UNIT 42

5 KEY CLOUD SECURITY TRENDS

Plus Best Practices to Help Your Organization Reduce Risk in the Cloud

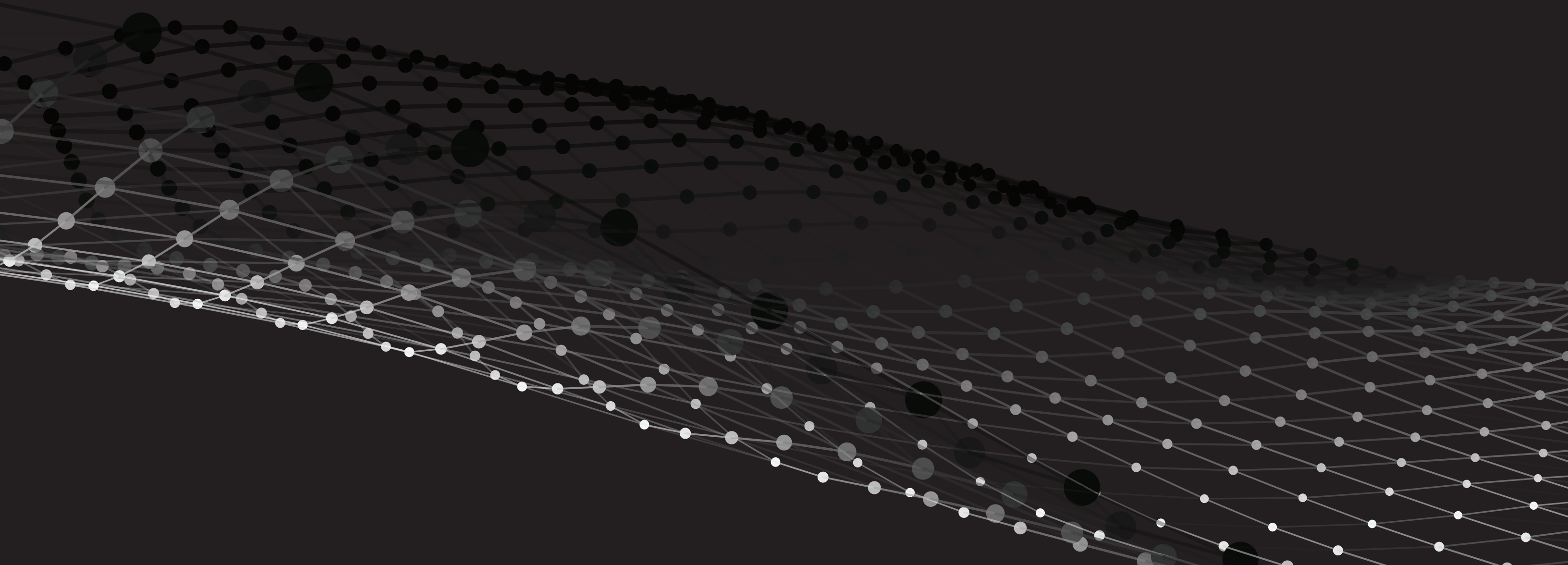


TABLE OF CONTENTS

Introduction 3

Key Trends and Takeaways 4

Account Compromises: Increasing in Scale and Velocity 5

Cryptojacking: Cooling Trend Ahead in the Cloud 6

Compliance: A Work in Progress 8

Vulnerability Management: A Silver Lining in the Cloud 9

Managed Container Services: Security 101 10

Introduction

The Shared Responsibility Model of cloud security clearly outlines the respective responsibilities of cloud service providers and their customers (see Figure 1). Providers of cloud services, such as Amazon Web Services (AWS®), Microsoft Azure®, and Google Cloud Platform (GCP™), are responsible for protecting the infrastructure that runs all the services offered in the cloud. Meanwhile, the customer's obligations in the Shared Responsibility Model include monitoring for risky configurations, anomalous user activities, suspicious network traffic, and host vulnerabilities.

