



The Agenda

- 01 Introduction
- 02 The Growing Importance of WFH Security
- 03 Cloud Security Now Mandatory



Introduction





About Horangi.

Horangi is a leading cybersecurity company founded by ex Palantir Technologies engineers and is headquartered in Singapore. Horangi's best-in-class Warden cloud security platform protects organizations in the public cloud, complemented by an elite team of cybersecurity experts providing CREST-accredited offensive and strategic cybersecurity services to customers across the world.

- Gartner-recognized cloud security platform for AWS, GCP, Azure
- AWS Security Competency Partner and ISV Accelerate Member
- Backed by CREST-certified global cybersecurity experts
- Founded by ex-Palantir cybersecurity experts in 2016
- Trusted by cloud-native innovators and enterprises





KEVIN LEE

Chairman

Kevin is the executive chairman of Horangi Cyber Security.

Previously, Kevin was the Head of GIC Labs at GIC, where he led GIC's efforts to harness innovation, technology and data science in investing. Before that, he was VP Data and Growth at Grab, where he started and built out Grab's capabilities in AI and data science.

Earlier, he was Head of Asia at Palantir Technologies, where he started and built out Palantir's Asia business, working with customers from a wide variety of industries to harness the power of data in their organizations.

Kevin also served in the Administrative Service in the Singapore Government in the Prime Minister's Office and Ministry of Finance. Kevin graduated with Distinction from Stanford University where he majored in Computer Science.

PREVIOUS POSITIONS

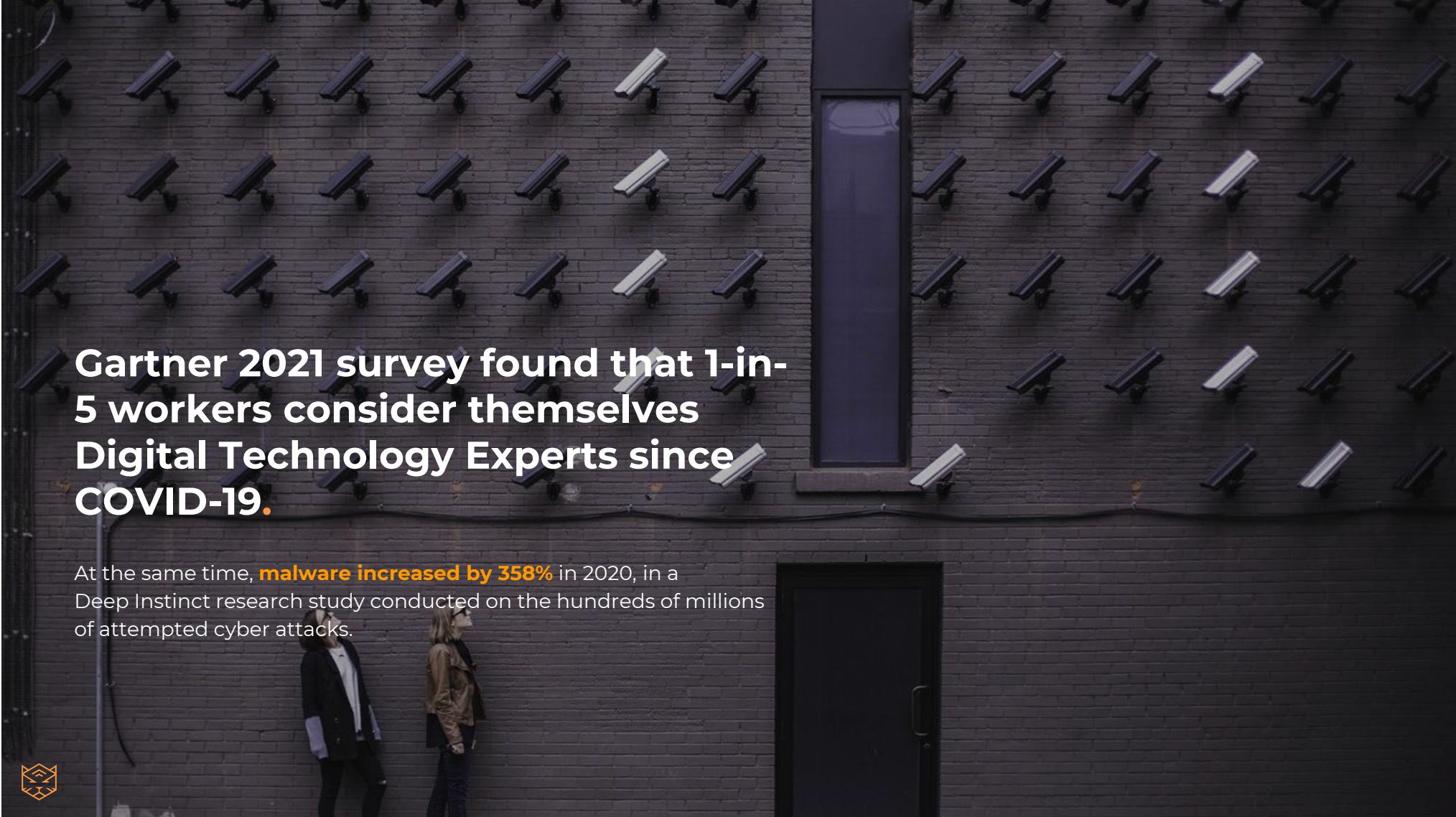
Head of GIC Labs, GIC

VP Data and Growth, Grab

Head of Asia, Palantir Technologies

The Growing Importance of WFH Security





Gartner 2021 survey found that 1-in-5 workers consider themselves Digital Technology Experts since COVID-19.

