGN APPS TO GROUPS WITH MICROSOFT INTUNE: <https://docs.microsoft.com/en-us/intune/apps-deploy>

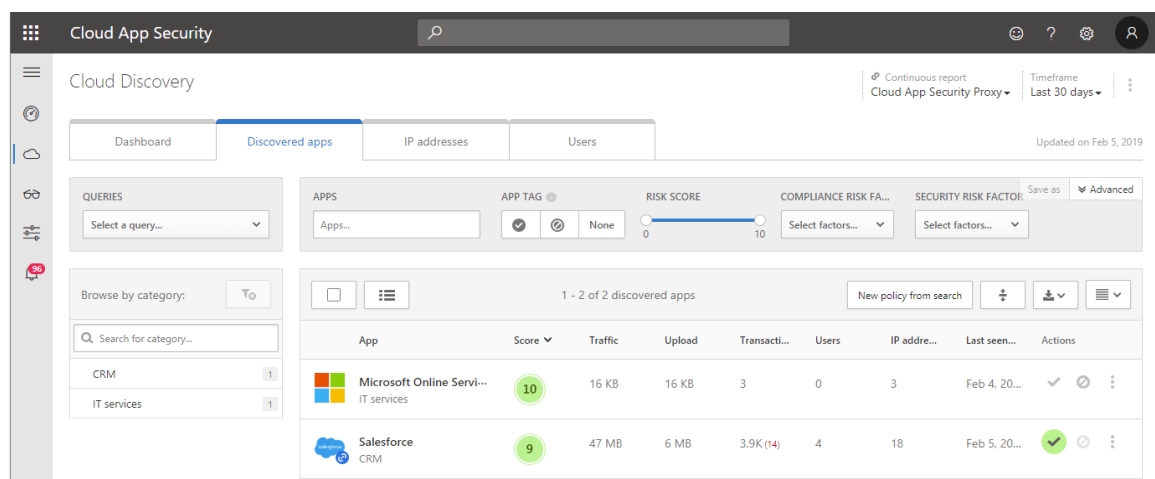
<sup>119</sup> APPLICATION CONFIGURATION POLICIES FOR MICROSOFT INTUNE: <https://docs.microsoft.com/en-us/intune/app-configuration-policies-overview>

guarantee that these applications comply with the security and compliance standards, and that the security controls that should be put in place do exist. For example, the LOBs can subscribe to a SaaS application and store company data subject to regulation such as GDPR. If the application is not properly secured, any leakage of personal data may have significant consequences on the organization who may only discover the leakage after the event.

**The “Zero Trust” vision requires complete control of applications** including cloud applications that are most exposed because they are accessible from the Internet. However, "Shadow IT" is an extension of the perimeter and an increase in exposure, without any visibility or guarantee of compliance with security rules.

The solution to regain control is the use of Cloud Access Security Broker (CASB) solutions that provide a cloud discovery feature: through analysis of outgoing network flows from the various firewalls and proxies logs, the CASB identifies the cloud applications that are used and generates reports on these applications, users who access them, and so on.

The Microsoft CASB solution is [Microsoft Cloud App Security](https://www.microsoft.com/en-us/enterprise-mobility-security/cloud-app-security)<sup>120</sup> that provides the cloud discovery feature with the ability to identify more than 16,000 cloud applications through the analysis of traffic logs. Not only does it provide visibility across all accessed cloud applications, but it can also determine who in the organization uses them. If required, you can block access to applications that are considered to be non-compliant by relying on risk level evaluations provided by Microsoft Cloud App Security (MCAS).



In the above screenshot, you can confirm that only two SaaS solutions are used in your company that are the Microsoft Online Services and the Salesforce App (not representative of a real case).

**Note** For more information, see articles [MICROSOFT CLOUD APP SECURITY OVERVIEW](https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security)<sup>121</sup> and [CONFIGURE CLOUD DISCOVERY](https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery)<sup>122</sup>.

## Monitoring and managing application sessions

The core of the implementation of a “Zero Trust” approach, as we have seen, is to condition access to applications to dynamically evolving criteria.

<sup>120</sup> Microsoft Cloud App Security: <https://www.microsoft.com/en-us/enterprise-mobility-security/cloud-app-security>

<sup>121</sup> INTRODUCING MICROSOFT CLOUD APP SECURITY: <https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security>

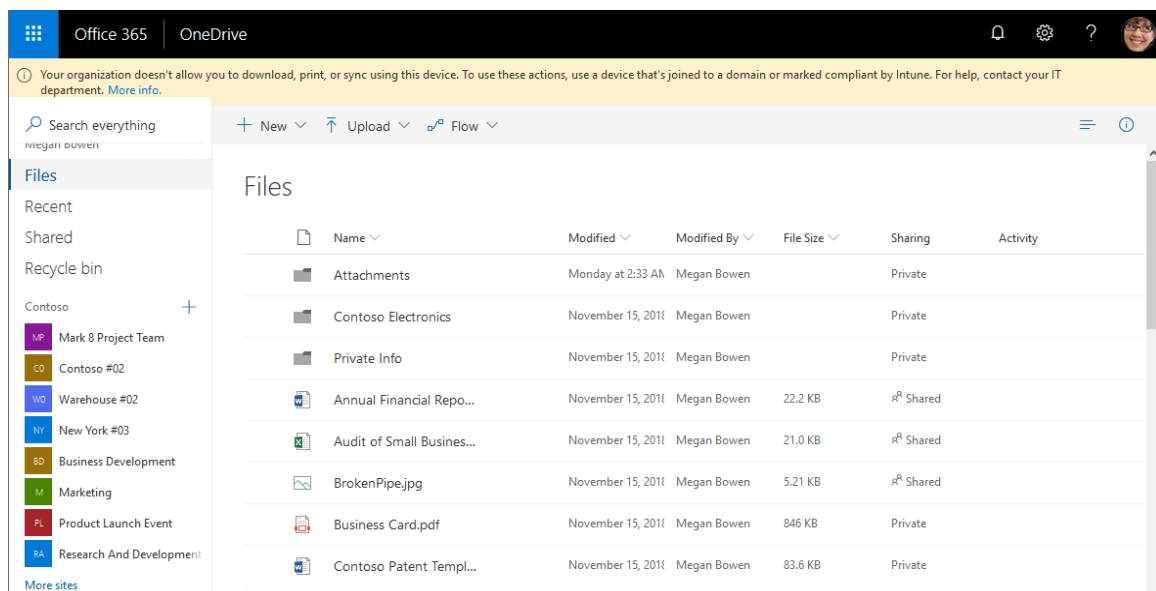
<sup>122</sup> CONFIGURE CLOUD DISCOVERY: <https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery>

When a user has passed the authentication stage, which may have forced a second factor to be taken into account, such as proof of possession of a smartphone, the user accesses the application with the permissions linked to his profile. However, if the device used for this access is considered non-compliant, having imposed a multi-factor authentication provides a guarantee only on the identity of the user.

