The Agenda

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

Introduction

aws partner network

Advanced
Technology Partner

Security ISV Partner

AWS Public Sector Partner

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

gojek vodacom Singlife SAFEGRAPH

BukaLapak tiket.com direct asia A HISCOX COMPANY income made different CARDUP

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.

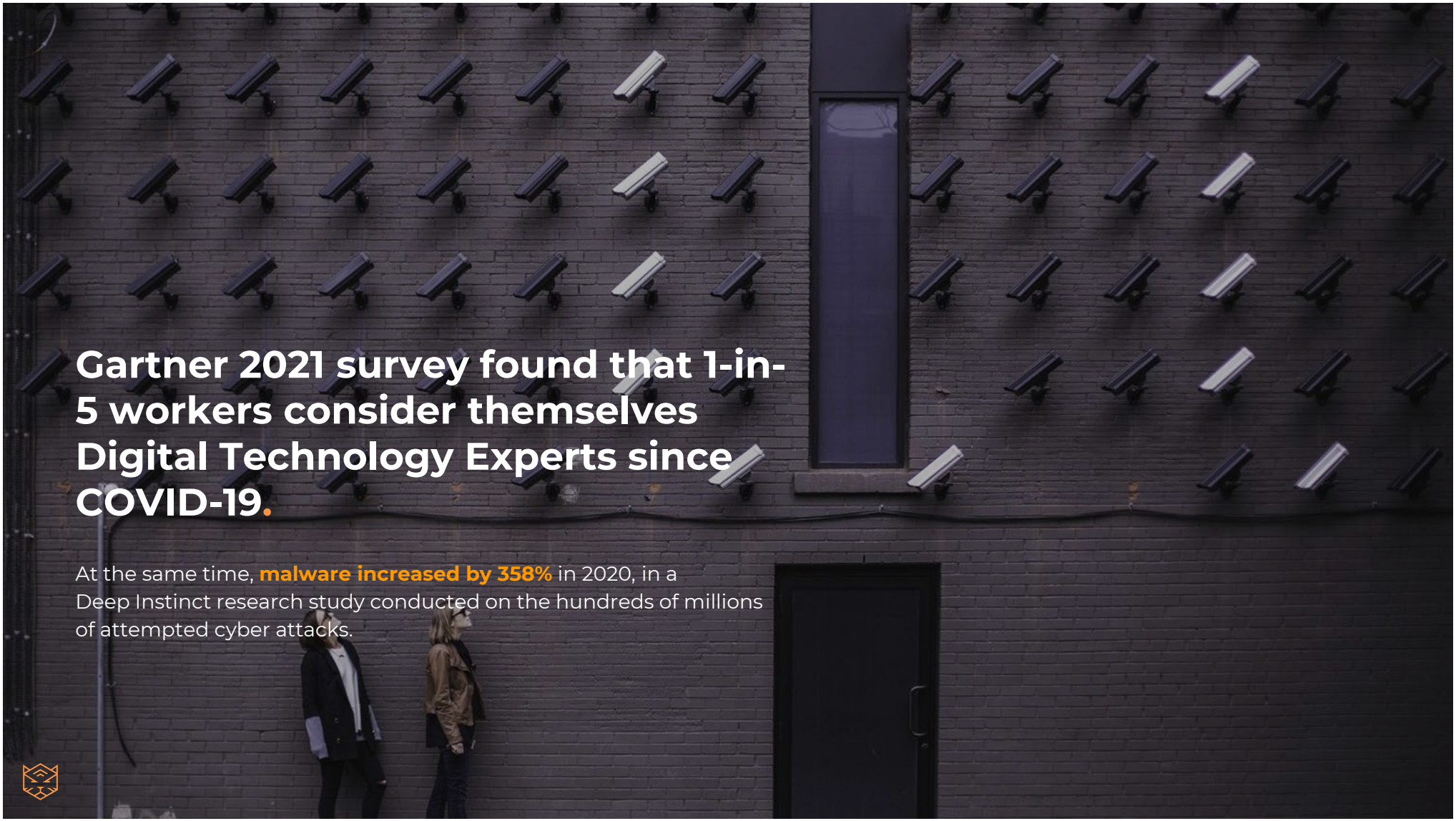
PREVIOUS POSITIONS

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.