At the same time, **malware increased by 358%** in 2020, in a Deep Instinct research study conducted on the hundreds of millions of attempted cyber attacks.



WHAT IS THE BIGGEST RISK?

**According to Verizon,
70% of cyber attacks
use phishing in some
way.**

A Deloitte report revealed that **47%** of individuals fall for phishing scams while working at home.





**Between Feb and May 2020,
there were more than 500,000
cyber attacks on video
conferencing services.**

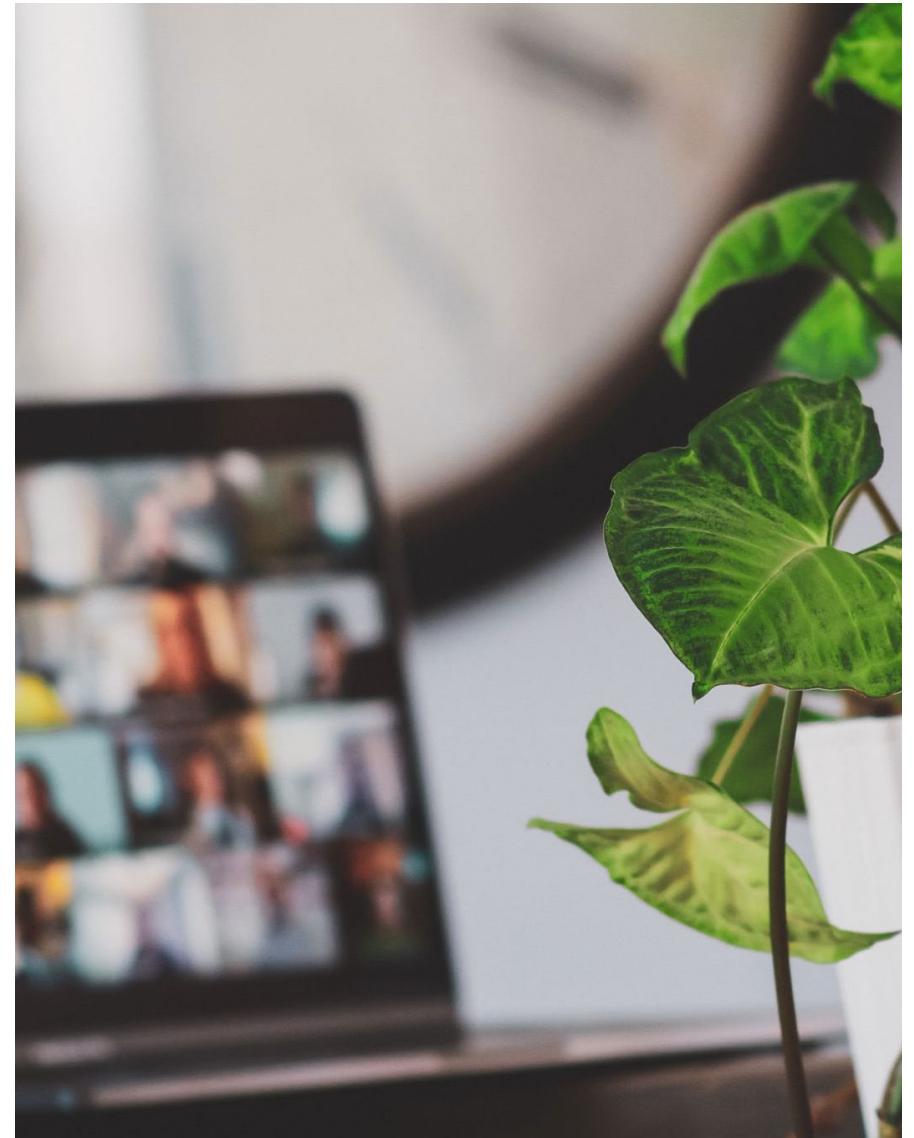


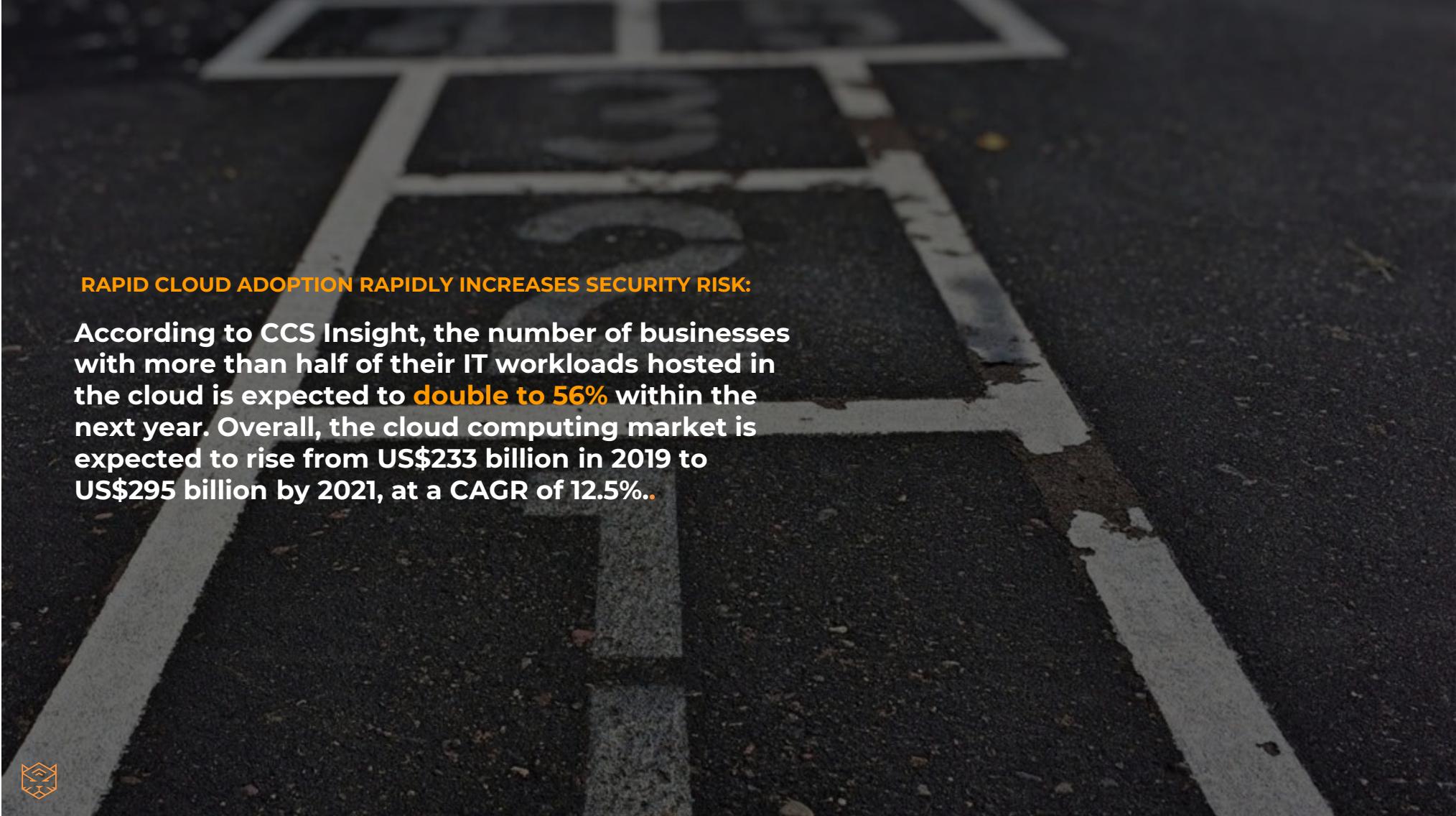
New attack vectors while working from home

Back in the office, it was easy for a user who received a malicious email to turn to the person next to them or walk over to a colleague to verify the email.

Being remote, this isn't an option anymore. And attackers will exploit this. A skilled attacker will create a sense of urgency within the email with the intent to make the user do as the attacker wants before the user has time to think too much about it.

When you are alone at home, the odds swing in the attacker's favor.