Over just four months in mid-2018, there were multiple high-profile breaches involving public cloud environments. It is important to note that none of these were due to negligence on the part of the cloud service providers. This report highlights key takeaways from these incidents, along with research by the cloud-focused division of Palo Alto Networks Unit 42 threat research team, to shed light on current and emerging trends.

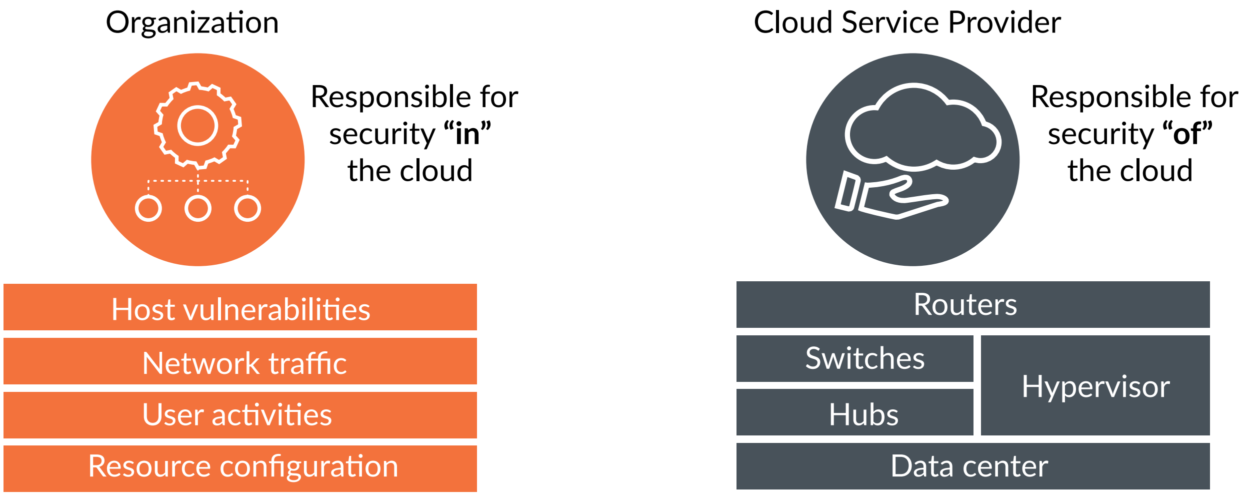


Figure 1: Shared Responsibility Model

Key Trends and Takeaways

Account compromises

29%

of organizations experienced potential account compromises

Crypto-jacking

11%

of organizations had cryptojacking activity within their public cloud environments

Risky configurations

32%

of organizations publicly exposed at least one cloud storage service

Host vulnerabilities

23%

of organizations have hosts missing critical patches in the cloud

Container security

46%

of organizations accept traffic to Kubernetes pods from any source

Account Compromises: Increasing in Scale and Velocity

Credential compromises are becoming increasingly common, and organizations need to enforce strong governance and access hygiene. Operating under the assumption that account compromises are inevitable, organizations also need to implement monitoring to detect and rapidly respond to suspicious user activities.

Cryptojacking: Cooling Trend Ahead in the Cloud

The diminishing value of cryptocurrencies, combined with better detection capabilities, is leading to fewer cryptojacking attacks in the cloud. Organizations have an opportunity to get ahead and implement the necessary countermeasures before the next wave of attacks.

Compliance: A Work in Progress

Risky resource configurations are the root causes of many high-profile breaches. A slowing trend in exposure of public cloud storage services suggests organizations are implementing countermeasures to address this issue, but they still have a long way to go to achieve comprehensive compliance and governance across their public cloud environments.

