The Microsoft Defender For Cloud

Written for KAMIND IT, Inc.

By Ravi Das

Contents

Introduction

In today's world, both individuals and businesses alike need as much protection as they can, in order to fend off the latest threat variants. There are many tools out there, but the one that has stayed around for probably the longest time is the antivirus software. There have been many vendors creating this kind of package, but one has stood out the most and is continued to be the most, especially when it comes to Cloud based deployments.

This is called Microsoft Defender, and is the focal point of this whitepaper.

A Brief History of Defender

Microsoft Defender first made its debut with the Windows XP Operating System (OS). It was initially designed to be a free download, and it eventually also shipped with the Windows 7 and Vista OSs. However, during these releases, Defender was not deemed to be a full antivirus package. It wasn't until the release of the Windows 8 OS that it became a complete package. During this launch, Defender completely replaced the Microsoft Security Essentials, the forerunner.

In March of 2019, Microsoft announced the release of Defender for the Mac OS environment. Although this was designed to protect the personal devices of the end user, Defender eventually made its splash onto the Android OS and the iOS, which included extra features, such as the following:

- Microsoft Smart Screen.
- A native Firewall.
- Sophisticated malware scanning.
- A special block corporate data stored on a smartphone if a rogue malicious app was installed.

Now, in Windows 10, Defender is centrally monitored and located in what is known as the "Windows Defender Security Center". Some of the latest features in this version include the following:

- Allows for regular scanning either on an automated or manual basis.
- "Block At First Sight": Artificial Intelligence (AI) and Machine Learning (ML) are both used to determine if a file from an email or any other source is malicious or not.
- Integration with Edge: This is the latest web browser version from Microsoft, can now scan any files first before they are downloaded by the end user to their local device.
- The "Application Guard": With this tool, any web browsing done by the end user can be contained in a sandbox environment in order to determine if a particular website is authentic or not. This was first only available for Edge, but it has now become available for both Google Chrome and Firefox.
- The "Controlled Access Folder": This is has been created to protect the files marked by the end user as "important" from a Ransomware attack. The catalyst for this new tool was the deployment of the Petya family of Ransomware threat vectors.

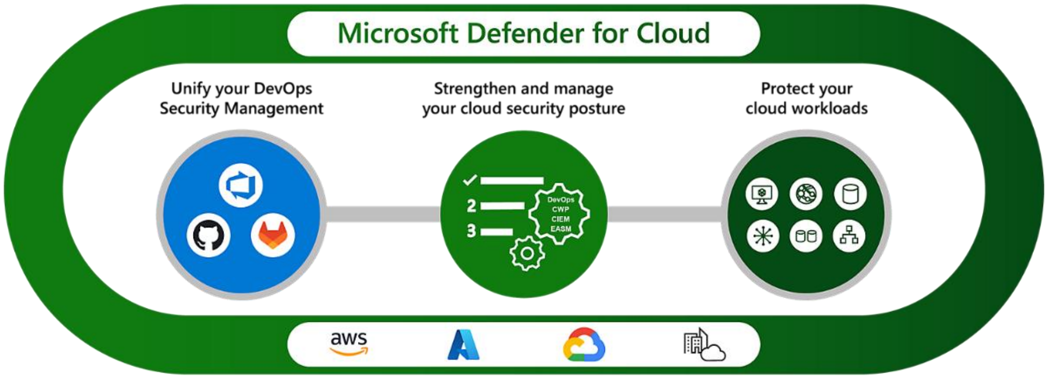
With the high adoption rate now happening for Microsoft Azure, there are now four flavors of Defender which are available, and are as follows:

- The Microsoft Defender XDR (this was formerly known as the "M365 Defender".
- The Microsoft Defender For Cloud.
- The Microsoft Defender For Business.
- The Microsoft Defender For Individuals.

For the remainder of this whitepaper, we now focus on the Microsoft Defender For Cloud.

The Overall Features of Microsoft Defender For Cloud

It is important to note at this point that Defender is technically known as the "Coud-Native Application Protection Platform, also known as "CNAPP". The overall structure of Defender For The Cloud can be seen below:


Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
2
3
DevOps
CWP
CIEM
EASM
aws

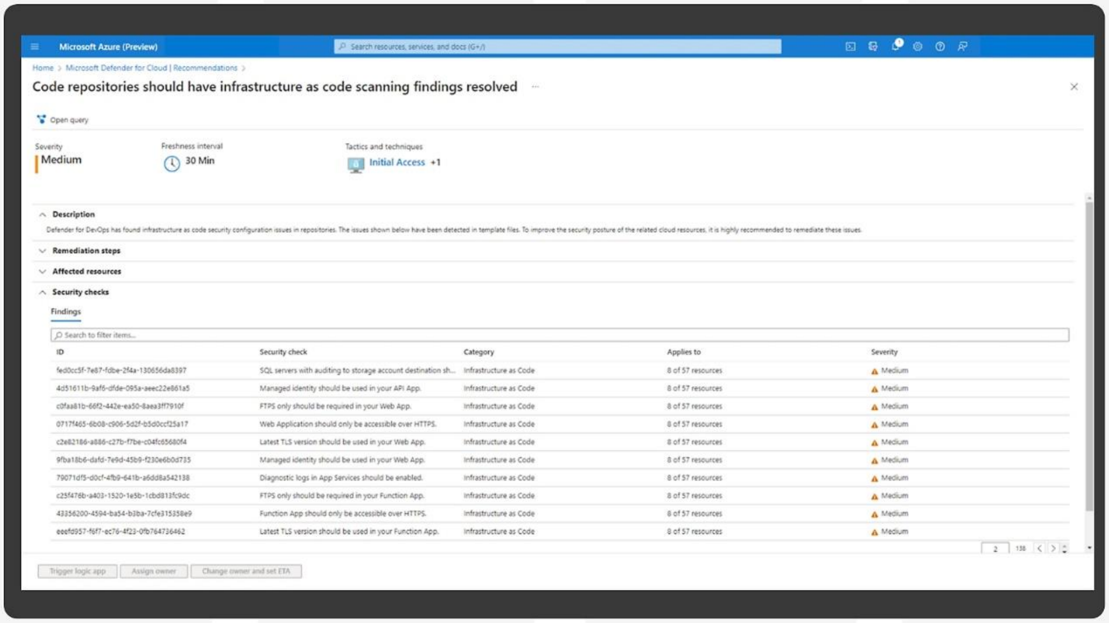
(SOURCE: 1).

The above illustration demonstrates the various scenarios Defender for Cloud can do:

- Unifying DevOps security management.
- Strengthening of the cloud security environment with contextual insights (powered by Generative AI).
- The protection of the different Cloud Workloads against all of the major threat variants.

The Defender for Cloud supports the other major Cloud Platforms, such as those of the AWS, the Google Cloud Platform (GCP), and Hybrid environments which require the use of On Premises workloads.

The major components of the Defender For Clous are illustrated below:


Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
Home > Microsoft Defender for Cloud | Recommendations >

Code repositories should have infrastructure as code scanning findings resolved

Severity: Medium

Freshness interval: 30 Min

Tactics and techniques: Initial Access +1

Description

Defender for DevOps has found infrastructure as code security configuration issues in repositories. The issues shown below have been detected in template files. To improve the security posture of the related cloud resources, it is highly recommended to remediate these issues.

ID	Security check	Category	Applies to	Severity
fed0cc5f-7e87-fdbe-2f4a-130656da8397	SQL servers with auditing to storage account destination sh...	Infrastructure as Code	8 of 57 resources	Medium
4d51611b-9af6-dfde-095a-aeec22e861a5	Managed identity should be used in your API App.	Infrastructure as Code	8 of 57 resources	Medium
c0faa81b-66f2-442e-ea50-8aea3ff7910f	FTPS only should be required in your Web App.	Infrastructure as Code	8 of 57 resources	Medium
0717f465-6b08-c906-5d2f-b5d0ccf25a17	Web Application should only be accessible over HTTPS.	Infrastructure as Code	8 of 57 resources	Medium
c2e82186-a886-c27b-f7be-c04fc65680f4	Latest TLS version should be used in your Web App.	Infrastructure as Code	8 of 57 resources	Medium
9fba18b6-dafd-7e9d-45b9-f230e6b0d735	Managed identity should be used in your Web App.	Infrastructure as Code	8 of 57 resources	Medium
79071df5-d0cf-4fb9-641b-a6dd8a542138	Diagnostic logs in App Services should be enabled.	Infrastructure as Code	8 of 57 resources	Medium
c25f476b-a403-1520-1e5b-1cbd813fc9dc	FTPS only should be required in your Function App.	Infrastructure as Code	8 of 57 resources	Medium
43356200-4594-ba54-b3ba-7cfe315358e9	Function App should only be accessible over HTTPS.	Infrastructure as Code	8 of 57 resources	Medium
eeefd957-f6f7-ec76-4f23-0fb764736462	Latest TLS version should be used in your Function App.	Infrastructure as Code	8 of 57 resources	Medium

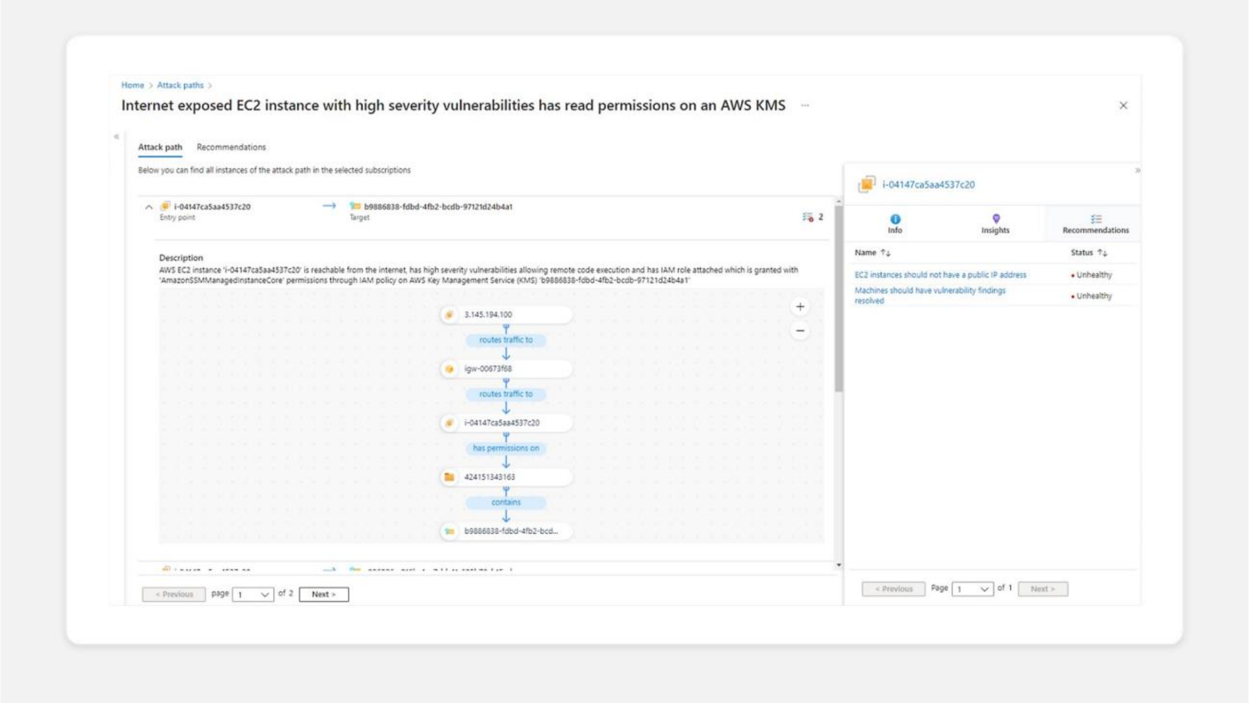
(SOURCE: 1).

These include the following:

- The Security Posture Monitoring
- The Regulatory Compliance
- The Cyberattack-Path Analysis
- The Workload Protection
- The Vulnerability Scanning
- The DevOps Posture Visibility
- The Infrastructure-as-Code Security
- The Code Security Guidance

These and other components will be examined in more detail in later sections in this whitepaper.

Another powerful functionality of the Defender For The Cloud is the ability for it to give you a holistic view of what exactly is happening in your Azure environment, from the standpoint of Cybersecurity. This is illustrated below as well:



Internet exposed EC2 instance with high severity vulnerabilities has read permissions on an AWS KMS

Below you can find all instances of the attack path in the selected subscriptions

Description

AWS EC2 instance 'i-04147ca5aa4537c20' is reachable from the internet, has high severity vulnerabilities allowing remote code execution and has IAM role attached which is granted with 'AmazonSSMManagedInstanceCore' permissions through IAM policy on AWS Key Management Service (KMS) 'b9886838-fdbd-4fb2-bcdb-97121d24b4a1'

Name ↑↓	Status ↑↓
EC2 instances should not have a public IP address	• Unhealthy
Machines should have vulnerability findings resolved	• Unhealthy

(SOURCE: 1).

The Cloud based functionalities that can be viewed with this are as follows:

- The Microsoft Entra Permissions Management
- The Azure Network Security
- The GitHub Advanced Security
- The Microsoft Defender External Attack Surface Management

The Defender For Cloud & DevSecOps

What Is DevSecOps

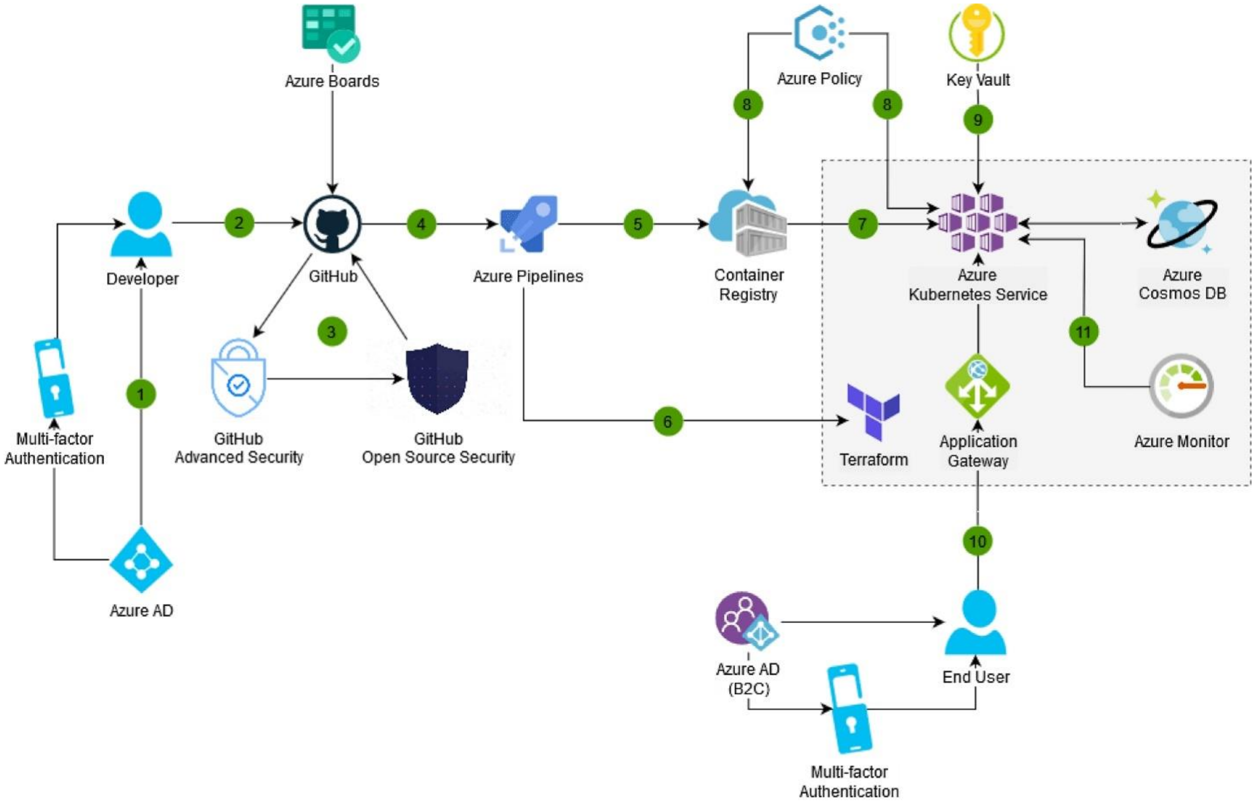
DevSecOps is an acronym that stands for Development, Security, and Operations. Source Code security has always been a problem, the basic premise here is to combine both teams from the IT Security and Operations team to offer a second look at the Source Code, to make sure that all gaps, weaknesses, and vulnerabilities have been fixed. In fact, DevSecOps, is also a major component of Microsoft Azure, and the Defender For The Cloud can even keep a close eye here, as well.