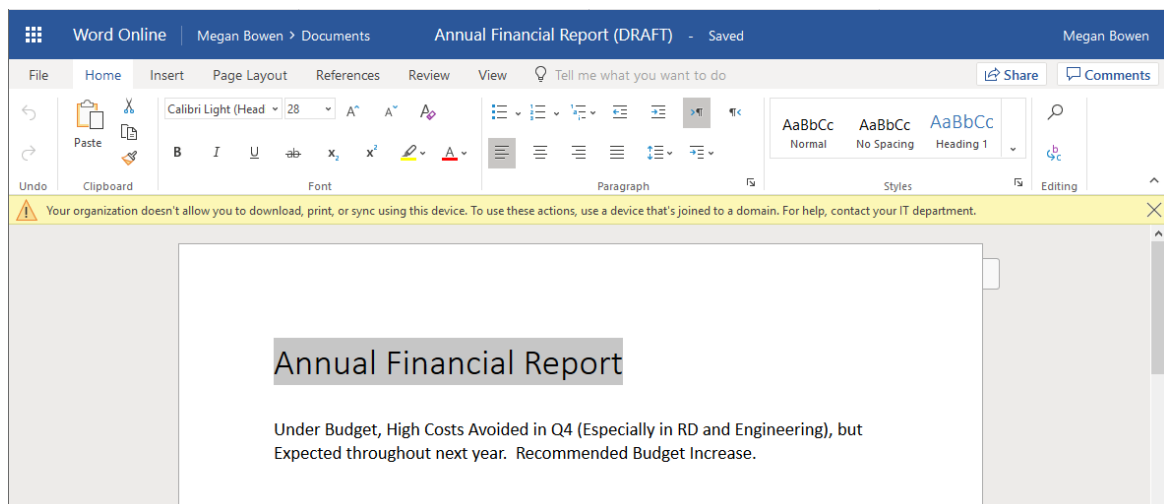
When access is made from a non-compliant device, one may choose a security policy that prohibits access to the application or, in a more nuanced way, allows access while limiting the user's rights within the session. For example, access to cloud storage with reduced rights can be granted: the user will be able to open and edit his documents but will not be able to download or print them. This helps to limit the risk of information leakage to a non-trusted device.

## SharePoint Online/OneDrive for Business and Exchange Online

In Office/Microsoft 365, SharePoint Online and OneDrive for Business can be configured to restrict user rights when accessing from a non-compliant device. A yellow banner is displayed at the top of the browser to indicate to the user that he will not be able to download, print or synchronize locally the documents that he accesses.



If the user opens a document, here in Word online, a banner will warn him that it cannot be saved locally or printed.

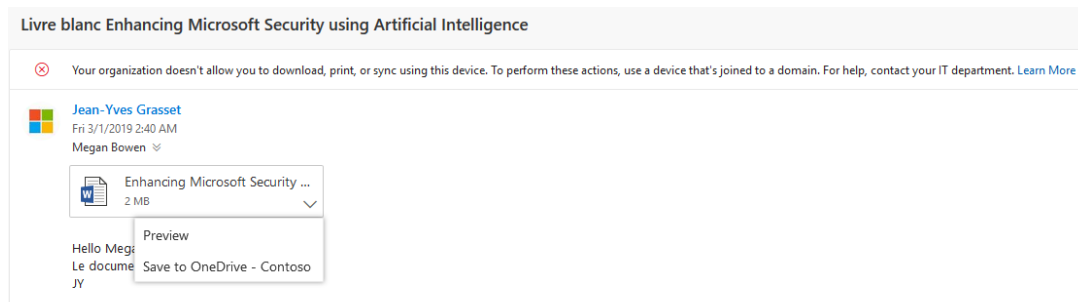


This protection helps to prevent even unintentional information leaks while allowing the user to access his documents and modify them, knowing that they will not be able to leave the company's secure storage.

This behavior is made possible by configuring a conditional access control policy in Azure AD together with an ad hoc SharePoint Online/OneDrive for Business service configuration.

**Note** For more information, see article [WHAT ARE ACCESS CONTROLS IN AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS?](#)<sup>123</sup> and blog post [CONDITIONAL ACCESS "LIMITED ACCESS" POLICIES FOR SHAREPOINT ARE IN PUBLIC PREVIEW!](#)<sup>124</sup>.

Exchange online offers the same type of restrictions when the user accesses his or her email from a non-compliant device. He can read his mails, read the attachments or save them on his OneDrive for Business but without being able to copy them locally.



The above example shows a warning message that appears in the top banner of the mail and that specifies that the document will not be able to be downloaded locally. The user has the choice to preview the attached document or save it on its OneDrive for Business.

**Note** For more information, see blog post [CONDITIONAL ACCESS IN OUTLOOK ON THE WEB FOR EXCHANGE ONLINE](#)<sup>125</sup>.

## Controlling session with Microsoft Cloud App Security

Beyond SharePoint Online/OneDrive for Business and Exchange Online, conditional access control can be used to control application sessions configured as single sign-on (SSO) with Azure AD with the SAML 2.0 and OpenID connect protocols (OIDC), as well as locally hosted Web applications that are configured with the [Azure AD application proxy](#)<sup>126</sup>.

This relies on MCAS reverse-proxy function which, by taking control of the session, may apply restrictions such as blocking a download or authorizing a download but protecting it by encryption.