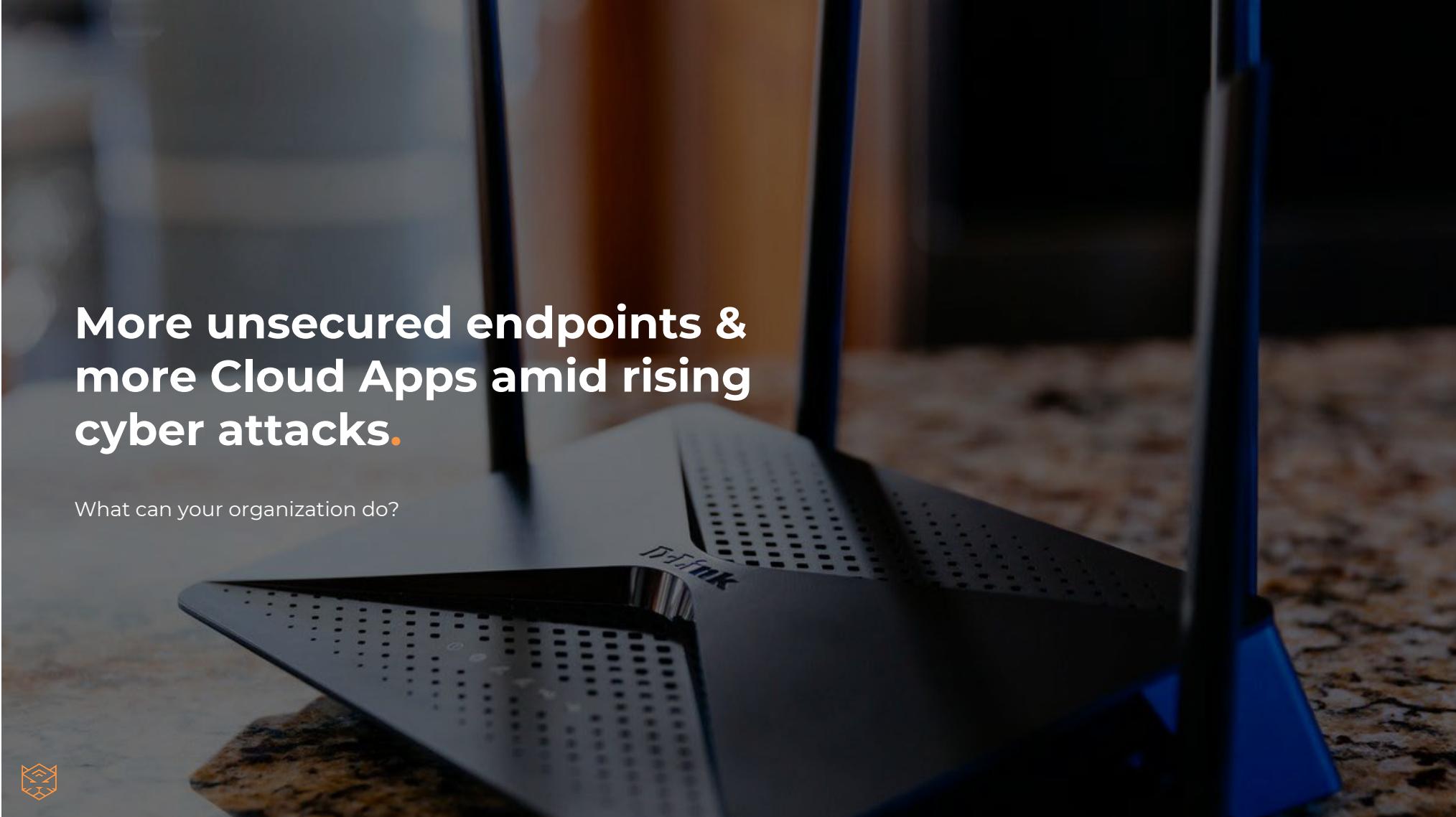




RAPID CLOUD ADOPTION RAPIDLY INCREASES SECURITY RISK:

According to CCS Insight, the number of businesses with more than half of their IT workloads hosted in the cloud is expected to double to 56% within the next year. Overall, the cloud computing market is expected to rise from US\$233 billion in 2019 to US\$295 billion by 2021, at a CAGR of 12.5%..





**More unsecured endpoints &
more Cloud Apps amid rising
cyber attacks.**

What can your organization do?



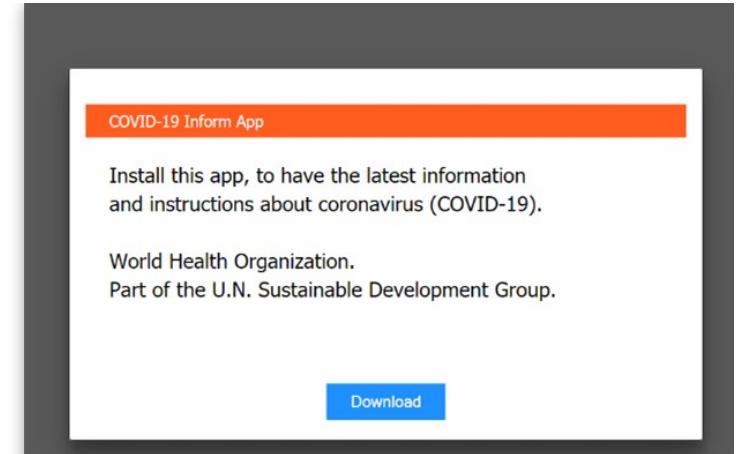
BEST PRACTICE:

Strong cybersecurity awareness and implementing additional security policies.

Adopt a robust phishing simulation program and ensure stronger home network security and enhanced endpoint protection.

The **Zero Trust Model** needs to be adhered to in light of the explosion of devices and users.

It also pays to conduct frequent security reviews.