DevSecOps and GitHub

DevSecOps also works with GitHub, probably the most popular Source Code repository which is also owned by Microsoft. Here are some of the major benefits that your business can derive from this:

- The ability to "Shift-left" security: This is all about deploying security methodologies at the earliest stages of Source Code development, all the way from planning to packaging the final deliverable to the client.
- You can quickly adopt the Azure Infrastructure as Code (also known as “IaC”) with the Azure Resource Manager (also known as the “ARM”) or other templates to implement security protocols with the software development team. The Microsoft Defender for Cloud IaC template can also be used to mitigate cloud misconfigurations before they reach the production environment.
- Further strengthen the security of your Software Supply Chain.
- You can confirm vulnerable container images in your software development team’s CI/CD workflow with automatic scanning available from Defender For The Cloud.
- Defender For The Cloud can also monitor the Identity and Access Management policies that you have implemented for your software development team.
- It will give you visibility into the security posture of pre-production Source Code and other Resource Configurations.

The combination of DevSecOps and the Defender For The Cloud is illustrated below:



(SOURCE: 2).

The Defender For Cloud & Cloud Security Posture Management (CSPM)

Definition of CSPM

The CSPM is also yet another powerful tool that is built into Microsoft Azure, and it can be technically defined as follows:

"CSPM provides detailed visibility into the security state of your assets and workloads, and provides hardening guidance to help you efficiently and effectively improve your security posture."

(SOURCE: 3).

Functionalities Of The CSPM

With the Defender For The Cloud, there are two different kinds of service offerings, which are as follows:

1) The Foundational CSPM:

   The capabilities offered here are free, and are automatically enabled by default for subscriptions that start to use the Defender for Cloud.

2) The Defender Cloud Security Posture Management (CSPM):

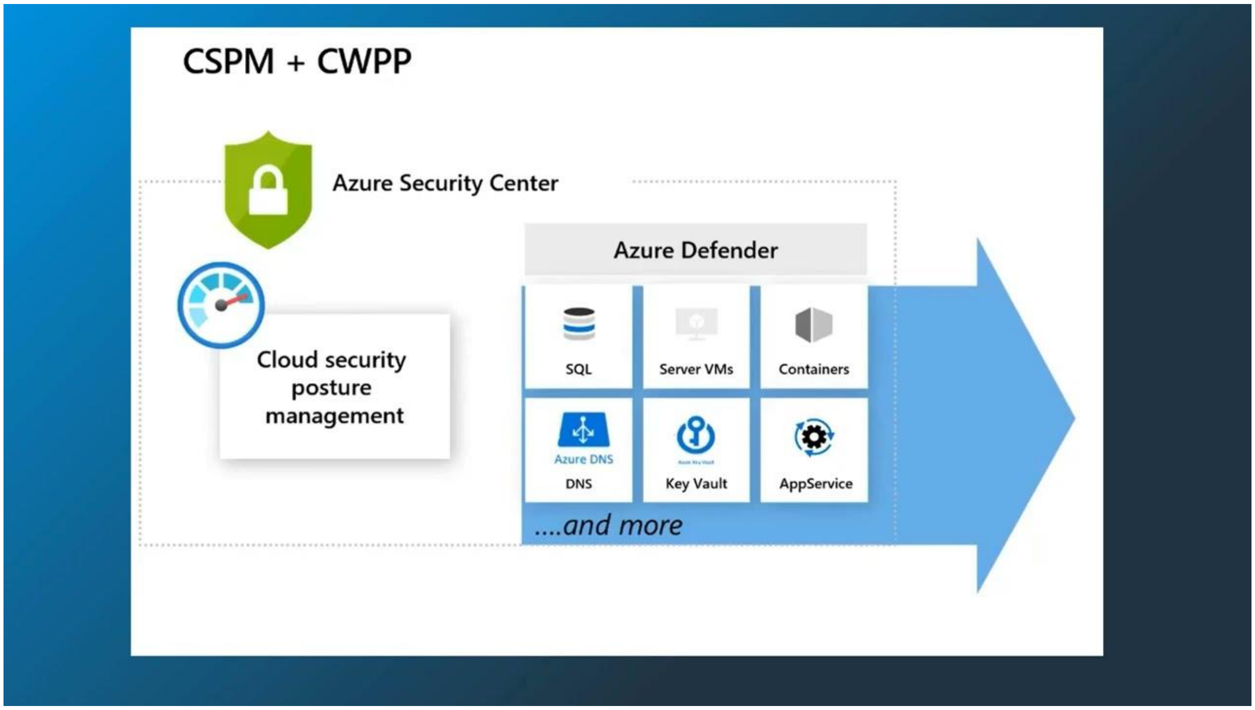
   This is a paid CSPM, and because of that, it offers additional, advanced security posture features.

The Defender for Cloud will assess and monitor against the Security Standards which have established the Azure subscription you have established for your business, and even AWS and the GCP. It will even provide recommendations based upon what it is seeing. It will even provide you with a secure score, and the higher the score is, the lower is your calculated risk level.

It is also important to note that Defender For The Cloud now has preconfigured integrations so that you can make use of third-party systems to do the following:

- Track and resolve support tickets
- Push recommendations to a member of your IT Security team so that they can be assigned responsibility for the remediation of a support ticket.

An example of the CSPM in conjunction with the Defender For The Cloud is below:



(SOURCE: 5).

The Defender For Cloud & Cloud Workload Protection Platform (CWPP)

Definition Of The CWPP

The CWPP can be technically defined as follows:

"A cloud workload protection platform is a comprehensive cybersecurity solution providing a series of protections across cloud environments in an organization connected to physical servers, serverless functions, virtual machines, and containers. Further, they continuously and automatically detect and address threats, vulnerabilities, and errors within any of the above infrastructures, supporting the workloads that interact with cloud environments."

(SOURCE: 4).

A Cloud Workload is any process, hardware, or software application that consumes both memory and power from the resources that it needs to use.

Functionalities Of The CWPP

Here are the functionalities of the CWWP, as it is used with the Defender For The Cloud:

1) <u>Memory Protection:</u>

The CWPPs can identify any gaps or abnormal behavior that appear in your Virtual Machines (VMs).

2) Allowlisting:

   This greatly mitigates the risk of Shadow IT Management from happening in our Azure Cloud Deployment. This is when your employees install unauthorized applications. With the CWPP, you enforce block mechanisms within your Cloud Deployment.

3) Intrusion Prevention:

   The CWPP will monitor your entire Network Infrastructure and alert your IT Security team for any abnormal behavior. If anything is detected, the CWPP will also act to mitigate any issues.

4) Endpoint Detection and Response (EDR):

   The CWPP will plays a critical role in monitoring devices connected to your endpoints in your IT and Network Infrastructure.

5) Antimalware Scanning:

   The CWPP can automatically scan for and detect malware in all of your Cloud workloads and eliminate malicious payloads before they enter your Azure Cloud .

6) Network Segmentation:

   With the this, the CWPP will allow for your IT Security team to deploy the Zero Trust Framework by segmenting or "subnetting" out your entire Network Infrastructure.

7) Immutability:

   The CWPP also supports Immutable Infrastructures. This is where the specific components of a software application are replaced rather than being upgraded over a period of time.

8) Integrity Protection:

   The CWPP is working constantly on a real time basis to make sure that all of the parts and components is running at the most optimal levels possible.

9) Vulnerability Management:

   The CWPP can also run Vulnerability Scans, based upon the time schedule and permutations that you have set forth.

Benefits Of The CWPP

The CWPP also brings in a number of strategic benefits which include:

1) Multi Cloud Protection:

   If you have multiple Azure Subscriptions, you can use just one CWPP to monitor all of them.

2) Scalability:

   The CWPP can adjust accordingly based upon increased Cloud Deployments and usage.

3) Increased Savings:

   By using the CWPP and the Defender For The Cloud in tandem with another, you will see a decrease in both CapEx and OpEx by using the additional security features that are available with both.

4) Compliance:

   The CWPP will also help your organization come into compliance quicker with the many data privacy laws that are quickly coming out.

The Defender For Cloud & Azure Pipelines

A key integration of the Defender For The Cloud is the Azure Pipelines. A technical definition of it is as follows:

"Azure Pipelines automatically builds and tests code projects. It supports all major languages and project types and combines continuous integration, continuous delivery, and continuous testing to build, test, and deliver your code to any destination."

(SOURCE: 6).

Each of the components is reviewed in the following subsections.

Continuous Integration

Also known as "CI", this allows for the software development team to detect and catch bugs early in the Software Development Lifecycle (also known as the "SDLC"), thus ensuring that all vulnerabilities, gaps, and weaknesses are remediated before final to delivery to the client. Also. automated tests are executed as part of the CI process to ensure Quality Assurance.

Continuous Delivery

Also known as "CD", this is a specific process by which Source Code is built, tested, and deployed to both testing and production environments. The end result of using two or more differing environments like this is that it greatly increases quality in the Source Code. Also, deployable software artifacts are also produced.

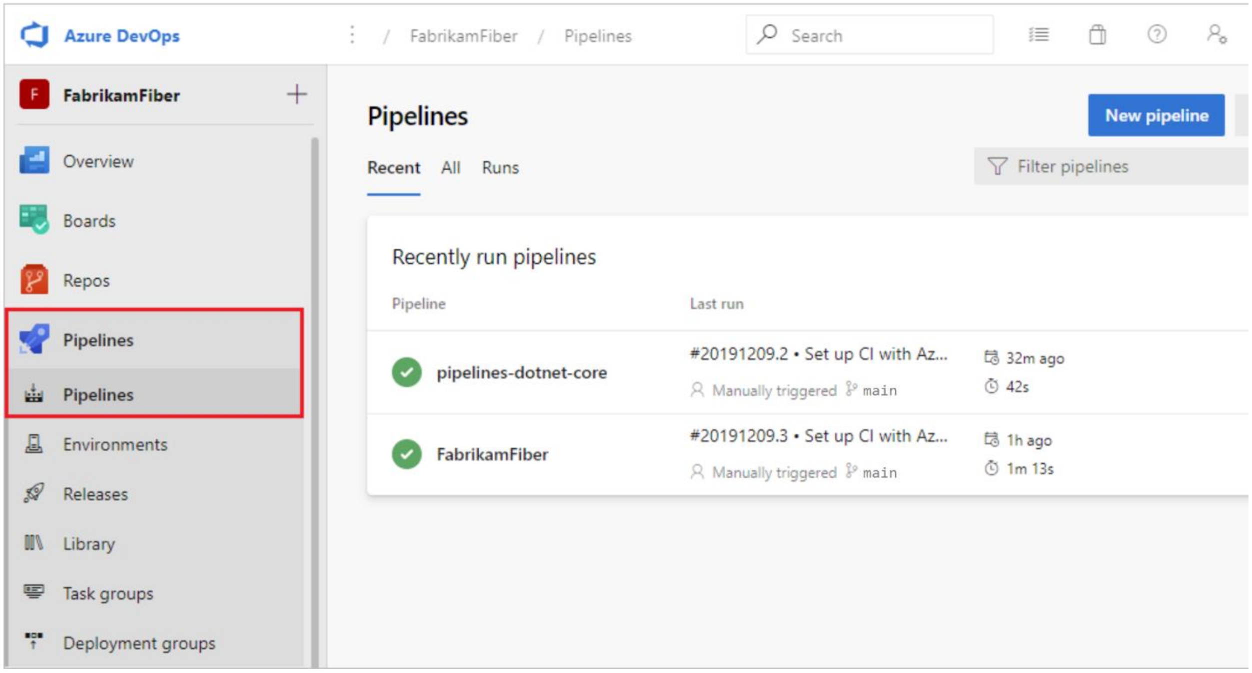
Continuous Testing

Also known as "CT", this allows you to test new releases of the Source Code in a fast, scalable, and efficient manner. It brings the following benefits:

- You can detect Source Code problems earlier in the SDLC by running tests automatically with each software build.
- You can use any kind of software testing framework that best needs the requirements of the client.
- You can also create detailed and customizable test results to effectively gauge the quality of the Source Code.

Integral to the Azure Pipeline is the "Code Pipeline Insights" that allows you to smoothly move your Source Code into any part fo your Azure Cloud Deployment, thus ensuring that any interaction between the two are as secure as possible.

An illustration of the Azure Pipelines is below:



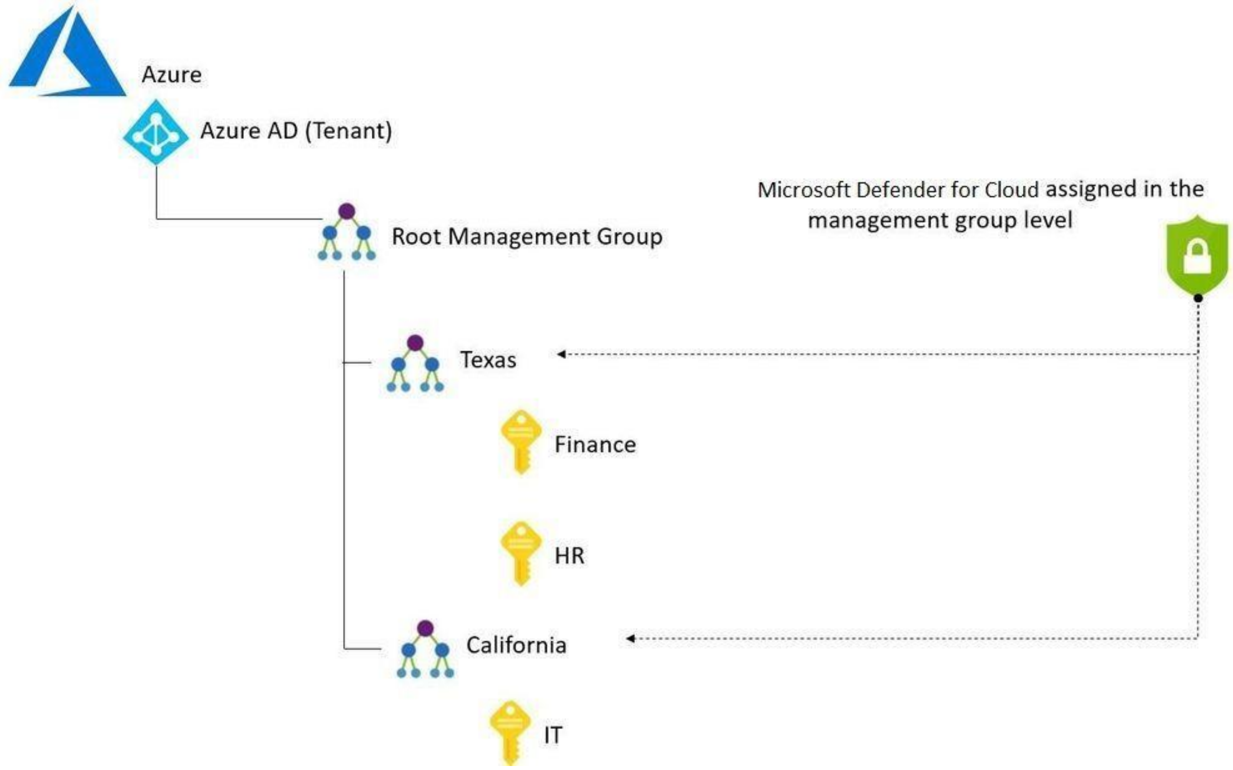
Recently run pipelines

Pipeline	Last run	
pipelines-dotnet-core	#20191209.2 • Set up CI with Az... Manually triggered main	32m ago 42s
FabrikamFiber	#20191209.3 • Set up CI with Az... Manually triggered main	1h ago 1m 13s

(SOURCE: 6).