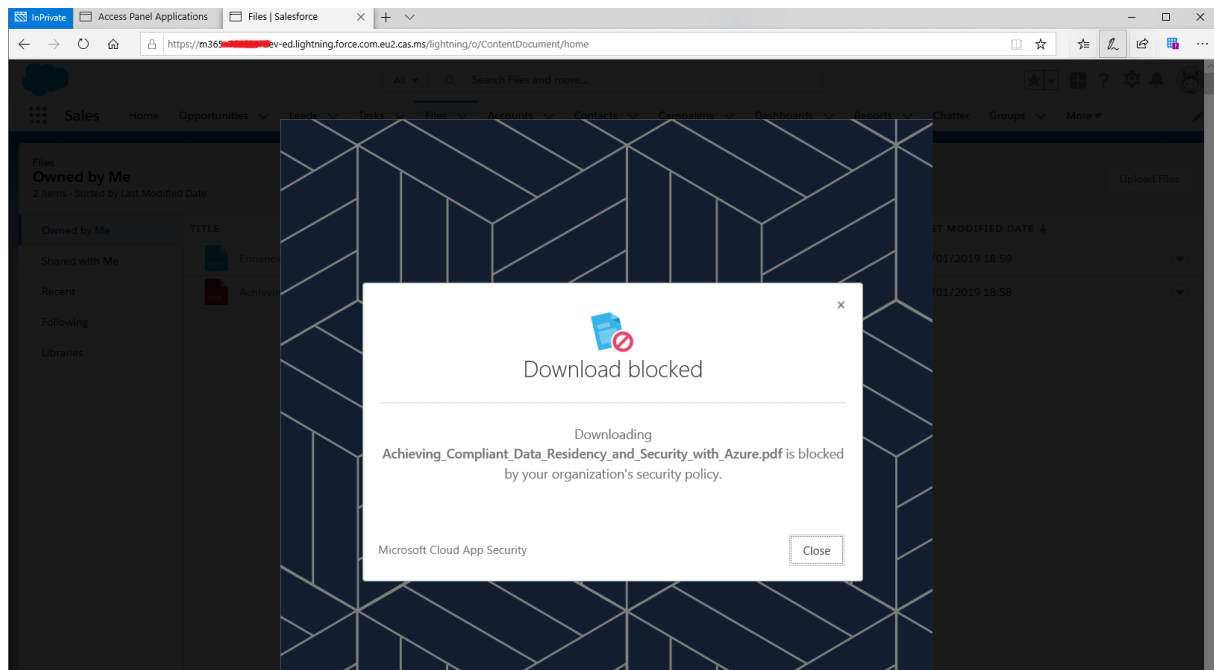
---

<sup>123</sup> WHAT ARE ACCESS CONTROLS IN AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS?: <https://docs.microsoft.com/en-us/Azure/active-directory/conditional-access/controls#session-controls>

<sup>124</sup> CONDITIONAL ACCESS "LIMITED ACCESS" POLICIES FOR SHAREPOINT ARE IN PUBLIC PREVIEW!: <https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Conditional-Access-8220-limited-access-8221-policies-for/ba-p/245228>

<sup>125</sup> CONDITIONAL ACCESS IN OUTLOOK ON THE WEB FOR EXCHANGE ONLINE: <https://techcommunity.microsoft.com/t5/Outlook-Blog/Conditional-Access-in-Outlook-on-the-web-for-Exchange-Online/ba-p/267069>

<sup>126</sup> Remote access to on-premises applications through the Azure Active Directory application proxy service: <https://docs.microsoft.com/en-us/Azure/active-directory/manage-apps/application-proxy>



The above screenshot illustrates how to block the download of a sensitive document from Salesforce if the user tries to copy it locally to a non-compliant device. The Salesforce application was pre-configured with federated single sign-on with Azure AD using the SAML 2.0 protocol (see article [TUTORIAL: AZURE ACTIVE DIRECTORY INTEGRATION WITH SALESFORCE](https://docs.microsoft.com/en-us/Azure/active-directory/saas-apps/salesforce-tutorial)<sup>127</sup>). Then, a policy was created in MCAS to cause the download blocking action under certain conditions.

---

<sup>127</sup> TUTORIAL: AZURE ACTIVE DIRECTORY INTEGRATION WITH SALESFORCE: <https://docs.microsoft.com/en-us/Azure/active-directory/saas-apps/salesforce-tutorial>

Edit session policy

View policy matches (0)

Policy template

No template

Policy name

Salesforce protect DOCX files on download

Description

Policy severity

Low

Category

DLP

Session control type

Select the type of control you want to enable:

Control file download (with DLP)

Activity source

Add activity filters to the policy

ACTIVITIES MATCHING ALL OF THE FOLLOWING

App

equals

Salesforce

+

Edit and preview results

Add file filters to the policy

FILES MATCHING ALL OF THE FOLLOWING

Extension

equals

docx

+

Actions

Select an action to be applied when user activity matches the policy.

Test

Monitor all activities

Block

Block file download & monitor all activities

Protect

Apply classification label to downloads & monitor all activities

Select an Azure Information Protection classification label to apply to matching files:

Confidential \ All Employees

Label will be applied to any supported file.

☐ Block download of any file that is unsupported by native protection or where native protection is unsuccessful.

The above snapshot shows part of the screen of a policy defined in MCAS defining that a Confidential label should be applied to all documents uploaded from Salesforce to a non-compliant device. All such documents are also encrypted by Azure Information Protection.

**Note** For more information about how to work and implement session access policies with MCAS, see article [PROTECT APPLICATIONS WITH CONDITIONAL ACCESS CONTROL TO MICROSOFT CLOUD APP SECURITY APPLICATIONS](#)<sup>128</sup>.

<sup>128</sup> Protect applications with conditional access control for Microsoft cloud app security applications: <https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad>



# Protecting data

One of the principles of the "Zero trust " model stipulates that all resources must be secure. As already emphasized, resources encompass the applications, as well as the data they manipulate or store.

Forrester's white paper [FORRESTER FIVE STEPS TO A ZERO TRUST NETWORK, ROAD MAP: THE SECURITY ARCHITECTURE AND OPERATIONS PLAYBOOK \(OCTOBER 1, 2018\)](#)<sup>129</sup> previously mentioned, proposes as a first step to identify sensitive data in order to protect them as a priority.

Indeed, it is clear that not all data have the same sensitivity: some will have low sensitivity and their disclosure outside the organization would have little impact; others, on the contrary, will be critical and their disclosure could have severe consequences. This may include confidential information about the organization's strategy or results, research and development documents that involved significant investments and whose leakage could endanger the very life of the company, patents, or data subject to regulation (such as personal data submitted to the GDPR) whose leak could be disastrous for the image of the company and would expose it to high fines.

The protection mechanisms that are put in place must be in relation to the sensitivity of the data. As a result, organizations need to set up an effective classification system to ensure that the most critical data is properly protected and accessible only to authorized users.

To this end, it is necessary to:

- Allowing users to label data based on its sensitivity
- Applying encryption at rest and in transit
- Setting rules and conditions to automatically apply labeling and encryption



**Note** The classification model for government entities generally comprises 3 levels: top secret, secret and confidential. The data are either classified according to one of these levels or unclassified.

For commercial enterprises, the recommendation of Microsoft is to rely on a more appropriate classification based on the damage in case of disclosure for the first three categories Highly Confidential, Confidential and General, then 2 other labels of Public and Non-Business. For more information, see article [CONCEPTS RELATED TO CLASSIFICATION LABELS](#)<sup>130</sup>.