Vulnerability Management: A Silver Lining in the Cloud

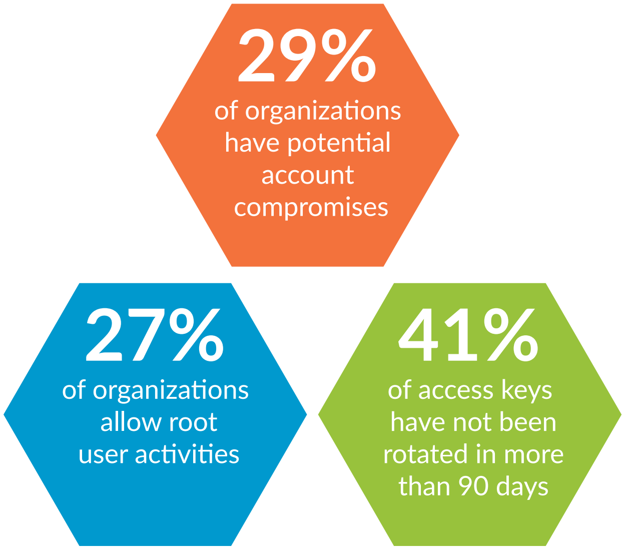
Organizations operating in public cloud environments have an extreme advantage over their on-premises peers when it comes to vulnerability management. Cloud service providers update their infrastructure and services, providing an initial line of defense. Organizations also need to do their part by identifying and patching vulnerable hosts. Unfortunately, they are unable to use their standalone vulnerability-scanning tools to achieve this because these tools were not designed for cloud architectures.

Managed Container Services: Security 101

Managed container services in the cloud are rapidly growing in popularity because they make it easy for developers to deploy, manage, and scale containerized applications. However, basic security hygiene is not being observed, which makes the Kubernetes pods vulnerable to attack.

Account Compromises: Increasing in Scale and Velocity

Although many organizations are still grappling with detecting risky configurations, such as publicly exposed cloud storage services, previous reports published by RedLock predicted that hackers are moving on to more advanced threat vectors, such as compromised account credentials. Recent analysis by Unit 42's cloud research team has determined that 29% of organizations have potential account compromises. Sure enough, since May 2018, we have seen multiple high-profile breaches resulting from this emerging threat vector.



29% of organizations have potential account compromises

27% of organizations allow root user activities

41% of access keys have not been rotated in more than 90 days

For instance, someone was able to compromise employee accounts of a popular online community at its cloud and source code hosting providers, leaving backups, source code, and various logs exposed. To its credit, the organization was enforcing multi-factor authentication (MFA) on its accounts, albeit the second factor used SMS, which is known to be vulnerable. Considering this, it is worrisome that the research indicates 20% of organizations do not enforce MFA for root users. This would be less of an issue if organizations followed well-established best practices that dictate the use of root accounts should be disallowed. However, the research also shows that 27% of organizations allow root user activities.

Unlike the breach described above, which was detected within days of the attack, some incidents take months to discover. Consider a breach that occurred in December 2017, in which an unauthorized user compromised an employee's credentials and logged in from an IP that resolved to the Netherlands. The unauthorized user went on to create an API access key on the employee's account, and then created a new user account, attached administrator access to that account, and created an API access key on that account as well. The unauthorized user performed reconnaissance over the next several months and ultimately siphoned off personally identifiable information, including access keys to social media sites. The day after the breach was discovered, the company that experienced the incident began enforcing MFA on all accounts.

Rotating access keys every 90 days is important because it reduces the window of exposure when credentials are compromised. However, our research reveals that 41% of access keys have not been rotated in more than 90 days. The research also indicates that 38% of user accounts are dormant, having seen no activity in more than 90 days. This is unsurprising as it is common for users to be granted access to an environment to perform specific tasks, only for the administrator to forget to revoke access once the tasks are completed.

The most important takeaway here is that organizations need to operate under the assumption that credentials will be compromised. For example, in June of 2018, another company suffered a breach because a Google Kubernetes® server was not password-protected, exposing an administrator's root credentials, access keys for 102 of the company's domains, and 31 IAM users—including users with administrative credentials—as well as applications with programmatic access. To identify and detect suspicious user activities that result from credential abuse, continuous monitoring must be in place.

