Cloud Threat Report

1H 2021: The COVID-19 Conundrum

Matt Chiodi | CSO, Cloud

About the report

The **largest** and **most global** threat research on cloud security **pre and post COVID-19 discovery**

Intel collected from **thousands of sensors** worldwide. **Not survey data!**

Data gathering Oct. 2019 - Feb. 2021

Download the full report:
cloudthreat.report/1h21

PRISMA CLOUD | UNIT 42 BY PALO ALTO NETWORKS

CLOUD THREAT REPORT
1H 2021

The COVID-19 Conundrum: Cloud Security Impact and Opportunity

© 2021 Palo Alto Networks, Inc. All rights reserved.

Why this topic?

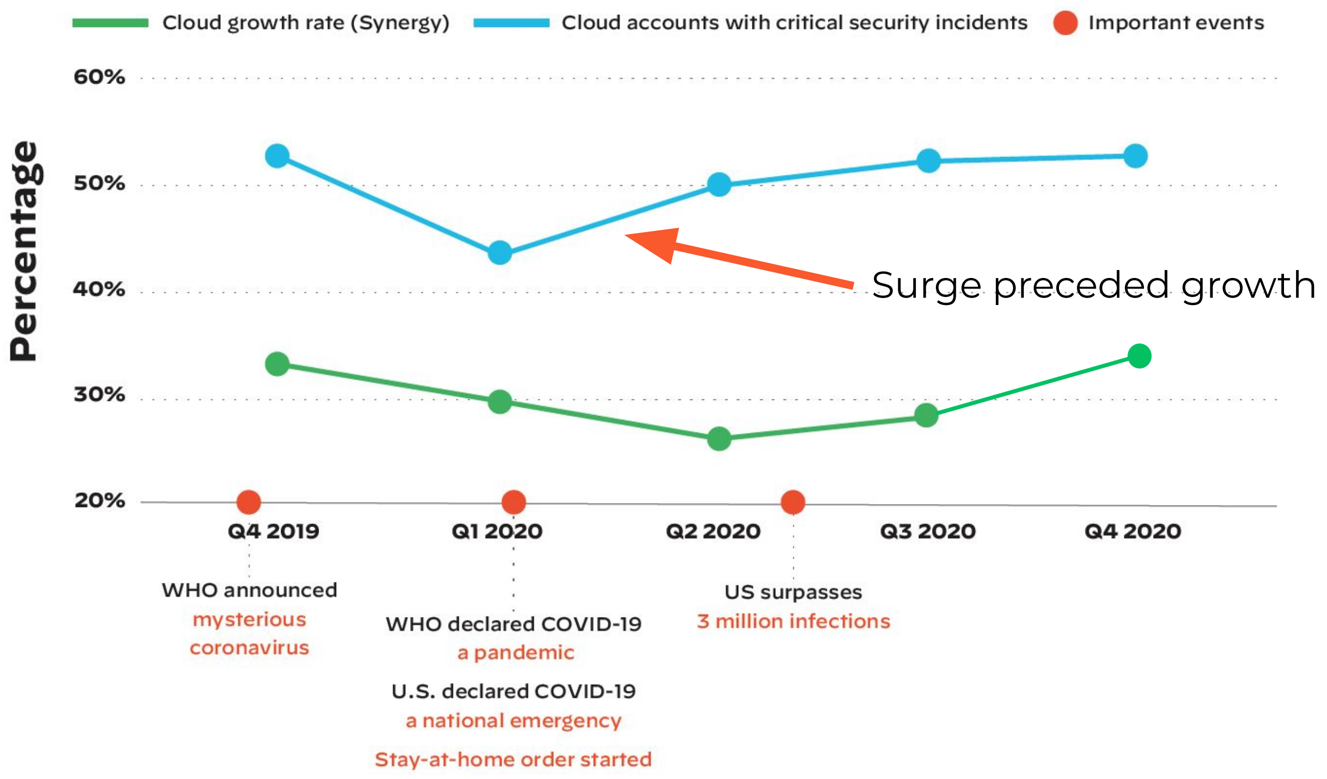
Increased cloud spend

Mostly remote workforce

Crypto became mainstream

© 2021 Palo Alto Networks, Inc. All rights reserved.