The Defender For Cloud & Centralized Policy Management

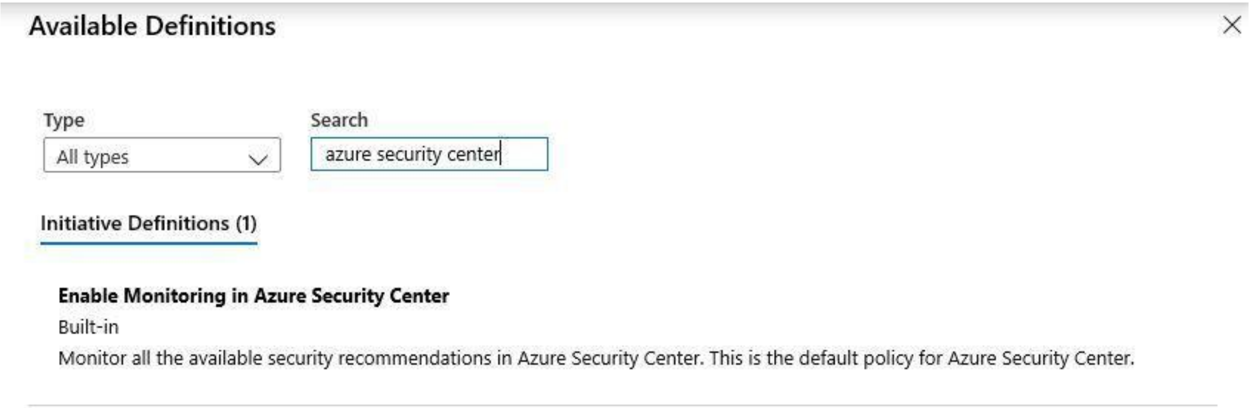
One of our previous blogs reviewed in detail the components of Centralized Policy Management. So at this point, let us review an example of how it can be used with the Defender For The Cloud. Large businesses (such as the Fortune 500) that have and make use of multiple subscriptions in just one tenant are more than likely using the Azure Management Groups to make more efficient use of their multiple subscriptions. In these cases, a hierarchy is deployed which shows the separate needs of the various remote offices, and their individual departments, such as Human Resources, Finance, Accounting, Marketing, IT, etc. All of the rights, privileges, and permissions for each of the same departments will be inherited, according to this hierarchical structure. This is illustrated in the diagram below:



(SOURCE: 7).

To help eliminate any security risks of duplicate and overlapping rights, privileges, and permissions, it would be highly recommended to make use of the Defender For The Cloud to replace the use of the Azure Management Groups in order to trickle the privileges in a top-down fashion, rather than an inherited one.

This process is seen below:



Available Definitions

Type: All types

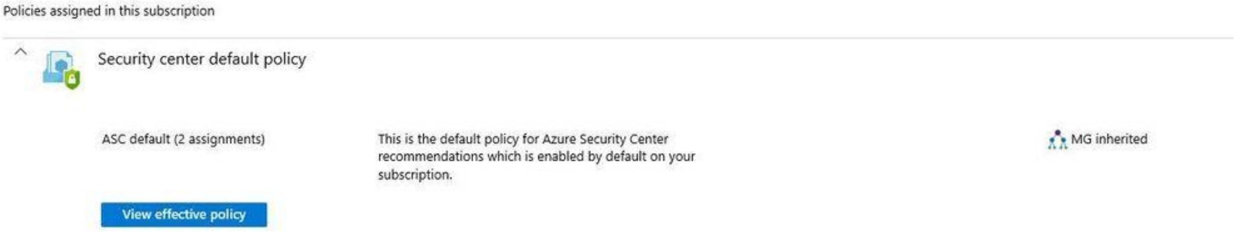
Search: azure security center

Initiative Definitions (1)

Enable Monitoring in Azure Security Center
Built-in
Monitor all the available security recommendations in Azure Security Center. This is the default policy for Azure Security Center.

(SOURCE: 7).

Once the above has been completed, the Defender For The Cloud will display the following screen:



Policies assigned in this subscription

Security center default policy

ASC default (2 assignments)

This is the default policy for Azure Security Center recommendations which is enabled by default on your subscription.

MG inherited

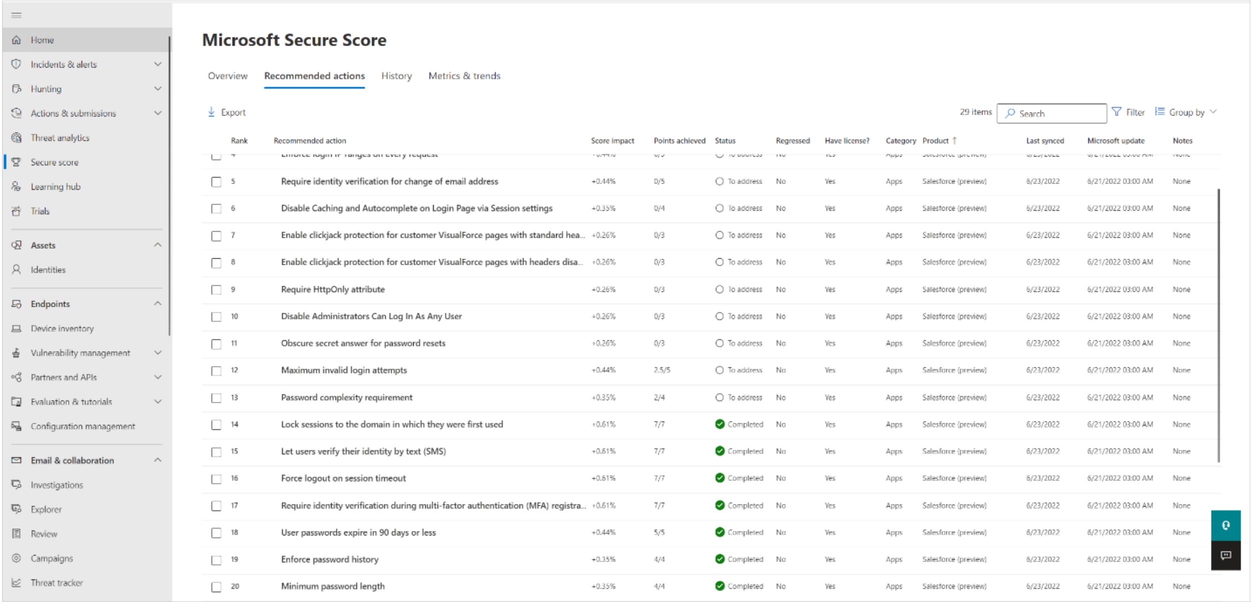
From the right-hand side of the above illustration, you can see now that the Defender For The Cloud has inherited everything from the Azure Management Groups, and now is control with respect to giving out the privileges to the other branch offices and their respective departments.

The Defender For Cloud & Security Posture Management

The Microsoft Security Score

No matter what Cloud Platform that you are using, there are always security risks that are involved, no matter how proactive that you and your IT Security team might be. As it was previously stated in this whitepaper, the Defender For The Cloud can provide an assessment of your entire IT and Network Infrastructure, and from there, provide recommendations as to how you can decrease your level of risk, among other things.

Btu equally important, it can also provide you with what is known as a “Microsoft Secure Score”, to not only quantify your risk level, but to also give a holistic view of the processes in your IT/Network Infrastructure that make up this category. An example of this is illustrated below:



Microsoft Secure Score

	Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product ↑	Last synced	Microsoft update	Notes
□	4	Enforce login IP ranges on every request	[illegible]	[illegible]	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	5	Require identity verification for change of email address	+0.44%	0/5	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	6	Disable Caching and Autocomplete on Login Page via Session settings	+0.35%	0/4	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	7	Enable clickjack protection for customer VisualForce pages with standard hea...	+0.26%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	8	Enable clickjack protection for customer VisualForce pages with headers disa...	+0.26%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	9	Require HttpOnly attribute	+0.26%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	10	Disable Administrators Can Log In As Any User	+0.26%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	11	Obscure secret answer for password resets	+0.26%	0/3	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	12	Maximum invalid login attempts	+0.44%	2.5/5	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	13	Password complexity requirement	+0.35%	2/4	○ To address	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	14	Lock sessions to the domain in which they were first used	+0.61%	7/7	✓ Completed	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	15	Let users verify their identity by text (SMS)	+0.61%	7/7	✓ Completed	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	16	Force logout on session timeout	+0.61%	7/7	✓ Completed	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	17	Require identity verification during multi-factor authentication (MFA) registra...	+0.61%	7/7	✓ Completed	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	18	User passwords expire in 90 days or less	+0.44%	5/5	✓ Completed	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	19	Enforce password history	+0.35%	4/4	✓ Completed	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None
□	20	Minimum password length	+0.35%	4/4	✓ Completed	No	Yes	Apps	Salesforce (preview)	6/23/2022	6/21/2022 03:00 AM	None

(SOURCE: 8).

For more information on the “Security Score”, click on the link below:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-security-recommendation?view=o365-worldwide

How To Enable The Security Posture Management Tool

To start using this powerful service, follow these steps below:

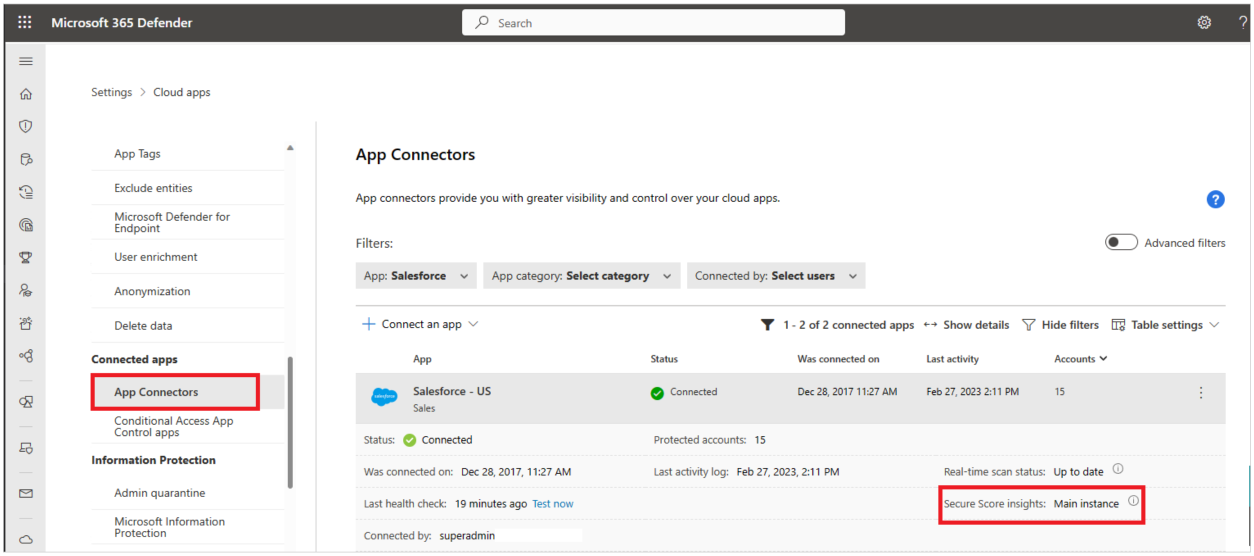
1) Connect to the SaaS based app that the Defender The Cloud to manage. For a listing of compatible apps, click on the link below:

   https://learn.microsoft.com/en-us/defender-cloud-apps/enable-instant-visibility-protection-and-governance-actions-for-your-apps

2) To initiate the Microsoft Security Score, log into your Azure or M365 account, and:

   - Select “Settings”
   - Select “Cloud Apps”
   - Select “App Connectors”
   - Then select “Secure Score insights: Main Instance”.

   This is illustrated in the diagram below:



App Connectors

App connectors provide you with greater visibility and control over your cloud apps.

Filters: Advanced filters

App: **Salesforce** | App category: **Select category** | Connected by: **Select users**

+ Connect an app | 1 - 2 of 2 connected apps | Show details | Hide filters | Table settings

App	Status	Was connected on	Last activity	Accounts
Salesforce - US Sales	Connected	Dec 28, 2017 11:27 AM	Feb 27, 2023 2:11 PM	15

Status: Connected | Protected accounts: 15

Was connected on: Dec 28, 2017, 11:27 AM | Last activity log: Feb 27, 2023, 2:11 PM | Real-time scan status: Up to date

Last health check: 19 minutes ago Test now | Secure Score insights: Main instance

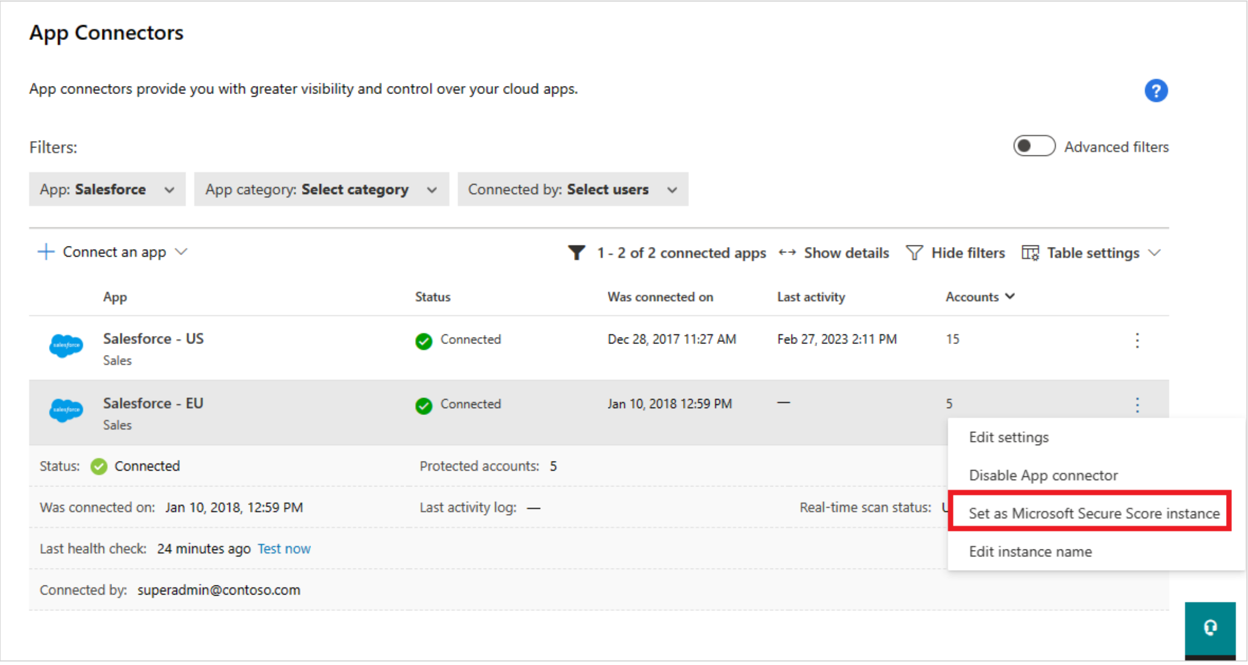
Connected by: superadmin

(SOURCE: 8).

3) If for some reason you cannot enable the Microsoft Security Score in the above step, then enable the three vertical dots that you see, and from there select the following:

“Microsoft Secure Score Instance”

This is also illustrated in the diagram below:



App Connectors

App connectors provide you with greater visibility and control over your cloud apps.

