PRISMA CLOUD | UNIT 42 BY PALO ALTO NETWORKS

CLOUD THREAT REPORT 1H 2021

The COVID-19 Conundrum: Cloud Security Impact and Opportunity

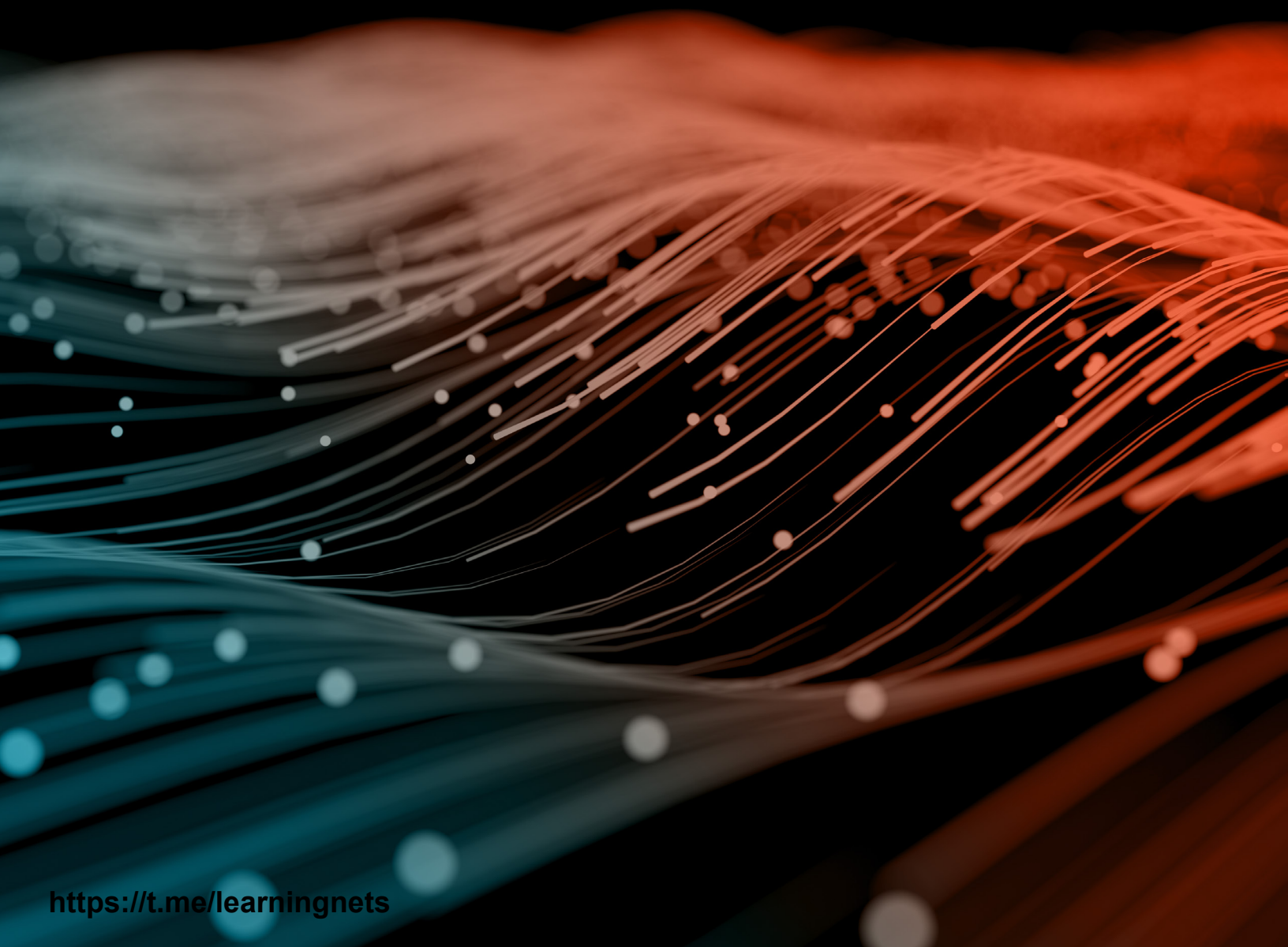

Table of Contents

Foreword

In the early days of the COVID-19 pandemic, there was a rapid uptick in demand for cloud services. In a matter of months, the percentage of employees working remotely jumped from 20% to 71%.[1] Additionally, enterprises quickly scaled their cloud spend in the third quarter of 2020 (July–September), an increase of 28% from the same quarter in 2019.[2] The timing is significant because the World Health Organization (WHO) declared COVID-19 a pandemic in March 2020. Remote work surged, and organizations accelerated cloud migration plans, with Q3 of 2020 seeing a massive year-over-year spike.

Utilizing data pulled from our global array of sensors, our elite cloud threat researchers **found a correlation between the increased cloud spend due to COVID-19 and security incidents**.[3] Organizations globally increased their cloud workloads by more than 20% (between December 2019 and June 2020), leading to an explosion of security incidents. Our research shows that cloud security programs for organizations globally are still in their infancy when it comes to automating security controls (i.e., DevSecOps and shifting left). This all leads to our conclusion that **rapid cloud scale and complexity without automated security controls embedded across the entire development pipeline are a toxic combination**. Case in point: in previous research, we found that 65% of publicly disclosed security incidents in the cloud were the result of customer misconfigurations. This is the impact to businesses that operate in the cloud, at scale, without automated security controls.

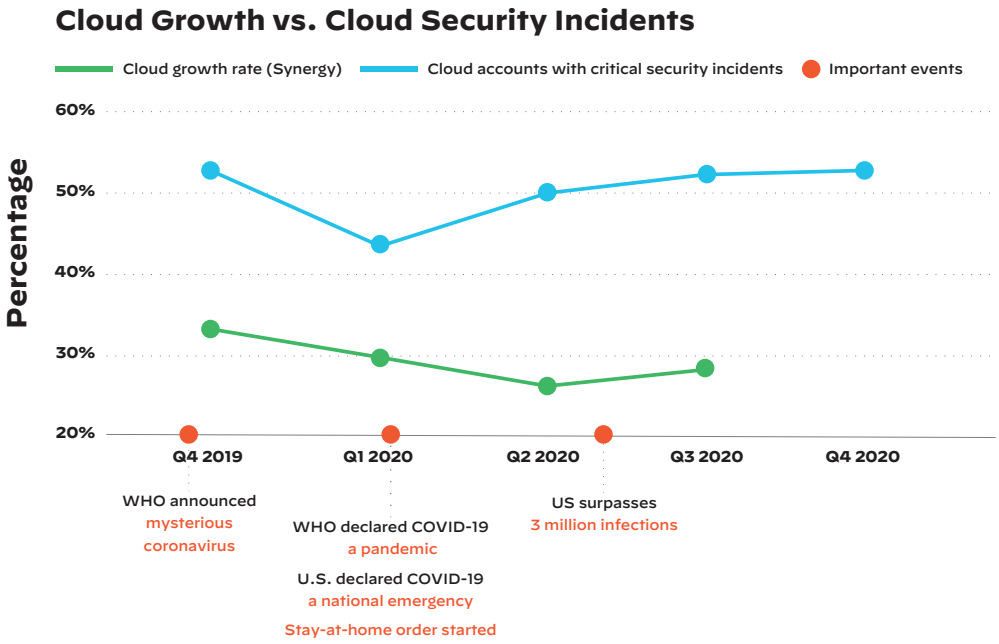

Figure 1: Cloud growth and security incidents

Read on to learn how the latest cloud threats globally may be affecting your organization as well as how focusing on a common security platform and standards can go a long way toward maturing your cloud security program.

