Global Threat Intelligence Center

Monthly Threat Report

February 2022

Contents

Cloud security posture management

Lead Analyst: Nicolas Blot, Cloud Security, European Practice Manager, CISM, Europe

Gartner predicts that by 2025, 99% of cloud security failures will be the client's fault. Cloud security posture management is increasingly important, as is a clear understanding of the Shared Responsibility Model to mitigate the cybersecurity risks of cloud computing.

According to PwC's 2022 Global Digital Trust Insights Survey, business leaders are beginning to create a blueprint for the securable enterprise. Throughout the pandemic, the cloud has become a 'must-have,' not just a 'nice-to-have,' and we expect cloud security posture management to follow the same trajectory. We expect to see this evolution as more business-critical and sensitive data becomes stored in the cloud – while in parallel, organizations look to reduce the business and operational risk of a breach to their business.

What is cloud security posture management?

Cloud security posture management (CSPM) allows for the more seamless management of cloud security. CSPM is a relatively new class of tools, but as businesses increase the use of the cloud and continuously adjust the make-up and mixture of cloud services they consume, CSPMs help to ensure you:

- have visibility across your cloud assets
- can configure your cloud infrastructure correctly and consistently
- can manage user access rights and entitlements with ease
- can respond and remediate any issues as quickly as possible (often as an automated process)
- can evaluate the effectiveness of your security, benchmarked against key industry standards
- are meeting your data security obligations
- can generate consolidated operational and business reports

As business consumption of cloud services scales across one or more providers, CSPM tools offer the means to improve threat/risk visibility, reduce complexity, minimize the risk of breach due to misconfigurations and provide the means to evaluate and demonstrate the effectiveness of your security and data privacy efforts.

CSPM tools offer the means to **improve threat/risk visibility, reduce complexity, minimize the risk of breach due to misconfigurations**

Cloud security: whose responsibility is it?

To fully realize the benefits of a CSPM, it's fundamental that businesses understand the Shared Responsibility Model (SRM). In short, SRM refers to the fact that cloud security providers (CSPs) and cloud service customers have distinct responsibilities to ensure the cloud is secure.

Figure 1 shows a framework created by the Cloud Security Alliances that demarcates the security duties between cloud providers and the consumers or the application owners. In most cases, the cloud provider is responsible for the security of the underlying cloud infrastructure, and the client is responsible for securing the workloads that run on said infrastructure. It's always the client's responsibility to ensure their applications and data remain secure and compliant – the Shared Responsibility Model helps to make that clear.

