LMNTRIX

BE THE HUNTER | NOT THE PREY

BUSINESS HEADS IN THE SECURITY CLOUDS:

A Summary of the Unique Security Challenges Enterprises face while moving to the Cloud

Introduction

For many enterprises, the migration and adoption of cloud platforms were already underway before 2020 started. As soon as many governments started instituting lockdowns and travel bans in an effort to curb the COVID-19 pandemic. As businesses looked for ways to try and mitigate the devastating financial effect of the pandemic they saw Cloud solutions as potential hedges against financial loss and improving workflow. This led to the rapid adoption of cloud solutions be they provided from a third-party or looking to develop a private cloud.

The security risks posed to the rapid adoption of other technologies that help facilitate remote working, like video conferencing, has been well-documented with not only the InfoSec community and related publications dedicating time to highlighting security concerns but also large media outlets. What did not receive as much attention were the security concerns relating to the adoption of cloud solutions be they for storage or improved workflow purposes. Before these concerns are discussed it is necessary to look at why security concerns have arisen in the first place.

The Rise and Rise of Cloud Computing

Older research conduct by Gartner estimated that enterprises will adopt cloud policies, be they cloud-first or cloud-only, as a matter of policy by 2020. Given the experiences of many industries in the first quarter of 2020, it would seem that those original estimates have been exceeded due to the current trend of migrating to cloud solutions as well as external factors, like the above-mentioned pandemic, forcing organizations to adopt cloud solutions. More recent research conducted by IDC estimates that by 2021 more than half of the enterprise IT infrastructure will be cloud-based. Given current realities, this estimated appears to be on the nose concerning current trends.

This radical shift from what can now be considered traditional IT infrastructure to one that is cloud-based has many advantages for enterprises. A treasure trove of research already proves this assumption. While enterprises scramble to migrate it is often the cybersecurity policies that are ignored in the drive to improve workflow, collaboration, and ultimately improve profits in future endeavors. While the security policies have been ignored threats to cloud infrastructure have risen along with its adoption. Many of the legacy security solutions enterprises have come to rely on simply cannot adequately protect the infrastructure they were tasked to. The main reason for this is visibility, legacy products are simply not capable of monitoring activity and behavior once the infrastructure is migrated to the cloud.

Securing the Non-Traditional

As cloud migration has caused a shift in how enterprises approach business it has also caused a shift in how cybersecurity should be approached. The rest of this whitepaper is dedicated to how that shift in mindset regarding security is to be approached. Along with security threats posed, security vendors have advertised products supposedly specifically designed to secure cloud networks and migration, however, in many cases this was just a rebranding of legacy products with little or no development regarding the securing of enterprise cloud assets.

Evaluating Needs

One of the lessons learnt by many enterprises regarding cloud migration is that it is definitely not a one size fits all scenario. Neither is the security solution needed to ensure migration and the future daily operations involving cloud assets. This requires a thorough evaluation of the current needs and those of the future.

No matter how far along with the enterprise in question with their cloud migration plans or even what type of cloud, be it private, public, or hybrid, the security needs are to be tailored to that organization. Below are some of the common security issues encountered by the type of cloud the enterprise has chosen.

Private, Public, and Hybrid Security Concerns

Looking at each type of cloud in turn in this context to help familiarize organizational leaders with certain security concerns that have found to affect certain cloud types. This is by no means an exhaustive list, there is already a mass of academic material available that does a deep dive on very specific concerns, but rather to prove the point that no matter the type of cloud security issues exist and these need to be considered when migrating and managing the risk associated with the type of cloud in future.

Private

With organizations that have either implemented or on their way to implementing a private cloud, there is sometimes a miss conception that now their data is completely secure. The reality is that private clouds are still susceptible to data breaches. Such breaches may be a result of employees acting as an insider threat but the data stored in the private cloud is not completely safe. This misconception is a result of organizations that implement private clouds that are just as likely to implement strong security controls to go with it. To that extent, the organization will likely hire a third-party provider capable of dedicating a lot more resources to manage what they have been entrusted with.