Matthew Chiodi
Chief Security Officer, Public Cloud, Palo Alto Networks

1. "How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work," Pew Research Center, December 9, 2020, https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work.
2. "COVID-19 Boosts Cloud Service Spending by $1.5 Billion in the Third Quarter," Synergy Research Group, December 5, 2020, https://www.srgresearch.com/articles/covid-19-boosts-cloud-service-spending-15-billion-third-quarter.
3. Security incidents, defined as events that caused violations in security policies and put sensitive data at risk.

Executive Summary

To understand the global impact of COVID-19 on the security posture of organizations, the Unit 42 cloud threat intelligence team analyzed data from hundreds of cloud accounts around the world between October 2019 and February 2021 (before and after the onset of the pandemic). **Our research indicates that cloud security incidents increased by an astounding 188% in the second quarter of 2020 (April to June). We found that, although organizations quickly moved more workloads to the cloud in response to the pandemic, they struggled many months later to automate cloud security and mitigate cloud risks.** While infrastructure as code (IaC) offers DevOps and security teams a predictable way to enforce security standards, this powerful capability continues to go unharnessed.

This report details the scope of COVID-19's impact on the cloud threat landscape and explains which types of risks are most prevalent in specific geographies and industries. It also identifies actionable steps organizations can take to reduce the security risks associated with their cloud workloads.

COVID-19 Critical Industries Suffer Spike in Security Incidents

Organizations experienced large expansions in the size of cloud workload deployments following the onset of the pandemic, but they also suffered an uptick in cloud security incidents. Of note, **cloud security incidents for the retail, manufacturing, and government industries rose by 402%, 230%, and 205%, respectively**. This trend is not surprising; these same industries were among those facing the greatest pressures to adapt and scale in the face of the pandemic—retailers for basic necessities, and manufacturing and government for COVID-19 supplies and aid.

Industries that play crucial roles in combating the pandemic are struggling to secure their cloud workloads, underscoring the danger of underinvesting in cloud security. Such spikes in cloud security incidents make clear that, although the cloud allows businesses to quickly expand their remote work capabilities, automated security controls around DevOps and continuous integration/continuous delivery (CI/CD) pipelines often lag behind this rapid movement.

Cryptojacking in the Cloud Is on the Decline

While the pandemic raged, cryptocurrencies such as Bitcoin (BTC), Ethereum (ETH), and Monero (XMR) grew in popularity and market value. Despite this, cryptojacking is trending down: from December 2020 through February 2021, only 17% of organizations with cloud infrastructure showed signs of this activity, compared to 23% from July through September 2020. **This is the first recorded drop since Unit 42 began tracking cryptojacking trends in 2018**. Organizations appear to be blocking cryptojacking more proactively. This can be done effectively through workload runtime protections that mitigate an attackers' ability to run malicious cryptomining software undetected in enterprise cloud environments.

Sensitive Data in the Cloud Remains Publicly Exposed

Our findings indicate that 30% of organizations expose some sensitive content to the internet, such as personally identifiable information (PII), intellectual property, and healthcare and financial data. Anyone who knows or can guess the URLs can access this data. When this data is exposed directly to the internet, organizations face significant risks associated with unauthorized access and regulatory compliance violations. This degree of exposure suggests that organizations continue to struggle to enforce proper access controls for the hundreds of data storage buckets that may operate in the cloud, especially when those buckets are spread across multiple cloud providers and accounts.

01

Evidence-Based Findings

Top COVID-19 Cloud Security Incidents

Unit 42 research revealed significant increases in a wide variety of security risks during the COVID-19 pandemic. Risks ranged from unencrypted cloud data to the public exposure of cloud resources, insecure port configurations, and more. Figure 2 details more than a dozen categories of security incidents that increased substantially in frequency.