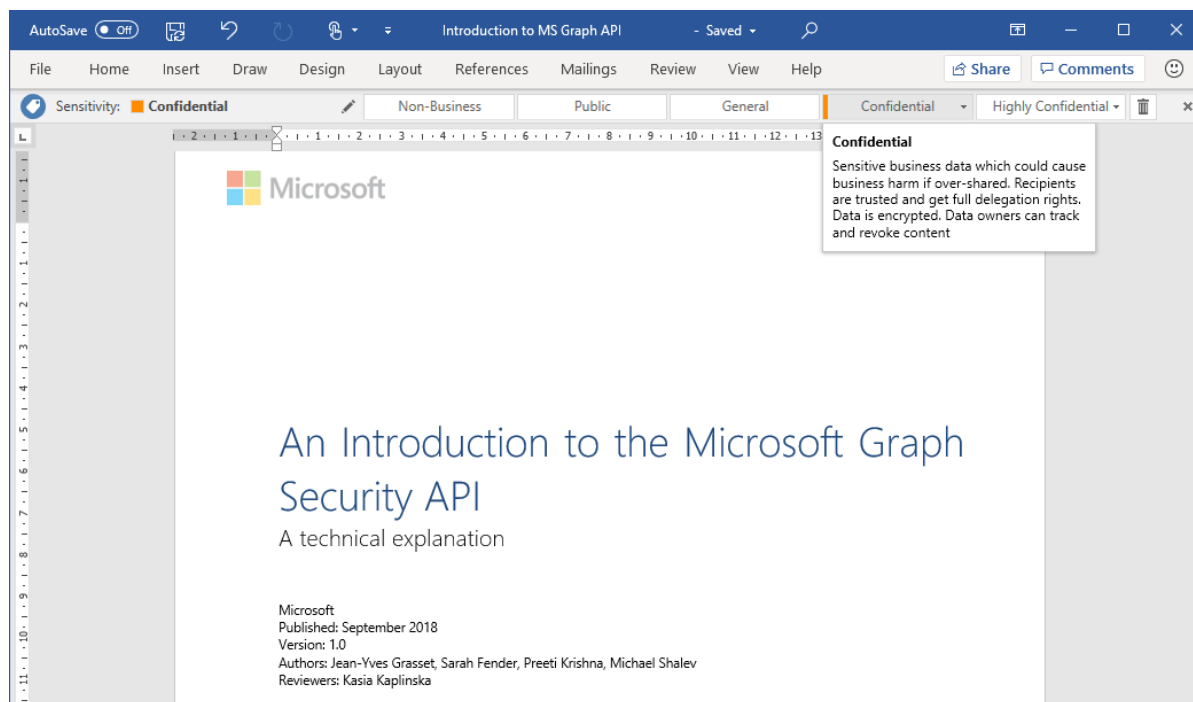
## Allowing users to label data based on its sensitivity

Users are the main information producers and, as a result, they are best able to assess the sensitivity of the data they create and manipulate. The pre-requisite is that they should have been made aware of the criticality of information protection and trained to use simple tools that the organization makes available for them to classify documents by assigning them labels.

---

<sup>129</sup> Five Steps To A Zero Trust Network, Road Map: The Security Architecture And Operations Playbook: <https://www.forrester.com/report/Five+Steps+To+A+Zero+Trust+Network/-/E-RES120510>

<sup>130</sup> CONCEPTS RELATED TO CLASSIFICATION LABELS: <https://docs.microsoft.com/en-us/information-protection/develop/concept-classification-labels>



As an example, the above screenshot shows the Word interface available for the users to classify the document they edit. The classification banner indicates that the document is classified Confidential and offers the user the option to change the level of sensitivity through a series of buttons. An explanation is available for each button to guide and inform the users on the selected level.

The [Microsoft Information Protection](https://www.microsoft.com/en-us/security/technology/information-protection)<sup>131</sup> (MIP) platform provides, among other services and functionalities, a unified labelling system between [Azure Information Protection](https://docs.microsoft.com/en-us/Azure/information-protection/what-is-information-protection)<sup>132</sup> and Office 365 to manage all labels from a single portal in the security and compliance Center.<sup>133</sup> This means that the labels that allow to classify and protect the sensitive data, as well as to manage the retention associated with the life cycle of data (for example, data retention and expiration) can be created from a single location.

Labels are defined according to your own classification policy and will appear to users in the applications that are used to manipulate the information. The programs from the Office Suite (Word, Excel, PowerPoint, Outlook) allow, on Windows systems<sup>134</sup>, to classify documents and emails from their interface. Users can also access document classification on the MacOS X (Word, PowerPoint, Excel) platforms, and on mobile Office applications for iOS and Android (in public pre-release at the time of publication)<sup>135</sup>.

On Windows, File Explorer also offers a right-click option to classify selected files.

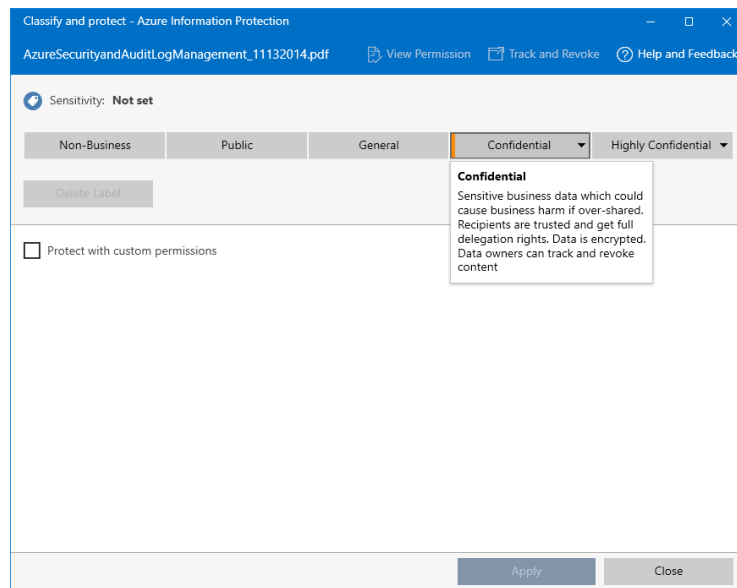
<sup>131</sup> Microsoft Information Protection: <https://www.microsoft.com/en-us/security/technology/information-protection>

<sup>132</sup> WHAT IS AZURE INFORMATION PROTECTION? : <https://docs.microsoft.com/en-us/Azure/information-protection/what-is-information-protection>

<sup>133</sup> ANNOUNCING AVAILABILITY OF INFORMATION PROTECTION CAPABILITIES TO HELP PROTECT YOUR SENSITIVE DATA: <https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Announcing-availability-of-information-protection-capabilities/ba-p/261967>

<sup>134</sup> USER GUIDE: CLASSIFY AND PROTECT A FILE OR EMAIL WITH AZURE INFORMATION PROTECTION: <https://docs.microsoft.com/en-us/Azure/information-protection/rms-client/client-classify-protect>

<sup>135</sup> LABELING EXPERIENCES BUILT NATIVELY INTO OFFICE APPS: <https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Announcing-availability-of-information-protection-capabilities/ba-p/261967>



More recently, the support of the classification – with the possibility of associated encryption – is available with Adobe Acrobat Reader for Windows<sup>136</sup>.