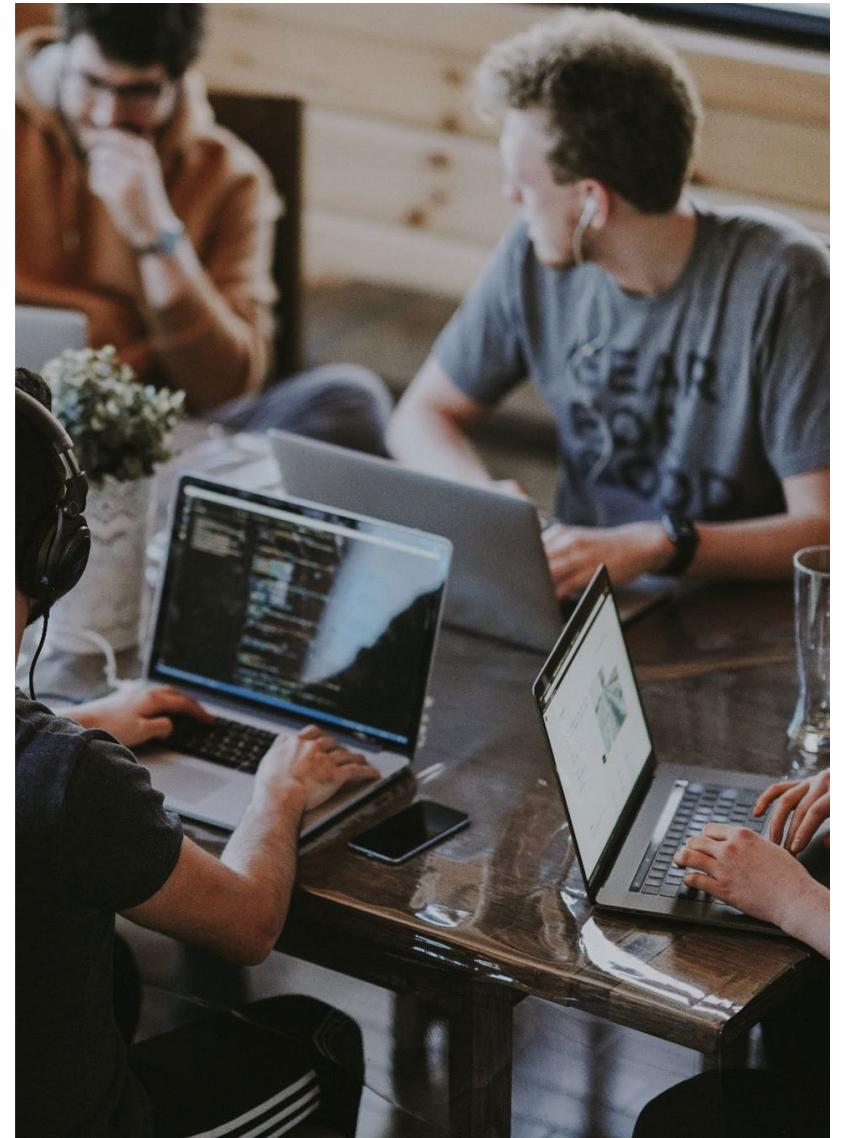


BEST PRACTICE:

Don't forget about the workers who are out of sight.

Use a remote desktop (e.g. AWS Workspaces) for temporary employees or other personnel who aren't issued a company laptop.

Adopt stringent onboarding and offboarding processes and policies to mitigate insider threat risk.