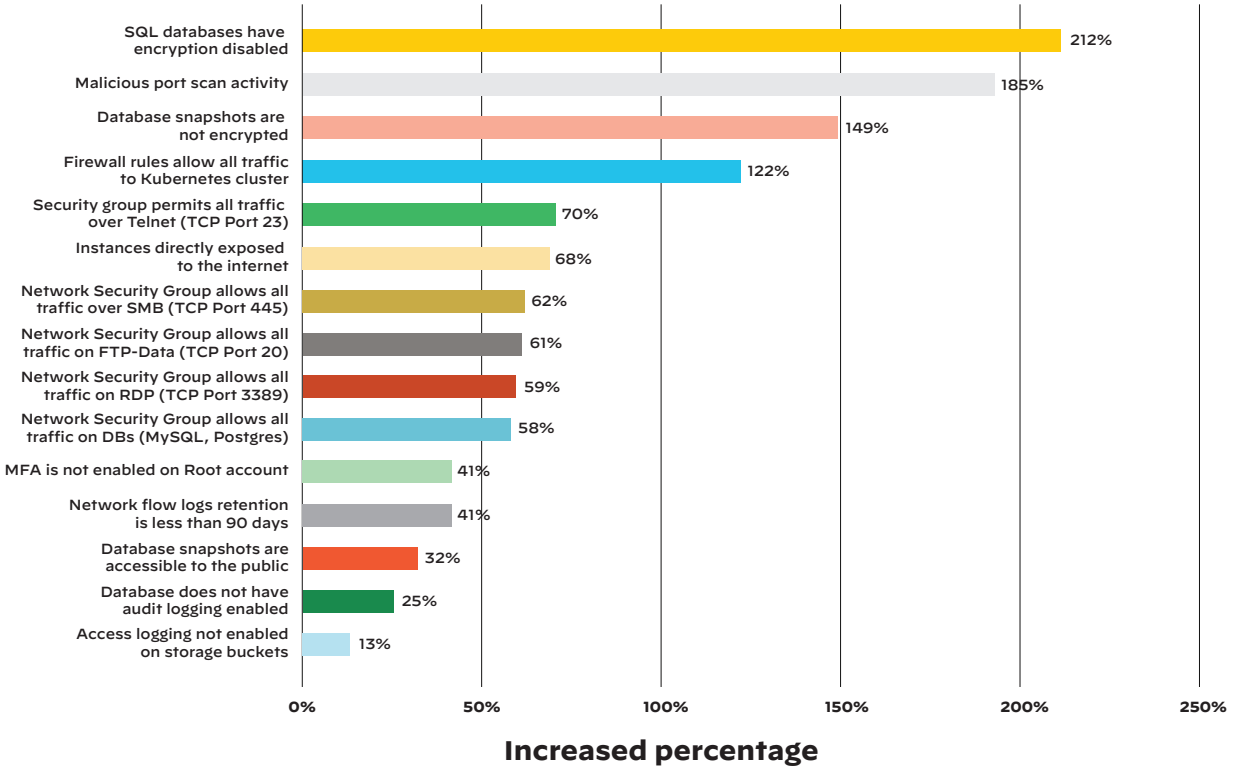

Figure 2: Security incidents with the greatest increases during the pandemic

Taken as a whole, **these incidents underline the failure of most organizations to scale cloud governance and security automation at the same rate that they scaled their cloud workloads**. Many of these misconfigurations can be addressed through the use of infrastructure as code (IaC) templates. As we've noted in previous reports, IaC templates, when consistently scanned for common security vulnerabilities, help secure cloud infrastructure from development through production.

For example, failure to encrypt SQL and relational databases (e.g., Microsoft Azure® SQL Database)—both among the types of security incidents that saw the greatest uptick in frequency—is a mistake that can be easily identified and corrected by automatically auditing cloud environments for signs of misconfigurations. Although port scanning is not a new type of threat, its increased prevalence during the pandemic suggests that attackers have been actively searching for vulnerabilities created through ineffective cloud governance.

Insufficient governance and security automation are not new problems. Although the frequency of alerts related to cloud security incidents of various types increased over the past year, our findings regarding the most prevalent types of incidents are broadly similar to those of our previous reports.

This suggests that, even as organizations have moved more workloads to the cloud over the past year, they continue to make key security mistakes and oversights. Many of these mistakes can be addressed through the effective use of IaC templates. IaC templates are already used by many teams, but not to maximum effect. Most are created through a simple three-step process: design, code, and deploy. What's getting DevOps and security teams in trouble is the lack of automated security reviews. Just like application code, IaC templates must be scanned for security issues every time they are created or updated.

Our research indicates, however, that as the pandemic raged, teams were either not using IaC at all or simply failing to scan templates for common security vulnerabilities. Otherwise, they would not have been making mistakes such as failing to encrypt potentially sensitive data or enable logging, which is a critical feature for security monitoring and auditing in cloud environments.

COVID-19's Impact on Cloud Security by Region

The pandemic's impact on cloud growth was evident in all global regions, but as figure 3 shows, some grew more than others.

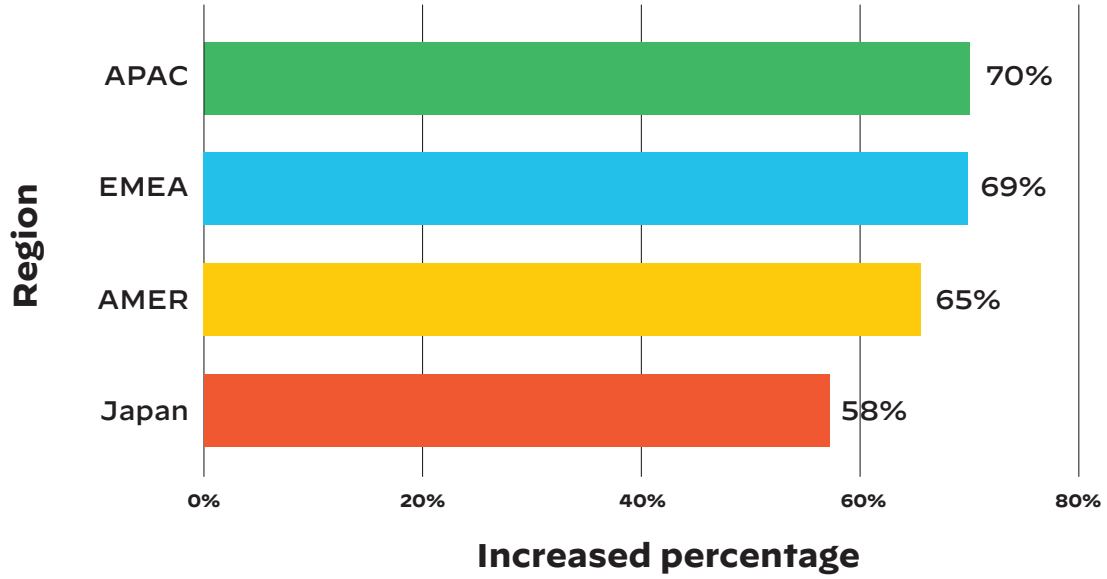

Figure 3: Increase in cloud workloads by region

Overall, Japan has had a slower rate of cloud adoption during COVID-19. As a result, only 32% of Japanese organizations had insecure configurations that allowed all network traffic (TCP/UDP on any port) into at least one of their cloud-hosted virtual machines (VMs), and only 39% exposed port 22 (SSH) on at least one of their cloud-hosted SSH services.

By comparison, 60% of organizations worldwide allowed all network traffic into their cloud platforms, and 58% of organizations worldwide exposed port 22.