Other unique security issues that arise with private clouds include compliance issues and physical security concerns. Data centers will have security cameras and other physical security barriers that make unauthorized entry incredibly difficult. Further, they have several redundancy measures in the event something was to take down one location, another will then handle the redirected traffic so that clients can still bring their business to the enterprise. Private clouds will not have the same physical measures as a data center. In turn, migrating to a private cloud requires leaders to acknowledge that data stored still needs to comply with the various laws instituted to ensure compliance be it GDPR, PCI DDS, or HIPAA to name a few.

Public

Like with private clouds, public clouds also suffer from misconceptions, the prime suspect of which is that they are insecure when compared to private clouds. However, there is more myth than fact to this as all clouds are vulnerable under the right conditions. The myth was spread by unscrupulous vendors looking to sell the idea of a private cloud to enterprises which in turn would net a vendor more profit as private clouds require a greater investment. When all is considered public clouds are often hardened due to the number of hacking attempts they experience and public clouds are managed by tech giants capable of recruiting better security minds than an enterprise simply looking to shore up their defenses.

That does not mean public clouds are immune, there are several concerns that need to be addressed primarily of which is shred access. As public clouds offer their services to a wide range of unrelated clients, all of which share the computing resources a number of unique problems can arise. This reality is sometimes referred to as multitenancy and can result in the accidental leak of data from one unrelated customer to another. Further, what could be done accidentally could be weaponized via a known cloud software flaw allowing hackers to access data across the customers and the cloud.

Hybrid

Often for companies in the process of migrating or have invested heavily in a physical data center and have strict compliance requirements often the best approach is to adopt a hybrid of cloud and existing infrastructure. As more enterprises move towards looking to improve workflow and project collaboration, cloud solutions are attractive but they cannot move completely away from their physical infrastructure.

This presents a problem regarding the transfer of data between the physical and the cloud solution. If data is not properly encrypted or company policy does dictate this as a requirement an attacker may be overwhelmed with the amount of sensitive data at their disposal. Stolen data can then be sold on the dark web or several other uses can be found for the information contained within the data. Access management is another area that needs to be carefully considered. Allowing the entire organization privileges normally reserved for admins is asking for trouble. Restricting access needs to implement for both the physical infrastructure and the cloud solution chosen.

Other Concerns

Numerous research papers and articles across the internet have been dedicated to unraveling the security issues moving to the cloud may involve. Be they cloud-specific or simply generic concerns there are a whole host of them and taken individually could fill textbooks themselves. No matter which cloud type is chosen there are several other concerns that influence the entire decision-making process, that being the hiring of security professionals.

Hiring talent is always a massive undertaking to ensure the success of the business. When it comes to hiring security professionals this is doubly so. First of all, a budget is needed to dedicate to bringing on new employees which will typically exclude a majority of SMEs. If the budget is in place the next hurdle presents itself, that being the massive shortage globally of security professionals. By 2020 this skills shortage gap is estimated to reach 1.8 million, this will place a greater demand on an already strained workforce. The other side of the coin is that it will be harder and harder to source the right person for the job of securing cloud migration and other operations. For companies they will need to compete with organizations that specialize in this to that extent outsourcing cloud security has become an attractive option and one that can reap the rewards of a secure cloud platform as long as the right partner is chosen. This will be dealt with in detail in the next section.

It should also be noted that cloud security is not only needed for the initial migration but is a constant requirement. As the threat landscape changes with the adoption of newer technologies, so too does the securing of the implemented cloud platform. Security, and cybersecurity, as a whole is a constant affair that requires the right technology and the right people being on constant alert. Modern threats are best defended against by actively hunting and seeking out the threat before it happens, rather than waiting for an attack to respond. Security considerations regarding cloud implementation extend far beyond when the migration phase is completed.

Necessary Requirements

It is clear, like with all adoption of new technology, security cannot be overlooked nor any assumptions made. Whether the enterprise is looking to create and staff its own cloud security solution or bring in a third party with the required knowledge and expertise the enterprise needs to understand what is required. Defining your specific requirements is a must in preventing future heartache.

Defining Requirements

There are six major requirements that need to be clearly defined when looking at implementing a cloud security solution that best fits the enterprise's needs. These six not only look at addressing the current threat landscape but look to provide a level of future-proofing that will shore up future threats.