Filters: Advanced filters

App: **Salesforce** | App category: **Select category** | Connected by: **Select users**

+ Connect an app | 1 - 2 of 2 connected apps | Show details | Hide filters | Table settings

App	Status	Was connected on	Last activity	Accounts
Salesforce - US Sales	Connected	Dec 28, 2017 11:27 AM	Feb 27, 2023 2:11 PM	15
Salesforce - EU Sales	Connected	Jan 10, 2018 12:59 PM	—	5

Status: Connected | Protected accounts: 5

Was connected on: Jan 10, 2018, 12:59 PM | Last activity log: — | Real-time scan status: U

Last health check: 24 minutes ago Test now

Connected by: superadmin@contoso.com

(SOURCE: 8).

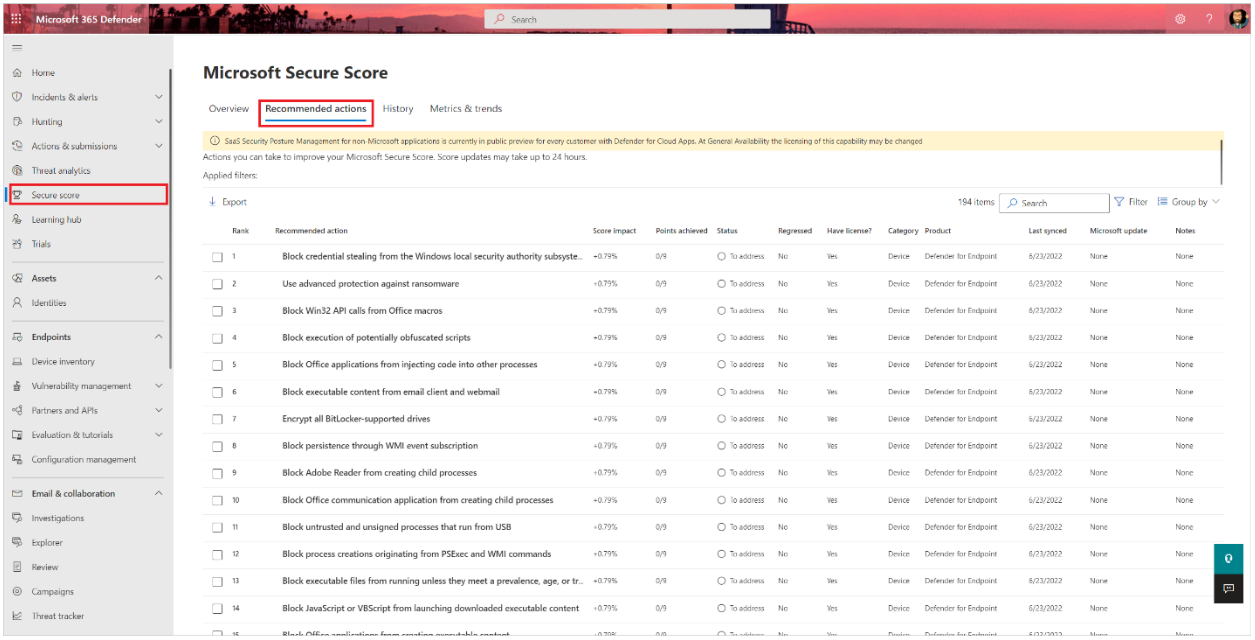
To See The Microsoft Security Score & Recommended Actions

Now that you have the service enabled, follow these steps to view your actual Security Score, and the actions that are needed to improve it:

1) Log into the Defender For The Cloud from either your Azure or M365 subscription:

   - Select "Secure Score"
   - Go the "Recommended Actions" Tab.

   This is illustrated below:



Microsoft Secure Score

SaaS Security Posture Management for non-Microsoft applications is currently in public preview for every customer with Defender for Cloud Apps. At General Availability the licensing of this capability may be changed

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

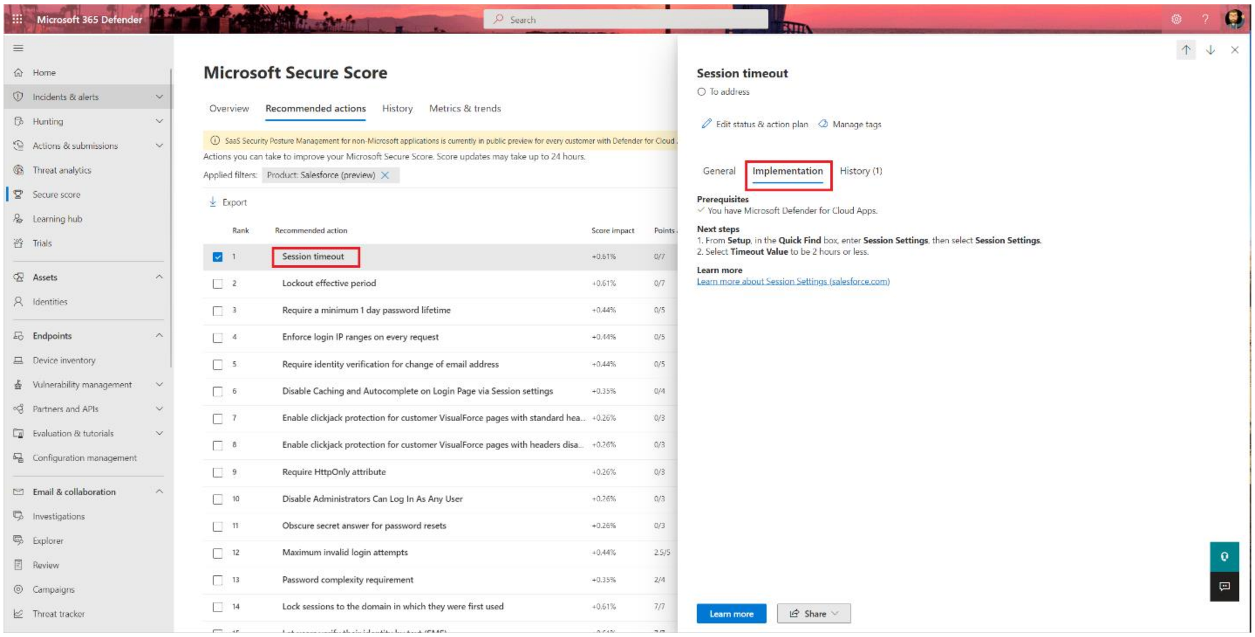
Applied filters:

	Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product	Last synced	Microsoft update	Notes
☐	1	Block credential stealing from the Windows local security authority subsyste...	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	2	Use advanced protection against ransomware	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	3	Block Win32 API calls from Office macros	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	4	Block execution of potentially obfuscated scripts	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	5	Block Office applications from injecting code into other processes	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	6	Block executable content from email client and webmail	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	7	Encrypt all BitLocker-supported drives	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	8	Block persistence through WMI event subscription	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	9	Block Adobe Reader from creating child processes	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	10	Block Office communication application from creating child processes	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	11	Block untrusted and unsigned processes that run from USB	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	12	Block process creations originating from PSExec and WMI commands	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	13	Block executable files from running unless they meet a prevalence, age, or tr...	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	14	Block JavaScript or VBScript from launching downloaded executable content	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None
☐	15	Block Office applications from creating executable content	+0.79%	0/9	○ To address	No	Yes	Device	Defender for Endpoint	6/23/2022	None	None

   (SOURCE: 8).

2) Select any product to see the controls that have been deployed with it.

3) To see the "Recommended Actions", go the "Implementation Tab". This is illustrated below:



Microsoft Secure Score

Overview | Recommended actions | History | Metrics & trends

SaaS Security Posture Management for non-Microsoft applications is currently in public preview for every customer with Defender for Cloud .

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Applied filters: Product: Salesforce (preview)

Export

	Rank	Recommended action	Score impact	Points .
☑	1	Session timeout	+0.61%	0/7
□	2	Lockout effective period	+0.61%	0/7
□	3	Require a minimum 1 day password lifetime	+0.44%	0/5
□	4	Enforce login IP ranges on every request	+0.44%	0/5
□	5	Require identity verification for change of email address	+0.44%	0/5
□	6	Disable Caching and Autocomplete on Login Page via Session settings	+0.35%	0/4
□	7	Enable clickjack protection for customer VisualForce pages with standard hea...	+0.26%	0/3
□	8	Enable clickjack protection for customer VisualForce pages with headers disa...	+0.26%	0/3
□	9	Require HttpOnly attribute	+0.26%	0/3
□	10	Disable Administrators Can Log In As Any User	+0.26%	0/3
□	11	Obscure secret answer for password resets	+0.26%	0/3
□	12	Maximum invalid login attempts	+0.44%	2.5/5
□	13	Password complexity requirement	+0.35%	2/4
□	14	Lock sessions to the domain in which they were first used	+0.61%	7/7

Session timeout

○ To address

Edit status & action plan | Manage tags

General | Implementation | History (1)

Prerequisites

✓ You have Microsoft Defender for Cloud Apps.

Next steps

1. From **Setup**, in the **Quick Find** box, enter **Session Settings**, then select **Session Settings**.
2. Select **Timeout Value** to be 2 hours or less.

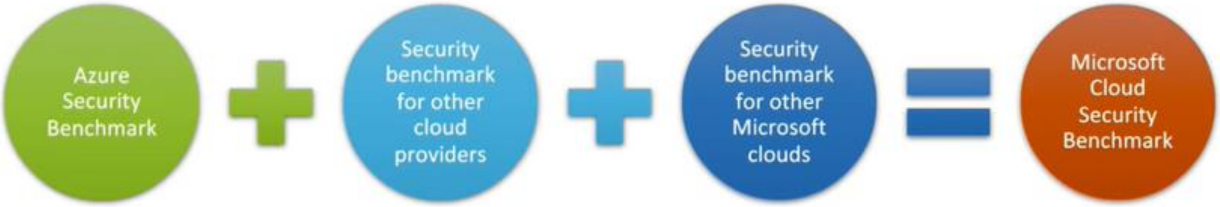
Learn more

Learn more about Session Settings (salesforce.com)

(SOURCE: 8).

The Defender For Cloud & Regulatory Compliance

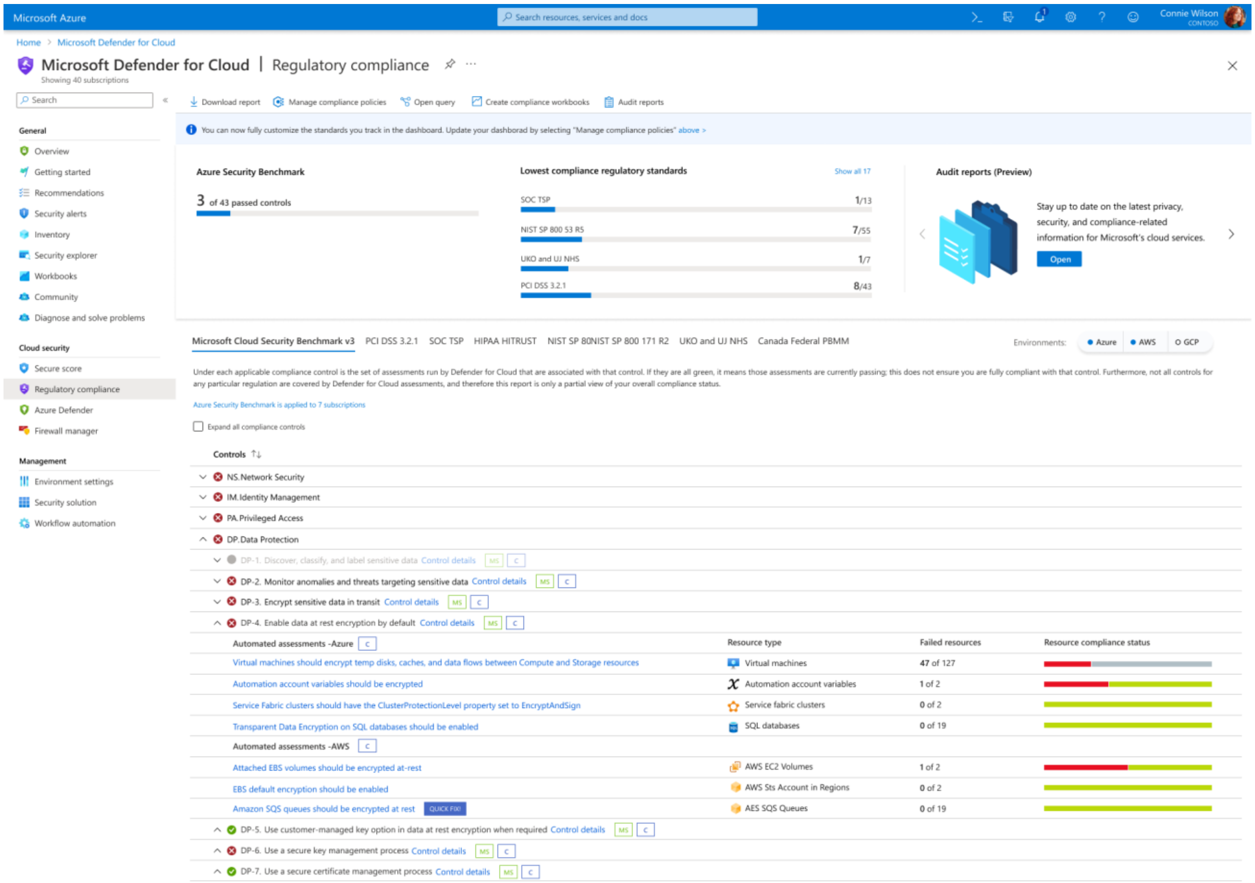
As mentioned earlier in the whitepaper, the Defender For The Cloud can also allow your business to come into compliance with the major data privacy and compliance laws, most notably those of the GDPR, the CCPA, and HIPAA, among others. At the heart of this is what is known as the "Azure Security Benchmark", and this is illustrated below:


Azure Security Benchmark
+
Security benchmark for other cloud providers
+
Security benchmark for other Microsoft clouds
=
Microsoft Cloud Security Benchmark

(SOURCE: 9).

The Compliance Dashboard

It is important to note at this point that from the Defender For The Cloud, you and your IT Security team can access what is known as the "Compliance Dashboard", which gives you a centralized view of how your business stands with regards to these laws and regulations. This is also illustrated below:



You can now fully customize the standards you track in the dashboard. Update your dashborad by selecting "Manage compliance policies" above >

Stay up to date on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to 7 subscriptions

□ Expand all compliance controls

- NS.Network Security
- IM.Identity Management
- PA.Privileged Access
- DP.Data Protection
  - DP-1. Discover, classify, and label sensitive data Control details MS C
  - DP-2. Monitor anomalies and threats targeting sensitive data Control details MS C
  - DP-3. Encrypt sensitive data in transit Control details MS C
  - DP-4. Enable data at rest encryption by default Control details MS C

Automated assessments -Azure C	Resource type	Failed resources	Resource compliance status
Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources	Virtual machines	47 of 127	
Automation account variables should be encrypted	Automation account variables	1 of 2	
Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign	Service fabric clusters	0 of 2	
Transparent Data Encryption on SQL databases should be enabled	SQL databases	0 of 19	
Automated assessments -AWS C			
Attached EBS volumes should be encrypted at-rest	AWS EC2 Volumes	1 of 2	
EBS default encryption should be enabled	AWS Sts Account in Regions	0 of 2	
Amazon SQS queues should be encrypted at rest QUICK FIX!	AES SQS Queues	0 of 19	

  - DP-5. Use customer-managed key option in data at rest encryption when required Control details MS C
  - DP-6. Use a secure key management process Control details MS C
  - DP-7. Use a secure certificate management process Control details MS C

(SOURCE: 9).