Cloud growth vs. cloud security incidents



Top COVID-19 cloud security incidents worldwide

Unencrypted SQL databases

212%

Malicious port scans

185%

Unencrypted database snapshots

149%

Increased percentage

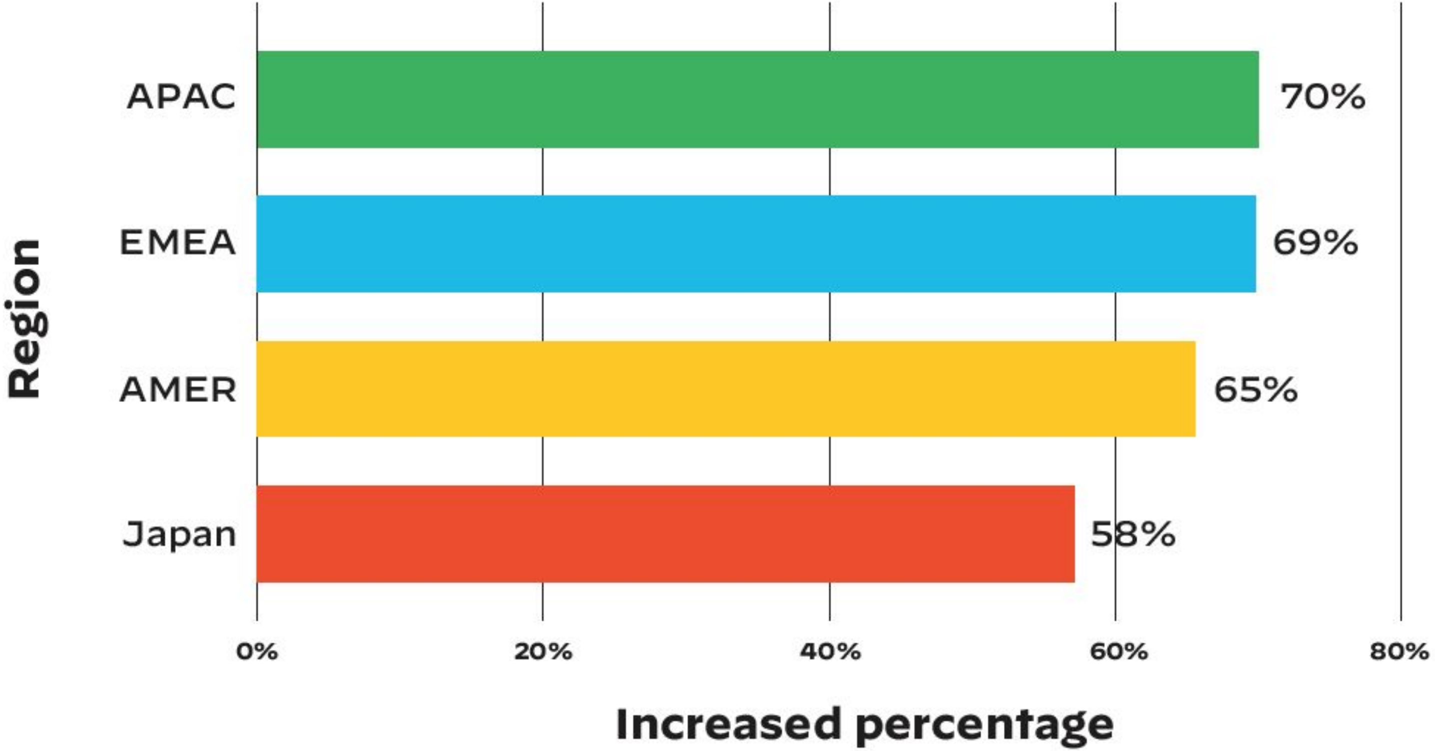
© 2021 Palo Alto Networks, Inc. All rights reserved.

Without automation, sudden increases in cloud workloads lead to dramatic increases in security incidents… Overwhelming security teams.

© 2021 Palo Alto Networks, Inc. All rights reserved.

Regional Intel

Increase in cloud workloads by region



© 2021 Palo Alto Networks, Inc. All rights reserved.

Sometimes it pays to grow slowly

32%

of Japanese organizations had *insecure network configurations

60%

of organizations globally had insecure network configurations

*(TCP/UDP on any port to at least one workload)

