Cybersecurity Insurance – Is Your IT Infrastructure Up To Snuff?

Written for KAMIND, IT, Inc.

By Ravi Das

Introduction

As the Cyber Threat Landscape becomes even more daunting and hard to cope up with, the one peace of mind that business owners had was if they had Cybersecurity Insurance. For the most part, if they followed some rules, they knew that they would get a complete payout. But fast forward to today's times. Not only is not guaranteed that a payout may or may not happen, but now, even being able to apply for a reasonable Cyber insurance policy has become a total nightmare.

It's like almost trying to survive an IRS audit – you literally need to have the paperwork now to back up all of your attestations that you are fully compliant. If the insurance company has any doubts in their mind about your paperwork, they will come out the physical location of your business, and even do an audit to confirm that what you have attested to is in full force.

In this whitepaper, we look at some of the key features of your IT Infrastructure that need to come into compliance before you can even think of applying for a Cyber Insurance Policy.

What You Need To Do

With the recent rise in Ransomware attacks, it is no doubt that insurance companies are now honing in on the technologies and the practices that you have in place in order to mitigate the risk of this security breach from happening in the first place. Here are things that you need, the business owner, need to stay focused on and address as a high and urgent priority:

1) Email Filtering:

   On a technical level, filtering simply means that your firewalls, network intrusion devices, routers, VPNs, etc. are following a specific set of rules and permutations that you have established in order block malicious data packets from entering into your IT and Network Infrastructures. In this regard, the insurance company does not need to know all about the nitty gritties of what you are doing, they just want to make sure that you have in place will be sufficient to block any suspicious emails from penetrating through, or even better yet, quarantining any suspicious attachments or links even before they reach the inbox. That way, a network administrator can inspect whatever has been blacklisted before it is allowed even to move forward down the line to the employee.

2) Management of suspicious Emails:

   This all stems down to the level and amount of security awareness training that your employee has undergone with you. As it has been said many times before, simply providing this training once a year is not suffice enough. Rather, you must do it at least once a quarter so that the employee is kept abreast of the latest security threats, and how to help avoid them from becoming a risk to your company. In this instance, the insurance company wants to know how do your employees react when they see a suspicious Email? Will they simply look for the telltale signs of a Phishing Email and know enough to at least delete it, or in a best-case scenario, forward it onto the IT Security team for further examination? One of the best ways you can prove to an insurance carrier that your metrics are high in this regard (in other words, the chances that ***your employee will not respond to a Phishing Email***) is to test your employees with a simulated Phishing attack a few days after training. If most of them don't fall prey to it,