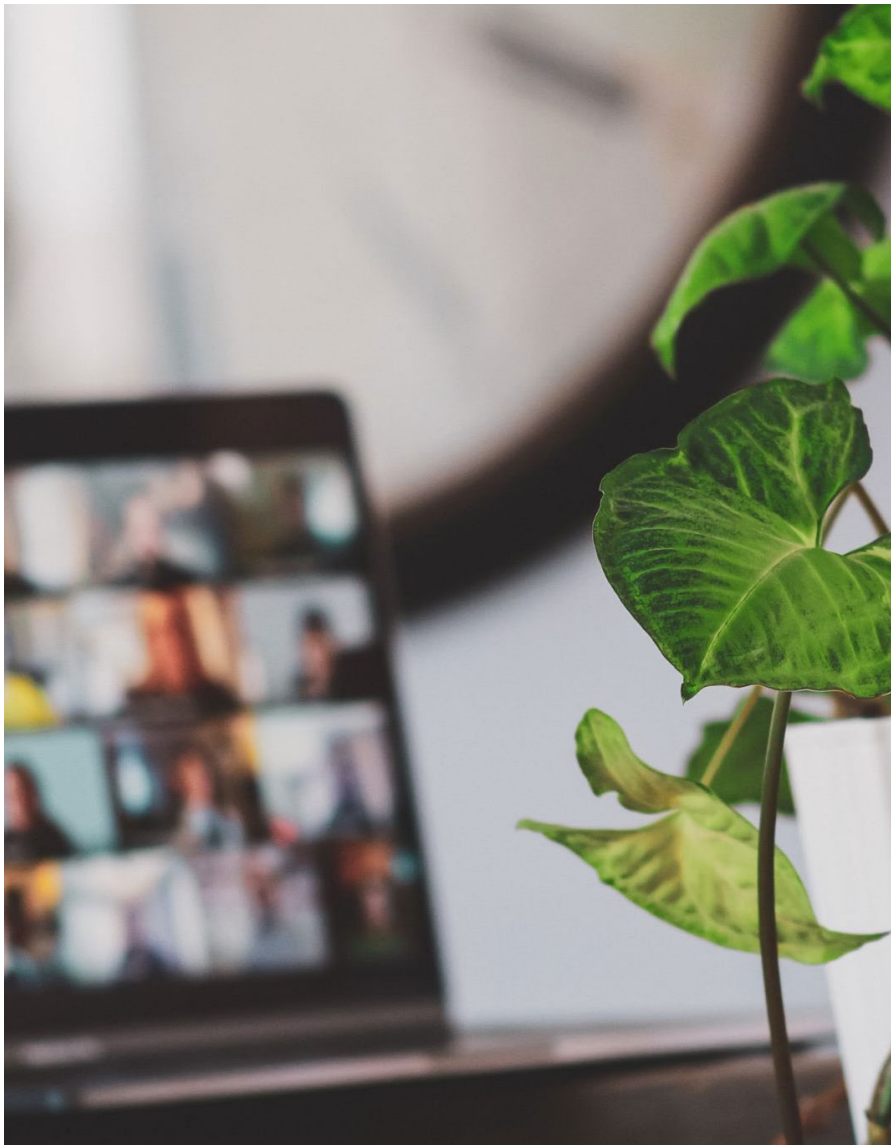
Between Feb and May 2020, there were more than 500,000 cyber attacks on video conferencing services.

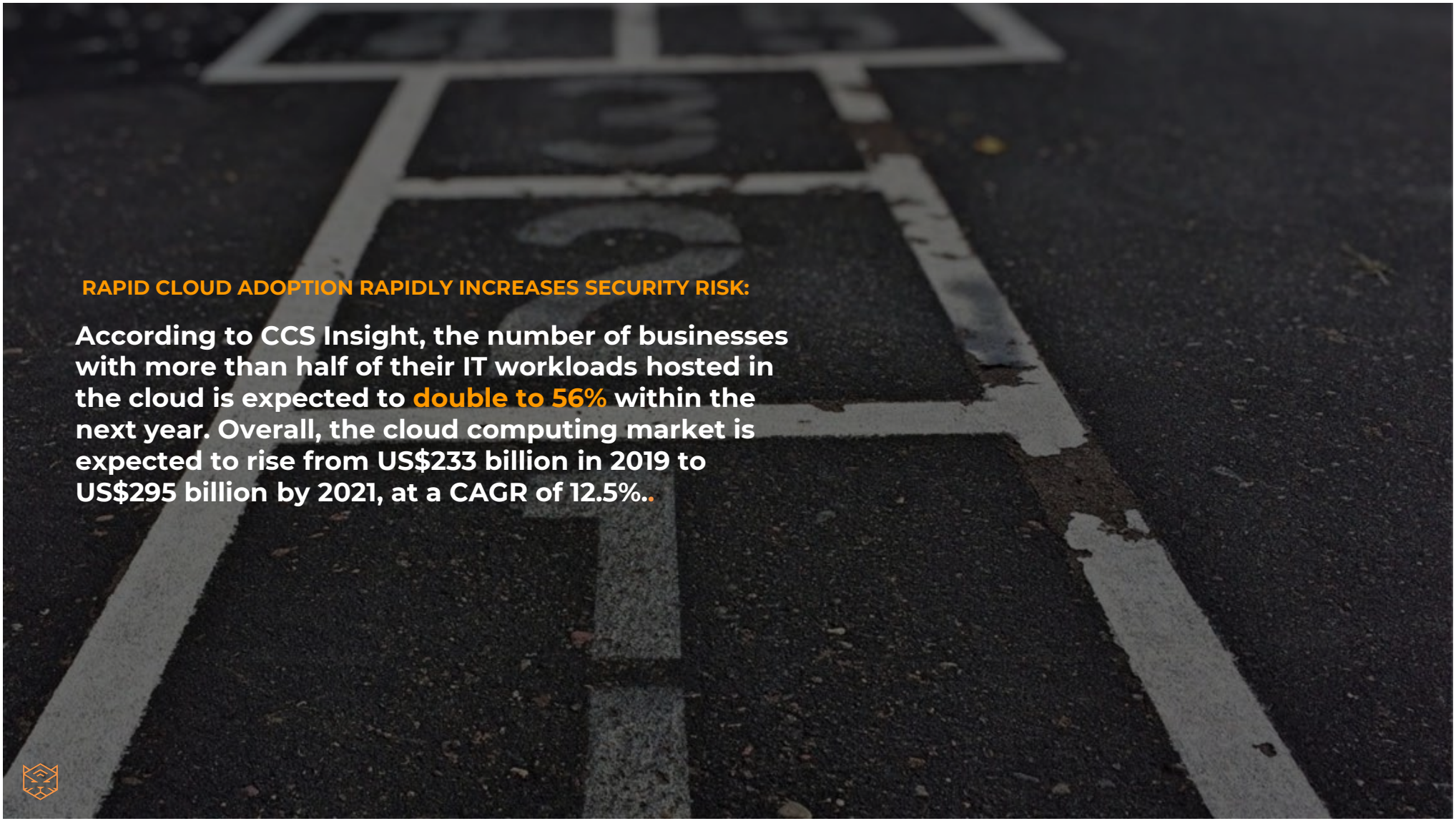
New attack vectors while working from home

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.