Setting Up The Compliance Manager

Before you can start using the Defender For The Cloud to see where you stand in terms of compliance, you first need to configure according to your security requirements and the laws/regulations that you need to follow. To do this, follow these steps:

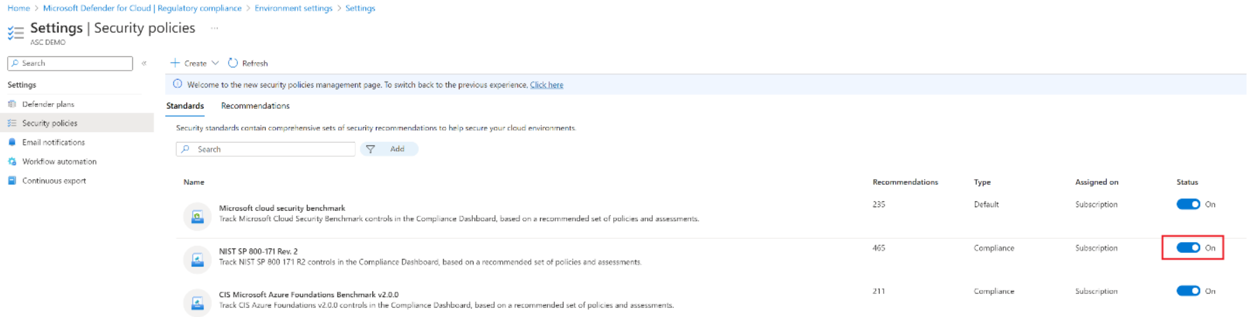
1) From the Defender for Cloud portal, select "Regulatory Compliance". From the top of the page, select Manage compliance policies.

2) Select the subscription(s) to which the particular security standard should be applied to.

3) Select "Security Policies".

4) For the laws/regulations you want to enable, from the "Status Column", position the toggle button to "On".

If any information is needed for this enablement process, the "Set Parameters" page appears in order for you to enter in the needed information. This is illustrated in the diagram below:



Home > Microsoft Defender for Cloud | Regulatory compliance > Environment settings > Settings

Settings | Security policies

ASC DEMO

Welcome to the new security policies management page. To switch back to the previous experience, Click here

Security standards contain comprehensive sets of security recommendations to help secure your cloud environments.

Name	Recommendations	Type	Assigned on	Status
Microsoft cloud security benchmark Track Microsoft Cloud Security Benchmark controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	235	Default	Subscription	On
NIST SP 800-171 Rev. 2 Track NIST SP 800 171 R2 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	465	Compliance	Subscription	On
CIS Microsoft Azure Foundations Benchmark v2.0.0 Track CIS Azure Foundations v2.0.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	211	Compliance	Subscription	On

(SOURCE: 9).

5) Now select "Regulatory Compliance" again to take you back to the Compliance Dashboard.

6) You should now be able to see the enabled laws and regulations that are associated with each subscription.

NOTE; These are the steps for Azure only. If you want to enable this for the AWS or GCP, click on this link:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

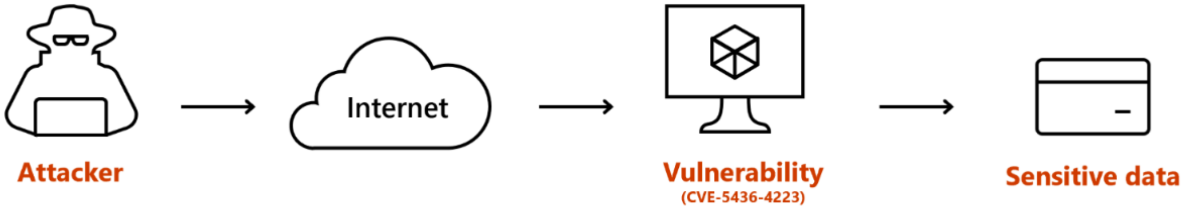
The Defender For Cloud & Attack Path Analysis

Apart from remediating threat vectors and providing compliance/regulation recommendations, the Defender For The Cloud is also quite efficient in mapping out a threat variant in its evolution and growth stages. This is known as "Attack Patch Analysis", and it is technically defined as follows:

"Attack path analysis are scans that expose exploitable paths that attackers might use to breach your environment to reach your high-impact assets. Attack path analysis exposes attack paths and suggests recommendations as to how best remediate issues that will break the attack path and prevent successful breach."

(SOURCE: 11).

This is illustrated in the diagram below:



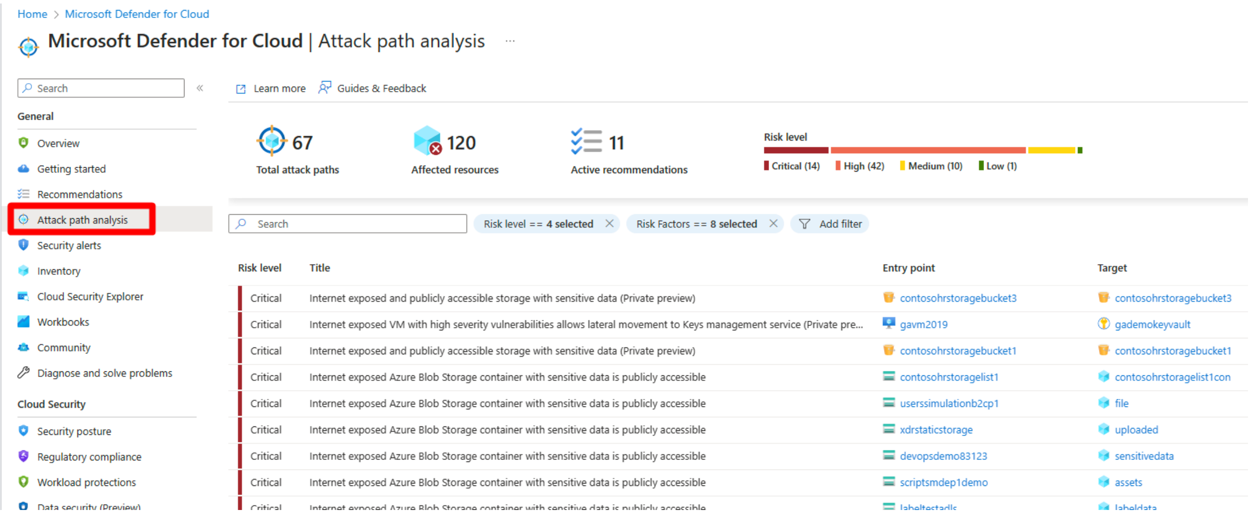
(SOURCE: 11).

Initiating The Attack Path Analysis

To start using this, follow these steps:

1) Login into your Azure Portal.

2) Go to “Microsoft Defender For Cloud”, and select “Attack Path Analysis.” This is illustrated below:



67 Total attack paths

120 Affected resources

11 Active recommendations

Risk level: Critical (14) High (42) Medium (10) Low (1)

Risk level == 4 selected

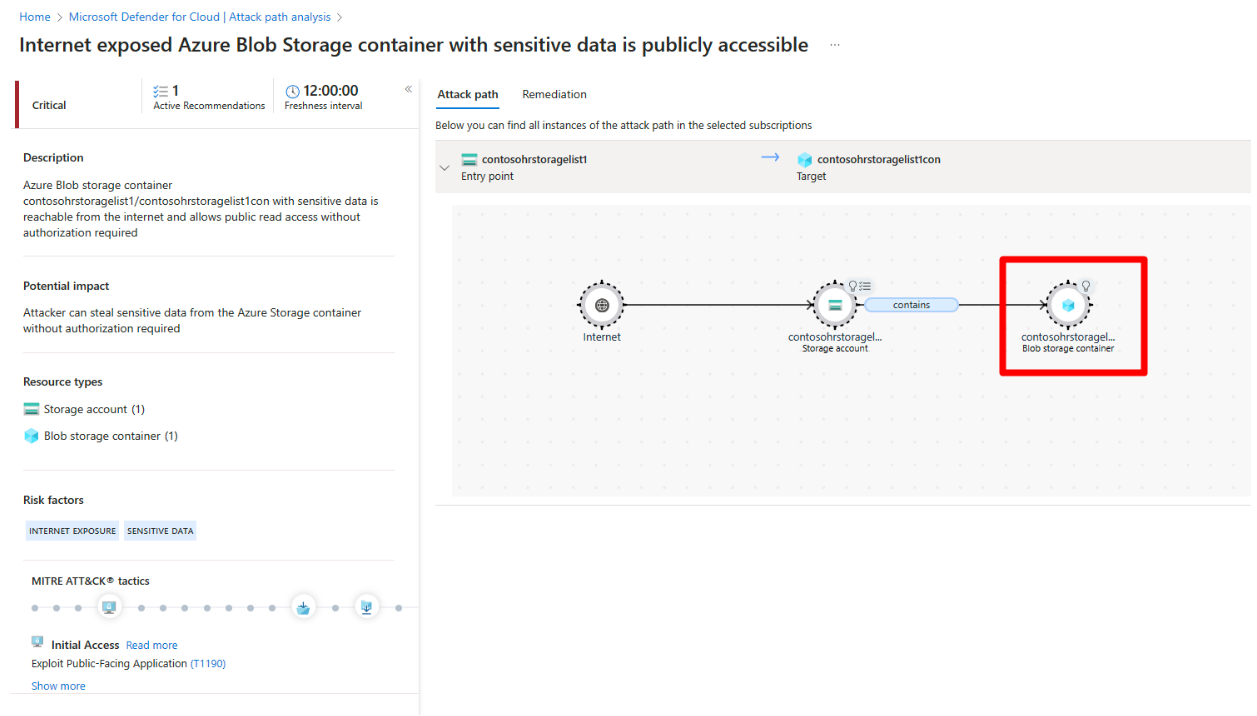
Risk Factors == 8 selected

Risk level	Title	Entry point	Target
Critical	Internet exposed and publicly accessible storage with sensitive data (Private preview)	contosohrstoragebucket3	contosohrstoragebucket3
Critical	Internet exposed VM with high severity vulnerabilities allows lateral movement to Keys management service (Private pre...	gavm2019	gademokeyvault
Critical	Internet exposed and publicly accessible storage with sensitive data (Private preview)	contosohrstoragebucket1	contosohrstoragebucket1
Critical	Internet exposed Azure Blob Storage container with sensitive data is publicly accessible	contosohrstoragelist1	contosohrstoragelist1con
Critical	Internet exposed Azure Blob Storage container with sensitive data is publicly accessible	userssimulationb2cp1	file
Critical	Internet exposed Azure Blob Storage container with sensitive data is publicly accessible	xdrstaticstorage	uploaded
Critical	Internet exposed Azure Blob Storage container with sensitive data is publicly accessible	devopsdemo83123	sensitivedata
Critical	Internet exposed Azure Blob Storage container with sensitive data is publicly accessible	scriptsmdep1demo	assets
Critical	Internet exposed Azure Blob Storage container with sensitive data is publicly accessible	labeltestadls	labeldata

(SOURCE: 13).

3) Select an “Attack Path” of interest.

4) Select the appropriate “Node”. This is illustrated in the diagram below:



Home > Microsoft Defender for Cloud | Attack path analysis >

Internet exposed Azure Blob Storage container with sensitive data is publicly accessible ···

Critical | 1 Active Recommendations | 12:00:00 Freshness interval

Description

Azure Blob storage container contosohrstoragelist1/contosohrstoragelist1con with sensitive data is reachable from the internet and allows public read access without authorization required

Potential impact

Attacker can steal sensitive data from the Azure Storage container without authorization required

Resource types

Storage account (1)

Blob storage container (1)

Risk factors

INTERNET EXPOSURE SENSITIVE DATA

MITRE ATT&CK® tactics

Initial Access Read more

Exploit Public-Facing Application (T1190)

Show more

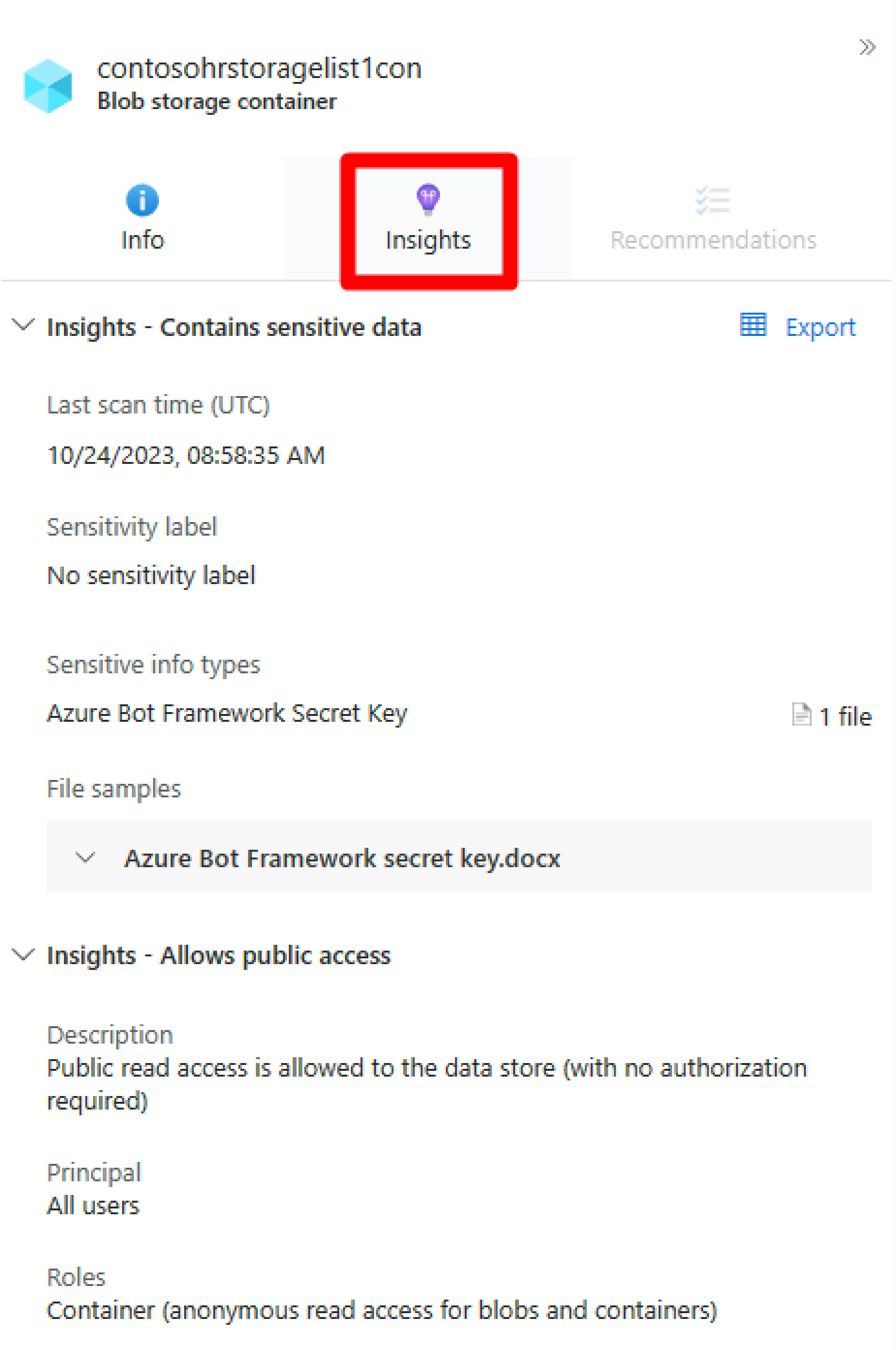
Attack path | Remediation

Below you can find all instances of the attack path in the selected subscriptions

contosohrstoragelist1 Entry point → contosohrstoragelist1con Target

(SOURCE: 13).