Shared responsibility model

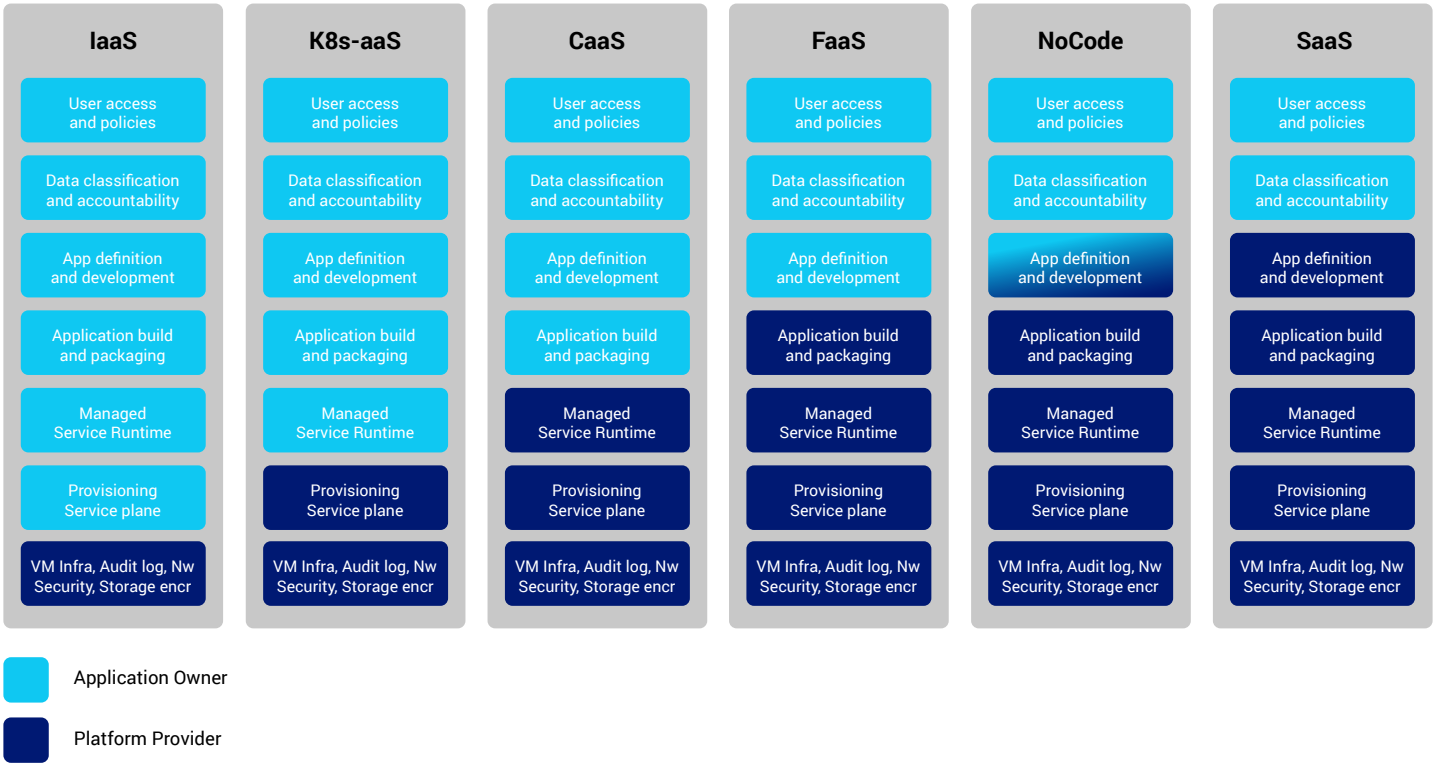

Figure 1: Cloud Security Alliance's Shared Responsibility Model

This is a useful high-level framework for understanding and learning about the division of responsibility. It's also critical to validate this framework against those provided by the Service Providers themselves.

Amazon Web Services, Microsoft Azure, Google Cloud Platform and other providers have clearly defined their views on the Shared Responsibility Model. There are subtle but critical differences between them all. Public cloud providers have no choice but to take their security and compliance responsibilities seriously. Still, they need to draw a line over how far it is reasonable for them to go to perform basic security functions, monitor and ensure compliance on behalf of their service consumers. This makes sense as CSPs can't control everything users do in their cloud. But likewise, users can't expect to control the security across the CSPs servers and networks. The SRM helps to ensure that both parties are aware of the rules and take ownership for securing the resources they control.

Unfortunately, the Shared Responsibility Model is not well understood and studied by businesses – consumers of cloud services. CSPs understand the SRM better. Hence Gartner's bold predictions about where the fault for breaches will lie in 2025. It can be confusing, but the SRM helps understand shared responsibility since it varies across IaaS, SaaS and PaaS, which are different, as shown in Figure 1.

Clear, understood, and well-defined roles on security are critical to security risk management in any enterprise. Cloud risk management may be even more critical to the success of the business blueprint. Having a clear understanding of the Shared Responsibility Model will also help ensure that there's less finger-pointing in the event of a breach. More importantly, it can ensure there is good security in place across the entire threat surface, cloud environment and local data security obligations.

The role of CSPM in the future – asks of industry

CSPM helps to ensure visibility across assets as well as security tools and controls, and that both parties are holding up their part of the shared responsibility.

There are many third-party providers offering CSPM tools today. Still, there is tremendous potential for innovation, especially in CSPM-as-a-Service that can provide integrated visibility across multiple major cloud service providers to truly deliver on the promise of reducing complexity.

It would also be tremendously valuable for CSPM vendors to invest in and enrich their identity protection and monitoring capabilities. User access entitlements and permissions in the cloud are increasingly broad and detailed, and traditional Identity and Access Management tools struggle to keep up with the complexity. Businesses would greatly benefit from Cloud Infrastructure Entitlement Management (CIEM) as a 'specialized identity-centric solution' as part of their CSPM solution. CIEMs can inventory your people and non-people identities, determine what they can and can't access, as well as what they have permissions to do with that data. But the real value is that they can do it at the scale, speed, granularity and agility of the dynamic multi and hybrid environments that businesses operate in today.

Summary

The importance of CSPM will only increase in coming years as businesses move towards increasingly cloud-based, identity-driven and data-centric approaches that support remote working, adopt zero-trust and SASE models. The greatest cybersecurity risk to businesses remains lack of visibility, and CSPMs are promising a front-row seat.

Window of Exposure – a powerful lens for application security risks

Lead Analyst: Zach Jones, Sr. Director Detection Research, NTT Application Security, US

Since 2006, NTT Application Security (formerly WhiteHat Security) has collected and published statistical data and analysis gathered from continuously updated security testing information in our Sentinel Dynamic.