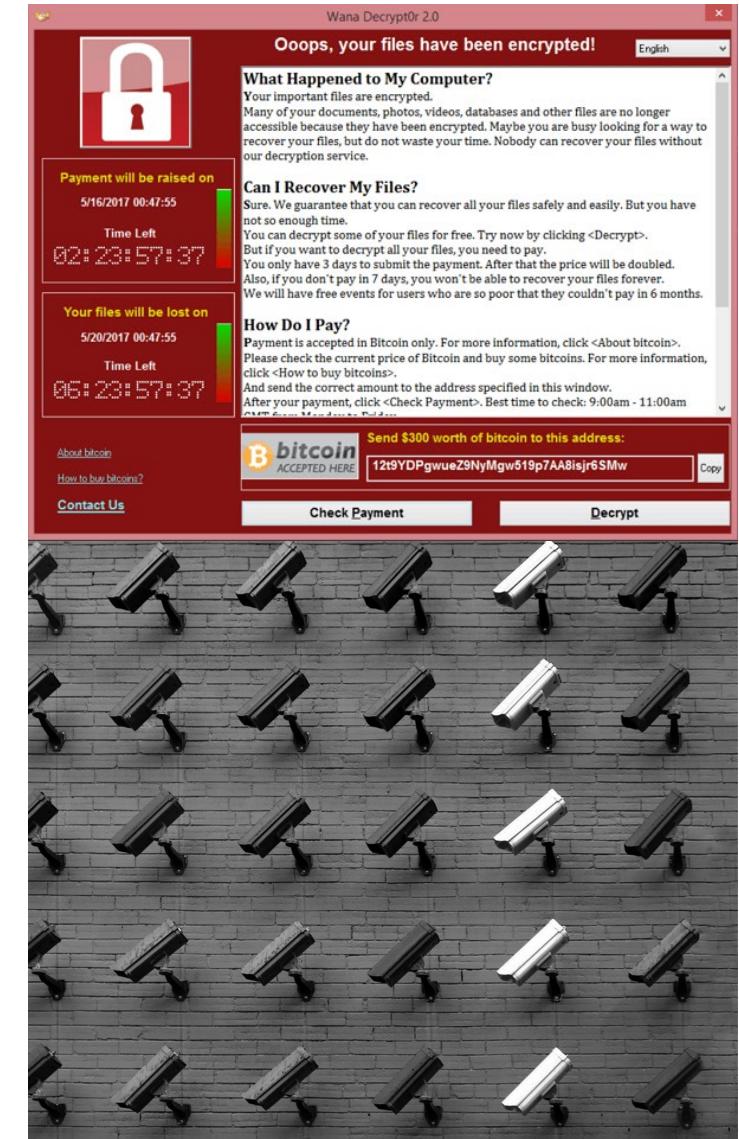


BEST PRACTICE:

Data Loss Prevention (DLP) in the cloud.

In spite of continuously trying to improve access management, there is still a high possibility that someone downloads sensitive data to an unprotected environment when working from home.

Horangi procured Google DLP solution to monitor potential leak of data from the cloud storage. This is a focus on visibility and monitoring, **taking a proactive stance** that mistakes and attacks will happen.



BEST PRACTICE:

Monitor threats to your VPN.

VPNs are the most used and often most vulnerable tool in the WFH setup. If you host the VPN in the cloud (like how Horangi hosts it on AWS), you have to monitor threats to VPN.

Currently Horangi uses GuardDuty, but we are developing our own threat monitoring functions on Warden and look forward to using that.



threatPost Cloud Security / Malware / Vulnerabilities / Waterfall Security Spotlight / Podcasts f t in d Search

← Responding to the New Normal: How to Prevent Added Risk in Your Business

As Zoom Booms, Incidents of 'ZoomBombing' Become a Growing Nuisance →

Hackers Hijack Routers to Spread Malware Via Coronavirus Apps



Author:
Lindsey O'Donnell
March 26, 2020
10:47 am

1 minute read

The router DNS hijacking attacks have targeted more than a thousand victims with the Oski info-stealing malware.

Cybercriminals are hijacking routers and changing Domain Name System (DNS) settings, in order to redirect victims to attacker controlled sites promoting fake coronavirus information apps. If victims download these apps, they are infected with information-stealing Oski malware.

New DNS Hijacking Attack Exploiting DLink Routers to Target Netflix, PayPal, Uber, Gmail Users

By BALAJI N · April 8, 2019 · 0



DNS Hijacking Attack Exploiting D-Link Routers to Target Netflix, PayPal, Uber, Gmail Users

Cybercriminals continuously perform DNS hijacking attack to the consumer's routers over the past 3 months, and the sites targeted for phishing includes Netflix, PayPal, Uber, Gmail.

DNS hijacking is a type of malicious attack that used to redirect the users to the malicious website when they visit the website via compromised routers or attackers modifying a server's settings.

Attackers abusing the hosts on the network of Google Cloud Platform to conduct this exploit attempts against consumers routers.

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security
January 15, 2020



7 Tips for Maximizing Your SOC December 31, 2019



Mean Time to Hardening: The Next-Gen Security Metric December 10, 2019



Combining AI and Playbooks to Predict Cyberattacks December 23, 2019



The Case for Cyber Risk Prospectives December 04, 2019



Newsletter
Subscribe to Threatpost Today
Join thousands of people who receive the latest breaking cybersecurity news every day.

Subscribe now

Twitter
During our live April 23 #webinar a panel of experts will discuss critical steps that you can take to secure your... <https://t.co/Qb5ScrvVjk>