5) Select "Insights" to get more information on this "Attack Path". This is illustrated in the diagram below:



contosohrstoragelist1con

Blob storage container

Insights - Contains sensitive data

Last scan time (UTC)

10/24/2023, 08:58:35 AM

Sensitivity label

No sensitivity label

Sensitive info types

Azure Bot Framework Secret Key 1 file

File samples

Azure Bot Framework secret key.docx

Insights - Allows public access

Description

Public read access is allowed to the data store (with no authorization required)

Principal

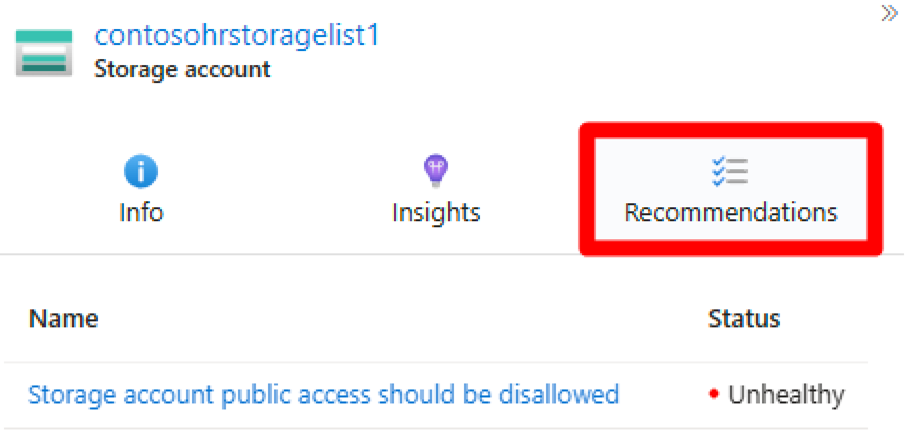
All users

Roles

Container (anonymous read access for blobs and containers)

(SOURCE: 13).

6) Select a “Recommendation”. This is also illustrated in the diagram below:



Name	Status
Storage account public access should be disallowed	• Unhealthy

(SOURCE: 13).

7) Select the specific “Recommendation” that you want to see.

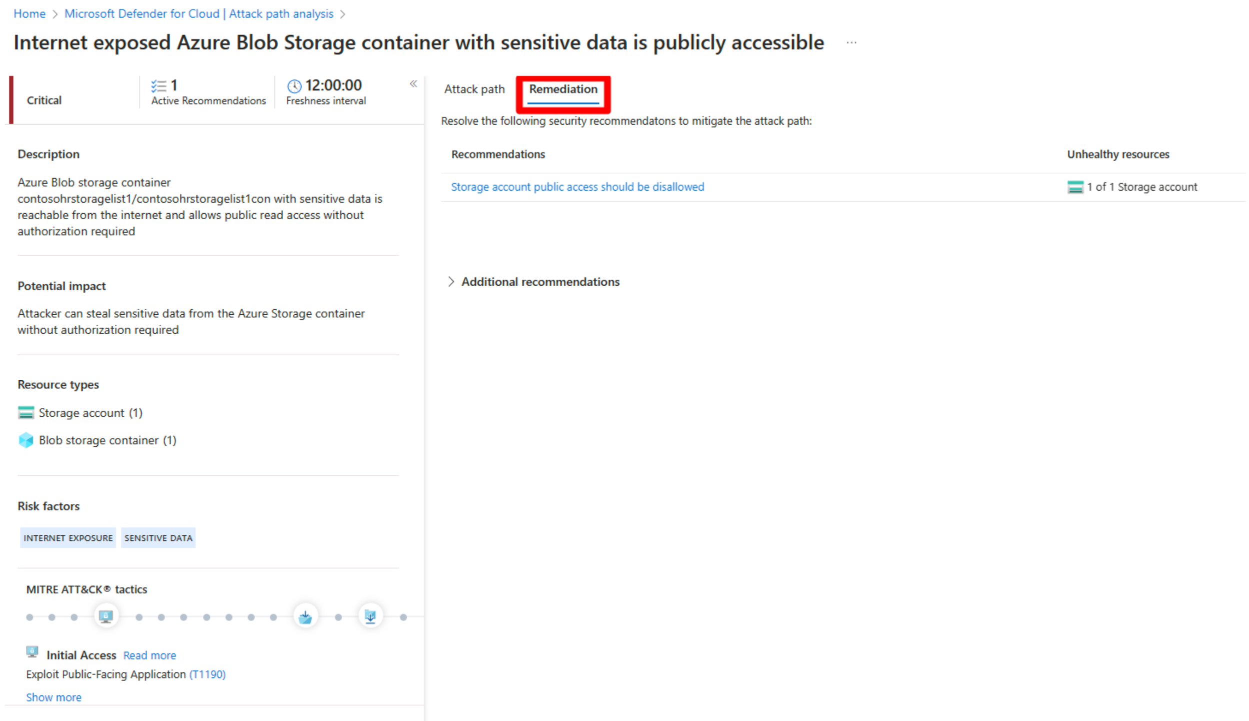
You can also select other nodes as well, and view their recommendations as well. Also note that once a particular Attack Path has been resolved, it can take up to 24 hours to show up as such in your dashboard.

Viewing All Of The Recommendations

Rather than viewing each Recommendation individually, you can also view them all at the same time. To this, follow these steps:

1) Follow steps #1 - #3 as detailed in the last subsection.

2) Select “Remediation”. This is illustrated in the diagram below:



Home > Microsoft Defender for Cloud | Attack path analysis >

Internet exposed Azure Blob Storage container with sensitive data is publicly accessible ...

Critical | 1 Active Recommendations | 12:00:00 Freshness interval

Description

Azure Blob storage container contosohrstoragelist1/contosohrstoragelist1con with sensitive data is reachable from the internet and allows public read access without authorization required

Potential impact

Attacker can steal sensitive data from the Azure Storage container without authorization required

Resource types

Storage account (1)

Blob storage container (1)

Risk factors

INTERNET EXPOSURE | SENSITIVE DATA

MITRE ATT&CK® tactics

Initial Access Read more

Exploit Public-Facing Application (T1190)

Show more

Attack path | Remediation

Resolve the following security recommendatons to mitigate the attack path:

Recommendations	Unhealthy resources
Storage account public access should be disallowed	1 of 1 Storage account

> Additional recommendations

(SOURCE: 13).

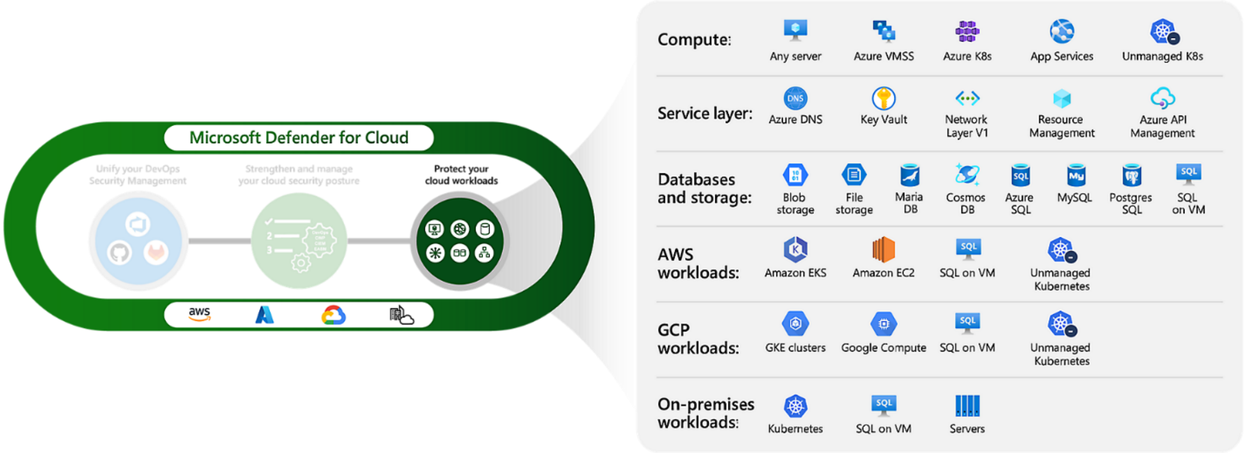
3) Follow the "advice" to resolve a "Recommendation".

The Defender For Cloud & Workload Protection

Earlier in this whitepaper, in a previous subsection, we reviewed in detail about the Cloud Work Protection Platform, also known as the "CWPP". In this subsection, we take a closer look at the specific workloads that can be protected.

What Is Protected

The illustration below depicts what can be protected:



(SOURCE: 13).

As you can see from above, the following workloads are protected:

- The Azure Compute Workloads
- The Azure Data Workloads
- The Azure Storage Workloads
- The Azure Service Layer Workloads
- The Amazon EKS
- The Amazon EC2
- The unmanaged Kubernetes
- The unmanaged SQL
- The GKE clusters
- The Google Compute

The Workload Protection will allow you and your IT Security team to achieve the following:

1) Protect A Hybrid Environment:

Protect your Azure Cloud Deployment and on-premises environment, which include critical workloads such as servers, databases, containers, storage, APIs, and service layers.

2) Real time respond to Cyberthreats:

The Defender For The Cloud integrates with your security information and events management (SIEM) system and unified extended detection and response (XDR).

3) Accelerate Forensics And Cyber investigations:

You can quite easily use connected investigation and hunting tools that come with the Microsoft Defender Threat Intelligence.

A Definition Of Vulnerability Scanning

A key component in not just Azure but in Cybersecurity in general is what is known as "Vulnerability Scanning". This can be technically defined as follows:

"Vulnerability scanning is a process of identifying and assessing security weaknesses in a computer system, network, or web application."

(SOURCE: 14).

It is important to note that a Vulnerability Scan does is just a passive scan, it only detects for known vulnerabilities, unlike Penetration Testing. The latter is considered to be an active scan, and also detects unknown vulnerabilities as well.

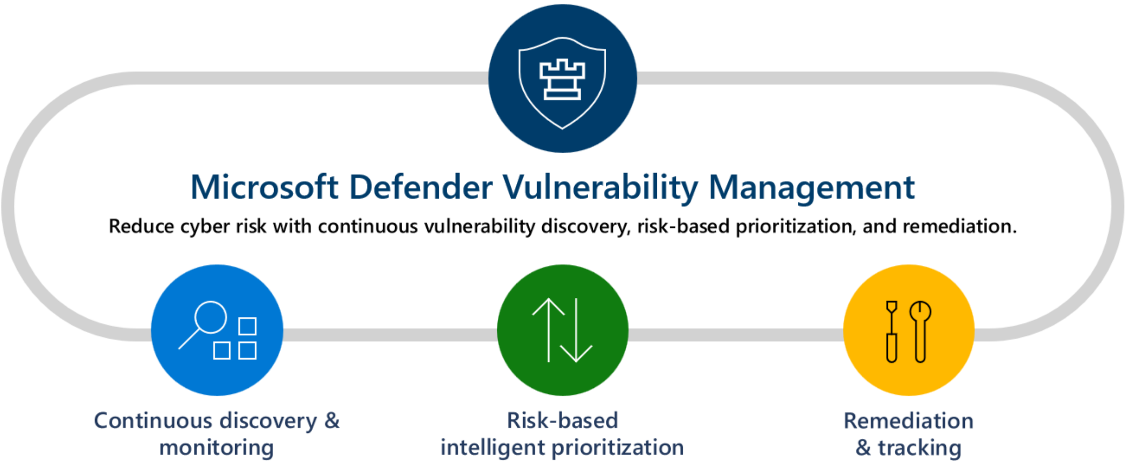
How Vulnerability Scanning Relates To The Defender For The Cloud

Now taking the above, the technical definition for Vulnerability Scanning as it relates to Defender For The Cloud is as follows:

"Defender Vulnerability Management delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices. Leveraging Microsoft threat intelligence, breach likelihood predictions, business contexts, and devices assessments, Defender Vulnerability Management rapidly and continuously prioritizes the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk."

(SOURCE: 15).

In other words, the Defender For The Cloud will observe any and unusual activity in your Azure based IT/Network Infrastructure, and not only notify you of any imminent threats, but it will even try to provide the best recommendations possible to your IT Security team. The Vulnerability Scanning/Management Methodology is illustrated in the diagram below:


Microsoft Defender Vulnerability Management
Reduce cyber risk with continuous vulnerability discovery, risk-based prioritization, and remediation.
Continuous discovery & monitoring
Risk-based intelligent prioritization
Remediation & tracking

(SOURCE: 15).

What The Defender For The Cloud Can Do For Vulnerability Scanning

Of course, the Vulnerability Scanning mechanism has specific functionalities as well, and they are broken down into these three major categories:

1) Continuous Asset Discovery And Monitoring

- Security baselines assessment: Create baseline profiles to measure risk against established benchmarks.
- Visibility into software and vulnerabilities: Get a holistic view of your software applications, and software installations and patches and patches that have been recently made.
- Network share assessment: Assess the entire state of your Network Infrastructure.
- Authenticated scan for Windows: Run automated Vulnerability Scans by providing the Defender For The Cloud with the login credentials to make this happen remotely.
- Threat analytics & event timelines: Use event timelines to project future threat variants.
- Browser extensions assessment: Get an entire listing of the web browser extensions across the different browsers deployed, such as Edge, Chrome, Firefox, Safari, etc.
- Digital certificates assessment : Get a listing of all of the SSL certificates deployed on all of your digital assets. You can even get a central certificate inventory page to locate the SSL certificates before they expire.
- Hardware and firmware assessment: Get a listing of all of the hardware and firmware dispersed throughout the physical location of your business and remotely.

2) Risk-Based intelligent Prioritization:

- Focuses on emerging threats: See which new threat variants pose the highest risk to your business.
- Locate active breaches: Prioritize which vulnerabilities need to be addressed first.
- Protects high-value assets: Determine which have devices with business-critical applications or confidential PII datasets.

3) Remediation and Tracking:

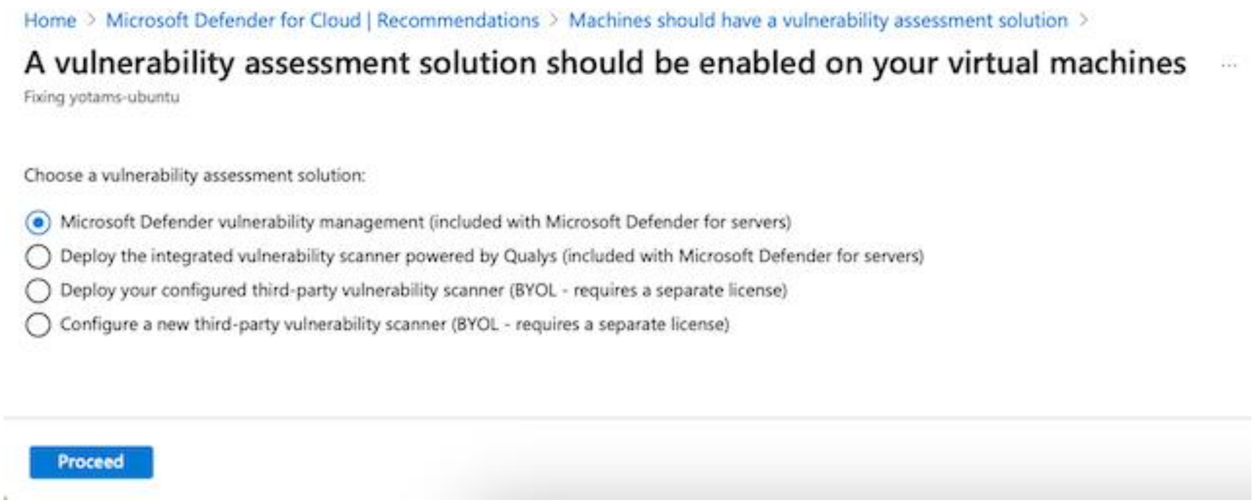
- Remediation requests sent to IT: View the status of submitted tech support tickets.
- Block vulnerable applications: Have the ability to block vulnerable applications, such as those that are unauthorized.
- Alternate mitigations - Gain advice on other risk mitigation strategies.
- Real-time remediation status: Get real-time monitoring of how your remediation activities are going, both on a high and device specific level.