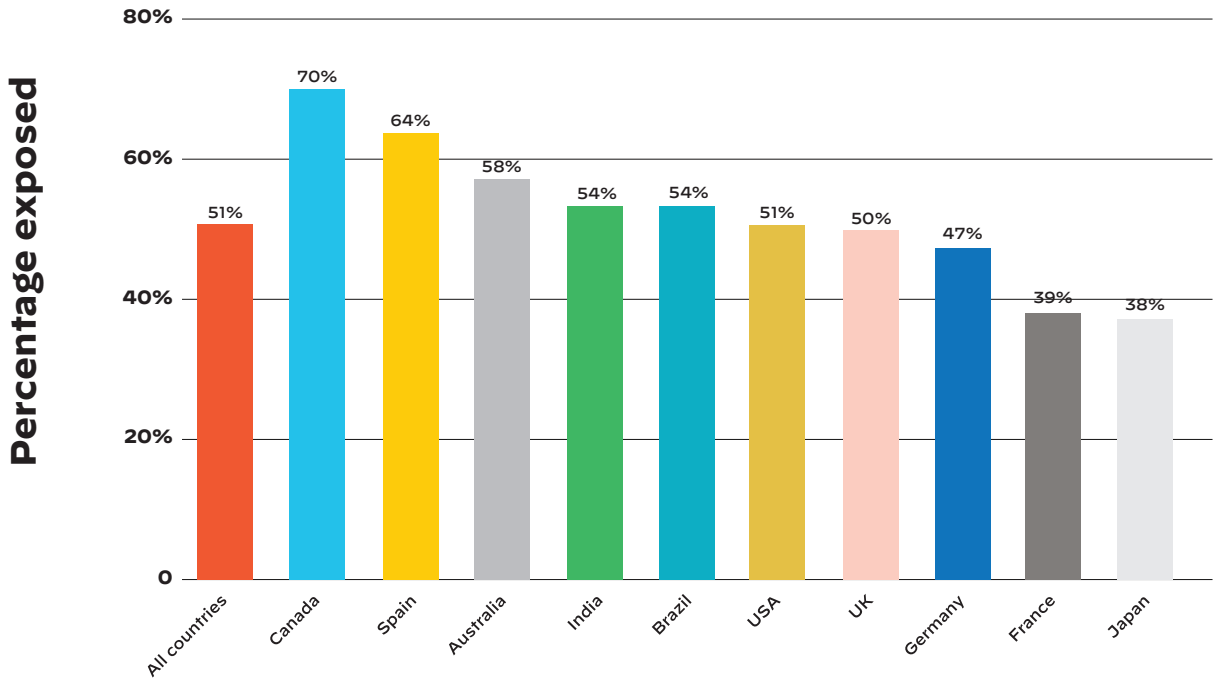

Figure 4: Percentage of organizations exposing RDP by country

Exposure of Windows Remote Desktop Protocol (RDP, port 3389) also varied significantly between regions (see figure 4). Tracking this exposure is critical as RDP is one of the most popular attack vectors. Attackers can use open RDP ports to breach company networks in order to disrupt operations or steal sensitive data. Canadian organizations struggled the most in this area, with 70% exposing RDP.

In comparing region workload growth with the exposure of RDP per country, a pattern emerges around COVID-19. Unit 42 researchers found a direct correlation with increased security incidents. Across all major cloud providers, the average exposure of RDP increased by 27%.

Here, again, failure to secure critical ports is a mistake with potentially serious business consequences. However, it is also one that can be prevented with a combination of secure IaC and continuous security enforced by a common security platform.

COVID-19's Impact on Cloud Security by Industry

The scale of cloud workloads increased across virtually all industries, with energy being the only exception, likely due to weak demand and cuts in oil and gas production during the pandemic. Of particular note are the chemical manufacturing, government, and pharmaceuticals and life sciences industries, which experienced the most significant increases in cloud usage—a trend likely owing to their uptick in operations in response to the pandemic.