RDP attacks grow dramatically with cloud scale

27%

Increase in **RDP exposure** across all major cloud providers

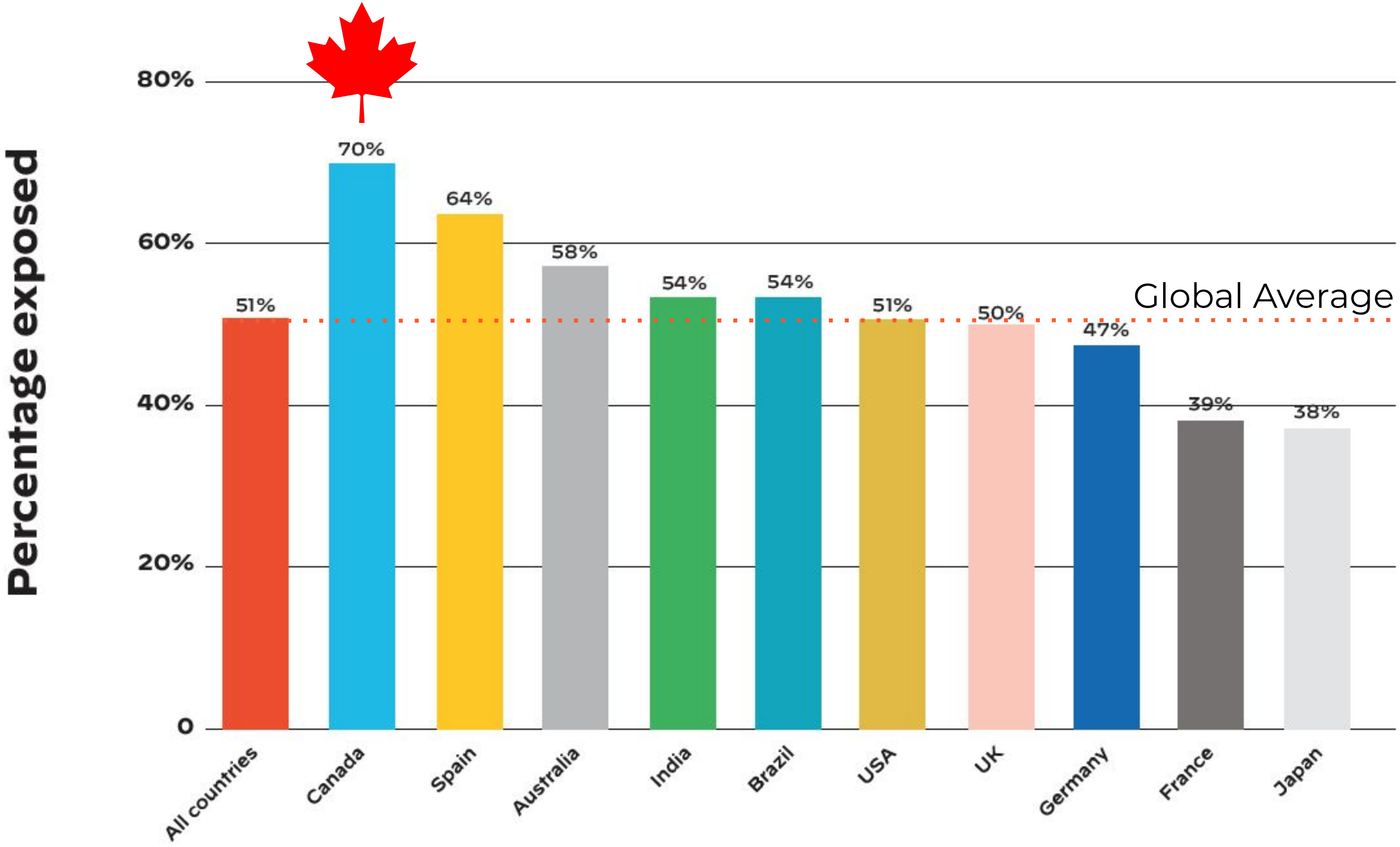
768%

Increase in **RDP attacks** between Q1 and Q4 2020*