Deploying The Vulnerability Scanner

To automate the processing of deploying and configuring the Vulnerability Scanner, click on the link below:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-defender-vulnerability-management#learn-more

To do this process manually, examine the illustration below:



Home > Microsoft Defender for Cloud | Recommendations > Machines should have a vulnerability assessment solution >

A vulnerability assessment solution should be enabled on your virtual machines

Fixing yotams-ubuntu

Choose a vulnerability assessment solution:

● Microsoft Defender vulnerability management (included with Microsoft Defender for servers)
○ Deploy the integrated vulnerability scanner powered by Qualys (included with Microsoft Defender for servers)
○ Deploy your configured third-party vulnerability scanner (BYOL - requires a separate license)
○ Configure a new third-party vulnerability scanner (BYOL - requires a separate license)

(SOURCE: 16).

The Defender For Cloud & DevOps Posture Visibility

The Functions of The Defender For The Cloud And DevOps

The concept of DevSecOps was reviewed earlier in this whitepaper, and in this same regard, the Defender For The Cloud can also work with the DevOps component of your business. This is acronym that stands for "Development and Operations", and this is where teams from both areas come and work together in order to develop the source code for a web application in a seamless fashion. It is also an important part of Azure, and can work with the Defender For The Cloud. Here is how it is possible:

1) <u>Get a unified perspective into your DevOps security posture</u>:

   You and your IT Security team can now get a full visibility into the security posture of the Source Code across and Hybrid Cloud environments.

2) <u>Fortify Cloud resource configurations throughout the SDLC</u>:

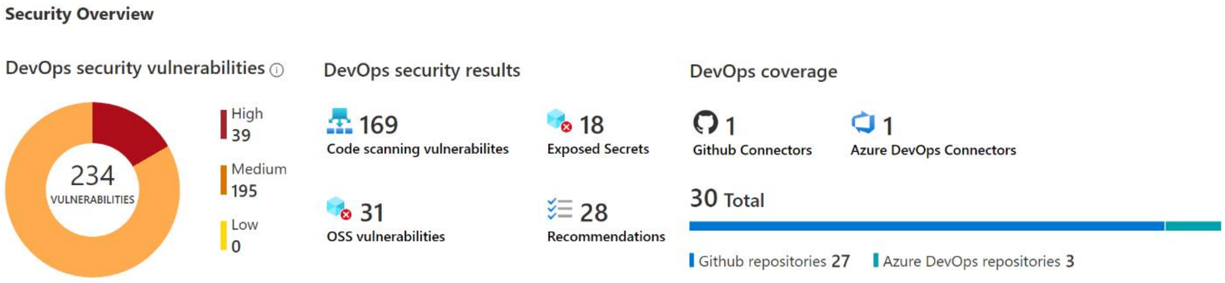
   You can deploy Infrastructure as Code (IaC) templates and container images to mitigate Cloud misconfigurations before they reach the production environment.

3) <u>Prioritize remediation of critical issues in code</u>:

   ` You can easily apply code-to-cloud contextual insights within Defender for Cloud. This will allow for your IT Security team to assist your software development team to prioritize critical Source Code.

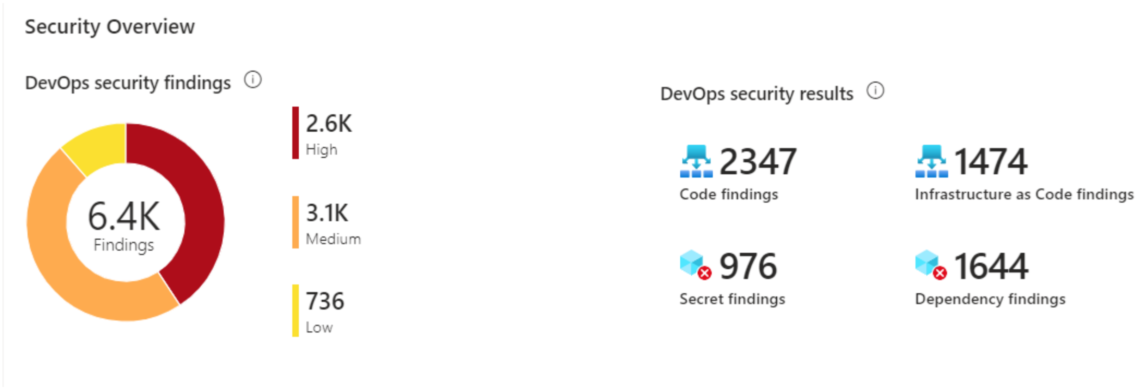
Managing The DevOps Environment

The illustration below demonstrates how you can manage your DevOps environment:



(SOURCE: 17).

The illustration below demonstrates how you can get a breakdown of your DevOps Security Posture from a single scan:



Security Overview

DevOps security findings ⓘ

6.4K Findings

2.6K High

3.1K Medium

736 Low

DevOps security results ⓘ

2347 Code findings

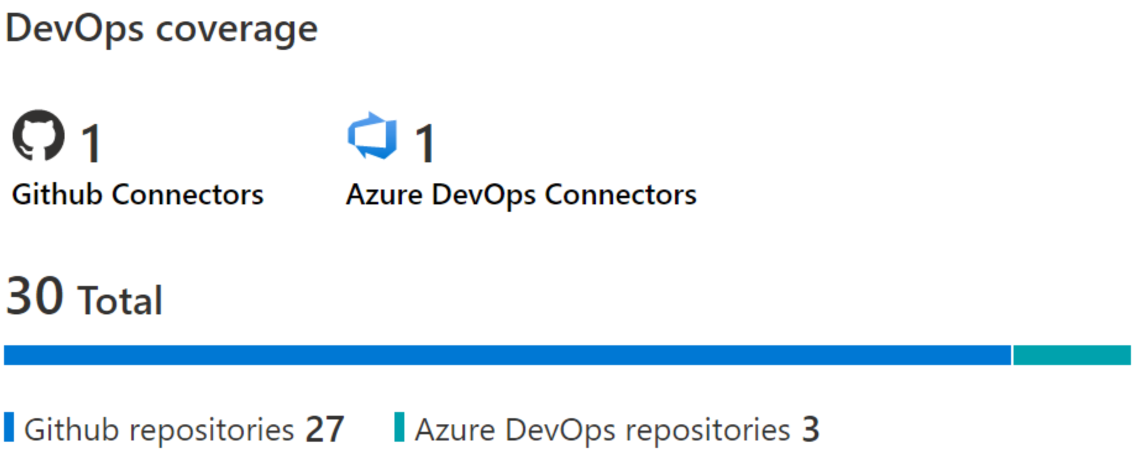
1474 Infrastructure as Code findings

976 Secret findings

1644 Dependency findings

(SOURCE: 17).

The illustration below demonstrates how you can get a breakdown of the total number of DevOps Security Posture recommendations:



DevOps coverage

1 Github Connectors

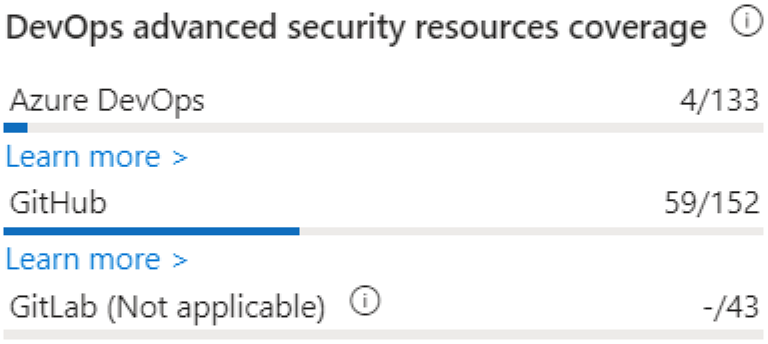
1 Azure DevOps Connectors

30 Total

Github repositories 27

Azure DevOps repositories 3

The illustration below demonstrates how you can get a breakdown of the total number of DevOps resources that have advanced security features incorporated into them:



DevOps advanced security resources coverage ⓘ

Azure DevOps 4/133

Learn more >

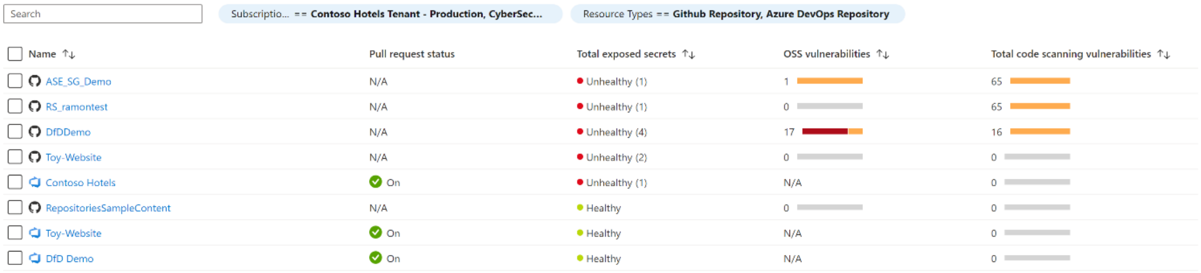
GitHub 59/152

Learn more >

GitLab (Not applicable) ⓘ -/43

(SOURCE: 17).

The illustration below demonstrates how you can get a breakdown of the Security Posture security information across all of your DevOps Resources:



Subscriptio... == **Contoso Hotels Tenant - Production, CyberSec...**

Resource Types == **Github Repository, Azure DevOps Repository**

□ Name ↑↓	Pull request status	Total exposed secrets ↑↓	OSS vulnerabilities ↑↓	Total code scanning vulnerabilities ↑↓
□ ASE_SG_Demo	N/A	● Unhealthy (1)	1	65
□ RS_ramontest	N/A	● Unhealthy (1)	0	65
□ DfDDemo	N/A	● Unhealthy (4)	17	16
□ Toy-Website	N/A	● Unhealthy (2)	0	0
□ Contoso Hotels	✓ On	● Unhealthy (1)	N/A	0
□ RepositoriesSampleContent	N/A	● Healthy	0	0
□ Toy-Website	✓ On	● Healthy	N/A	0
□ DfD Demo	✓ On	● Healthy	N/A	0

Note the following for the above:

- Name: This lists the DevOps resources from Azure DevOps, GitHub, and/or GitLab. You can view the resource health page by clicking it.
- DevOps environment – This describes the DevOps environment for the resource.
- Advanced security status – This shows the security status:

  *On - Advanced security is enabled.

  *Off - Advanced security is not enabled.

  *Partially enabled - Certain Advanced security features is not enabled (for example, code scanning is off).

  *N/A - Defender for Cloud doesn't have information about enablement.

How To Deploy DevOps

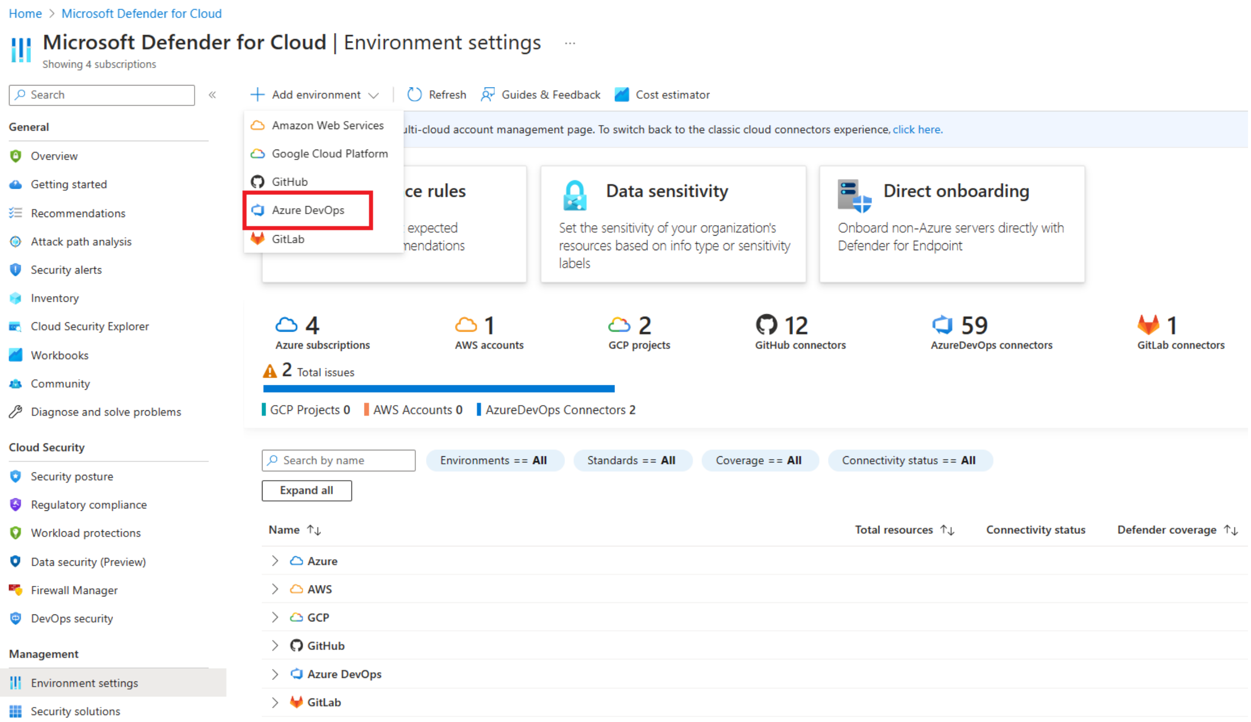
To start using the DevOps Posture Visibility with the Defender For The Cloud, follow these steps:

1) Sign into your Azure Portal.

2) Go to:
   - Microsoft Defender for Cloud
   - Then “Environment Settings”

3) Select “Add Environment”.

4) Select “Azure DevOps”. This is illustrated in the diagram below:



Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Environment settings

Showing 4 subscriptions

...lti-cloud account management page. To switch back to the classic cloud connectors experience, click here.

...ce rules — ...expected ...mendations

Data sensitivity — Set the sensitivity of your organization's resources based on info type or sensitivity labels

Direct onboarding — Onboard non-Azure servers directly with Defender for Endpoint

4	1	2	12	59	1
Azure subscriptions	AWS accounts	GCP projects	GitHub connectors	AzureDevOps connectors	GitLab connectors

2 Total issues

GCP Projects 0 | AWS Accounts 0 | AzureDevOps Connectors 2

Name ↑↓	Total resources ↑↓	Connectivity status	Defender coverage ↑↓
Azure			
AWS			
GCP			
GitHub			
Azure DevOps			
GitLab			

(SOURCE: 18).

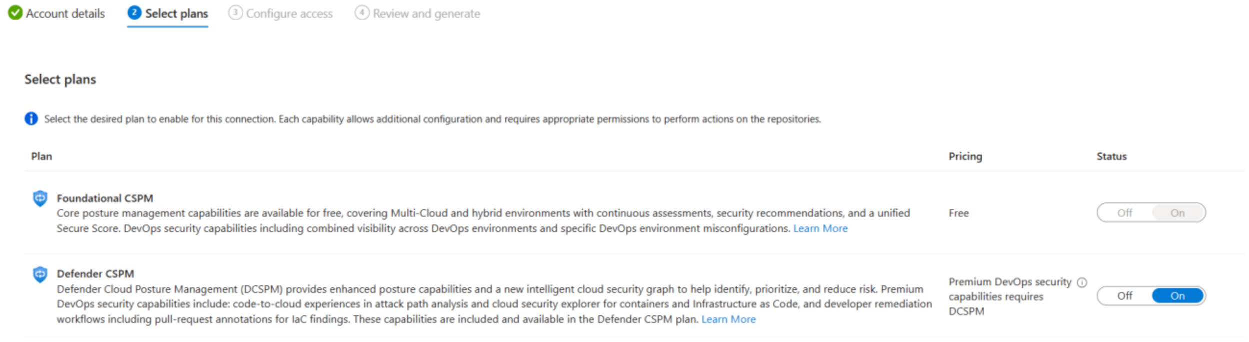
5) Enter in the following information:

- Name
- Subscription
- Resource Group
- Region

6) Select the following:

- Next
- Select Plans.

This is illustrated below:



Select plans

Select the desired plan to enable for this connection. Each capability allows additional configuration and requires appropriate permissions to perform actions on the repositories.