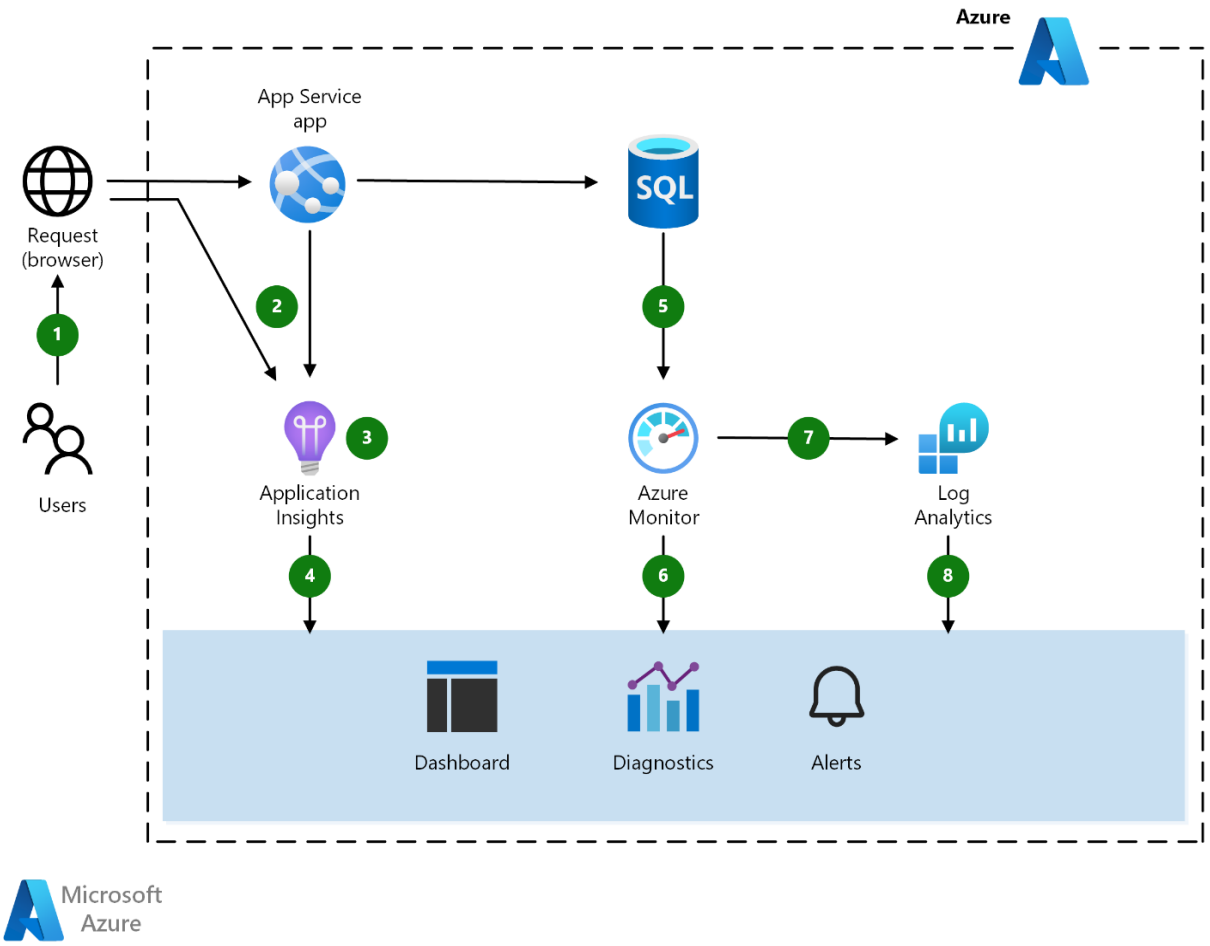
then this proof to the insurance company that your security awareness training programs are effective for the time being, until the next quarter, when the next round of training will occur. You also then need to demonstrate that you have a plan in place for those employees that did fall prey to this simulation attack, and how you will remediate the situation for the future.

3) Authentication:

Technically, this refers to the process of confirming the identity of an individual before they are allowed access to shared resources. Here, you will hear all of the techno jargons of Two Factor Authentication (2FA), Multifactor Authentication (MFA), etc. While there is no doubt that this is extremely important to have in place (in fact, the insurance carrier will be checking up on this as well), this is especially relevant for the sending and receiving of Emails, as this is how most Ransomware attacks start in the first place. Your employees need to make sure that the Emails they are receiving and responding to are coming in from legitimate sources, and if there is any doubt on this, the steps they will take to confirm the authenticity of it (such as calling the sender to confirm if they have truly sent it or not). Likewise, the receiver of the Email needs to know that the actual message has not been tampered with. In this regard, deploying encryption will be one of the best tools that you can use to confirm the integrity of the original message. You can even take it one step further, and make use of what are called hashing messages. These are simple algorithms that compute a number. If the number stays the same from the point of origination to the point destination, then you have guarantees the message has not been tampered with while it was transit.

4) Web Filtering:

In a way, this can also be thought of as in the same way as Email filtering. But in this instance, you need to create a whitelist of the good domains that your employees are allowed to visit, as well as a blacklist of those domains that are known to be malicious in nature, and that your employees cannot access. To prove to the insurance company that you are trying to prevent employees from visiting websites with heisted domain names, you can even set up a proxy server in which your employee has to enter in a separate set of login credentials to further confirm their identity, as a means to show that you have set up MFA at different points from within your IT and Network infrastructure. To a certain degree, the proxy server can even check on the website requested to be accessed if it is a phony or not. An example of Web Filtering in Azure illustrated below:

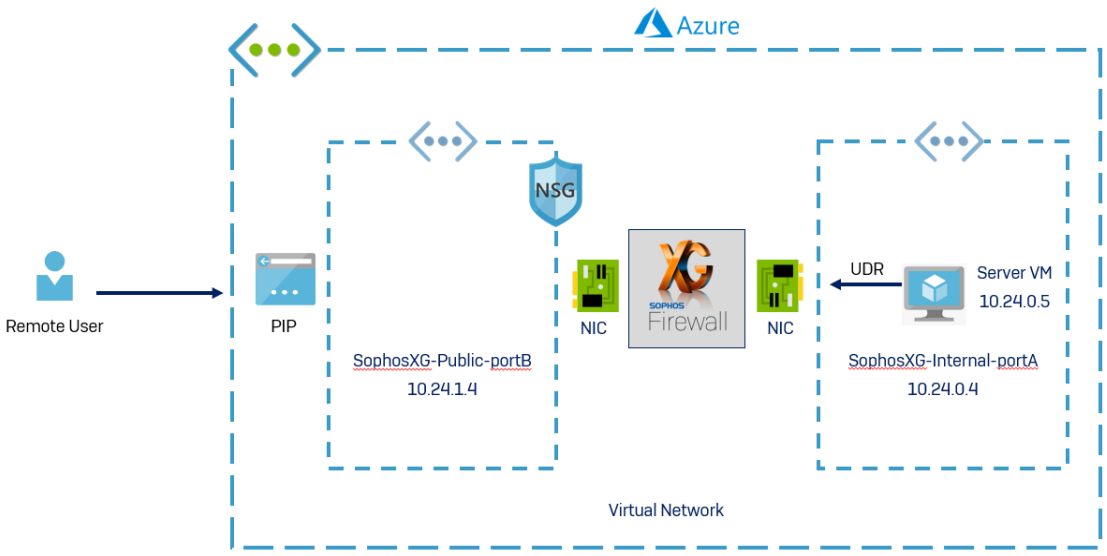


(SOURCE: 1).

5) Remote Access:

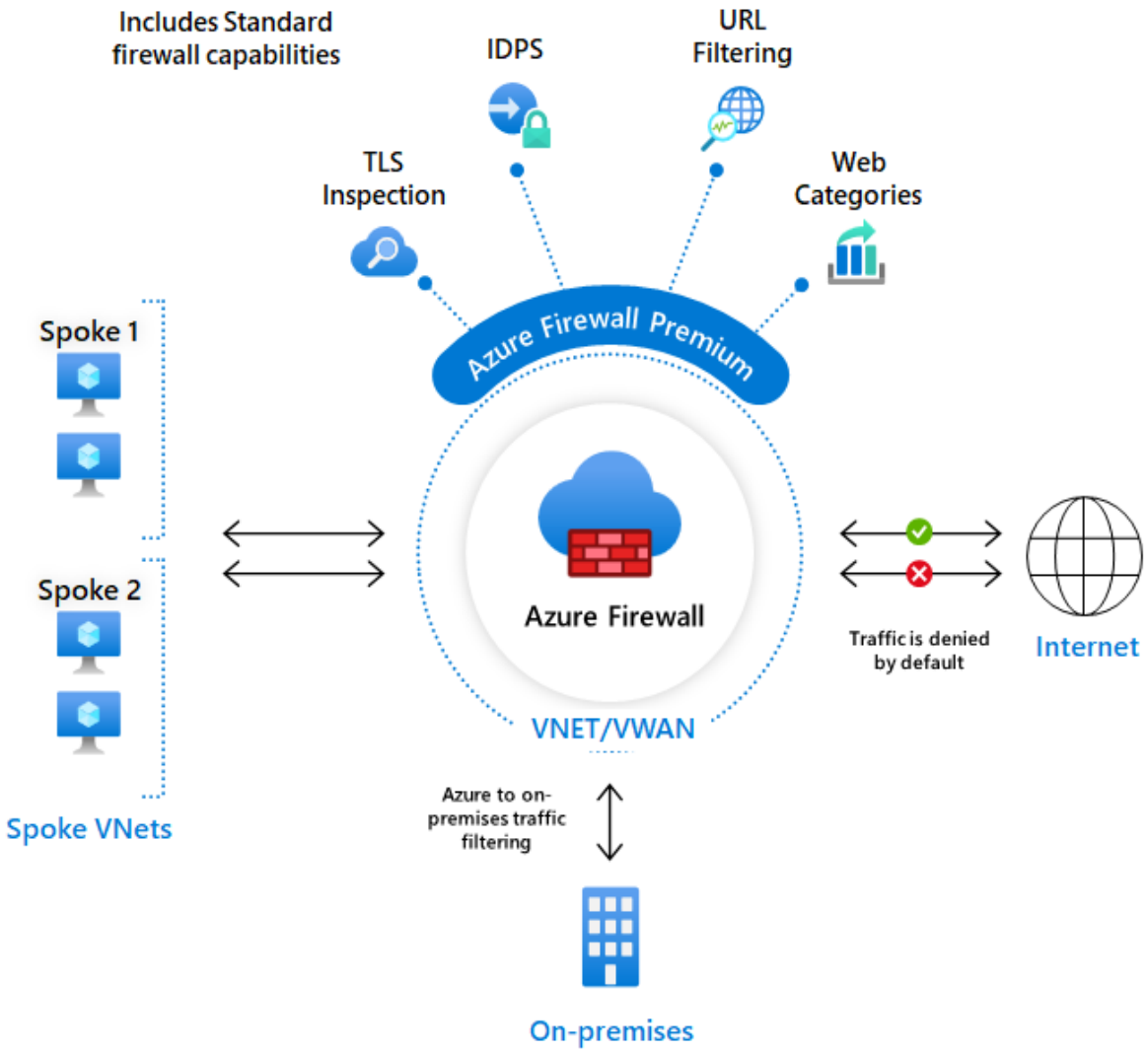
Although Remote Access has always been a concern to businesses, the concerns about it did not explode until the COVID-19 pandemic first came out. Back then, there was a rush to work from home to stop the spread of the virus, and in this haste, many companies were not prepared at all to provision and deploy to employees company issued devices with the needed security protocols in place. Because of this, many employees were using their own personal devices to conduct their work-related matters, which is also known as Bring Your Own Device, or BYOD for short. There was also the intermingling of the home networks with the corporate networks, which caused even a greater security risk. At this time, many insurance companies overlooked this facet, as companies were desperate to try to get some sort of financial backing with all of the newer threat variants that were coming out. But two years later, Corporate America has now come to a greater understanding of what the security risks are and what needs to be done to done to correct it. For example, although VPNs were the true security warrior here, they now have started to show their signs of breakdown, because they were not designed to handle the network demands of a near 99% Remote Workforce. Now many have started to use what is known as the Next Generation Firewall, which has been created to specifically handle this