Tips

1. Forbid the use of root accounts for day-to-day operations.
2. Enforce MFA on all privileged user accounts.
3. Implement a policy to automatically force periodic rotation of access keys.
4. Take advantage of machine learning to establish user and access key behavior baselines as well as monitor for deviations to detect account compromises or malicious insider activity.

Cryptojacking: Cooling Trend Ahead in the Cloud

It was in 2017 that Unit 42's cloud research team first started uncovering the latest emerging threat to public cloud environments: cryptojacking. Incidents at established organizations with mature cybersecurity programs illustrated that many organizations have yet to notice this threat.

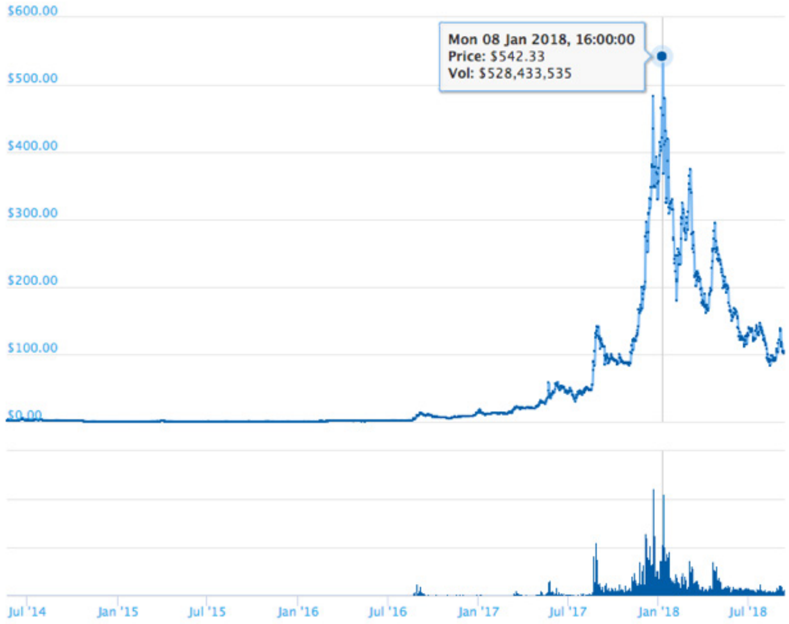


Figure 2: Monero cryptocurrency price spike (Source: CoinGecko)

The latest Unit 42 cloud research findings suggest that 11% of organizations have cryptojacking activity within their environments. Though this number is still significant, it is lower than previously reported (25% in May 2018). We believe this directly correlates with the falling prices of cryptocurrencies. The spikes in price in late 2017 and early 2018 caught the attention of hackers, who started scaling up attacks in early 2018. However, the price drop seen in the latter half of the year changed the economics of the attacks, making them less lucrative for hackers. Combined with greater awareness of the threat and better detection capabilities, this means hackers are being forced to consider alternate revenue opportunities.

11% of organizations have cryptojacking activity within their environments

26% of resources do not restrict outbound traffic at all

28% of databases receive inbound connections from the internet

Despite the pricing downturn, we do not anticipate cryptojacking attacks to cease entirely; future increases in prices will certainly lure attackers back. Until then, organizations have an opportunity to get ahead and implement countermeasures to address this threat.

Strong network configuration hygiene and network monitoring are imperative. Unfortunately, our research determined that 11% of resources accept traffic from any public IP address on any port. Overly permissive access makes hosts vulnerable to attack. Our research shows it only takes 10 to 15 minutes for attackers to discover an unsecured host and perform brute force attempts. Moreover, 26% of cloud resources do not restrict outbound traffic at all. This makes it easy for cryptomining scripts to connect to mining pools from within compromised environments. Best practices dictate that outbound access should be restricted to prevent data exfiltration as well as stop malicious traffic from leaving the network in the event of a breach.