Plan	Pricing	Status
Foundational CSPM Core posture management capabilities are available for free, covering Multi-Cloud and hybrid environments with continuous assessments, security recommendations, and a unified Secure Score. DevOps security capabilities including combined visibility across DevOps environments and specific DevOps environment misconfigurations. Learn More	Free	Off On
Defender CSPM Defender Cloud Posture Management (DCSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Premium DevOps security capabilities include: code-to-cloud experiences in attack path analysis and cloud security explorer for containers and Infrastructure as Code, and developer remediation workflows including pull-request annotations for IaC findings. These capabilities are included and available in the Defender CSPM plan. Learn More	Premium DevOps security capabilities requires DCSPM	Off [✓ On]

(SOURCE: 18).

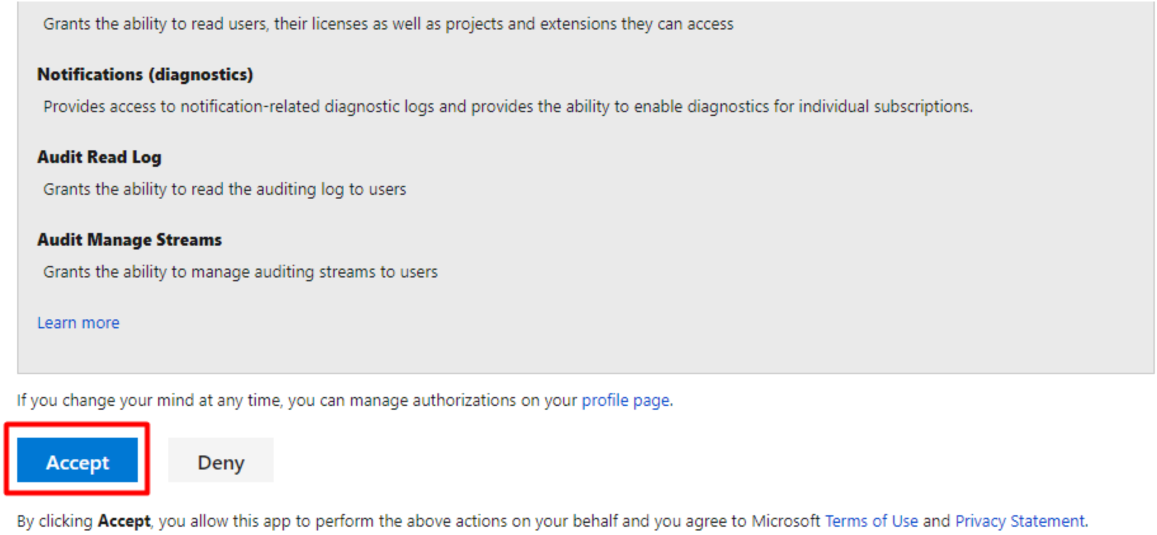
NOTE: Select the appropriate plan for your DevOps environment, these can be seen at the bottom of the illustration.

7) Select the following:

- Next
- Configure Access

8) To make sure that you authorize the correct Azure Cloud Tenant, select the appropriate from the drop-down menu in the DevOps. This will confirm that you are in the correct Azure Tenant in Defender for Cloud.

9) Select the appropriate permissions, and from there, click on "Accept". This is illustrated in the diagram below:



Grants the ability to read users, their licenses as well as projects and extensions they can access

Notifications (diagnostics)

Provides access to notification-related diagnostic logs and provides the ability to enable diagnostics for individual subscriptions.

Audit Read Log

Grants the ability to read the auditing log to users

Audit Manage Streams

Grants the ability to manage auditing streams to users

Learn more

If you change your mind at any time, you can manage authorizations on your profile page.

By clicking **Accept**, you allow this app to perform the above actions on your behalf and you agree to Microsoft Terms of Use and Privacy Statement.

(SOURCE: 18).

The Defender For Cloud & Infrastructure as a Code (IaC)

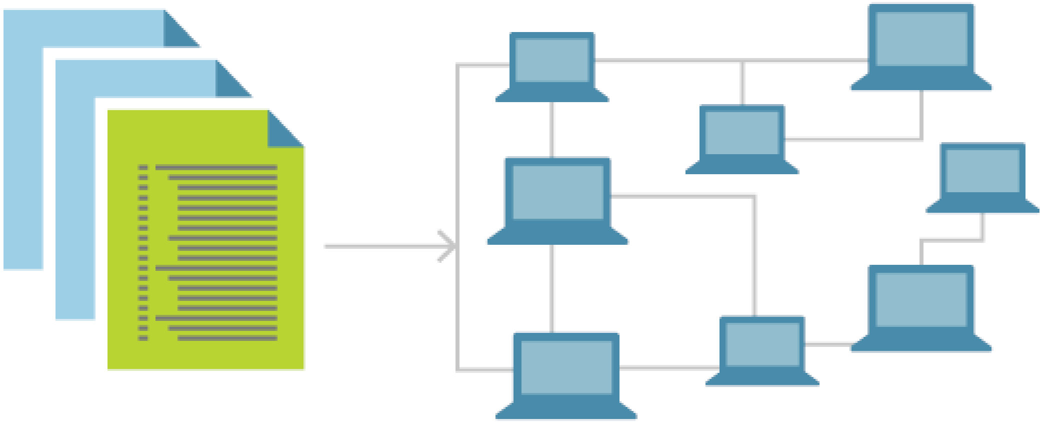
A Definition Of IaC

The Defender For The Cloud also supports the Infrastructure as a Code, also known as the "IaC" for short. It can be defined technically as follows:

"Infrastructure as code (IaC) uses DevOps methodology and versioning with a descriptive model to define and deploy infrastructure, such as networks, virtual machines, load balancers, and connection topologies. Just as the same source code always generates the same binary, an IaC model generates the same environment every time it deploys."

(SOURCE: 19).

Put in simpler terms, the IaC lets you and your IT Security manage the fundamentals of your Azure Cloud Deployment through the use of the actual Source Code, and not having to rely on manual processes if automated ones are not available. This is illustrated in the diagram below:



(SOURCE: 19).

Deploying The IaC

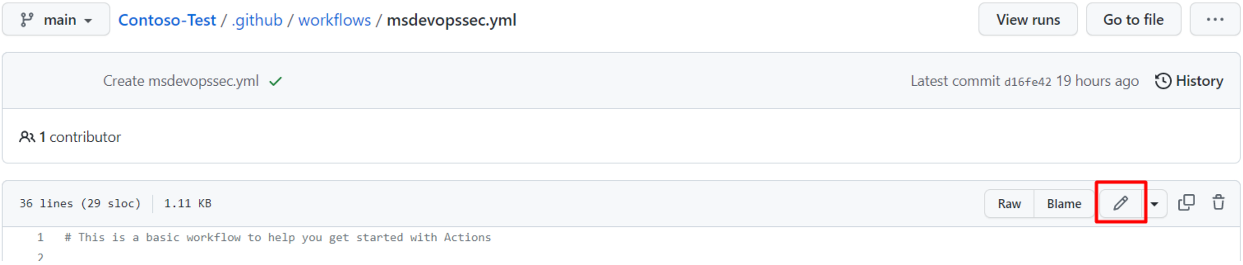
To deploy this with the Defender For The Cloud, there are two ways of doing it, with both GitHub and through the Azure DevOps. First, we examine how to do it with GitHub:

1) From your Azure Portal, sign into your GitHub account.

2) Go to the home page of your Source Repository, follow this directory path:

   github/workflows > msdevopssec.yml

3) Select “Edit File”. This is illustrated in the diagram below:



Contoso-Test / .github / workflows / msdevopssec.yml

Create msdevopssec.yml ✓

Latest commit d16fe42 19 hours ago

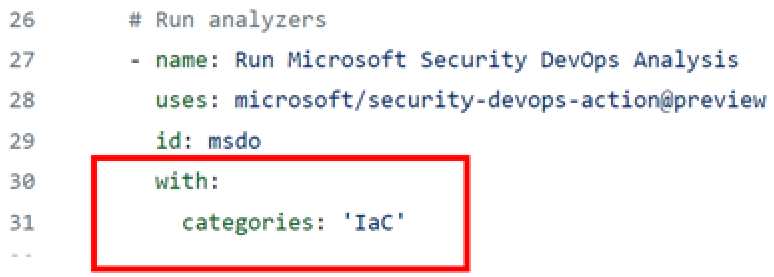
1 contributor

36 lines (29 sloc) | 1.11 KB

```
# This is a basic workflow to help you get started with Actions
```

(SOURCE: 20).

4) Under the “Run Analyzers” tab, enter in the following commands, as demonstrated in the diagrams below:

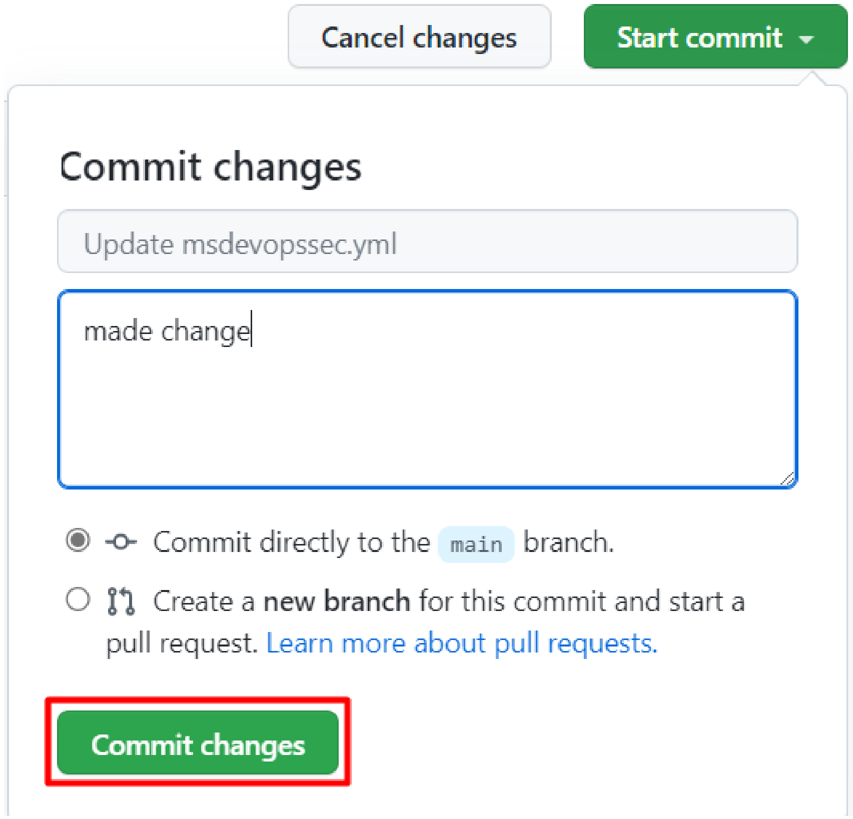


```
# Run analyzers
- name: Run Microsoft Security DevOps Analysis
  uses: microsoft/security-devops-action@preview
  id: msdo
  with:
    categories: 'IaC'
```

(SOURCE: 20).

5) Select “Start Commit”.

6) Select “Commit Changes.” This is demonstrated in the illustration below:



Commit changes

Update msdevopssec.yml

made change

● Commit directly to the `main` branch.

○ Create a **new branch** for this commit and start a pull request. Learn more about pull requests.

(SOURCE: 20).

7) To confirm that the IaC is indeed connected to the DevOps:

- ➢ Select “Actions”
- ➢ Click on any workflow to confirm the connection

8) If there are security alerts that you need to be aware of:

- ➢ Go to “Security”
- ➢ Select “Code Scanning Alerts”

Now, we examine how to deploy the IaC in Azure directly, by following these steps:

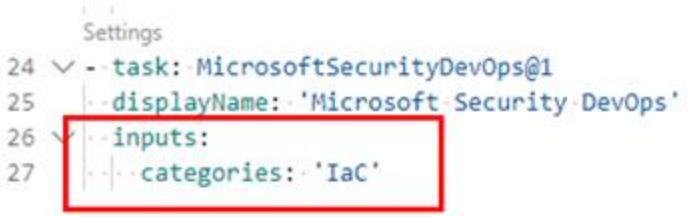
1) Sign into the “Azure DevOps” from your Azure Portal.

2) Select any Project.

3) Select “Pipeline”.

4) Select the Pipeline where the Azure DevOps has been configured.

5) If need be, edit the above configuration by inputting the commands in the illustration below:



```
- task: MicrosoftSecurityDevOps@1
  displayName: 'Microsoft Security DevOps'
  inputs:
    categories: 'IaC'
```

(SOURCE: 20).

6) Select “Save”.

7) To confirm the connection between the IaC and the Azure DevOps:

- ➢ Select “Pipeline”
- ➢ Go to “Your Created Pipeline”

Conclusions

Overall, this whitepaper has examined in great detail the various ways in which the Defender For The Cloud can be used in your Azure Cloud Deployment(s). The following matrix summarizes these methods:

Function	*Purpose*

Centralized Policy Management	Define the security conditions that you want to maintain across your environment.
Secure Score	Defines your security posture based on the security recommendations.
Multicloud Coverage	Connect to your multicloud environments with the CSPM.
Cloud Security Posture Management (CSPM)	Use the dashboard to see weaknesses in your security posture.
Advanced Cloud Security Posture Management	Get advanced tools to identify weaknesses in your security posture.
Data-Aware Security Posture	Automatically discovers datastores containing sensitive data, and helps reduce risk of data breaches.
Attack Path Analysis	Model network traffic to identify potential risks.
Cloud Security Explorer	A map of your cloud environment that lets you build queries to find security risks.
Security Governance	Drive security improvements through your organization by assigning tasks to resource owners.
Microsoft Entra Permissions Management	Provide comprehensive visibility and control over permissions for any identity and any resource in Azure.
Protect Cloud Servers	Provide server protections through Microsoft Defender for Endpoint.
Identify Threats To Your Storage Resources	Detect unusual and potentially harmful attempts to access or exploit your storage accounts.
Protect Cloud Databases	Protect your entire database estate with attack detection and threat response tools from Azure.
Protect Containers	Secure your containers so you can improve, monitor, and maintain the security of your containers.
Infrastructure Service Insights	Diagnose weaknesses in your application infrastructure.

(SOURCE: 16).

Finally, you can also use the Defender For The Cloud for guidance on how to create secure Source Code, this is called the "Code Security Guidance". If you have any questions about this whitepaper, or would like to try out Microsoft Defender, contact us today.

Sources

1) https://azure.microsoft.com/en-us/solutions/devsecops#tabxac5cdc429ab04cf9aca7b6b5724553c2
2) https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management

3) https://www.microsoft.com/en-us/security/business/security-101/what-is-cwpp#:~:text=A%20cloud%20workload%20protection%20platform%20is%20a%20comprehensive%20cybersecurity%20solution,comes%20more%20potential%20security%20risks.
4) https://www.youtube.com/watch?app=desktop&v=Tp2u_P2Cp04
5) https://learn.microsoft.com/en-us/azure/devops/pipelines/get-started/what-is-azure-pipelines?view=azure-devops
6) https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/centralized-policy-management-in-microsoft-defender-for-cloud/ba-p/1276331
7) https://learn.microsoft.com/en-us/defender-cloud-apps/security-saas
8) https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-regulatory-compliance
9) https://www.microsoft.com/en-us/security/business/cloud-security/microsoft-defender-cloud
10) https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-attack-path
11) https://learn.microsoft.com/en-us/azure/defender-for-cloud/how-to-manage-attack-path
12) https://www.microsoft.com/en-us/security/business/solutions/cloud-workload-protection#
13) https://purplesec.us/learn/what-is-vulnerability-scanning/
14) https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide
15) https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-defender-vulnerability-management#learn-more
16) https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-devops-introduction
17) https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-devops
18) https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code
19) https://learn.microsoft.com/en-us/azure/defender-for-cloud/iac-vulnerabilities