gargantuan workload. In fact, on top of this, the bulk of the companies have now shifted their entire On Premises infrastructure to Cloud based one, such as that of Microsoft Azure. Using a platform like this has all of the security tools that one would ever need to have a secure environment for remote access. But the key thing to remember here is that while you have these tools in place, it is up to you to configure them properly to your own security requirements. ***Never rely upon the default settings!!!*** By showing that you are in the Cloud, you should have pretty much satisfied the questions that insurance carrier has about how you are securing your remote access functionalities to your employees that work from home (WFH). A key issue here has been the weaknesses of using the Remote Desktop Protocol (RDP), in which an employee can gain access to another machine directly. But with creating and using Virtual Machines (VMs), an employee can now bypass this risk and access the server directly with an Internet based connection, assuming that they have the privileges to do so. Also, by making use of Azure, the employees are also eligible to use M365, which is the online version of all of the popular Office based products, such as Word, Excel, PowerPoint, and Excel. By giving access to your employees in this manner, you will have reasonable assurances that your products will be updated with the latest software patches and upgrades. This will be looked upon very favorably by the insurance carrier as you apply for a Cyber Policy. Also, the chances of Shadow IT from occurring are now greatly lowered, as employees can only download and use those applications that are available to them in their account. An illustration of securing Remote Access in Azure is seen below:



(SOURCE: 2)

An example of the Next Generation Firewall in Azure is illustrated below:



(SOURCE: 3).