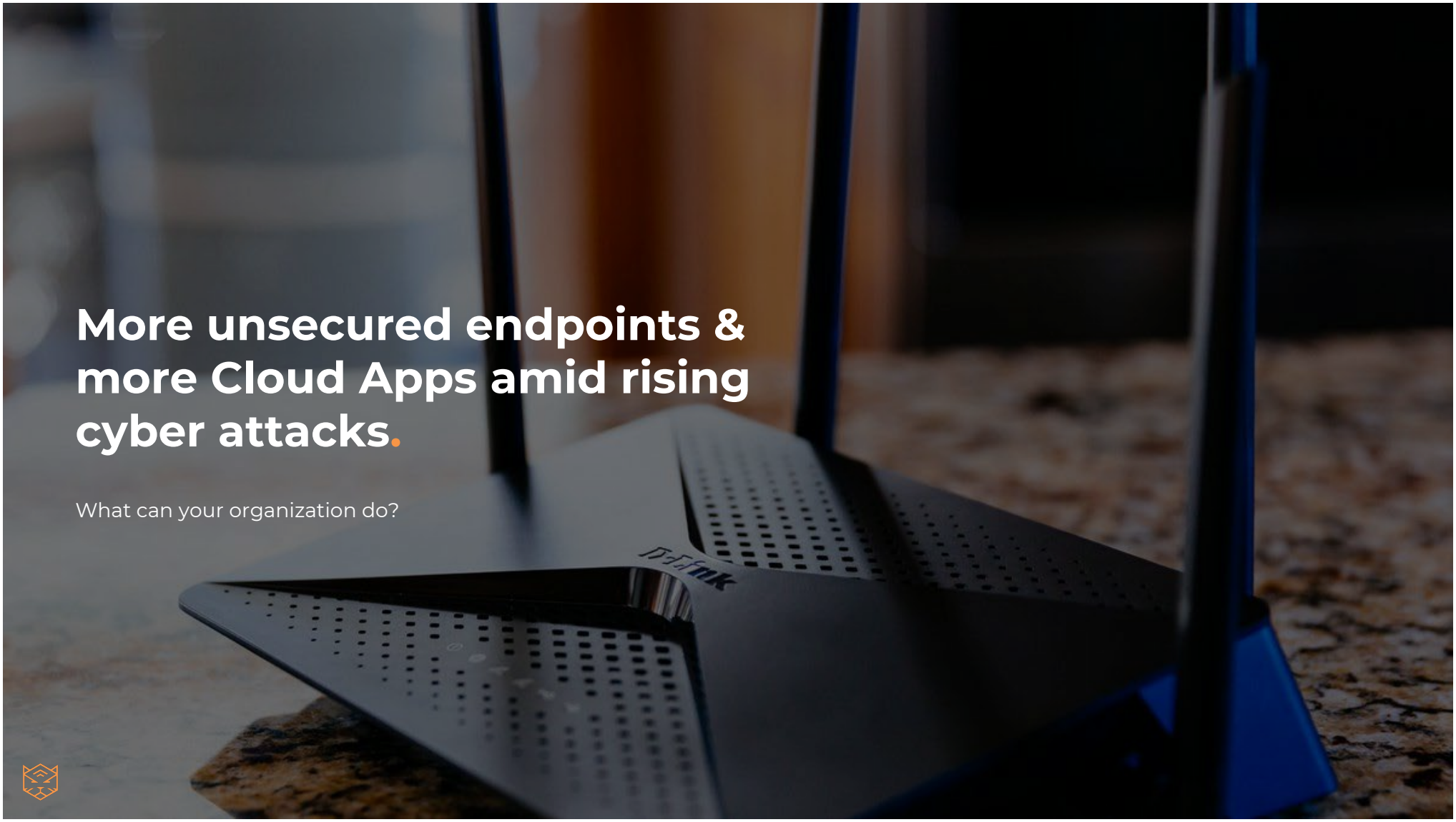
When you are alone at home, the odds swing in the attacker's favor.





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?