*ESET Threat Report Q4 2020

© 2021 Palo Alto Networks, Inc. All rights reserved.

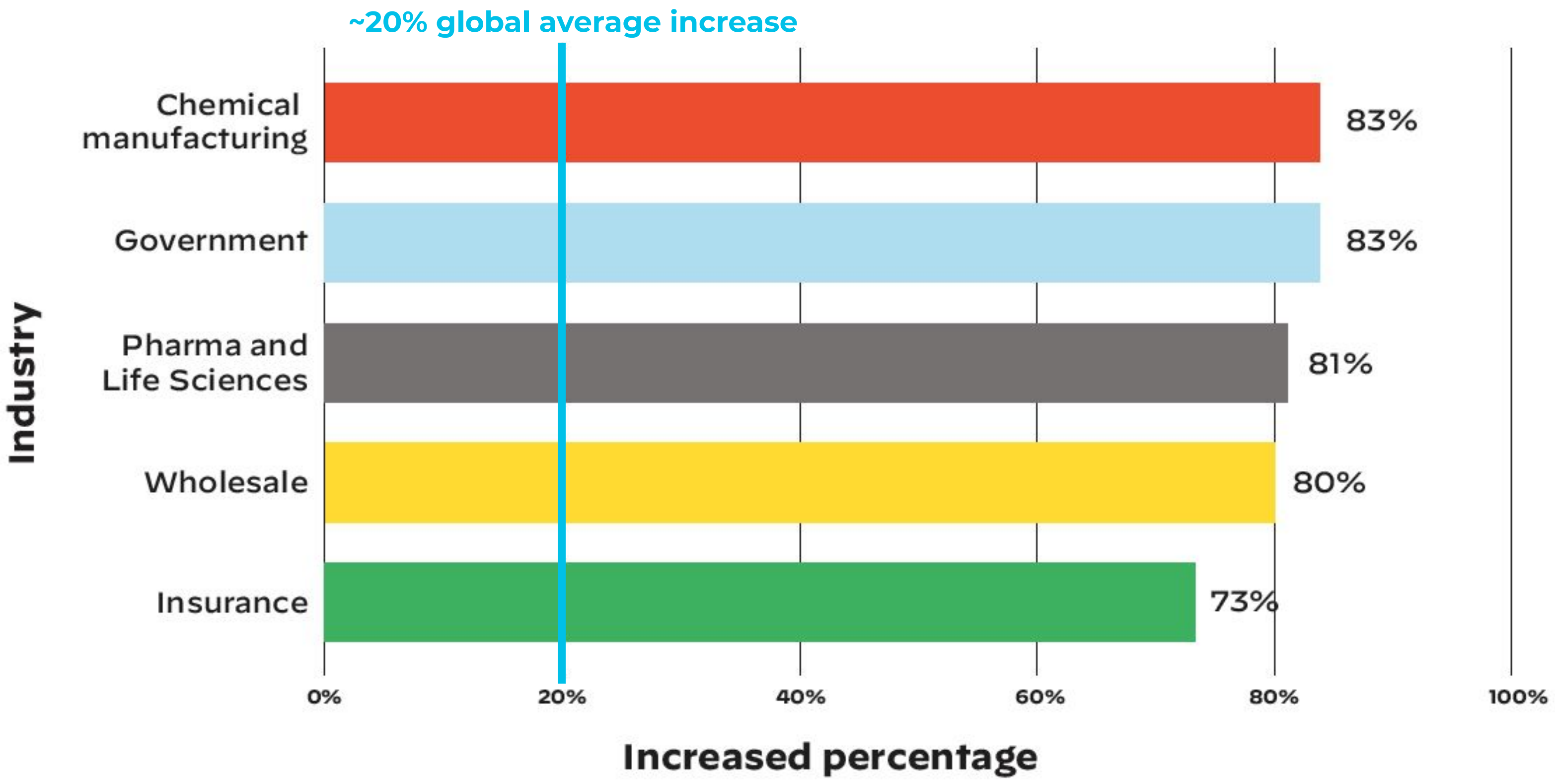
Remote work leads to risky practices...especially for Canadians