The team also observed that 28% of databases are receiving inbound connections from the internet. In previous reports, this statistic varied between 31% and 37%. This goes against network architecture best practices and is a common issue in public cloud environments. This issue can be attributed to the lack of security oversight as developers create and deploy cloud resources on demand.

Tips

1. Implement a “deny all” default outbound firewall policy.

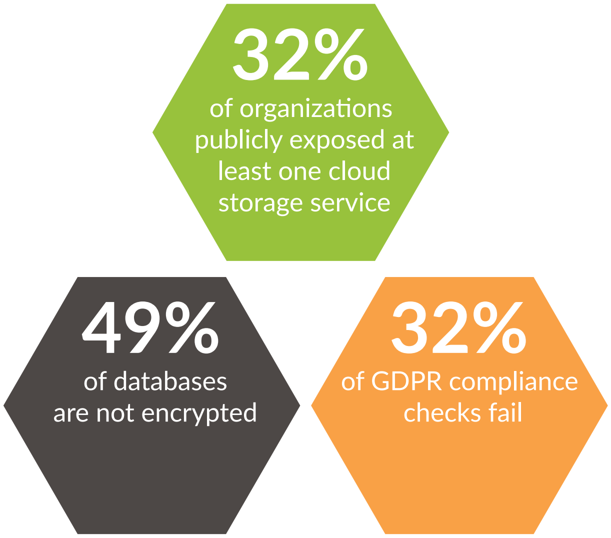
2. Monitor north-south and east-west network traffic to identify suspicious activities, including cryptojacking.

3. Automate remediation of critical issues to keep up with the speed of change in the public cloud.

Compliance: A Work in Progress

Public exposure of data in cloud storage has become so common that there are websites that maintain lists of exposed instances and confidential files. Two recent incidents had significant impact. In one case, attackers were able to expose 48 million records containing psychographic data, which connects users' identities, online behaviors, and activities. Malicious actors can use this data to perform traditional identity theft and fraud, and it can also serve as ammunition for social engineering scams, such as phishing. In another case, tens of thousands of accounts containing children's Apple ID email addresses and plain-text passwords were exposed. A malicious actor could use these credentials to compromise children's accounts and access their personal content data, raising serious privacy concerns.

The good news is that the latest Unit 42 cloud research indicates a slowing trend for publicly exposed cloud storage services: 32% of organizations in September 2018, compared to 58% back in May. Perhaps the proactivity of cloud service providers in adding security features to help organizations detect these issues is paying off.



32%
of organizations publicly exposed at least one cloud storage service

49%
of databases are not encrypted

32%
of GDPR compliance checks fail

The bad news is that organizations are still not employing best practices, such as encryption, to protect sensitive data. Forty-nine percent of databases are not encrypted, which is exactly in line with the figure from May 2018. Data encryption is an important technique that could help meet the pseudonymization requirement for the GDPR and should be enforced as a security best practice.

A broader compliance assessment against industry standards revealed that organizations fall short of multiple mandates, failing, on average:

- 43% of CIS Foundations best practices
- 36% of NIST CSF best practices
- 32% of GDPR requirements
- 24% of SOC 2 requirements
- 12% of HIPAA requirements
- 10% of PCI DSS requirements

Clearly, organizations have a long way to go before they can claim compliance in their public cloud environments.

Tips

1. Maintain a central asset inventory of all cloud resources across multiple cloud providers.

2. Implement policy guardrails to ensure that resource configurations adhere to industry standards, such as CIS, SOC 2, PCI, HIPAA, NIST CSF, and GDPR.