After applying a classification label, the user can open the PDF document from Acrobat Reader even if it is protected by encryption, as long as the user has authenticated and has sufficient rights. The information banner displays the label corresponding to the classification level and the details about the permissions are available by displaying the security settings of the file.

<sup>136</sup> USING AZURE INFORMATION PROTECTION TO PROTECT PDF'S AND ADOBE ACROBAT READER TO VIEW THEM:  
<https://techcommunity.microsoft.com/t5/Azure-Information-Protection/Using-Azure-Information-Protection-to-protect-PDF-s-and-Adobe/ba-p/282010>

**Note** For more information on the implementation and the use of the classification, see article [OVERVIEW OF PRIVACY LABELS](#)<sup>137</sup>, as well as blog posts [ANNOUNCING AVAILABILITY OF INFORMATION PROTECTION CAPABILITIES TO HELP PROTECT YOUR SENSITIVE DATA](#)<sup>138</sup> and [ANNOUNCING THE AVAILABILITY OF UNIFIED LABELING MANAGEMENT IN THE SECURITY & COMPLIANCE CENTER](#)<sup>139</sup>.

## Applying encryption at rest and in transit

Encryption is the means of protecting the confidentiality of data, whether stored on a mobile device, transiting through a communication channel or residing in the application itself, inside the data center.

In the case of on-premises applications, the encryption at rest allows handling the risk of access by an internal rogue administrator or, for an application in the cloud, usually a matter to address regulatory requirements.

All Office Services/Microsoft 365<sup>140</sup> services natively offer encryption at rest with the ability to use your own encryption keys (Customer Managed Key or CMK) with the ability to generate them in your local Hardware Security Module (HSM) and import them securely via the BYOK (Bring-Your-Own-Key) feature.

The Azure<sup>141</sup> storage services (blob, queue, table or file storage) systematically encrypt the data at rest, transparently for the application or developer. High-level services such as Azure SQL database, Azure Cosmos DB and Azure Data Lake also protect the data they host with encryption, and provide the option to use your own encryption keys (CMK) and support for BYOK.

**Note** For more information about how to implement BYOK with the services mentioned above, see [whitepaper BRING YOUR OWN KEY \(BYOK\) WITH AZURE KEY VAULT FOR OFFICE 365 AND AZURE](#)<sup>142</sup>.

In a “Zero Trust” context, where end-to-end protection is the rule, the data protection on mobile devices is crucial as these are the most exposed and most likely to be the stolen. To ensure that, in the event of a theft, sensitive data cannot be disclosed, devices storage spaces must be encrypted. In the case of Windows 10, [BitLocker](#)<sup>143</sup> natively provides encryption of the device's storage media. [Windows Information Protection](#)<sup>144</sup> (WIP) provides additional protection for organizational data by encrypting them at the file level, to limit the possibility of information leakage without interfering with the user experience.

---

<sup>137</sup> OVERVIEW OF PRIVACY LABELS: <https://docs.microsoft.com/en-us/Office365/SecurityCompliance/sensitivity-labels>

<sup>138</sup> ANNOUNCING AVAILABILITY OF INFORMATION PROTECTION CAPABILITIES TO HELP PROTECT YOUR SENSITIVE DATA: <https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Announcing-availability-of-information-protection-capabilities/ba-p/261967>

<sup>139</sup> ANNOUNCING THE AVAILABILITY OF UNIFIED LABELING MANAGEMENT IN THE SECURITY & COMPLIANCE CENTER: <https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Announcing-the-availability-of-unified-labeling-management-in/ba-p/262492>

<sup>140</sup> ENCRYPTING IN OFFICE 365: <https://docs.microsoft.com/en-us/office365/securitycompliance/encryption>

<sup>141</sup> AZURE ENCRYPTION OVERVIEW: <https://docs.microsoft.com/en-us/Azure/security/security-Azure-encryption-overview>

<sup>142</sup> BRING YOUR OWN KEY (BYOK) WITH AZURE KEY VAULT FOR OFFICE 365 AND AZURE: <http://download.microsoft.com/download/F/6/3/F63C9623-053F-44DD-BFA8-C11FA9EA4B61/Bring-Your-Own-Key-with-Azure-Key-Vault-for-Office-365-and-Azure.docx>

<sup>143</sup> BITLOCKER: <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>

<sup>144</sup> USE WINDOWS INFORMATION PROTECTION (WIP) TO HELP MAKE ACCIDENTAL DATA LEAKAGE A THING OF THE PAST: <https://www.microsoft.com/security/blog/2018/05/15/use-windows-information-protection-wip-to-help-make-accidental-data-leakage-a-thing-of-the-past/>

More recently, it was announced that WIP is now able to take in account file classification, to automatically apply encryption to files labeled as sensitive, in addition to first level encryption provided by BitLocker<sup>145</sup>.

Azure Information Protection manages classification through labeling and can, if necessary, leverage [Azure Rights Management](#)<sup>146</sup> (Azure RMS) to encrypt documents or mails classified as critical by the company defined policies. This service applies its protection by encrypting the content and applying identity-related access rights. In the case of a file, even if it is copied to non-secure storage or leaked outside the company, it incorporates its protection and will be accessible only by authorized persons.

Data protection during transfer addresses the risk of eavesdropping by ensuring confidentiality. Access to Office services/Microsoft 365 (for emails with Exchange online, documents stored in SharePoint Online or OneDrive for Business) relies on TLS 1.2 for all exchanges. In addition, all e-mail messages sent to other Office 365 customers transit via encrypted connections using the TLS Protocol and secured using Perfect Forward Secrecy (PFS)<sup>147</sup>.

For Azure, client access to Azure services is also protected by the encryption associated with the TLS protocol. Administration access through RDP or SSH also benefit from encryption<sup>148</sup>.

## Setting rules and conditions to automatically apply labeling and encryption

Labelling can be performed directly by the user as seen previously in ALLOWING USERS TO LABEL DATA BASED ON ITS SENSITIVITY but also automatically according to rules or policies defined by the administrator.