These are not the only six requirements as different enterprises will need a tailored solution depending on how far cloud migrations are and whether the enterprise is adopting a cloud-first or cloud-only policy moving forward. That being said if the following requirements are adhered too the enterprise is well on its way to securing its chosen cloud platform. The requirements include:

- Elasticity and Scalability: A key to any successful cloud migration and security solution is whether it can grow with your business. Not only does it need to grow with your business but the growth should not lag behind, which in turn can leave several security vulnerabilities while the solution catches up.
- Automation: Humans and by default, an organization's employees are not the best at doing mundane tasks from sun up to sun down. Having staff complete security tasks that can be automated should be avoided, thus automating the mundane is an important aspect to consider.
- API Compatibility: This requirement looks at how readily or easily APIs can be adopted into the current security stack in order to improve current capabilities and user experience. A good API can provide a well of information for analysis that can mean the difference between an attack prevented and becoming a victim of a potential threat.
- Intelligent Information: Fundamentally this comes down to whether the information provided by the security stack enables security analysts the ability to act effectively when a threat emerges. Ideally, the information provided by the security stack is readily interpretable and can be placed in graphing tools for a quick visual representation of the current situation.
- Proactive Detection: Having the right security professionals and technology can be meaningless if threat detection is not proactive. Today and more so in the future, security solutions need to adopt a hunting methodology by actively looking for threats and then acting accordingly. By waiting for an attack to occur the organization could be placed on the back foot incorrectly responding to the threat even before it has had a chance to occur.
- Ease of Use: An often overlooked factor but one that is most definitely worth considering. The less time spent by staff and security professionals learning new applications to the security stack the better. This frees up time to pivot between various data streams and make informed decisions regarding the hygiene of the cloud solution in general.

While some of these requirements have been true for several years, with companies migrating to the cloud they have gotten new meaning to adapt to this new reality. All too often we have seen legacy security solutions been offered as robust solutions capable of securing an organization's cloud but more often than not these do not offer anywhere close to the level of protection needed. Not only do they lack the necessary technology but this leads to a lack of visibility on both the cloud perimeter and within the cloud, meaning that cloud-specific attacks cannot effectively be defended against.

Any modern and truly cloud-capable solution will need to provide this level of visibility. Not only this but still work seamlessly with business applications and other products that have been added to the current security stack if that is needed. In providing proof as to why legacy products no longer can provide the necessary level of protection an organization migrating to, or fully migrated to, the cloud needs, we simply need to look at how alert fatigue is impacting the cybersecurity industry as a whole.

Alert Fatigue

In 2019, a report into the effects of alert fatigue published the following key findings:

70% of security professionals investigate more than ten alerts every day.	**78%** said that it takes over 10 minutes to look into each alert.	Almost half of the respondents reported that **50%** or higher alerts are false positives.	**35%** said their SOC (Security Operation Centre) has either tried to increase staff by hiring more analysts or turned off high-volume alerting features.

In an earlier report, dating back to 2017 it was revealed that on average an enterprise using cloud services generated 2.7 billion false positives during the time period covered by the report. Of that staggering number, only some 2,500 could be considered out of the ordinary and worth investigation. This number was generated retroactively meaning that at the time many of the alerts that constituted false positives were investigated wasting time and prevent analysts from doing other, potentially more productive tasks. Further, of those out of the ordinary alerts, only 23 could be considered a threat. This reality led to 32% of the survey's respondents saying they ignore alerts in their entirety.

All these stats serve to highlight the importance of having a modern solution with the correct level of visibility so as not to fatigue analysts. An efficient solution with correct cloud visibility should be a support structure on which analysts and network admins can rely upon to prevent attacks, rather than creating more misery and opening up the potential for an attacker to slip by the noise created by mass false positives.

In order to correct this the solution chosen needs to tick the following boxes:

- The technology adopted will need to correlate suspicious activity along with security events past and present to generate a map of the threats faced by the organization.

- It needs to minimise dependency on signature-based solutions and maximise the use of signatureless solutions across both endpoint and network.

- It needs to be focused on detecting threats that bypass perimeter controls as opposed to alerting on every single packet. It needs to rely on high level of signal fidelity (EDR, PCAP, Log, Vulnerability etc.)

- It needs to use multiple detection methods including anomaly detection, sandboxing, adversary hunting, retrospection, adaptive response, deceptions, and most importantly it needs to be intelligence-led.