3. Automate remediation of critical issues to keep up with the speed of change in the public cloud.

Vulnerability Management: A Silver Lining in the Cloud

If Spectre and Meltdown were not enough to cause massive fire drills across organizations earlier this year, the latest vulnerability affecting Intel processors—L1 Terminal Fault—and a remote code execution flaw in Apache® Struts 2 are certainly keeping security teams up at night. For organizations still operating large on-premises environments, the massive effort to identify vulnerable systems as well as apply patches and other system-level changes has only just begun. Like other critical patching efforts before it, the process will likely take many organizations months to address and validate, adding to the already overburdened IT workload.

Organizations largely operating in public cloud environments, such as AWS, Azure, or GCP, have an extreme advantage over their on-premises peers. As part of the Shared Responsibility Model, cloud service providers update their respective infrastructures and services, providing an initial line of defense. Organizations also need to address their obligations by identifying and patching vulnerable hosts. However, the latest Unit 42 cloud research reveals that 23% of organizations have hosts in the cloud that are missing critical patches.

23%
of organizations have hosts missing critical patches in the cloud

The crux of the issue is that organizations cannot use their legacy vulnerability scanning tools to effectively identify and remediate vulnerable hosts in cloud environments. These tools identify hosts that are missing patches by IP address, but IP addresses are constantly changing in the cloud, making this approach unreliable. Instead, organizations need cloud security tools that take advantage of cloud service providers' APIs to correlate configuration data, such as IP address, with vulnerability data from such tools.

Tips

1. Correlate vulnerability data with resource configuration data to identify vulnerable hosts.

2. Correlate network traffic data to determine whether the vulnerabilities are exploitable and prioritize remediation accordingly.

Managed Container Services: Security 101

Container adoption is exploding: one in three organizations uses native or managed Kubernetes orchestration. Twenty-five percent of organizations use popular managed container services in the cloud, such as Amazon Elastic Container Service for Kubernetes, Google Kubernetes Engine, and Azure Kubernetes Service. Such platforms make it easy for developers to deploy, manage, and scale containerized applications.

As container adoption continues to grow, organizations must ensure they have appropriate guardrails in place to prevent security incidents. By default, pods in a Kubernetes cluster can receive traffic from any source. By applying network policies, you can isolate the pods and enforce access control. However, it appears users are not changing the default behavior; Unit 42's cloud research team discovered 46% of organizations have not applied appropriate network policies for their managed Kubernetes services, leaving the pods vulnerable to network attacks.

Moreover, Unit 42 discovered that 15% of organizations don't use IAM roles to control access to the Kubernetes cluster; they use basic authentication, which is prone to brute force attacks. Instead, they should use IAM roles to control access to the instance and, when applicable, make use of client certificates.

46%
of organizations accept traffic to Kubernetes pods from any source

15%
of organizations don't use IAM policies to control access to Kubernetes instances

Tips

1. Follow the CIS best practices for configuring your managed and unmanaged Kubernetes environments.

2. Implement stringent network and IAM policies to manage access to your Kubernetes environments.

3. Leverage native security or third-party tools to continuously monitor your Kubernetes environment to ensure compliance and runtime security.

Ready to Identify the Threats in Your Cloud?

Prisma™ Cloud security and compliance technology analyzes more than 10 billion events every month. That analysis shows us that poor configuration, permissive behaviors and lack of policies lead to many openings for bad actors and unidentified risks to exploit. By proactively detecting security and compliance misconfigurations as well as triggering automated workflow responses, Prisma Cloud helps ensure you continuously and securely meet the demands of your dynamic cloud architectures.

Register for a free, 30-day trial of Prisma Cloud.

About Unit 42

Unit 42 is the global threat intelligence team at Palo Alto Networks. We believe threat intelligence should be free, shared, and available to all for the common good. We deliver high-quality, in-depth research on adversaries, malware families, and attack campaigns. Our analysts uncover and document adversary behaviors, and then share playbooks that give insight into the various tools, techniques, and procedures threat actors execute to compromise organizations.

We share our findings freely so defenders everywhere can access world-class threat intelligence. Unit 42 is a recognized authority on cyberthreats, frequently sought out by enterprises and government agencies around the world.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.