With Office/Microsoft 365, the administrator will be able to select predefined detection rules for detecting sensitive data and/or data subject to regulatory. For example, it is possible to recognize through pre-existing functions or regular expressions, a driver's license number, a Passport or an identity card number<sup>149</sup>.

DLP (Data Leak Prevention) strategy models are available to serve as a starting point for the development of company policies. The policies define, after detection and classification, what type of action should be applied such as adding a watermark, a specific header or footer, or an encryption protection based on Azure RMS.

---

<sup>145</sup> ANNOUNCING AVAILABILITY OF INFORMATION PROTECTION CAPABILITIES TO HELP PROTECT YOUR SENSITIVE DATA: <https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Announcing-availability-of-information-protection-capabilities/ba-p/261967>

<sup>146</sup> WHAT IS AZURE RIGHTS MANAGEMENT?: <https://docs.microsoft.com/en-us/Azure/information-protection/what-is-Azure-rms>

<sup>147</sup> HOW TO USE TLS BY EXCHANGE ONLINE TO SECURE MAIL CONNECTIONS IN OFFICE 365: <https://docs.microsoft.com/en-us/office365/securitycompliance/exchange-online-uses-tls-to-secure-email-connections>

<sup>148</sup> DATA ENCRYPTION IN TRANSIT: <https://docs.microsoft.com/en-us/Azure/security/security-Azure-encryption-overview#encryption-of-data-in-transit>

<sup>149</sup> ITEMS SOUGHT BY SENSITIVE INFORMATION TYPES: <https://docs.microsoft.com/en-us/Office365/SecurityCompliance/what-the-sensitive-information-types-look-for>

# Stopping cyber-attacks

The first implementation of Zero Trust Networks (see section § FROM THEORY TO A FIRST PRACTICAL IMPLEMENTATION) or even the extended approach (see section § A SECOND "ITERATION") did not address detection and response that represent two major components of cyber-attacks.

As noted above, a modern security approach of “assume breach” (see section § END-TO-END SECURITY) involves setting up a detection system associated with the most automated response possibilities. To be effective, the detection should apply to all the elements involved, that is to say identities, devices, resources, as well as the systems providing services such as directories, authorization, etc.

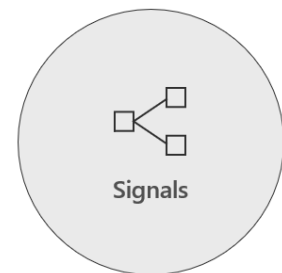
Moreover, in order to not be flooded with the alerts – while still being able to identify individual weak signals which, when correlated, could be indicators of an attack in progress –, it is imperative to be able to deal effectively with very large amounts of events, to minimize false positives, and to automatically process most of the alerts, so as to allow the SOC analyst to concentrate on investigating the most serious alerts.

Nowadays, detection solutions based on artificial intelligence algorithms and hosted in the cloud, can leverage virtually limitless processing and storage capabilities, to perform these tasks with an acuity beyond the ability of human resources, while drastically limiting the number of alerts to be processed manually.

Therefore, the ability to stop cyber-attacks resides in the ability to process an increasingly important set of signals and be able to react in real-time and, if possible, automatically to all threats, to stop or circumscribe them as quickly as possible.

It can be summarized in the following capabilities:

- Blocking or updating compromised identities;
- Properly enforcing multi-factor authentication to mitigate session risks;
- Denying access to infected devices;
- Revoking access to documents at risk;
- Automatically defending against emerging threats



## Blocking or updating compromised identities

It is crucial to be able to detect attacks on identities, to prevent them from being compromised and becoming a gateway to the service. This is even more crucial on privileged accounts that access sensitive information or are responsible for administering the service or the platform.

As noted earlier (see section § CONFIGURING CONDITIONAL ACCESS POLICIES IN AZURE AD), Azure AD Identity protection uses machine learning algorithms and adaptive heuristic templates to detect anomalies and suspicious incidents that reveal potentially compromised identities. This proactively prevents the misuse of compromised identities, detects potential vulnerabilities that would affect organization identities, configures automatic responses to detected suspicious actions, and investigate suspected incidents to take appropriate action to resolve them.

**Note** For more information about this functionality, see article [AZURE ACTIVE DIRECTORY IDENTITY PROTECTION OVERVIEW](#)<sup>150</sup>.

## Properly enforcing multi-factor authentication to mitigate session risks

As already mentioned, when a user authenticates, Azure AD Identity Protection analyzes the connection request and assigns it a level of risk (low, medium, or high) according to certain criteria. For example, if the connection is suspicious because it is an impossible trip, if the user logs in for the first time from an unusual location, if he uses an anonymous IP address through a Tor-type browser, etc., a medium or high risk level will be associated with the connection.

To enable automatic protection from a risky connection, the administrator can set up a conditional access policy in Azure AD that will impose a multi-factor authentication to the user (see section § USING MULTI-FACTOR AUTHENTICATION).

**Note** For more information about this functionality, see articles [HOW TO: CONFIGURE THE SIGN-IN RISK POLICY](#)<sup>151</sup> and [WHAT ARE AUTHENTICATION METHODS?](#)<sup>152</sup>.

## Denying access to infected devices

It is recommended that all devices be equipped with a Mobile Threat Defense (MTD) malware protection solution that can interface with MDM tools to trace device health status alerts and information.

Based on its analysis, the MTD solution returns a low, medium or high threat level, which Intune uses to indicate whether the device is compliant or not. This information can be considered by Azure AD conditional access policies to restrict or deny access to services or applications.

**Note** For more information, see section § SETTING UP THREAT DETECTION ON ENDPOINTS AND ANTI-MALWARE SOFTWARE ON ALL DEVICES.

## Revoking access to documents at risk

When a document has been protected by Azure information protection and shared by any means with different people, either by sending an email, making it available on a cloud sharing site, etc., the document owner can follow its use through the document tracking site<sup>153</sup>. The owner is able to see who accessed the document and from which location – as the access requires authentication – , and who attempted to access it but was not successfully authenticated. He is also able to revoke access to a document at any time, for example, for security reasons, if he believes that the identity of one of the authorized persons has been usurped.

It is possible to access the tracking portal from Office applications (as illustrated below with Word) or from the File Explorer.