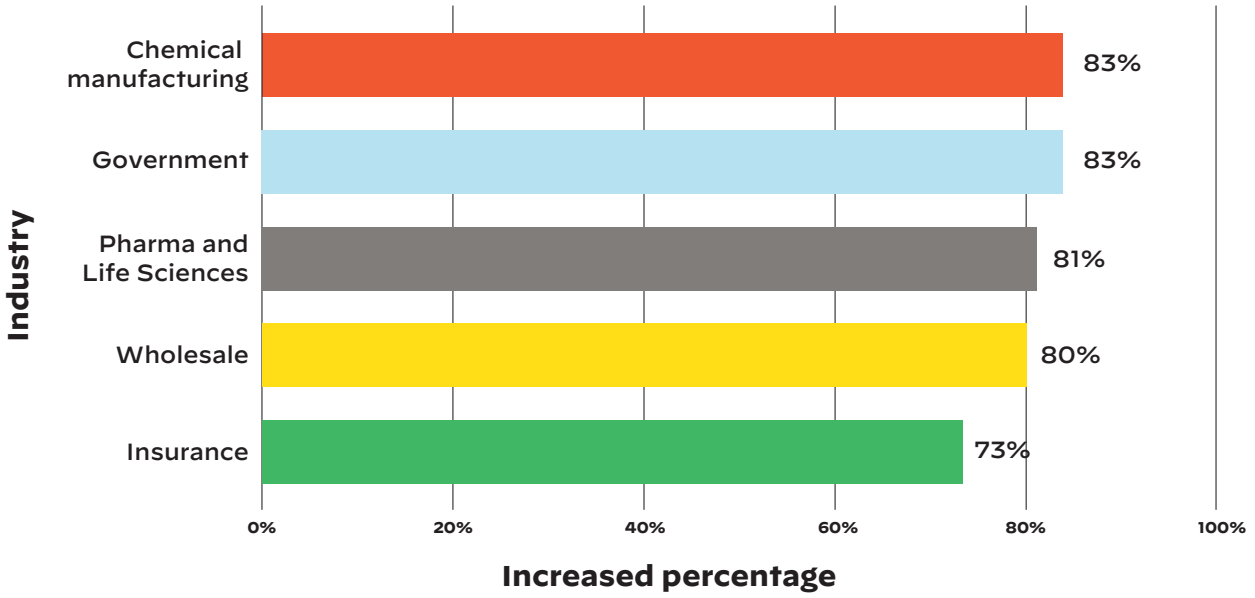

Figure 5: Percentage of organizations with increased cloud workloads by industry

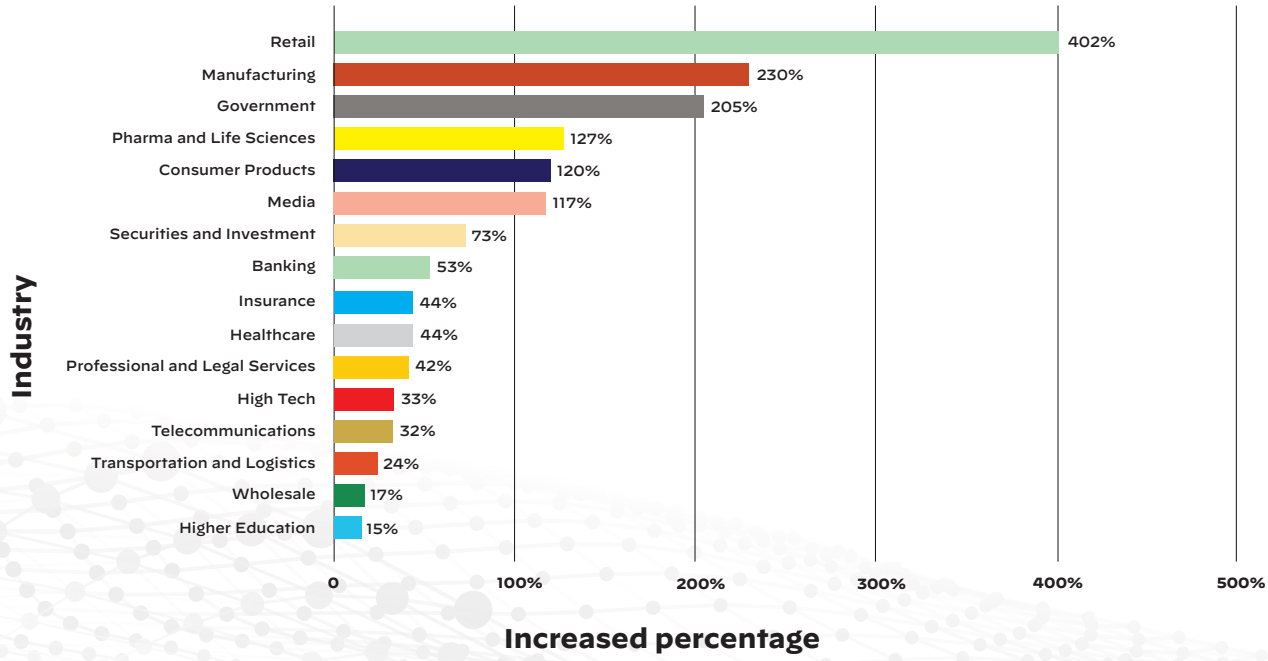

Figure 6: Percentage increase in security incidents by industry

Note: Industries with insufficient samples are not included in the figures.

Our research shows that when an organization's cloud workloads suddenly increase, the number of security incidents increases dramatically—often to the point that it overwhelms DevOps and Security teams. For example, the number of security incidents in the retail, manufacturing, and government industries rose by 402%, 230%, and 205%, respectively. This trend is not surprising as these industries were among those facing pressures to adapt and scale in the face of the pandemic—retailers for basic necessities, manufacturing and government for COVID-19 supplies and aid. These incidents expanded cloud environments' attack surfaces and made security auditing and forensic efforts difficult.

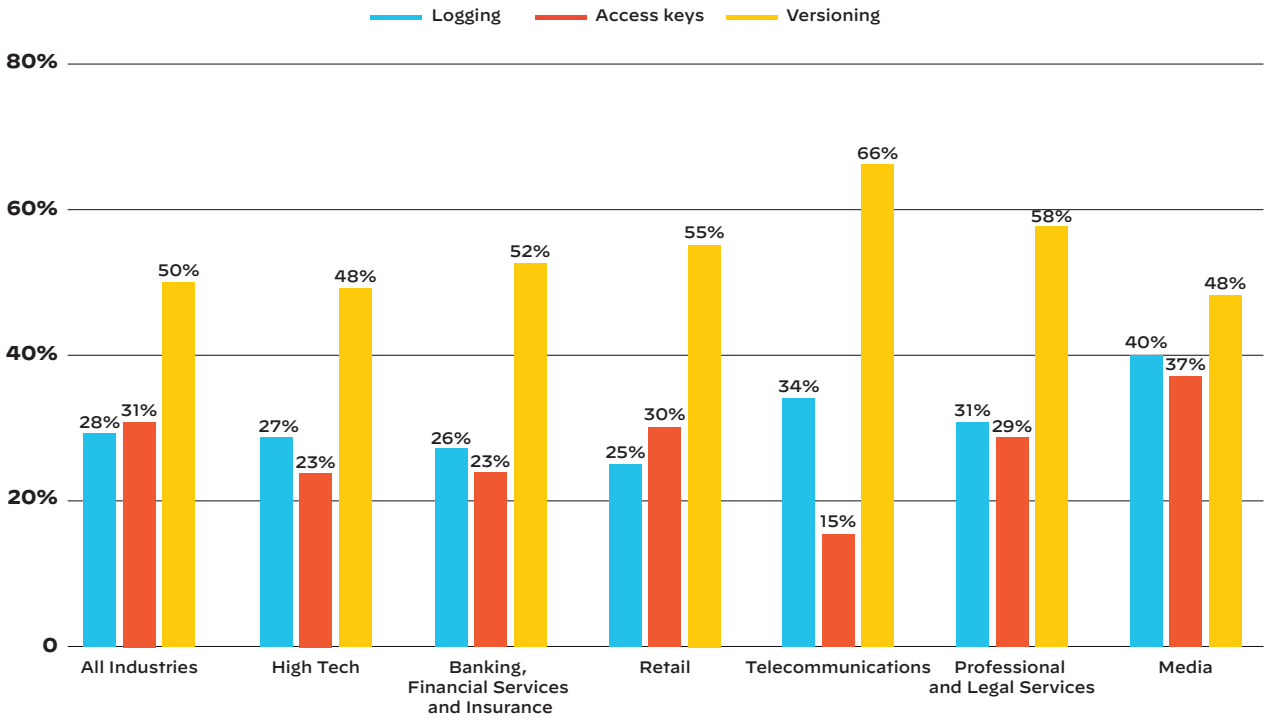

Figure 7: Percentage of organizations enabling critical security controls by industry

Nonetheless, businesses in some industries performed better than others with regard to security (see figure 7). For example, 40% of all media organizations globally applied access logging controls to each and every cloud storage container. In contrast, only 25% of retail organizations did the same. While the rationale for this is currently unknown, Unit 42 researchers theorize that media organizations tend to be very particular about access to content, especially considering the consequences of the Sony Pictures hack in 2014.

The media industry also performed better when looking at the rotation of access keys, with 37% maintaining access keys newer than 90 days, whereas telecommunication organizations only had 15%. Again here, Unit 42 researchers theorize that media organizations tend to prioritize access management. The telecommunications industry, on the other hand, maintained the second-highest logging controls but scored the lowest on key management, indicating that the industry prioritizes monitoring more than access control.

Version control within cloud storage containers is an important security measurement as it identifies whether an organization can recover from compromised cloud storage attacks or simple file corruption errors. In the telecommunications industry, 66% of organizations implemented version control in all of their cloud storage containers, whereas media and high tech industry organizations had the lowest such implementation, with only 48%. Unit 42 researchers believe it is noteworthy that the media and telecommunications industries essentially flipped their security prioritization models. Both appear to emphasize logging and monitoring controls, but where the media industry favors access key enforcement, the telecommunications industry favors versioning controls. The media industry's push to control access appears equal to the telecommunications industry's push to ensure data remains uncompromised.

COVID-19 and Data Security

Businesses are favoring cloud storage due to its reliability, availability, and scalability. Our research shows that 64% of data in the cloud contains sensitive information (e.g., PII, intellectual property, healthcare and financial data). Within that 64% subset, 69% contains PII, and 34% contains intellectual property (see figure 8).