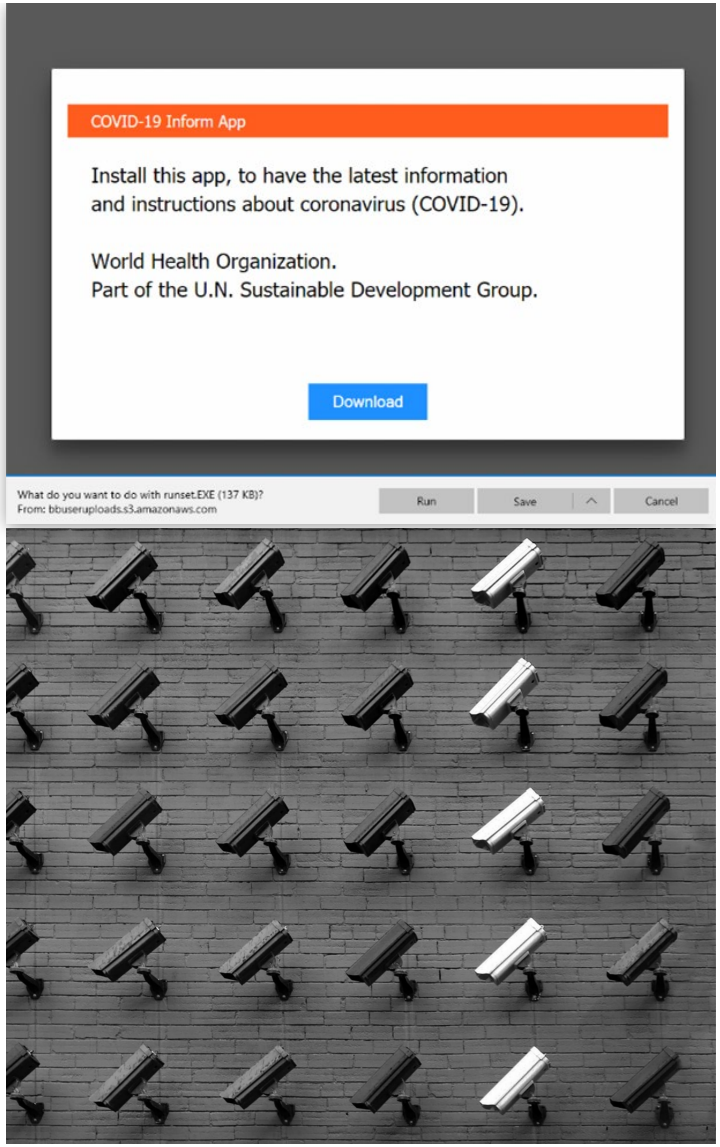
BEST PRACTICE:

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.

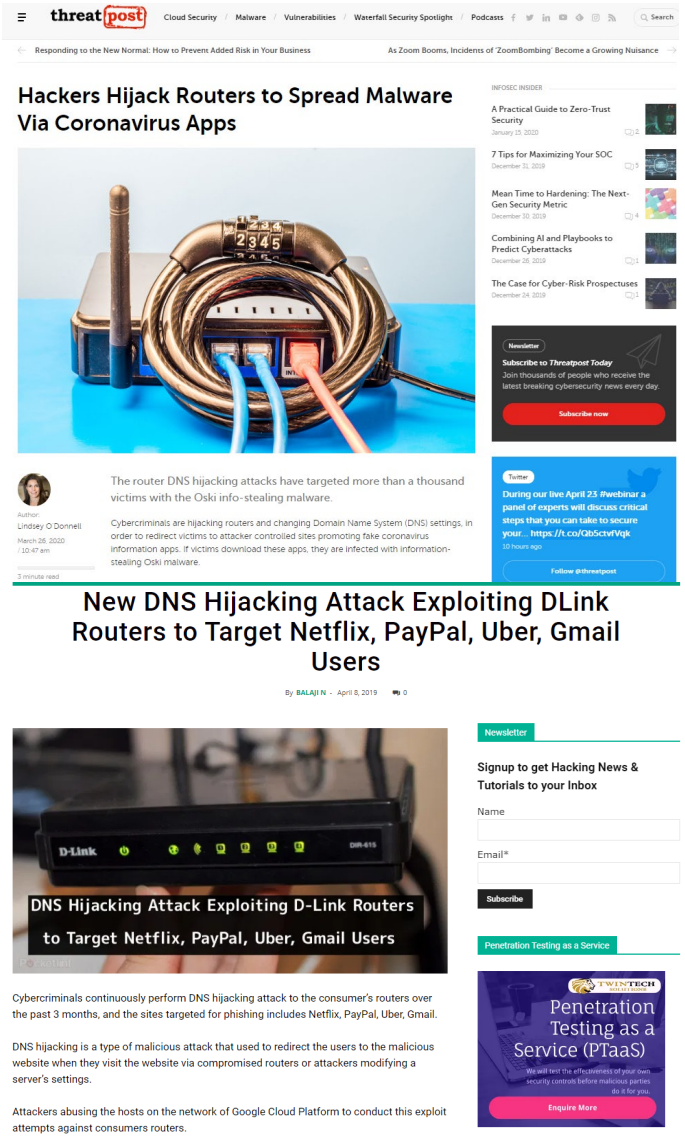
Horangi procured Google DLP solution to monitor potential leak of data from the cloud storage. This is a focus on visibility and monitoring, **taking a proactive stance** that mistakes and attacks will happen.