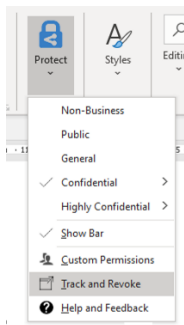
---

<sup>150</sup> WHAT IS AZURE ACTIVE DIRECTORY IDENTITY PROTECTION?: <https://docs.microsoft.com/en-us/Azure/active-directory/identity-protection/overview>

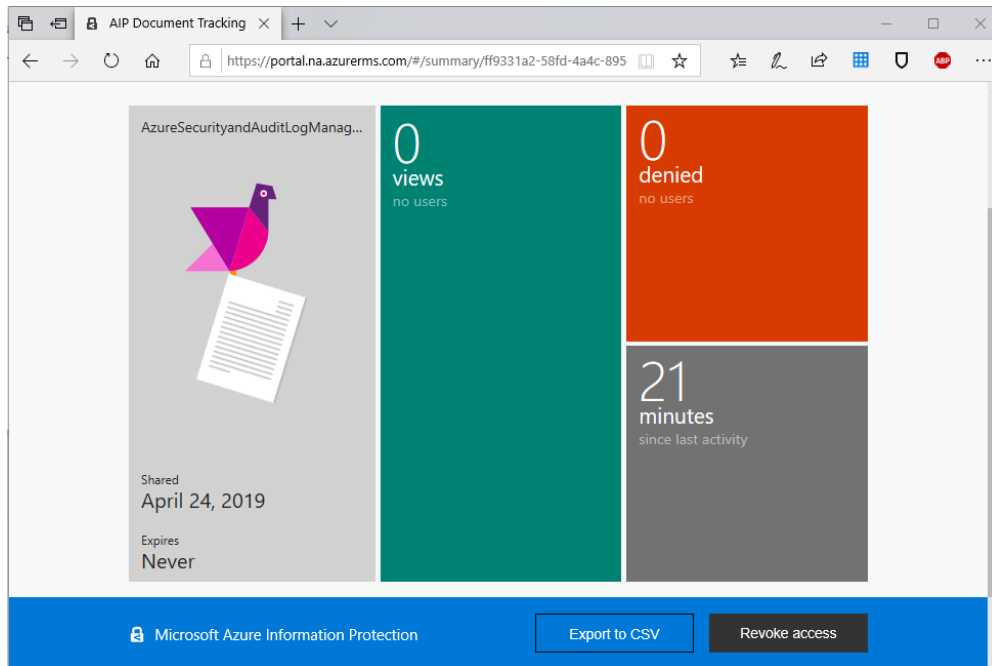
<sup>151</sup> HOW TO: CONFIGURE THE CONNECTION RISK POLICY: <https://docs.microsoft.com/en-us/Azure/active-directory/identity-protection/howto-sign-in-risk-policy>

<sup>152</sup> WHAT ARE AUTHENTICATION METHODS?: <https://docs.microsoft.com/en-us/Azure/active-directory/authentication/concept-authentication-methods>

<sup>153</sup> USER GUIDE: TRACK AND REVOKE YOUR DOCUMENTS WHEN YOU USE AZURE INFORMATION PROTECTION: <https://docs.microsoft.com/en-us/Azure/information-protection/rms-client/client-track-revoke>



Once on the portal, the user can revoke access with the **Revoke access** button.



## Automatically defending against emerging threats

Detection of threats involves analyzing abnormal flows and behaviors, whether on the internal network of the enterprise or in the cloud, at the level of the devices, users or servers.

Microsoft offers a portfolio of solutions that address different scopes and can be integrated with existing solutions : [Azure Advanced Threat Protection](https://docs.microsoft.com/en-us/Azure-advanced-threat-protection/what-is-atp)<sup>154</sup> is dedicated to internal network monitoring through the analysis of Active Directory domain controllers; [Microsoft Defender Advanced Threat Protection](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection)<sup>155</sup> relies on Windows 10 and MacOS X device behavior analysis; [Azure Security Center](https://docs.microsoft.com/en-us/Azure/security-center/)<sup>156</sup> strengthens workloads security posture and detects threats. Finally, [Azure Sentinel](https://docs.microsoft.com/en-us/Azure/sentinel/overview)<sup>157</sup> is a SIEM type solution that provides a global detection and response solution.

<sup>154</sup> WHAT IS AZURE ADVANCED THREAT PROTECTION?: <https://docs.microsoft.com/en-us/Azure-advanced-threat-protection/what-is-atp>

<sup>155</sup> Microsoft Defender Advanced Threat Protection: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection>

<sup>156</sup> Azure Security Center Documentation: <https://docs.microsoft.com/en-us/Azure/security-center/>

<sup>157</sup> WHAT IS THE PERVERSION OF AZURE SENTINEL?: <https://docs.microsoft.com/en-us/Azure/sentinel/overview>



Azure Advanced Threat protection monitors the internal network by collecting the traffic from and to Active Directory domain controllers as well as event logs to analyze and detect, among the volume of information, the suspicious behaviors that could be the key indicators of an attack. This service focuses on identity monitoring – the preferred attack vector– by establishing a baseline of the “normal” behavior inside the internal network, to then be able to more effectively identify suspicious activities in the general noise and finally raise relevant alerts.

Azure Advanced Threat Protection allows detecting internal attack attempts initiated by attackers, to identify compromised identities, to detect lateral movements based on Pass-The-Hash (PtH) or Pass-The-Ticket (PtT) attacks or highlight compromised domain controllers. Azure ATP helps to detect potential attempted attack as early as possible and allow the security teams to take action and prevent propagation.

Microsoft Defender Advanced Threat Protection falls into the category of threat detection and protection tools by analyzing events collected from Windows 10 devices and more recently from Mac OS X devices. When a threat matching a sequence of suspicious events is detected, an alert is created. If multiple alerts are correlated, they are grouped as an incident to facilitate the investigation work of the security analysts who are in charge of monitoring in the Security Operation Center or SOC.

Azure Security Center is a cloud-based security management solution that continuously monitors PaaS services in Azure as well as virtual machines and servers in Azure and on-premises. PaaS services are managed natively, Windows or Linux VMs requiring the installation of a monitoring agent (automatically performed by default for VMs in Azure). Configuration data and event logs are collected for analysis in a workspace that you own.

The result of the analysis of this data provides, through dashboards, a complete picture of the security posture of your environment, by providing the security status of all the resources. It highlights misconfigurations concerning predefined security policies or that you have adapted to your context and provides recommendations to be applied for remediation. Finally, the network mapping tool provides a view of the network topology of workloads.

In summary, Azure Security Center can both strengthen the security posture, protect itself by detecting threats while taking advantage of a cloud service that does not require infrastructure deployment and natively offering as much storage and compute resources as necessary.

Microsoft Azure Sentinel is a Security Information and Event Management (SIEM) and Security Orchestrated Automated Response (SOAR) solution based on the Azure cloud and designed to detect threats globally by collecting data from different sources of the company. Many connectors are available to collect logs from Microsoft services (Azure AD, Office 365, Azure Security Center, etc.), from third-party solutions (Cisco, Fortinet, Palo Alto, etc.), and from other clouds, or through the Syslog format<sup>158</sup>.