Dynamic Application Security Testing is an essential part of any application security program. Organizations can view their websites from an attacker's perspective by testing running applications in production and pre-production environments. Similarly, by viewing several indicators at a global or industry level, we can gain insight into the risks currently facing organizations developing and operating internet or intranet-facing web applications.

We track the aggregate Window of Exposure (WoE) as a key metric to help contextualize an organization's discovered application security risks. We express WoE in terms of the percentage of sites whose individual Window of Exposure (counted in days) falls within one of five buckets. That is, for each site, for each of the last 365 days, we ask, 'on this day, was the site exposed to a high or critical risk vulnerability?' We then count all the days where the answer was 'yes'. This is the individual site's WoE. Each site's WoE is associated with one of the five buckets: 0-30, 31-150, 151-270, 271-364, or 365 (always) days. To view the overall picture, and allow for comparison between groupings, we then express the number of sites that fall in each bucket as a percentage of total sites (for industry, organization, technology stack, etc.).

We've chronicled this statistic in a podcast and report series titled the NTT Application Security AppSec Stats Flash. The data is valuable when understanding the application security risks and efforts across our diverse client base. The numbers for 2021 and the last two decades remain a sobering reminder of the scale of challenges faced by many applications security teams. These are teams trying to improve the security of tens, hundreds, and thousands of applications across various architectural, infrastructural, and even millennia of origin. While there are significant differences in Window of Exposure outcomes across industries, the overall results show that 50% of applications were vulnerable to one serious exploitable vulnerability every day throughout the year. In contrast, only 27% of applications were vulnerable to one serious exploitable vulnerability every 30 days or less. This tells us that attackers continue to be in a target-rich environment.

Even the best-performing industries have significant percentages of their web applications vulnerable throughout the year. This fact is perhaps unsurprising in light of the continued pace of application attacks and breaches we see publicly reported. It is, however, more than that, as the high individual Window of Exposure (WoE) is a significant driving factor. Let's consider how a site's WoE affects an attacker. When the WoE is high, attackers can be more confident that efforts to enumerate attack surface, conduct vulnerability discovery, and develop an exploit will pay off. This ultimately means they have a greater chance to find and exploit a vulnerability that can result in compromise. However, when WoE is low, the same attacker's efforts are more likely to be 'wasted' by mitigation or remediation efforts, meaning the attacker will have a harder time isolating a vulnerability they can successfully exploit.

> A high or critical risk vulnerability, is one, that if exploited, could lead directly to the **attacker gaining control of that system, or to the direct exfiltration of internal information.**

This gives us another perspective on the reported 50% of sites falling into the 'always' vulnerable category. As an attacker, it won't take many sites before I find a vulnerable one. Once I've found even a small sample of vulnerable sites, at least half of my sample will likely continue to be vulnerable throughout the year. This is also reflective of the attacker's return on investment – a high WoE means an attacker can afford to hoard a host of vulnerability and associated exploits. At the same time, their urgency to attack is low. Yet, for a lower WoE, attackers could be driven to use exploits more quickly, before the organization has taken steps to mitigate known vulnerabilities in their environment.

While the risks are real and concerning, it's not all bad news. Organizations who track their own WoE, both in aggregate and per site, can be armed with real information about the risk profile of their assets and take proactive action to drive down that risk profile in a meaningful way. The Window of Exposure provides a powerful two-sided lens for quantifying application security risk that will focus attention on other key metrics surrounding vulnerability remediation like time-to-tix and remediation rate. We share such metrics in per-industry detail in our Global Threat Intelligence Report and the AppSec Stats Flash monthly report series. We recommend that organizations consider adopting some measure of Window of Exposure to quantify and reduce their application security risks.

Domain controller attacks – insight into recent attack surfaces

Lead Analyst: Ganesh Kumar Varadarajan, Principal Consultant, Australia

Over the past year, we've observed an increase in attacks targeting Windows Active Directory. Some of these attacks are SAM Account Name Spoofing, Shadow Coerce, Hive Nightmare, Remote Potato, Certificate services abuse, to name a few. This article will discuss how attackers conduct SAM Account Name Spoofing and ways to detect such attacks.

SAM account name spoofing

This spoofing vulnerability includes weaponization of exploits targeting CVEs 2021-42287 and CVE-2021-42278 released by Microsoft. An insider can elevate the credentials of a standard user to a domain admin by exploiting a combination of the two CVEs. The attack starts with the attacker editing the SAM account name of a standard user account to that of a Domain Controller account. A SAM Account Name is an Active Directory attribute set with a $ for a machine account.