BEST PRACTICE:

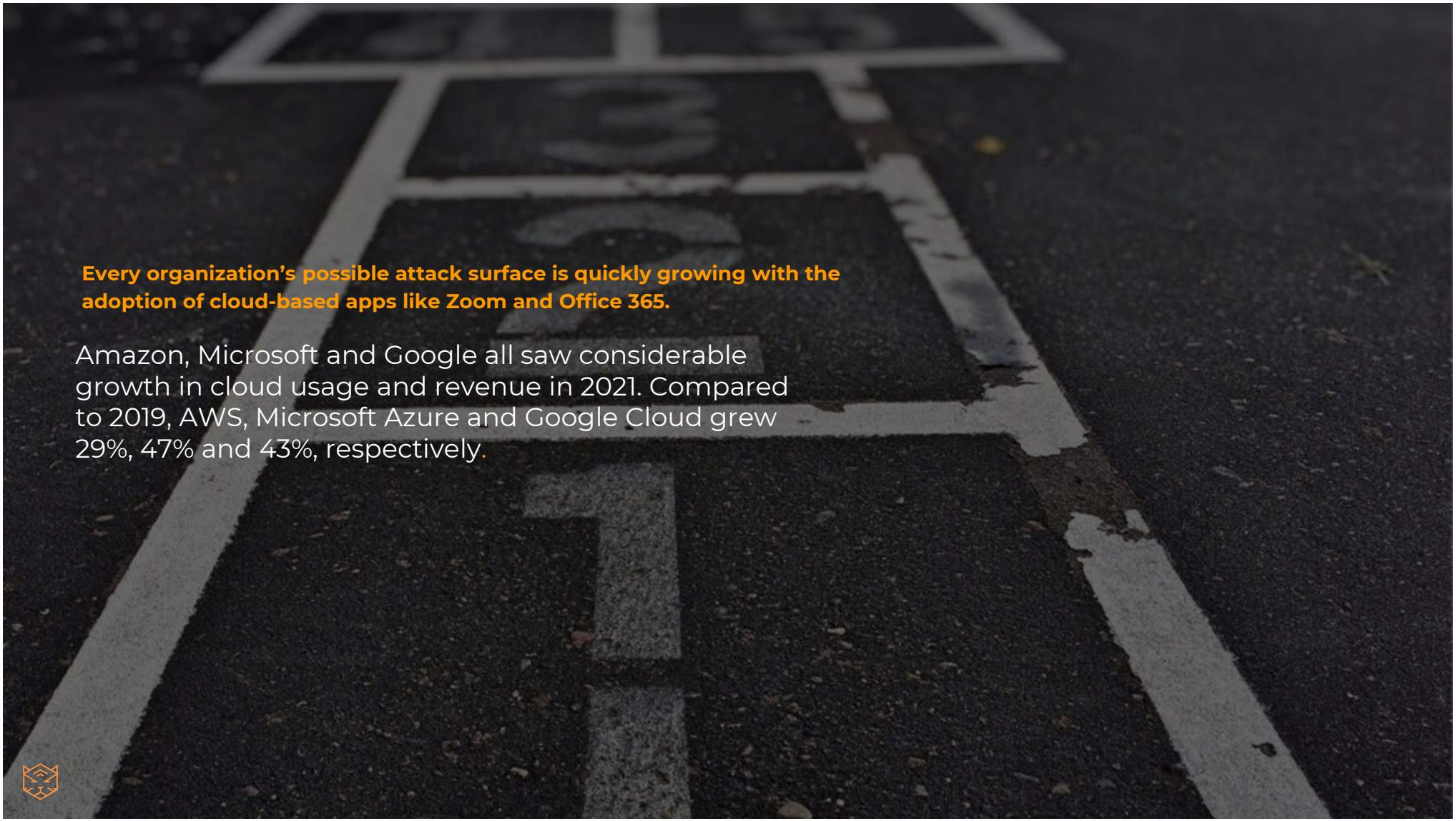
Monitor threats to your VPN.

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.