Publicly exposed RDP

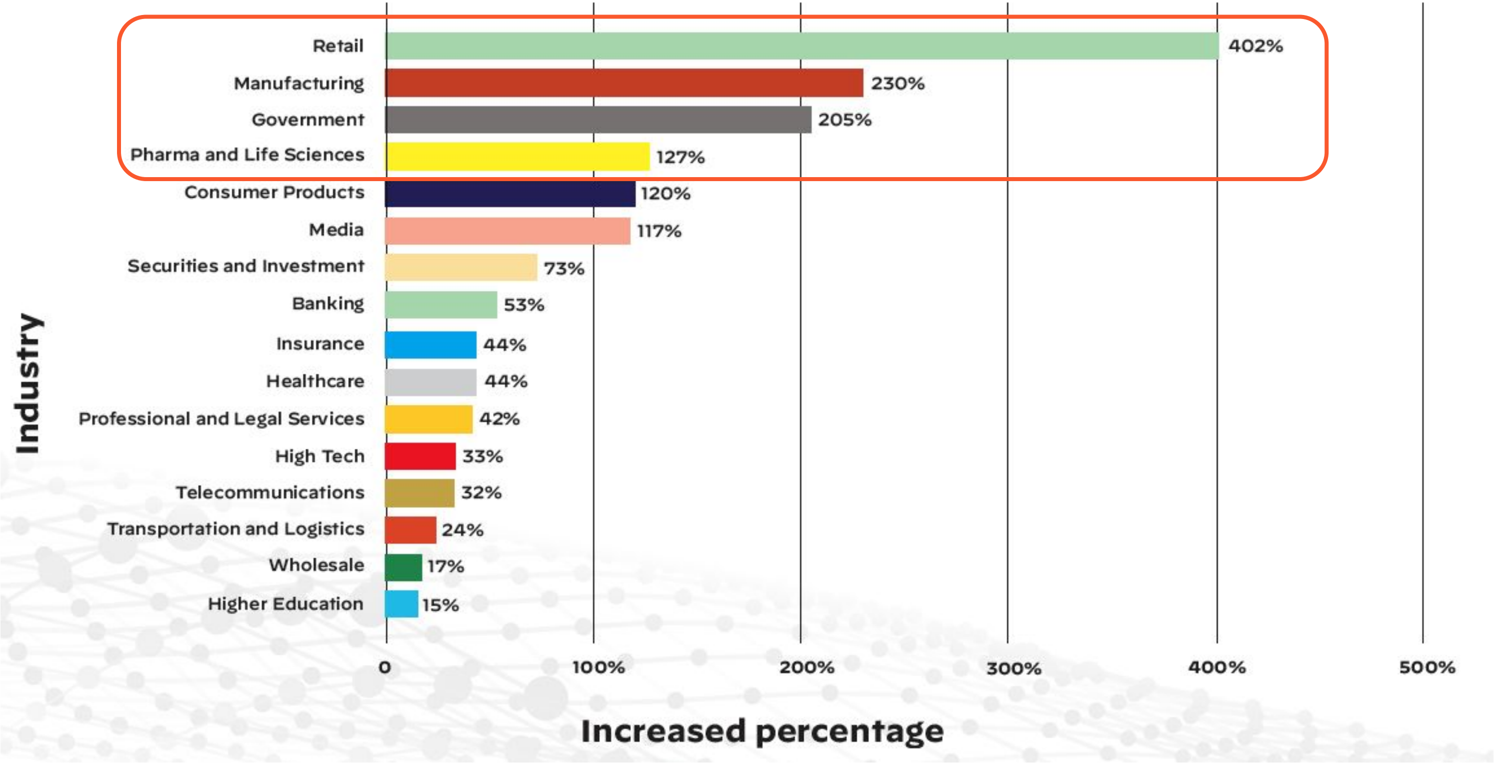
Industry Intel

Industries experiencing the greatest growth in cloud workloads



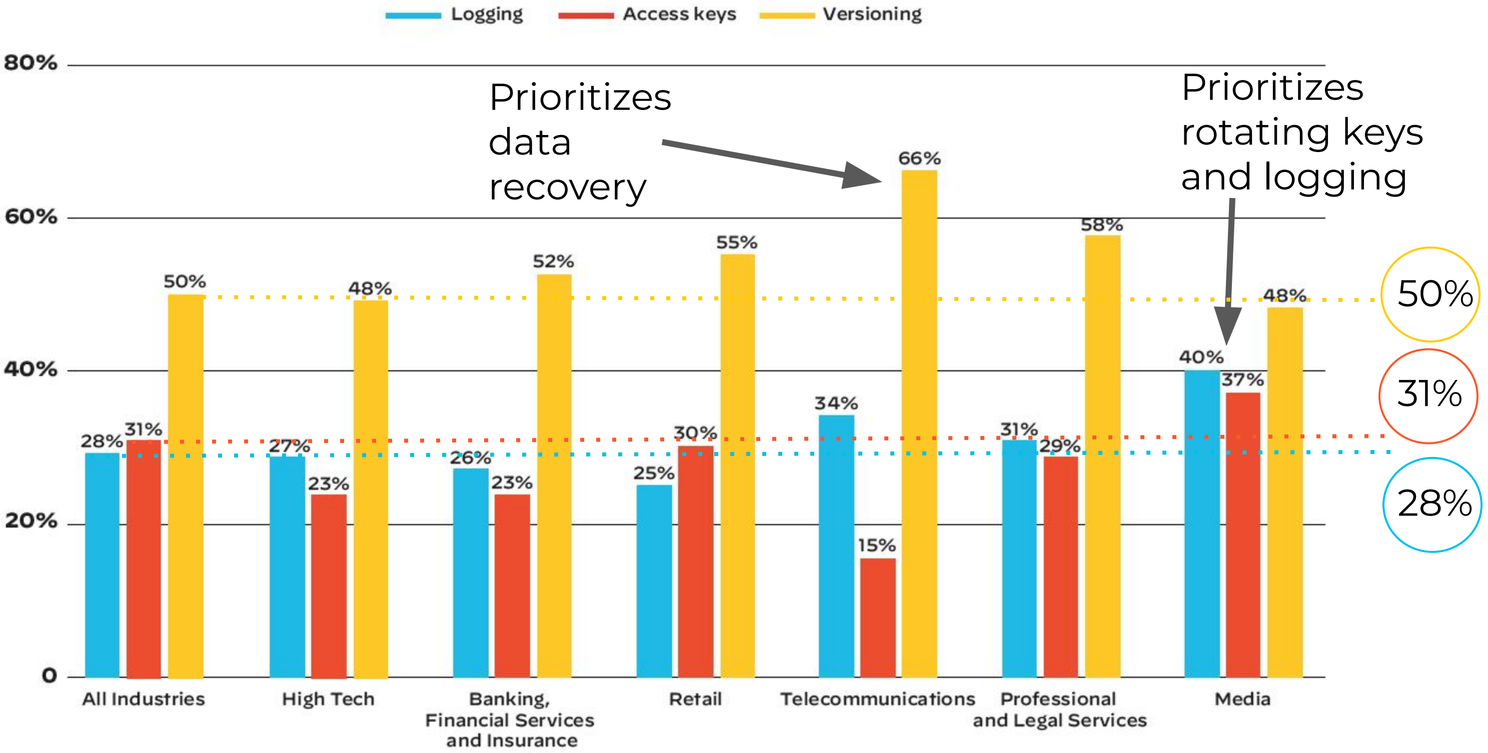
© 2021 Palo Alto Networks, Inc. All rights reserved.

Industries with the greatest increases in security incidents



© 2021 Palo Alto Networks, Inc. All rights reserved.