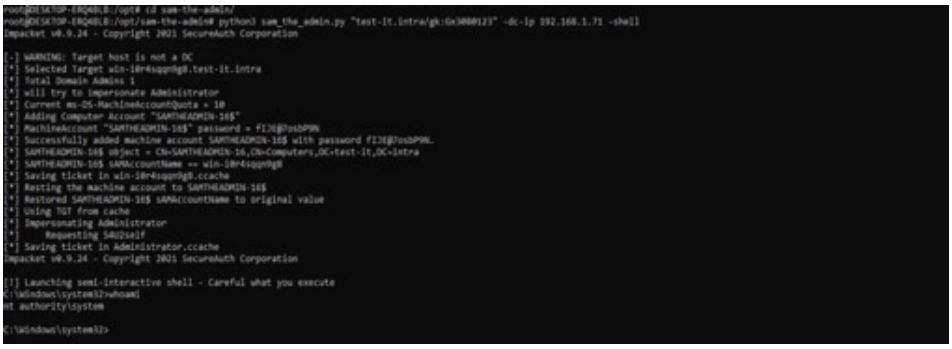

Figure 1:

For example, let's assume that DC01 is the Domain Controller's name, and user01 is the name of the attacker's account. In the Active Directory, the SAM Account Name attribute toDC01 is represented by DC01. The attacker will change the SAM Account Name user01 to DC01 by exploiting CVE 2021-42287. Next, the attacker would request a ticket-granting ticket (TGT) with the spoofed SAM Account Name DC01. The attacker would then reset the SAM Account Name to his original name other than the Domain Controller (user01). The attacker then requests a Service Ticket by user01 with the TGT obtained earlier. The Active Directory provides the service ticket for the Domain Controller using the Domain Controller machine credentials (because of CVE -2021-42278).

By chaining multiple vulnerabilities, the elevation of user credentials to a domain admin is not only possible, but practical. An attacker can also automate the attack so that a single python script can execute this attack from a non-domain joined machine. Figure 1 shows the attack from a machine not in the domain, executing the attack with standard user credentials which they have elevated to that of a domain admin account with SYSTEM credentials.

Of course, the best method to mitigate the vulnerabilities is to patch the system with the latest updates. In practice, that often does not take place in time for many environments.

Detection methods

The steps required for exploitation requires a specific sequence of SAM account changes followed by Kerberos ticket request and service ticket changes. These are typically seen in the Windows Security Event Log. Specifically, these show as event IDs 4781, 4769 and 4768. These IDs can be used for detection as documented in URL [Hunting for samAccountName Spoofing (CVE-2021–42278) & Domain Controller Impersonation (CVE-2021–42287) | by Mauricio Velazco | Dec, 2021 | Medium]

Other methods, such as looking at Active Directory objects, can provide a clue that an attacker has registered new workstations, as shown in Figure 2.

A dedicated attacker would try to clean up after the fact and delete these workstations, but such extra domain accounts are visible until then. A mature SOC could detect these by observing the creation and deletion of workstations within a short time interval.

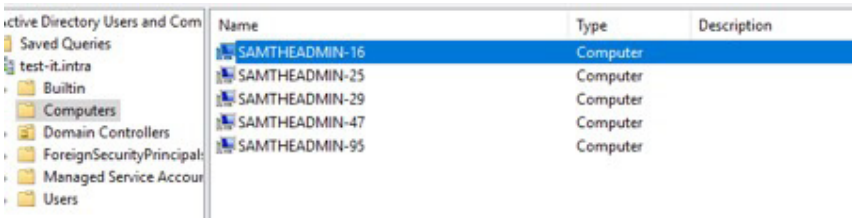

Figure 2: Sample Active Directory Objects

Summary

Attacker tactics and techniques tend to evolve rather quickly. The next generation of malware and ransomware will likely start using such chained exploits to cause mayhem in the enterprise. We already know that the Log4Shell issue was serious. Globally, there are still many systems still vulnerable to Log4Shell. This is just one vulnerability, but by chaining multiple exploits, it may be possible for an attacker to construct a payload that results in a total compromise of the target's active directory. We highly recommend that organizations prioritize patch management and that vulnerabilities are remediated regularly and proactively, rather than waiting for scheduled future change windows.

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs, and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2021 Global Threat Intelligence Report

Our 2021 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month. Sign up for our **Emerging Threat Advisory** and security bulletins for visibility of emerging threats and vulnerabilities that are being actively exploited across the world, sourced from our global threat intelligence platforms.


NTT