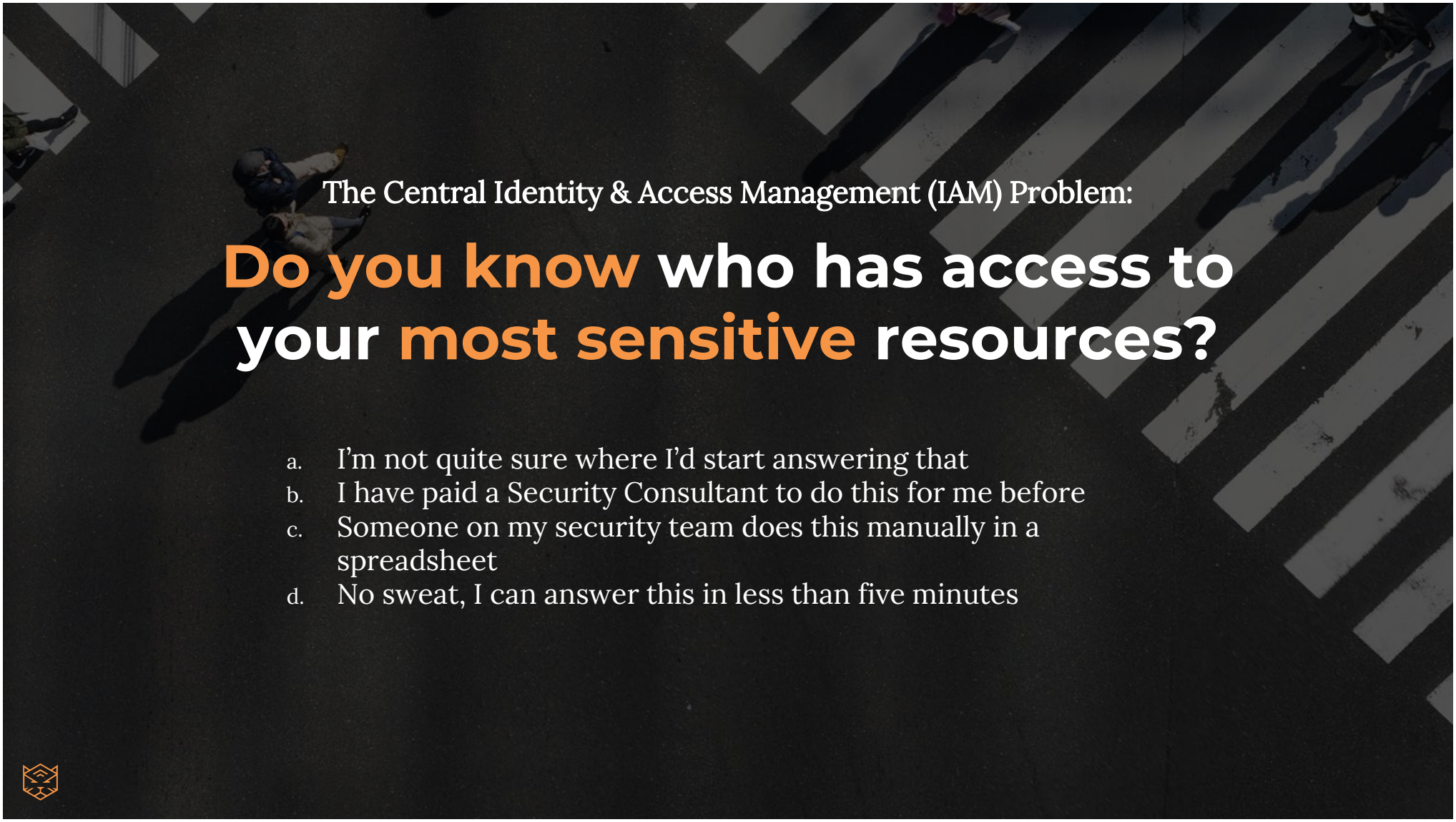
Cloud Security Now Mandatory



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 can 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.

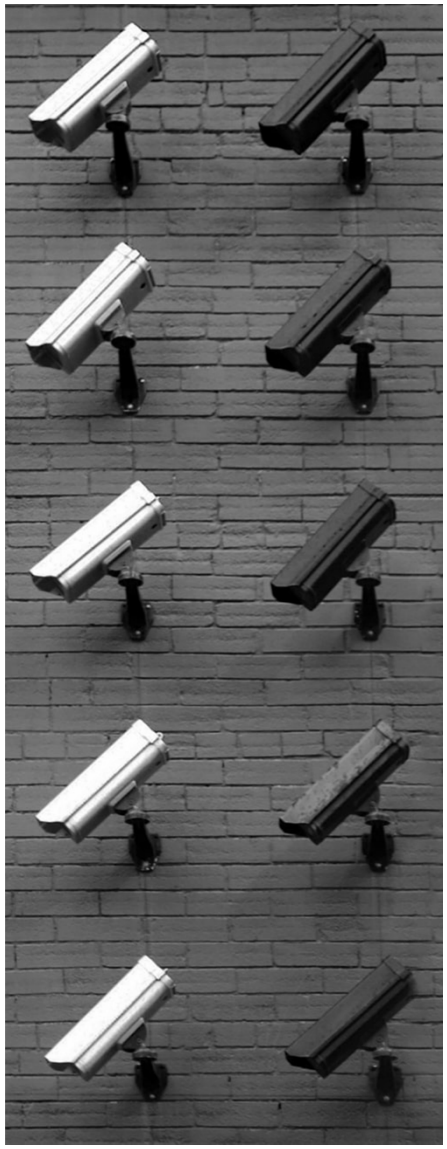

“
By 2023, 75% of security failures will result from inadequate management of identities, access, and privileges, up from 50% in 2020.
Managing Privileged Access in Cloud Infrastructure, Gartner

Identity Management

The cornerstone of IAM

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

9331
AWS Permissions

Complexity of **Scale**

Complexity of **Understanding**

Complexity of **Change**

2019 CAPITAL ONE DATA BREACH:

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

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.