Some industries do better than others enabling critical controls



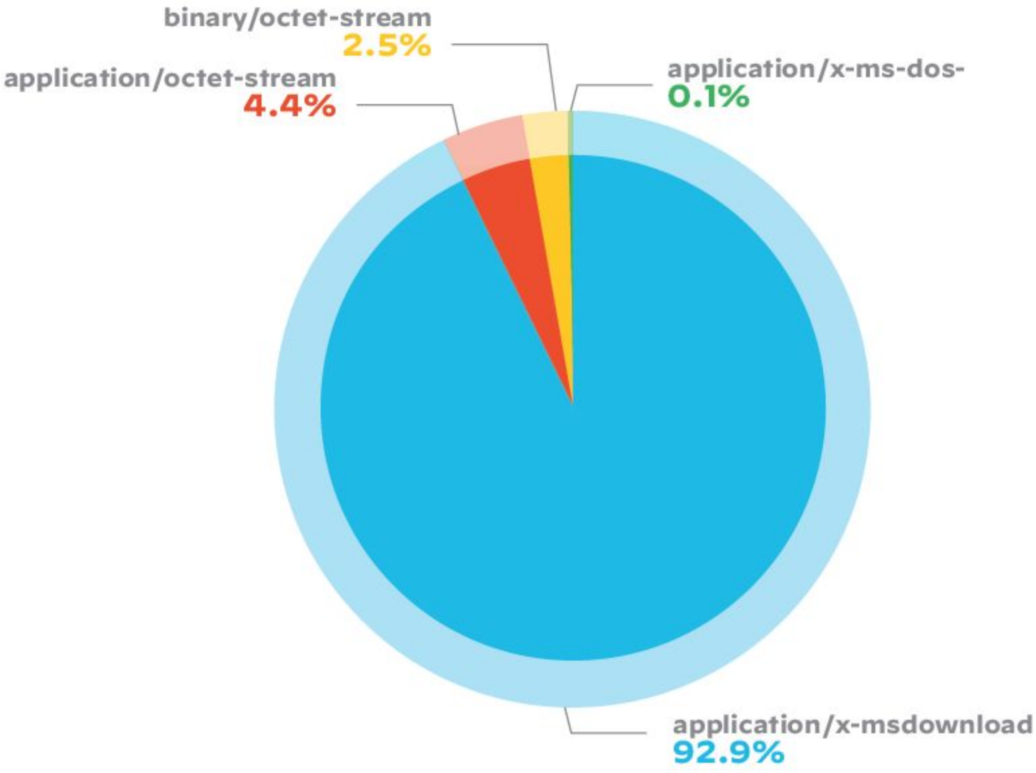
Prioritizes data recovery

Prioritizes rotating keys and logging

© 2021 Palo Alto Networks, Inc. All rights reserved.

COVID-19 and Data Security

Cloud storage and malware...good news



.01%

Malware found in cloud storage data

© 2021, Palo Alto Networks. All Rights Reserved.

What’s being stored in the cloud?

64%

of cloud data contains sensitive information

69% Contains PII

34% Contains IP

© 2020 Palo Alto Networks, Inc. All rights reserved.

30%

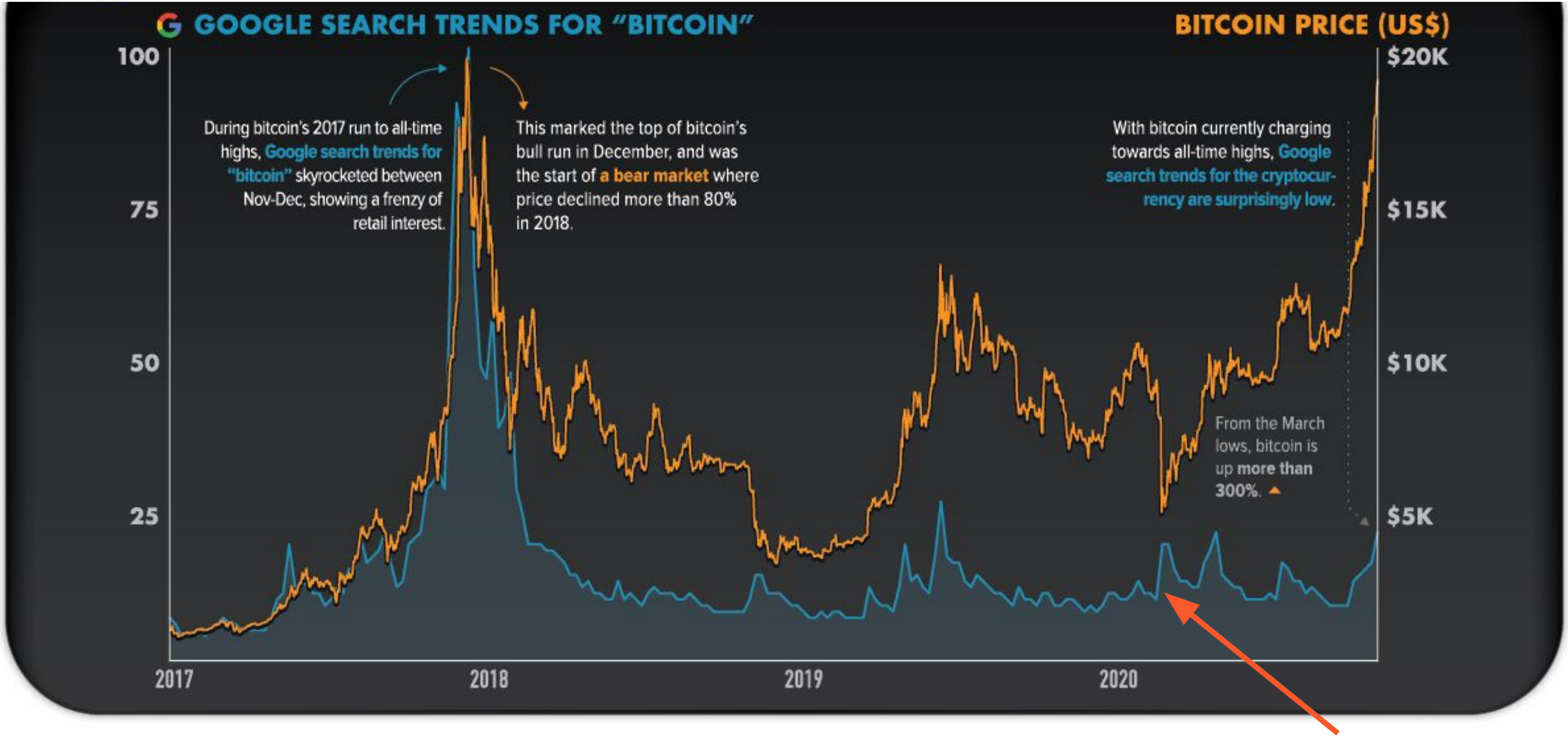
allow **public access** to sensitive data