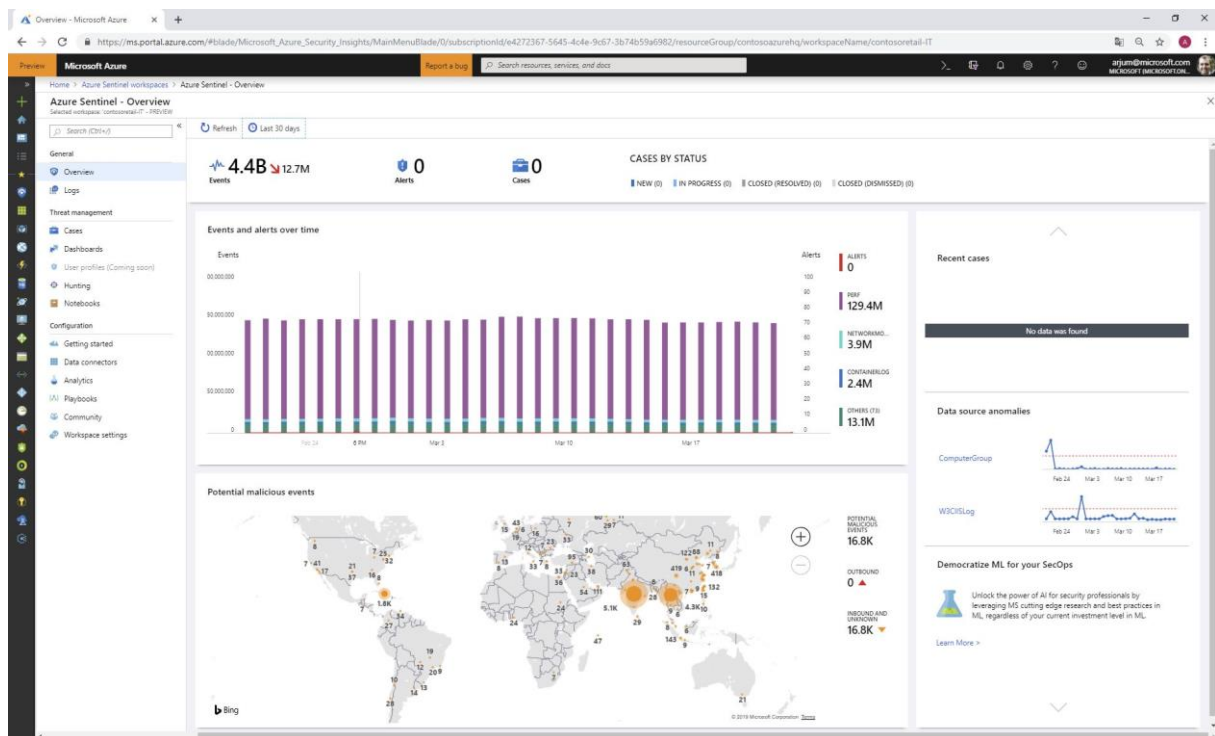
Azure Sentinel analyzes this data and, in case of suspicious items, generates aggregated alerts in the form of incidents that your analysts can detail thanks to investigation tools. It is possible to create your own detection rules (written in Kusto Query Language or KQL) tailored to your environment – many examples are available on GitHub. The analysis is based on predefined and pre-trained machine learning models that are applied to your own datasets. You even can use your own algorithms developed by your data scientists<sup>159</sup>.

---

<sup>158</sup> CONNECT DATA SOURCES: <https://docs.microsoft.com/en-us/Azure/sentinel/connect-data-sources>

<sup>159</sup> REDUCING SECURITY ALERT FATIGUE USING MACHINE LEARNING IN AZURE SENTINEL: <https://Azure.microsoft.com/en-gb/blog/reducing-security-alert-fatigue-using-machine-learning-in-Azure-sentinel/>

You can also import Threat Indicators or TI from external sources such as the open source MISP platform<sup>160</sup> or from your own internal sources. Finally, Automation and Orchestration Solutions are available in the form of “playbooks” to create, without coding, extremely fast responses to specific alerts scenarios without human intervention.



In the figure above, the Azure Sentinel dashboard shows the number of events collected and analyzed (4.4 billion) and their distribution in a graphical form. No alert has been raised even though many potential threats have been detected particularly from two areas in Asia, as depicted on the world map.

<sup>160</sup> MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing: <https://www.misp-project.org/>

# Conclusion

The principles discussed previously to build a Zero Trust approach follow 5 major steps to secure your identity infrastructure with Azure AD and thus provide the basics:

1. **Reinforce your credentials.** If the users of your identity system use weak passwords and do not reinforce them with multi-factor authentication (MFA), it is not a question of *whether* or *when* you are compromised, but rather *how often* you will be compromised.
2. **Reduce your attack surface.** To make life more difficult for attackers, eliminate the use of older, less secure protocols, limit access points, and exercise more meaningful control over administrative access to resources.
3. **Automate the response to threats.** Reduce costs and risks by reducing the time that attackers are inside your environment.
4. **Increase your level of awareness with auditing and monitoring of security alerts.** Use the auditing and logging of security-related events and associated alerts to help detect patterns that may indicate internal attacks or a successful external penetration of your network.
5. **Enable self-help for more complete and more predictable end-user security.** Reduce friction by allowing your users to stay productive while remaining vigilant.

5 steps to secure  
your identity  
infrastructure



[aka.ms/securitysteps](https://aka.ms/securitysteps)

# References

- **Reach the Zero Trust with conditional access in Azure AD:** <https://www.Microsoft.com/en-us/security/technology/identity-access-management/zero-trust>
- **Azure AD deployment plans:** <https://aka.ms/deploymentplans>
- **Security deployment banknote series :** <https://www.Microsoft.com/security/blog/security-deployment-3/>

Provides guidance on how you can successfully deploy and manage the adoption of Microsoft 365 security solutions in your organization.

Copyright © 2019 Microsoft. All rights reserved.

Microsoft France  
39 Quai du Président Roosevelt  
92130 Issy-les-Moulineaux

The total or partial reproduction of this work, as well as associated trademarks and logos, without written agreement of Microsoft France, is prohibited in accordance with the French and international laws in force in the field of intellectual property.

MICROSOFT DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO THE INFORMATION CONTAINED HEREIN.

Microsoft, Azure, Office 365, Microsoft 365, and other product and service names are or may be registered trademarks and/or trademarks in the United States and/or other countries.