10 hours ago

Follow @threatpost

Newsletter

Signup to get Hacking News & Tutorials to your Inbox

Name

Email*

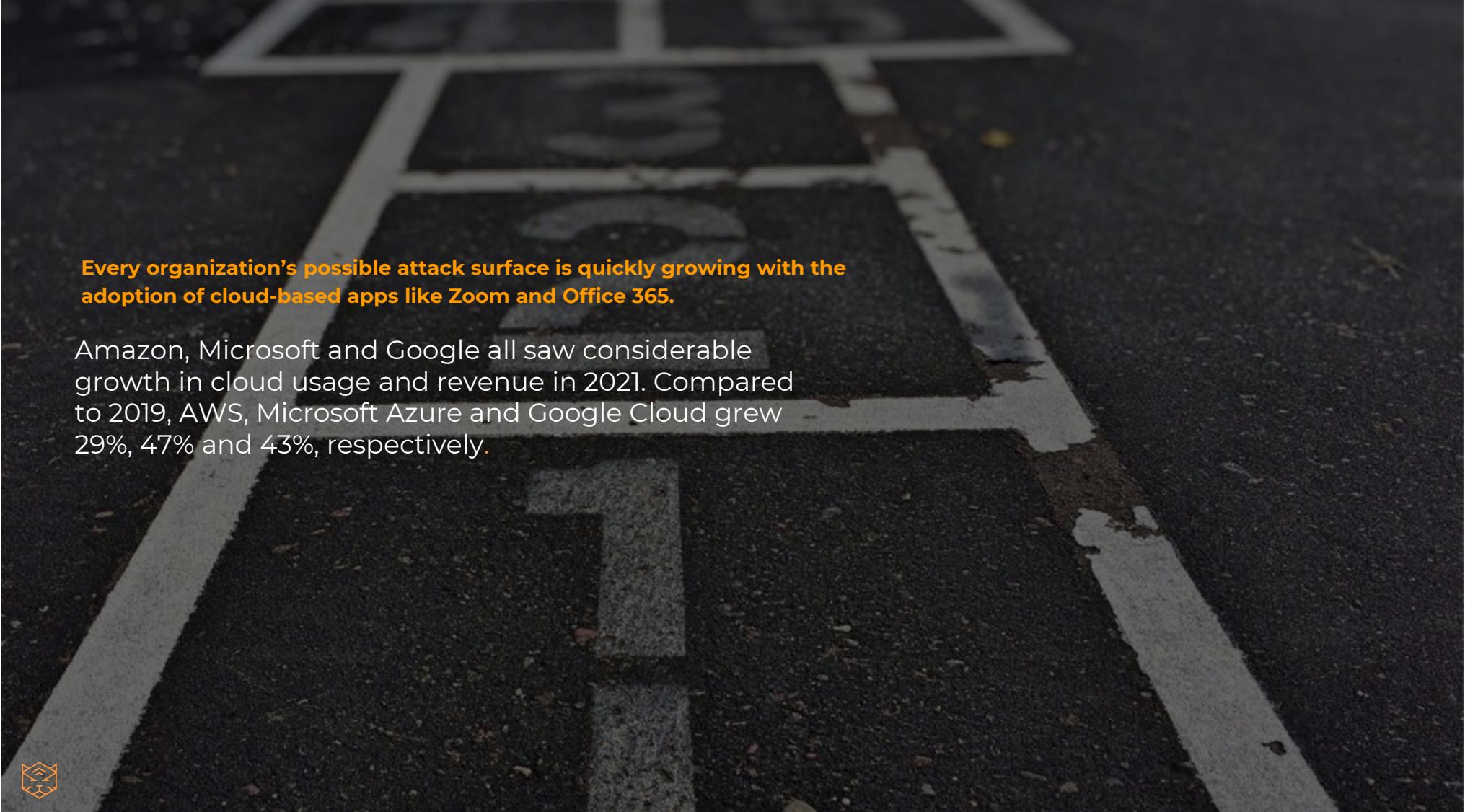
Subscribe

Penetration Testing as a Service

TWINTECH
Penetration Testing as a Service (PTaaS)
We will test the effectiveness of your own security controls before malicious parties do it for you.
[Enquire More](#)



**Cloud Security
Now Mandatory**



Every organization's possible attack surface is quickly growing with the adoption of cloud-based apps like Zoom and Office 365.

Amazon, Microsoft and Google all saw considerable growth in cloud usage and revenue in 2021. Compared to 2019, AWS, Microsoft Azure and Google Cloud grew 29%, 47% and 43%, respectively.



“

Through 2023, at least 99% of cloud security failures will be the customer's fault.

Only 10% of CISOs report they fully understand the shared responsibility model, and 82% have experienced security incidents due to confusion over who has responsibility for what's in the cloud. This can lead to the mistaken belief that executives aren't liable for losses as a result of a cloud breach.





The Central Identity & Access Management (IAM) Problem:

Do you know who has access to your most sensitive resources?

- a. I'm not quite sure where I'd start answering that
- b. I have paid a Security Consultant to do this for me before
- c. Someone on my security team does this manually in a spreadsheet
- d. No sweat, I can answer this in less than five minutes





Security teams cannot adapt fast enough and are ill- prepared for this cloud explosion.

If developers can spin up and shut down cloud instances in a few clicks, how can security teams gain full visibility of this growing and fast-changing network?

This lack of visibility makes risk assessment more challenging, and they either become overly permissive or they lock everything down.



“

**By 2023, 75% of security failures
will result from inadequate
management of identities,
access, and privileges, up from
50% in 2020.**

Managing Privileged Access in
Cloud Infrastructure, Gartner



Identity Management

The cornerstone of IAM



Nearly all breaches involve
misuse of an identity.

Number of identities is growing
exponentially.

Identity Management is **shared**
between functions.

Access Management

Who can do **what** to which resource?



Traditionally seen as a **balance between security and speed**.

Too much access

Security risks blow out of control

Too little access

Slows development and innovation

IAM Complexity



Complexity of **Scale**



Complexity of **Understanding**



Complexity of **Change**



2019 CAPITAL ONE DATA BREACH:

Personal data of 100M customers exfiltrated because of excessive permissions.