No **auth** required

© 2021 Palo Alto Networks, Inc. All rights reserved.

Cloud, COVID-19 and Cryptocurrency

COVID-19 enabled crypto to go mainstream



During bitcoin's 2017 run to all-time highs, Google search trends for "bitcoin" skyrocketed between Nov-Dec, showing a frenzy of retail interest.

This marked the top of bitcoin's bull run in December, and was the start of a bear market where price declined more than 80% in 2018.

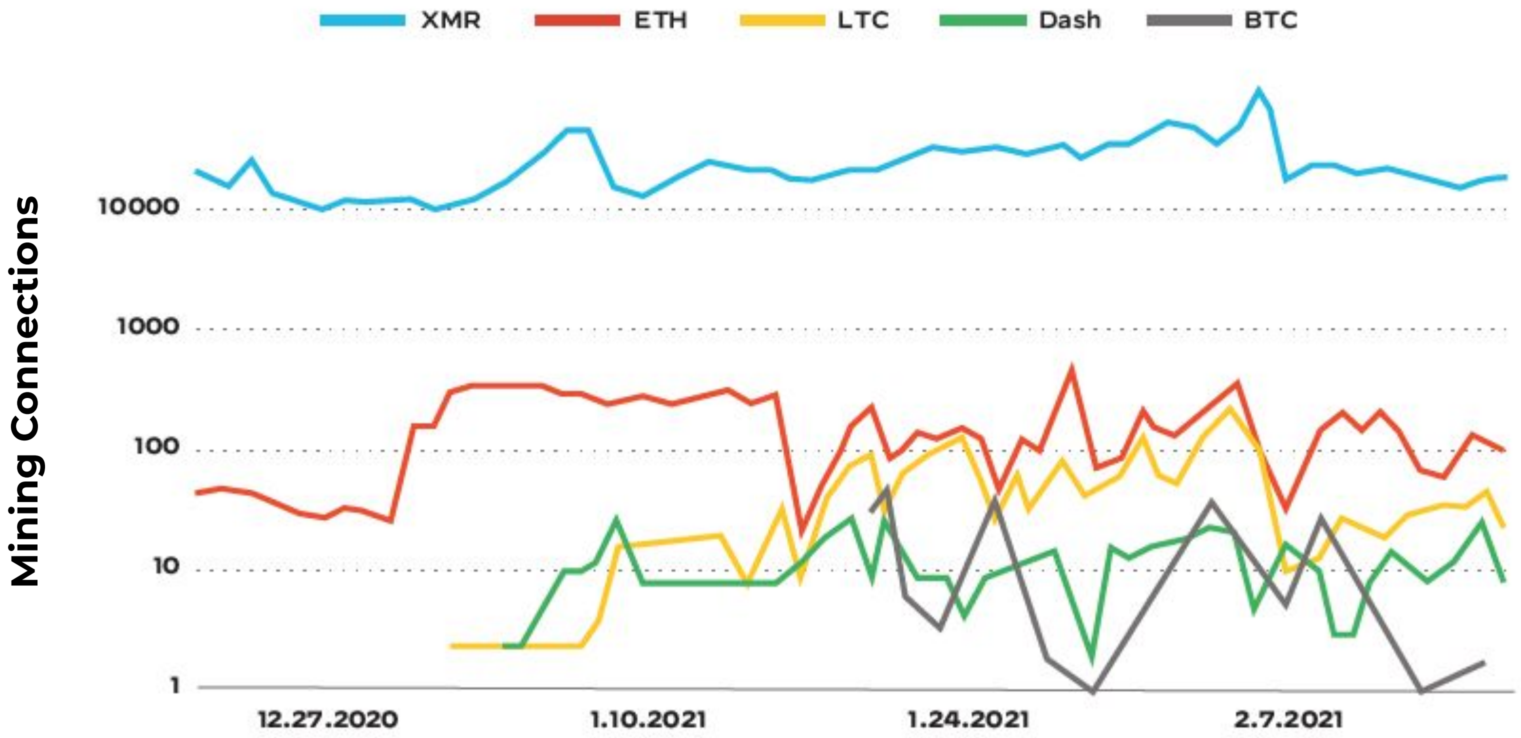
With bitcoin currently charging towards all-time highs, Google search trends for the cryptocurrency are surprisingly low.

From the March lows, bitcoin is up more than 300%.