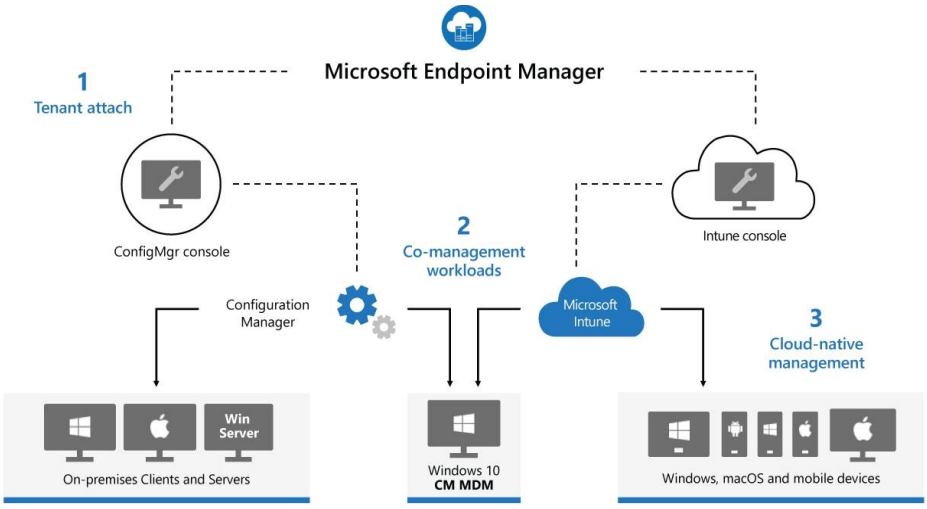
6) Network Access:

In the world of Cyber of today, this is now one of the biggest issues, because people still fail to follow the policies that have been instituted. As a result, this is an area that the insurance company keeps close tabs on. They want to see that employees are given access to what they need to have in order to conduct their everyday job functions. In others, they want assurances that you are abiding by the principles of least access. This also holds true of those accounts that are privileged in nature, such as those rights and permissions that have been assigned to both the IT Security team and employees of the IT department. You have to pay very close attention to them, as this is often a favored of the Cyberattacker to penetrate into. As a result, you need to have permutations set up so that any unused accounts are automatically deprovisioned, and even deleted, if necessary. In this regard, you also need to maintain a strict password policy, such as when they need to be replaced, how long they need to be, etc. A good password

manager will work here as well, and Azure has one that is ready to deploy in just a matter of minutes for your use.

7) Endpoint Security:

Even before the COVID-19 pandemic hit, many companies were only worried about securing the lines of network communication from the point of origination to the point of destination, and vice versa. The thinking here was that (and even still continues to be to this day) is that if a security were to happen, it would happen while the data was in transit. As a result, the endpoints of these lines of communications were totally ignored. The Cyberattacker became aware of this, and as a result, this became a great place for them to enter and just "hang out" until they determined their next move. But now, businesses are realizing the importance of securing these endpoints so that another backdoor will be closed to the Cyberattacker. Many insurance companies want to see you have secured endpoints to the best of your abilities. To your advantage, Azure has great tools already in place that you can deploy in just a matter to secure your endpoints as needed. An example of Endpoint Security is illustrated below:



A unified platform including both Configuration Manager and Microsoft Intune

(SOURCE: 4).

8) Open Ports:

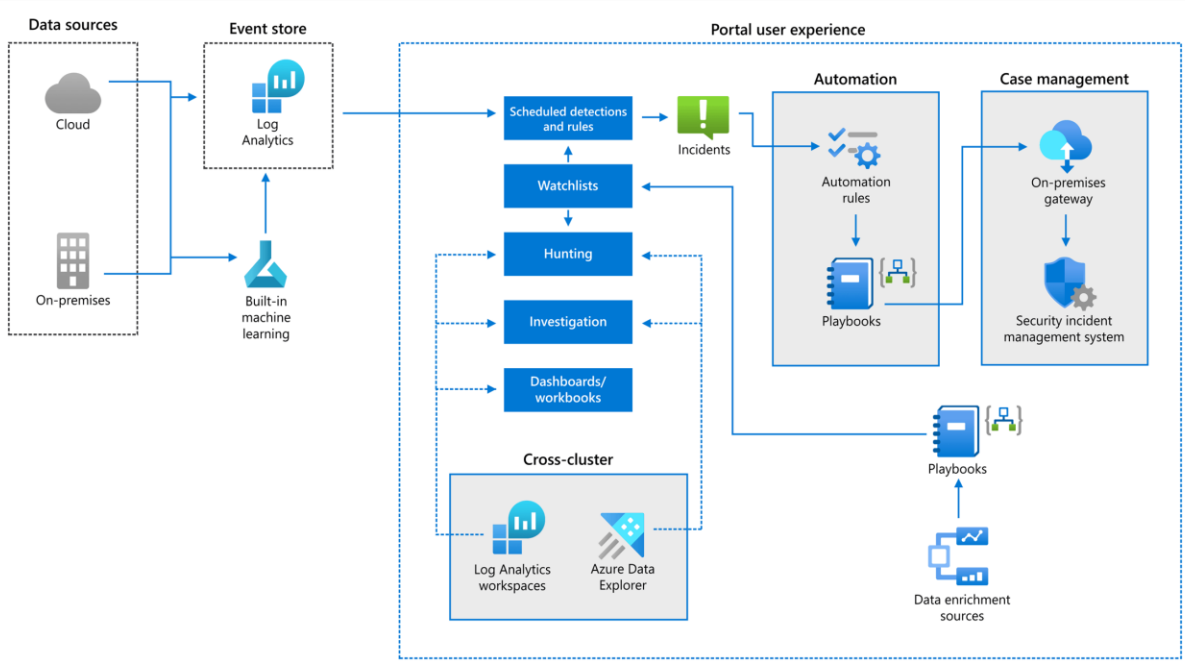
One of the most important principles to follow in Cyber is to make sure that any unused or open network ports are closed. This is yet another way for easy penetration, and the remediation for this this is quick and simple: Just close them off. The only way you can confirm what is open and closed is done by conducting a thorough Vulnerability Scan. Once you have done this, the report will show to all of the network ports that are open and closed. In order to maintain the best possible security possible, you should close off all the open ports. This will also show to the insurance provider that you are being proactive. But just like security training, this is not a one and done deal. This kind of scan should be conducted at least once a quarter, as ports can reopen yet once again after they have been closed.