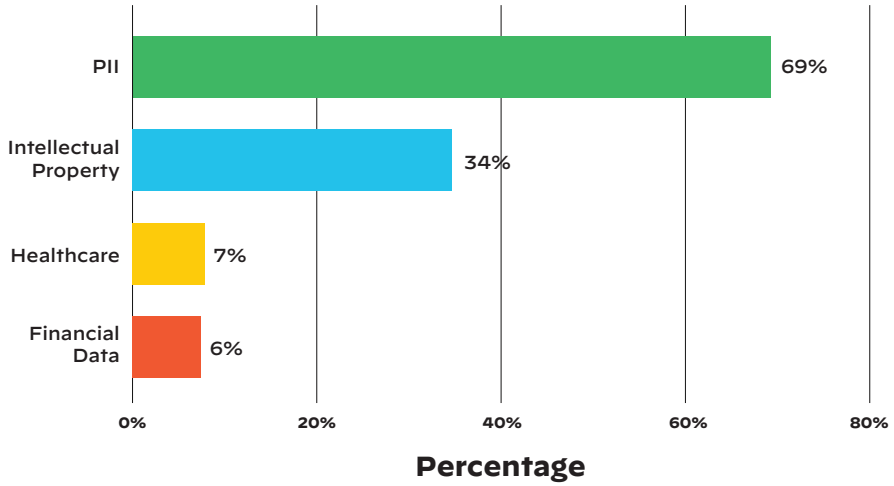

Figure 8: Prevalence of sensitive data types among sensitive data stored in clouds

While the scale of data stored in the cloud increased, many organizations failed to enforce proper security controls over their data. Our research indicates that 35% of businesses globally permitted their cloud storage resources to be publicly accessible from the internet. Although this configuration may be necessary in certain cases, it is likely that it usually results from an oversight that remained undetected due to a lack of security monitoring and auditing.

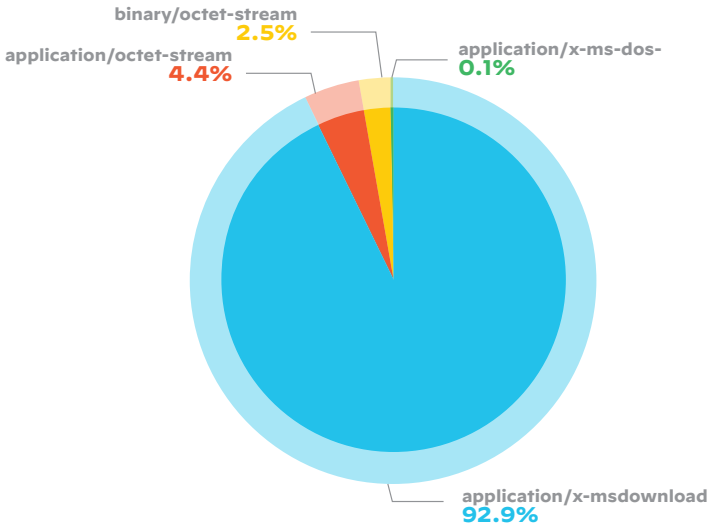

Figure 9: Types of malware found in cloud storage

Publicly accessible data represents a particularly serious risk to businesses as 30% of organizations globally with publicly accessible cloud data appear to be storing sensitive data. **This finding was shocking, given that anyone who knows the right URLs can access the data without passwords or other authentication**. In recent years, there have been numerous incidents wherein researchers or attackers found sensitive data in cloud storage inadvertently made public. For example, in different publicly exposed cloud storage environments, vpnMentor researchers found PII data for more than 30,000 individuals, and The Register researchers found more than 500,000 confidential files belonging to thousands of customers.

In addition to sensitive data, cloud storage may host malware. Unit 42 researchers found that 92.9% of malware in cloud storage is in the form of executable (.exe) files or dynamic link library (.dll) files. This percentage is consistent with VirusTotal's findings that most malware targets Windows systems and executable files are the most common delivery vehicle.

The good news is that we found malware in less than 0.01% of cloud storage data. For that 0.01%, however, it remains crucial to investigate how the malware got into the storage and who might have accessed the malware.

02

Cloud, COVID-19, and Cryptocurrency

Although movements in the cryptocurrency market and security issues associated with that movement cannot be linked solely to the COVID-19 pandemic, our research reveals interesting connections between cryptocurrency, the cloud, and the impact of COVID-19.

Unit 42 researchers focused on data associated with Monero (XMR), a cryptocurrency popular with hackers due to its strong anonymity protections and the fact that it can be easily mined in the cloud. Research took place between December 2020 and February 2021.

Mining Trends and Market Events

Our findings indicate that **connections to known XMR cryptomining pools increased 65%** during this period, with dramatic peaks and valleys in the total number of connections.

Of particular interest within this data was the fact that three instances of the lowest number of network connections took place during the highest market price points (see figure 10). This trend may indicate that cryptomining operators are performing the bulk of their mining during bear markets, and then closing operations to sell their gains during periods of higher prices. Also of note is the sustained decrease in XMR network connections between December 24, 2020, and January 3, 2021, suggesting that even illicit cryptomining operations need to take a holiday break.

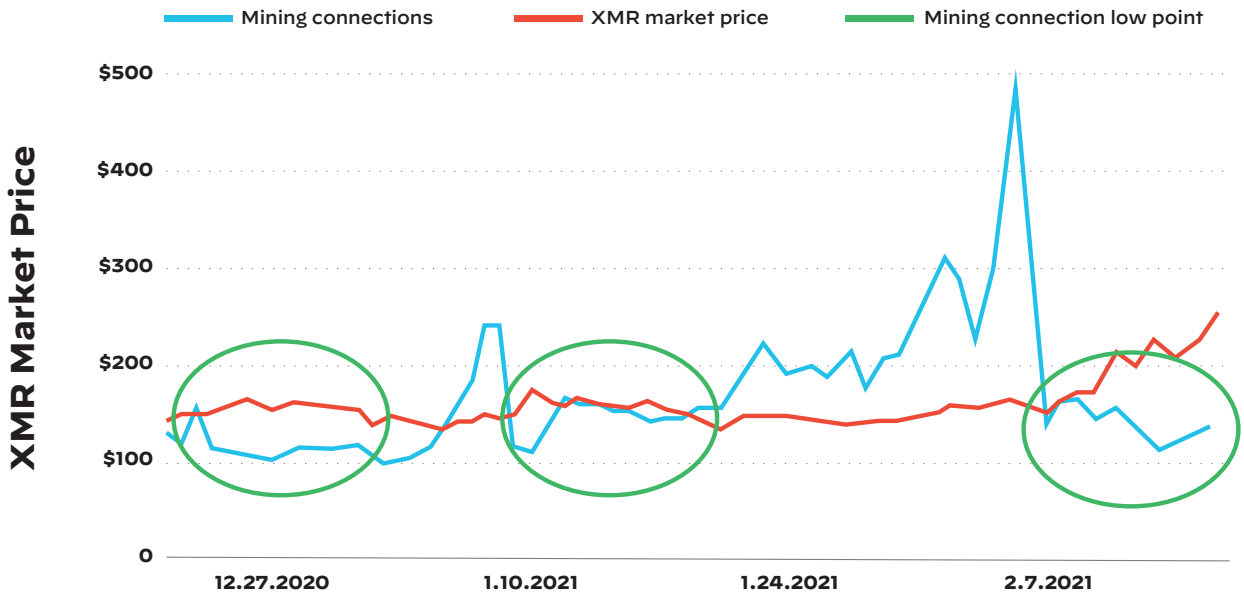

Figure 10: Comparison of cryptomining connections and XMR price

The Pandemic's Impact on Mining Operations

Unit 42 researchers noted clear correlation between XMR mining activity and events related to the pandemic. Figure 11 details the frequency with which XMR mining pools performed network connections overlaid with important dates from the pandemic.