Source: Visual Capitalist

Pandemic declared by WHO

Monero (XMR) dominates cloud mining traffic



Cryptojacking is on the decline

23%

of organizations globally experienced cryptojacking
July - Sept. 2020

17%

of organizations globally experienced cryptojacking
Dec. - Feb. 2021

Cryptojacking = unauthorized use of infrastructure for cryptomining

© 2021 Palo Alto Networks, Inc. All rights reserved.

Mitigation

Organizations have neglected to invest in the automated cloud governance necessary to ensure workloads remain secure.

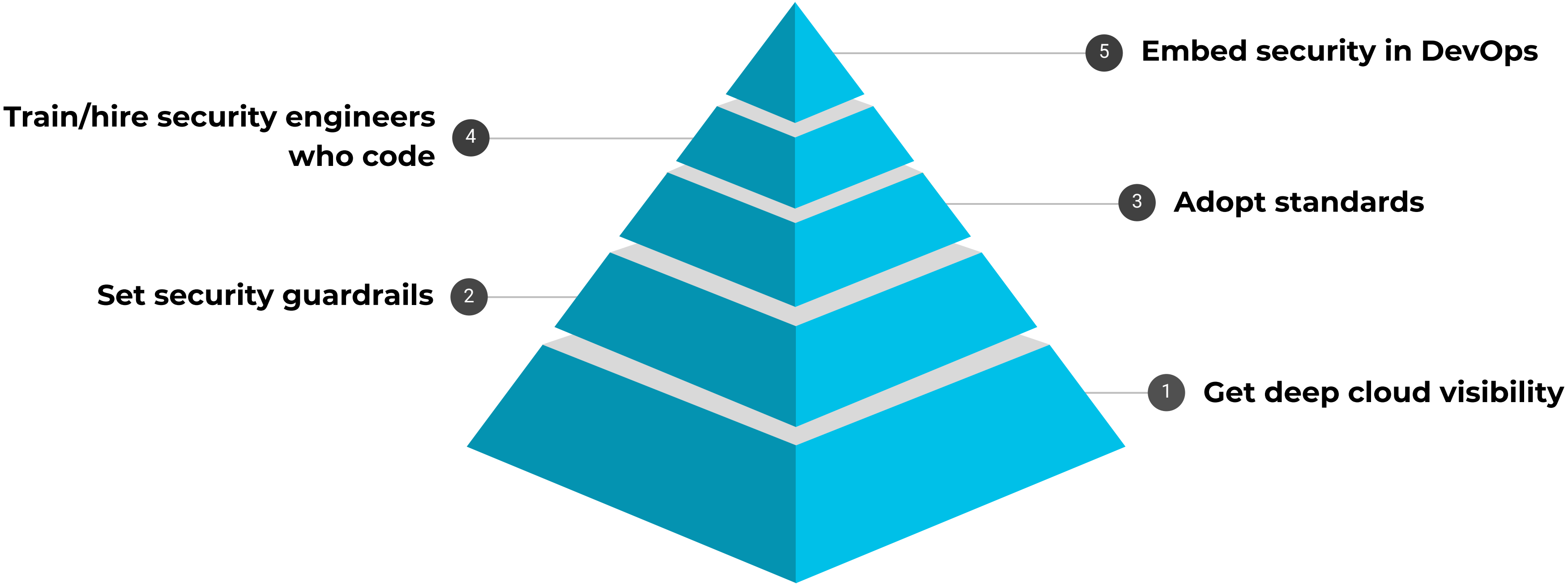
| © 2021 Palo Alto Networks, Inc. All rights reserved.

“Less than 5% of the global IT spend is **in the cloud** at this point. That’s going to **substantially change** in the coming years.”

- Andy Jassy, CEO Amazon (March 2021)

© 2021 Palo Alto Networks, Inc. All rights reserved.

The Big Cloud 5 - patterns of cloud security excellence



5 Embed security in DevOps

4 Train/hire security engineers who code

3 Adopt standards

2 Set security guardrails

1 Get deep cloud visibility

Blog: cloudthreat.report/bc5

| © 2020 Palo Alto Networks, Inc. All rights reserved.

How Prisma Cloud Can Help

Prisma Cloud:
Our Vision for Public Cloud Security

Comprehensive

Consistency across tech stacks, clouds, and app components

Best-in-Class

Each capability best by itself, and made better through integration

Full Application Lifecycle

Integrated from left to right, not only at runtime

© 2020 Palo Alto Networks, Inc. All rights reserved.

Prisma Cloud

Comprehensive cloud native security across the entire application lifecycle

DevSecOps

Integrate and perform infrastructure and application security in the CI/CD pipeline

Cloud Security Posture Management

Monitor posture, detect and respond to threats, maintain compliance

Cloud Workload Protection

Secure hosts, containers, and serverless across the application cycle

Cloud Network Security

Monitor and secure cloud networks, enforce microsegmentation

Cloud Infrastructure Entitlement Management

Enforce permissions and secure identities across workloads and clouds

Prisma Cloud Comprehensive Cloud Native Security.

Full Lifecycle. For Any Cloud.

paloalto NETWORKS