- It needs to provide visibility and detection for any cloud environment that holds critical data, this includes containers and container-orchestration systems, operating system security/audit events, application related events, system related events, and database related events.

- It would need to incorporate the latest in machine learning technology so as to remove the human error aspect as much as possible. Machine learning can also be implemented to develop a tailored cloud security policy for the organization as it can take into account client and staff behavior over time reducing false positives.

- It needs to minimise dependency on logs and legacy SIEM and deliver zero false positives and zero alert fatigue.

- The technology implemented needs to provide full telemetry regardless of deployment model and provide pervasive visibility of the cloud even if the organization makes use of public clouds.

- Lastly, it needs to provide full IR lifecycle support, managed remote threat containment for cloud/onsite/OT, validation, full forensics, and automated containment of known threats.

Intrusion Detection and Response

Many legacy products apply traditional Intrusion Detection Systems (IDS) that were developed around on-site networks and assumed that these were self-contained systems. For modern organizations this is not the current reality, it can be argued that since organizations needed to be connected to the wider Internet this hasn't been the reality for some time. Now businesses from small to medium enterprises to the largest multi-national corporations can have private and public clouds used to improve workflow. This is particularly true given the current COVID-19 pandemic that forced workplaces to adopt cloud-based remote working tools. Another reality faced by many organizations is the complexity of their network, which includes traditional on-site networks, clouds, and in some cases industrial control systems. All this has added complexity to traditional IDS solutions, complexity it was never meant to deal with.

This has the practical effect is making detection far harder as the initial system put in place cannot hope to cover all the ground a modern network presents. Attacks are now harder to detect by traditional IDS and attacks have further evolved to take advantage of these gaps in security by targeting cloud-based applications or industrial control systems. While detection has been made an issue as technology has evolved, legacy products with traditional IDS have another problem and that is the amount and type of information collected in the event it does detect a threat. Typically, legacy products will collect a packet of information when a detection rule is triggered. This packet of information is treated in isolation, meaning it lacks other information which can create an idea of what came before and after the intrusion. When the forensic analysis is required, analysts are presented with only part of the picture. This makes preventing similar attacks in the future all but impossible.

Our Technology Stack

In the previous section, some of the problems facing legacy software products were highlighted, this section shows how LMNTRIX adopts several proprietary forward-thinking technologies into a three-tier system to prevent those issues from cropping up. By applying our three-tiered system we have created a comprehensive solution that addresses all the modern needs of an organization in the process of migrating to the cloud in whatever form that is chosen. The three tiers that make up our approach are LMNTRIX Grid, our onsite technology stack, and our 24/7 Cyber Defence Centre.

LMNTRIX Grid

The Grid can be summarised as a cloud-based platform specifically designed and developed to increase visibility throughout the organization, including pervasive cloud visibility. One of the Grid's key features is the ability to provide chronological order to attacks whether they come from automated detection methods, attacker baiting, or attacker hunting methods. In order to do this with any kind of efficiency, we needed to create a system that not just detects threats but can predict and respond to threats in whatever form found on the current threat landscape. To help organizations map out such a landscape Grid includes advanced security visualizations for better threat intelligence interpretation and overall improved security policies moving forward.

Built on that foundation a solution was developed that is capable of integrating a variety of data streams and then sharing it to analysts and stakeholders at the same time creating a unified information system. This promotes an adaptive solution capable of combatting the most well-resourced cybercriminal gangs and state-sponsored groups, which are combatted via the constant exchange of actionable information. For many legacy products offered as a Software-as-a-Service (SaaS) package, this is not possible let alone be able to provide threat intelligence on threats targeting enterprise and cloud-based applications as well as industrial control systems. Due to the Grid's cloud-based nature, it is also scalable with the organization.

Technology Stack

The Grid, a technological feat in its own right, overlays our technology stack which is deployed on-site and within your cloud environment behind your existing controls. The need for the stack centers on the reality many organizations face with poorly configured prevention and detection solutions, firewalls, and badly configured internet-facing ports. All of which result in increased false positives and a waste of resources. To combat this we developed a proprietary technology stack which results in no reliance by LMNTRIX on pre-existing security controls the organization already has. In this regard our technology stack allows analysts to focus on current threats and even hunt threats before they have a chance to strike.