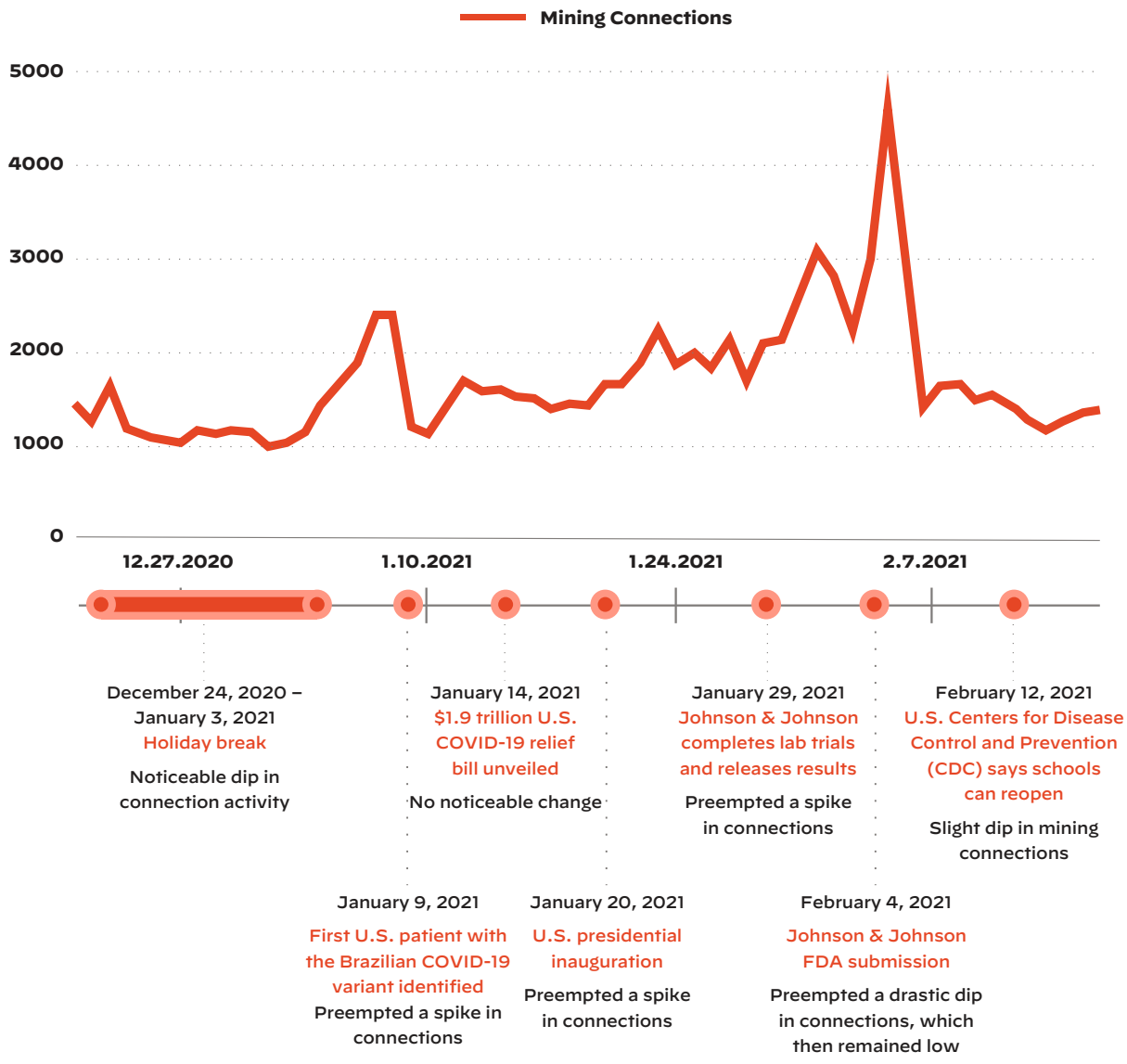

Figure 11: Mining pool connections and important dates

Although the amount of data available does not make it possible to draw definitive conclusions, it appears likely that political and health-related events exert a clear impact on malicious cryptomining operations, at least for XMR.

Cryptojacking Declines

Despite increased mining activity, cryptojacking (meaning unauthorized use of infrastructure for cryptomining) has decreased during the COVID-19 era. Globally, 23% of organizations with cloud workloads experienced cryptojacking from July through September 2020, compared to only 17% from December 2020 through February 2021, according to our findings. **This is the first recorded drop since we began tracking cryptojacking activity in 2018.**

While XMR is the most popular cryptocurrency for mining operations within the cloud, there are more popular cryptocurrencies in terms of market share. Unit 42 researchers investigated the network connections for Ethereum (ETH), Bitcoin (BTC), Litecoin (LTC), and Dash. In each case, XMR mining connections significantly outperformed the other currency mining operations, which combined for an average of 1% of the total network connections taken by XMR (see figure 12).