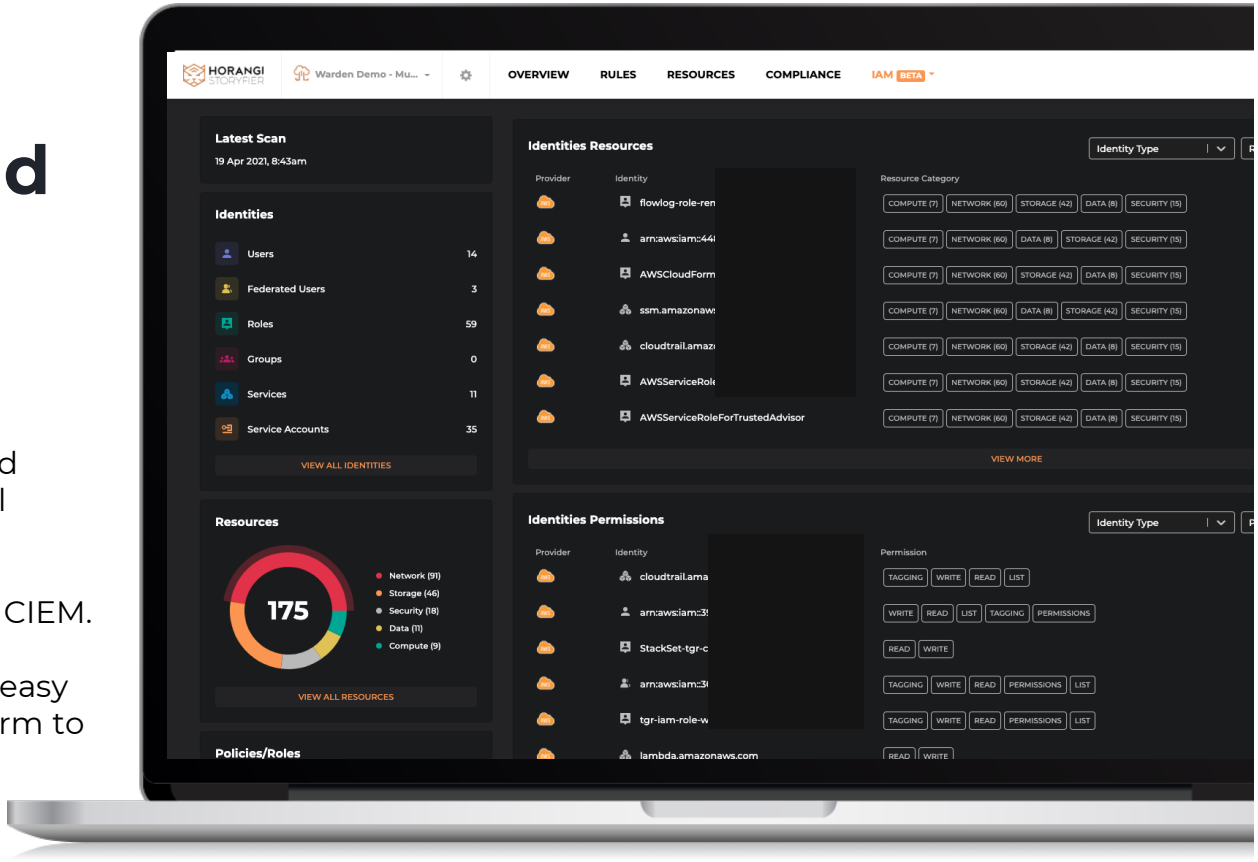
BEST PRACTICE:

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.



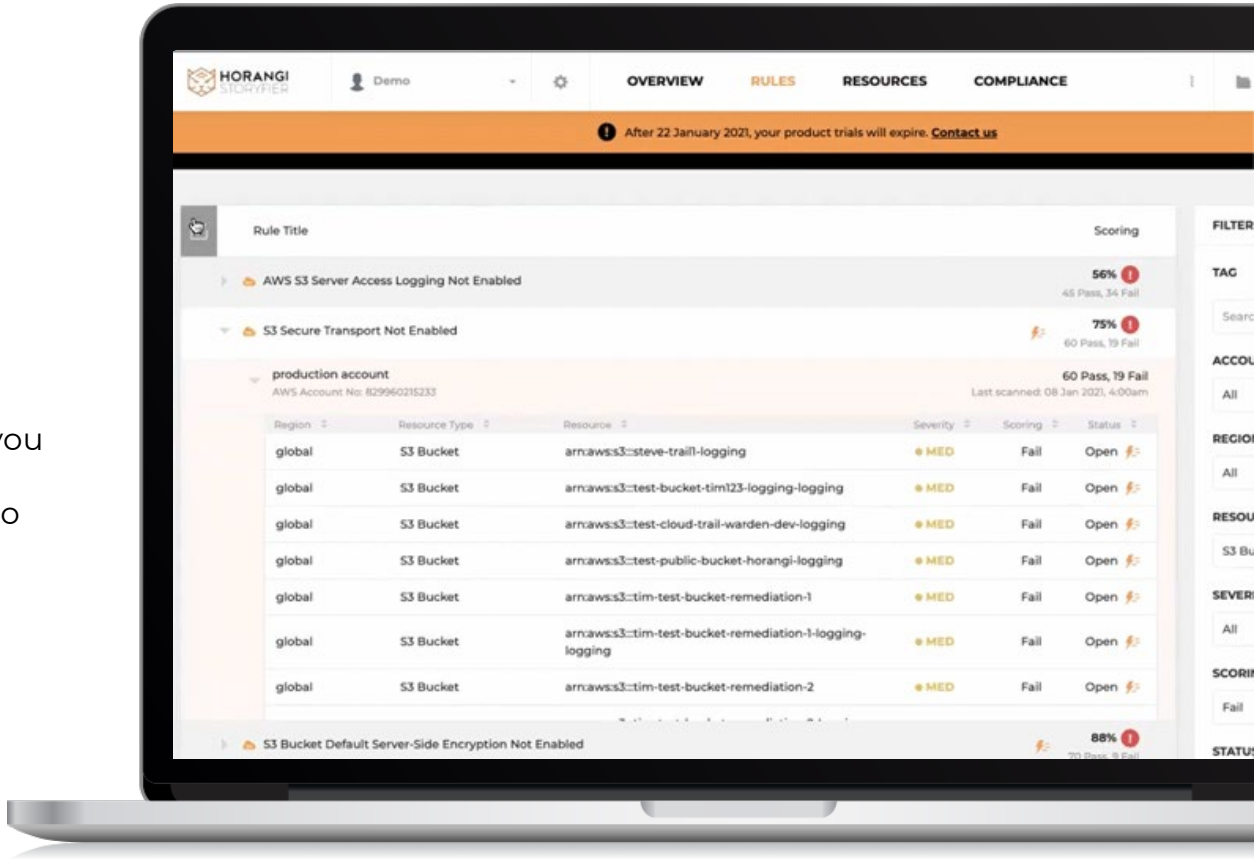
BEST PRACTICE:

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

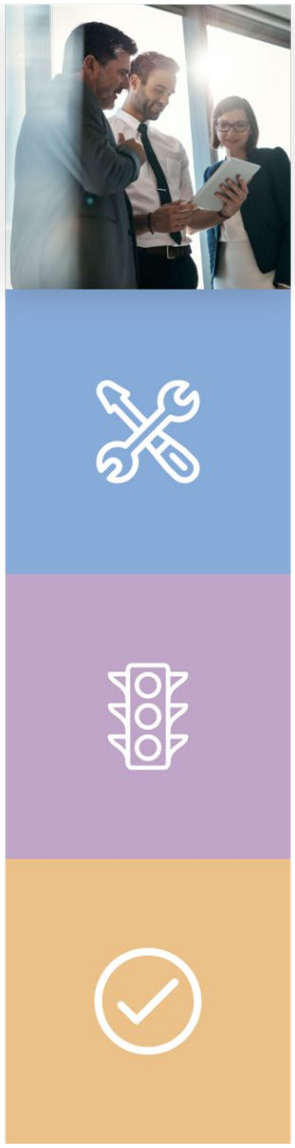
With the speed of change in the cloud, you can leverage security and compliance automation to fix threats as they come so they don't get forgotten.

Look at solutions classified as CSPM and CWPP.

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

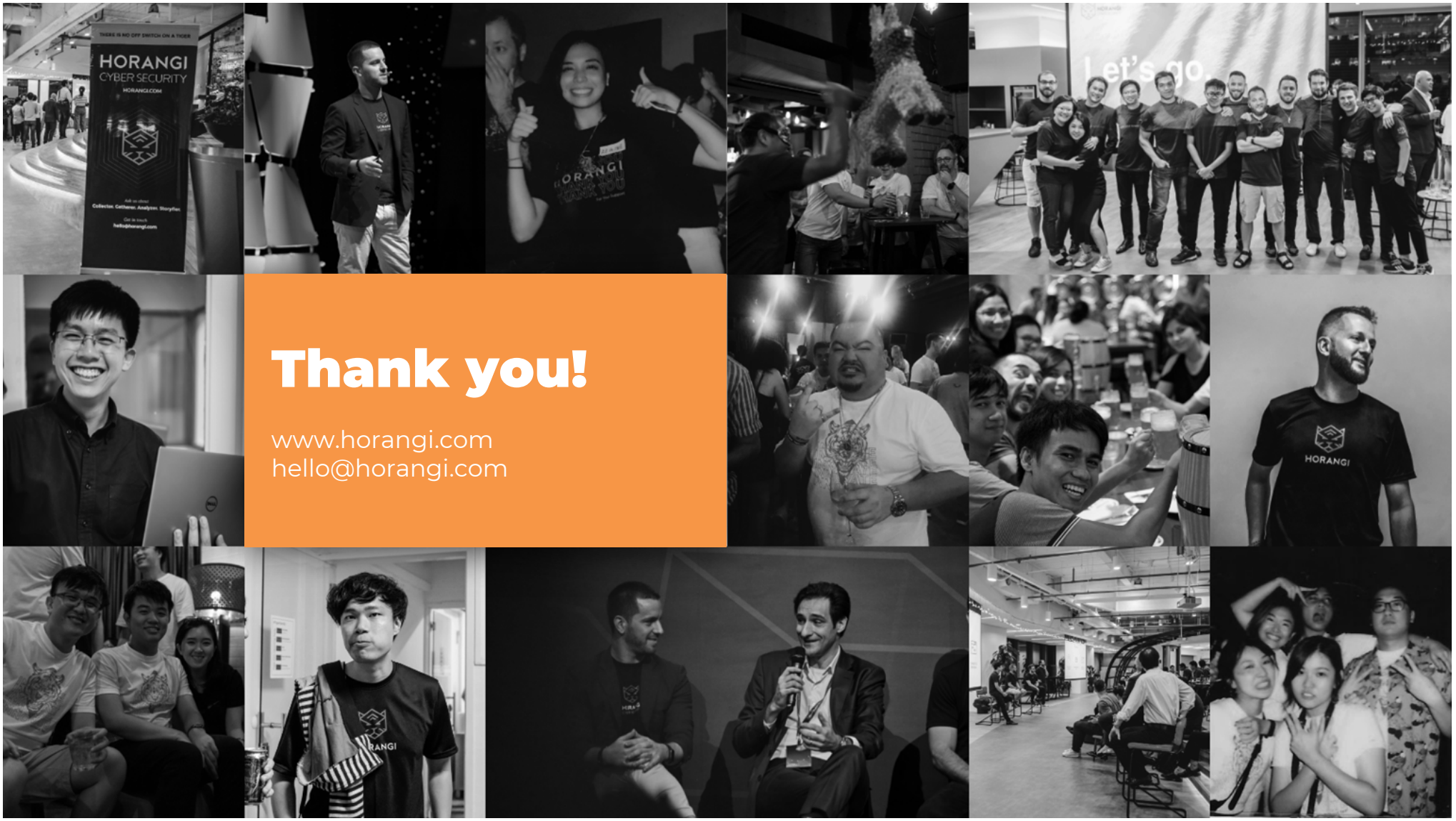


The Takeaway.



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.



Thank you!

www.horangi.com
hello@horangi.com