9) Software updates:

Once again, this is a topic that is heard all of the time: ***Make sure that your systems are updated with the latest patches and upgrades!!!*** Although it may sound simple enough, many companies still fail to follow a regular policy, especially if they have an On Premises infrastructure. Because of the lack in doing in this, this is an area that is hit hard upon by the insurance company. But keep in mind, if you are totally in the Azure Cloud environment, you really have nothing to worry about in this aspect. All of this is done for you by the datacenter wherever your deployments are hosted at. But it is always to ask what their schedule is for deploying and installing patches, and what has been applied.

10) Log files:

This is what is outputted by all of your network devices. Each and every detail of what happens in your infrastructure is recorded here, whether it is On Prem or in Azure. Also, the insurance carrier wants to know what procedures you have in place for analyzing all of this information and data. Of course, doing this manually can take forever, but if you have a Cloud based deployment in Azure, you can make use of a SIEM (which is known as Microsoft Sentinel) which has AI built into it to automate the process of combing through all of these files and presenting those events which appear to be suspicious in nature. The main benefit of this is that all of this is presented into one central dashboard, for easy and quick viewing by your IT Security team. From here, any events can be triaged up for further analysis and investigation. An example of Sentinel is illustrated below:



(SOURCE: 5).

11) Backups:

In the days of On Prem infrastructures, tape backup was the norm, and in some cases, still continues to be so. But these can take time to deploy properly, adding more to administrative headaches. Because of the increase in Ransomware attacks and the increasing trend of not paying the ransom, the backups that you have in place and how you maintain them will come under heavy scrutinization as you apply for a Cyber Insurance Policy. Many insurance carriers are now refusing to pay claims if any form of payment was made to the Cyberattacker. Therefore, it is in your best interest to have the best backup strategies in place. If you are using Azure, this is not a problem whatsoever. You have many tools at your disposal to create your backup plans, and even automate them so that you will not forget about it. As an extreme form of backup, you can even deploy your Cloud platforms across datacenters all over the world for extra redundancy. That way if one fails, you can roll over to a new one in just a matter of seconds so that there is no interruption that could potentially occur.

Conclusions

Even thought applying for a good Cyber Insurance Policy may now be harder than ever before, a lot of these tasks detailed in this whitepaper can be simplified by making the full move to Microsoft Azure. If you need help with this, contact us today.

Sources

1) https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/app-service-web-app/app-monitoring
2) https://news.sophos.com/en-us/2020/07/30/protecting-the-cloud-securing-user-remote-access-to-azure/
3) https://docs.microsoft.com/en-us/azure/firewall/overview
4) https://www.microsoft.com/en-us/security/business/microsoft-endpoint-manager
5) https://www.microsoft.com/en-us/insidetrack/moving-to-next-generation-siem-with-azure-sentinel