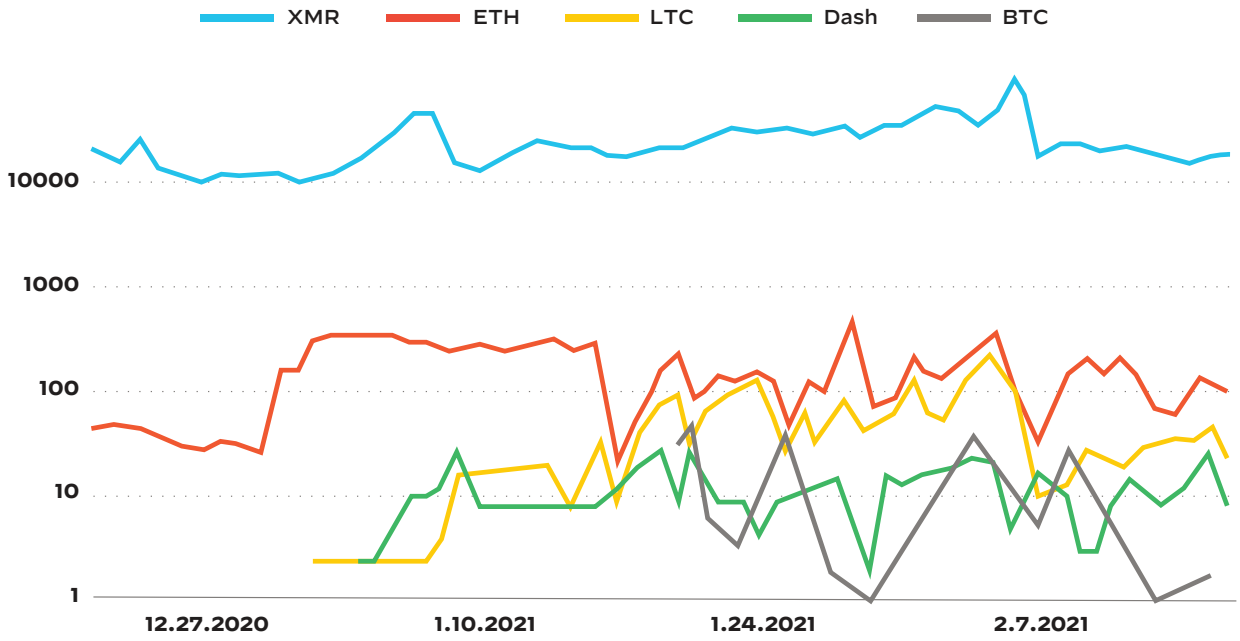

Figure 12: Mining connections by cryptocurrency

ETH, considered one of the most popular cryptocurrencies, has the highest number of network connections to currency-specific mining pools outside of XMR. This is not unexpected as ETH arguably leads the cryptocurrency market in terms of functionality. While mining ETH using CPU-based processing is not particularly efficient, all cloud service providers (CSPs) do provide graphics processing unit (GPU)-based VM instances, which are significantly more efficient than CPUs in cryptomining.

BTC, LTC, and Dash, surprisingly, were all witnessed making network connections to their own mining pools. The mining and proof of work processes for blockchain currencies like BTC, LTC, and Dash are more memory-intensive operations, and they require specialty hardware called application-specific integrated circuit (ASIC) miners to be profitable. Due to their inefficiency in cloud-based CPU/GPU mining operations and negative cost-benefit ratio, any network connections to these mining pools from enterprise cloud infrastructure should be considered highly suspicious.

03

Conclusion and Recommendations

The key takeaway from our data is clear: **organizations have neglected to invest in the cloud governance and automated security controls necessary to ensure that their workloads remain secure as they move to the cloud**. In turn, they have created serious business risks such as exposing unencrypted sensitive data to the internet and inviting breaches by leaving insecure ports open. While our Unit 42 Cloud Threat Reports in 2020 identified similar problems, the numerous crises unleashed by the COVID-19 pandemic have made the situation more challenging and widespread.

Faced with this threat, organizations must build a cloud security program focused evenly around all phases of the software development lifecycle. Doing this will enable organizations not only to win in the market, but also to establish sustainable cloud security programs that can expand and contract no matter what types of unpredictable events take place in the future.

Strategic Cloud Security Focus Areas

In particular, Unit 42 researchers recommend focusing on several strategic areas in cloud security.

Gain Awareness and Deep Cloud Visibility

The first step in making cloud security and compliance easier is to understand how your developers and business teams are using the cloud today. This means getting and maintaining situational awareness of what's happening in your cloud environments down to the API and workload layers.

Set Security Guardrails

Ask yourself: what misconfigurations should never exist in our environment? An example would be a database receiving direct traffic from the internet. Despite this being a "worst practice," our threat research has shown this misconfiguration exists in 28% of cloud environments globally. When misconfigurations like this are found, your security guardrails should correct them automatically. If your organization does not already do so, you should take a hard look at using IaC templates as another way to enforce security guardrails as you shift left. Be sure to scan these templates for common security misconfigurations.

Adopt and Enforce Standards

It's extremely difficult to automate what you haven't standardized. Many teams talk about automation without having a security standard in place. Don't start from scratch. The Center for Internet Security (CIS) has benchmarks for all major cloud platforms. Look to automate and codify these standards by leveraging IaC.

Train and Hire Security Engineers Who Code

Unlike most traditional data centers, public cloud environments are driven by APIs. Successful risk management in the cloud requires that security teams be able to leverage these APIs to manage workload security at scale. APIs are difficult to use without having engineers on your security team who know how to code and automate security processes as part of the CI/CD pipeline.

Embed Security in DevOps

Strive to map out the who, what, when, and where of how your organization pushes code into the cloud. Once this is done, your goal should be to locate the least disruptive insertion points for security processes and tools into your CI/CD pipeline. In this regard, getting early buy-in from DevOps teams is critical. From there, work to minimize human interaction over time by automating as many operations as possible.

Ready to Identify the Threats in Your Cloud?

Prisma Cloud analyzes more than 10 billion incidents every month. This analysis shows us that poor configuration, permissive behaviors, and lack of policies lead to many openings for bad actors and unidentified threats 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 workloads.

Methodology

All research discussed in this report was based on data collected between October 2019 and February 2021. The research focused on organizations and industries globally, including the Americas; Europe, the Middle East and Africa (EMEA); and the Japan and Asia-Pacific (JAPAC) region.

Palo Alto Networks Prisma Cloud

Prisma® Cloud trend data utilizes multiple threat intelligence sources. Unit 42 researchers used proprietary data sources to gather organizational alert and event data. This data was anonymized, and then analyzed and compared to the results of previous cloud threat report analytics to produce trend information.

Palo Alto Networks WildFire

The cloud-based WildFire® malware prevention service employs a unique multi-technique approach, combining dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.

Palo Alto Networks AutoFocus

The AutoFocus™ contextual threat intelligence service provides the intelligence, analytics, and context required to understand which attacks require immediate response. It also has the ability to make indicators actionable and prevent future attacks.

About

Prisma Cloud

Palo Alto Networks Prisma® Cloud delivers the industry's broadest security and compliance coverage—for applications, data, and the entire cloud native technology stack—throughout the development lifecycle and across multi- and hybrid-cloud environments.

Unit 42

Unit 42 is the global threat intelligence team at Palo Alto Networks. Our analysts are experts in hunting and collecting cyberthreat tactics and techniques as well as reverse-engineering malware to identify technical context wherever possible. Unit 42 bridges threat intelligence with Palo Alto Networks products to ensure customers are protected across the entire security suite.

Authors

Jay Chen, Senior Threat Researcher, Public Cloud Security, Palo Alto Networks

Nathaniel "Q" Quist, Senior Threat Researcher, Public Cloud Security, Palo Alto Networks

Matthew Chiodi, Vice President and Chief Security Officer, Public Cloud, Palo Alto Networks

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com