Both the Grid and our proprietary technology stack were developed with modern realities firmly at the forefront of our design philosophy. This means that the detection of threats is not limited to an organization's on-site and physical network as we assume those are breached. Our innovative approach has enabled us to detect and act against threats in the cloud, targeting industrial control systems, and attacks on traditional networks.

Cyber Defence Centre

Our cyber defense center serves as the foundation for our stack and Grid, put differently it is the bedrock that allows us to not only defend against threats but actively seek them out and neutralize them. To do this we ensure they are staffed by certified intrusion specialists and are available 24/7. Further, we always look to improve our proprietary methodologies that encompass our threat intelligence and subsequent response. Combined with our visibility over an organization's entire network, we perform in-depth analysis and respond to threats in unique and effective ways as we understand that cyber threats are not bound by conventional rules. For example, if the threat is capable of spreading laterally across a network, as many threats are capable of as we have seen a resurgence in worm-like malware functions, we will move rapidly to quarantine hosts, both on the network or not.

Combined in Practise

The next question is then, how do these three layers combine in order to prevent the failings of legacy software products and provide a layer of security necessary during and after cloud migration. For the issue of alert fatigue, often organizations are presented with the need for a SIEM, or to give it it’s less jargon-filled name, a Security Information and Event Management System. The problem is that even if properly configured they traditionally generate too many alerts to be investigated. A SIEM is a handy tool for log recording and can be what an organization needs for compliance but given the tidal wave of alerts, they cannot be relied upon.

To combat this the three layers mentioned above are combined with what we term Active Defense. We assume that a breach has already occurred of either the cloud or the network at large. This allows us to turn our gaze inward and adopt an adversarial pursuit methodology involving threat hunting and continuous response – not incident response. This methodology is gone into greater detail in the concluding section of this whitepaper. In summary, it is our unique combination of relevant technology and our hunter methodology that creates a holistic security solution with a great emphasis on protecting enterprise clouds no matter what type they are. For instance, many security products have their technology focussed on detecting outside threats, with little attention paid to insider threats. Such threats can be caused by disgruntled employees about to leave the company and willing to steal intellectual property for several malicious reasons. If the security product does not monitor employee behavior for irregularities and odd behavior, but merely log events these insider threats cannot be permitted. By combining technology and knowledge we have a view both inside and outside the business network, as well as the cloud.

Be the Hunter, not the Prey

One of our core philosophies is not to take a passive approach to combat threats, even those targeting or originating from the cloud. By being the hunter it means that we have to constantly be evolving to combat new threats. As soon as new technology reaches the market, as cloud-based solutions recently did, hackers will look to subvert the technology for their own gain. Unfortunately, this often means that a targeted organization will suffer financially, legally, and reputational damage is bound to follow. Actively hunting threats allows for the prevention of these nightmare scenarios playing out, and if they do the philosophy enables rapid action to contain and prevent lasting damage.

Automated Hunting

The reality is that legacy products cannot defend against sophisticated attacks, whether by nation-state threat actors or highly organized and experienced cybercriminal gangs. This is primarily because the technology has not evolved along with the threats. To combat stagnation on this scale we automated our threat hunting capability and focussed on being able to incorporate new hunting rules based on previous events. This effectively allows us to not only keep pace with current advanced threats but actively prevent a successful attack from occurring.

In order to do this and remain ahead of the curve, we utilize both our proprietary technology and intelligence-based off years of experience to hunt within the network and outside. For outside threat hunting we are willing to go where the cybercriminals go, the Dark Web, and underground hacker forums, to further advance our intelligence and see where hackers are looking to target next. This is then automated so that the active defense of your cloud never sleeps.

Partnering to Protect the Cloud

As has been shown legacy security products and SIEM offerings are ill-equipped to meet today's threats, even if not cloud-based or specifically targeting the cloud. Simply relying on new malware definitions to be defined, loaded, downloaded, and acted upon takes too long and results in compromised networks where hackers can roam freely. For security solutions that produce alerts and log them, alert fatigue will always be an issue that leaves openings for hackers to exploit.

Seeing this occur in the wild time after time meant a new solution that provides cloud visibility beyond logs was necessary, based on technology, that is cloud-based and scalable and supplemented by threat intelligence that could be quickly implemented into automated hunting protocols, needed to be developed. At LMNTRIX we believe we have done exactly that.