US\$80 million civil penalty levied on Capital One for failing to adequately identify and manage risk in this 2019 data breach.

Unnecessary permissions?

S3 List: The indictment states that the role used by the attacker did not require access to list S3 buckets “in the normal course of business”

S3 Sync: Allowed copying of entire S3 buckets to the attacker’s computer



Capital One Financial Corporation is an American bank holding company specializing in credit cards, auto loans, banking, and savings accounts.

BEST PRACTICE:

Visibility is everything. Take stock of your cloud apps and users in your cloud infrastructure.

You can only protect what you know, and having central visibility solves the pivotal problem created by cloud sprawl.

Look at solutions classified as SSPM and CIEM.

Because our customers did not have an easy solution to this, Horangi created a platform to help provide this cloud visibility.

The screenshot displays the Horangi Cloud Security Platform's user interface. At the top, there's a navigation bar with tabs for OVERVIEW, RULES, RESOURCES, COMPLIANCE, and IAM (BETA). The main area is divided into several sections:

- Latest Scan:** Shows the date "19 Apr 2021, 8:43am".
- Identities:** A list of categories: Users (14), Federated Users (3), Roles (59), Groups (0), Services (11), and Service Accounts (35). Below this is a "VIEW ALL IDENTITIES" button.
- Resources:** A circular progress bar indicating 175 resources across categories: Network (91), Storage (46), Security (18), Data (11), and Compute (9). Below this is a "VIEW ALL RESOURCES" button.
- Identities Resources:** A table listing identities categorized by provider (AWS) and their associated resources. The table includes columns for Provider, Identity, and Resource Category. Examples include "flowlog-role-ren" (Compute, Network, Storage, Data, Security), "arn:aws:iam::441" (Compute, Network, Storage, Data, Security), and "AWSCloudForm" (Compute, Network, Storage, Data, Security).
- Identities Permissions:** A table listing identities categorized by provider (AWS) and their associated permissions. The table includes columns for Provider, Identity, and Permission. Examples include "cloudtrail.lama" (TAGGING, WRITE, READ, LIST), "arn:aws:iam::31" (WRITE, READ, LIST, TAGGING, PERMISSIONS), and "StackSet-tgr-c" (READ, WRITE).



BEST PRACTICE:

Gain the ability to immediately fix cloud security threats. Eliminate human error.

With the speed of change in the cloud, you can leverage security and compliance automation to fix threats as they come so they don't get forgotten.

Look at solutions classified as CSPM and CWPP.

CSPM has now been classified as a **mandatory tool by Gartner**.

The screenshot shows the Horangi Storyfier web application interface. At the top, there's a navigation bar with the Horangi logo, a user profile icon labeled 'Demo', and tabs for 'OVERVIEW', 'RULES' (which is selected), 'RESOURCES', and 'COMPLIANCE'. A banner at the top right says 'After 22 January 2021, your product trials will expire. Contact us' with an exclamation mark icon. On the left, there's a sidebar with filters like 'FILTER', 'TAG', 'Search', 'ACCOL', 'All', 'REGION', 'All', 'RESOURCE', 'S3 Bu...', 'SEVER...', 'All', 'SCOR...', 'Fail', and 'STATUS'. The main content area displays a table of findings for a 'production account' (AWS Account No: 829960215233). The table has columns for 'Region', 'Resource Type', 'Resource', 'Severity', 'Scoring', and 'Status'. There are seven rows, each corresponding to an S3 Bucket with a specific ARN and a 'MED' severity level. All findings are marked as 'Fail' and 'Open'. The last row is for 'S3 Bucket Default Server-Side Encryption Not Enabled'.

Region	Resource Type	Resource	Severity	Scoring	Status
global	S3 Bucket	arnaws:s3::steve-trail1-logging	MED	Fail	Open
global	S3 Bucket	arnaws:s3::test-bucket-tim123-logging-logging	MED	Fail	Open
global	S3 Bucket	arnaws:s3::test-cloud-trail-warden-dev-logging	MED	Fail	Open
global	S3 Bucket	arnaws:s3::test-public-bucket-horangi-logging	MED	Fail	Open
global	S3 Bucket	arnaws:s3::tim-test-bucket-remediation-1	MED	Fail	Open
global	S3 Bucket	arnaws:s3::tim-test-bucket-remediation-1-logging-logging	MED	Fail	Open
global	S3 Bucket	arnaws:s3::tim-test-bucket-remediation-2	MED	Fail	Open
S3 Bucket Default Server-Side Encryption Not Enabled					



The Takeaway.



Attackers are always finding new ways to breach networks. To comprehensively tackle the new WFH and cloud security risks, keep your security posture robust with the latest innovative solutions:

- ✓ Nurture strong cyber hygiene and cloud security expertise in your organization
- ✓ Leverage software (VPN, SSPM, CSPM) to continuously audit and protect the data, apps, and endpoints in your network.
- ✓ Adopt the Zero Trust Model across existing, temporary, and departing users, while having a robust incident response plan.

