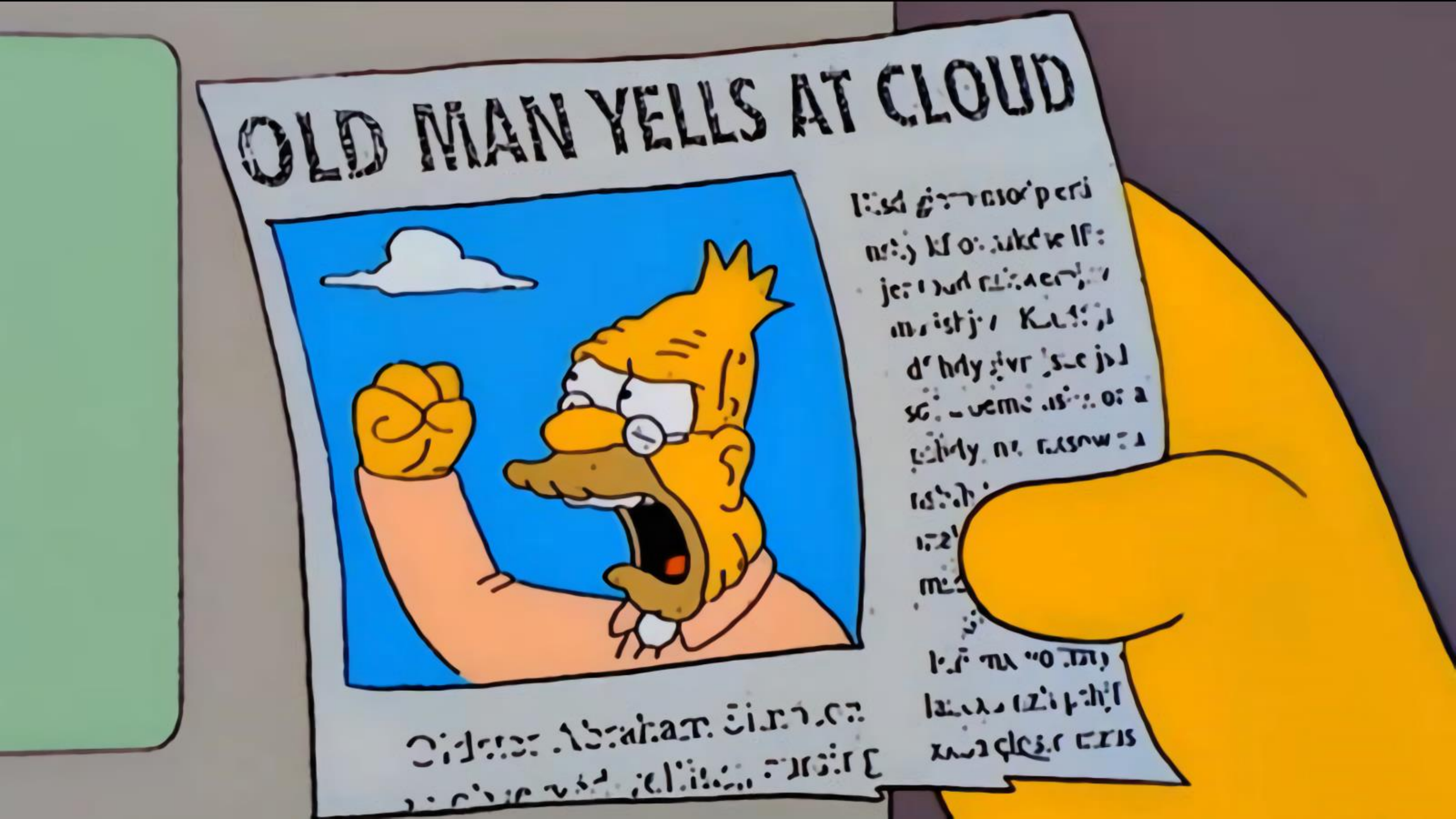
From Ground to Cloud

Mission Impossible?

James Burchell
Sales Engineer

June, 2020

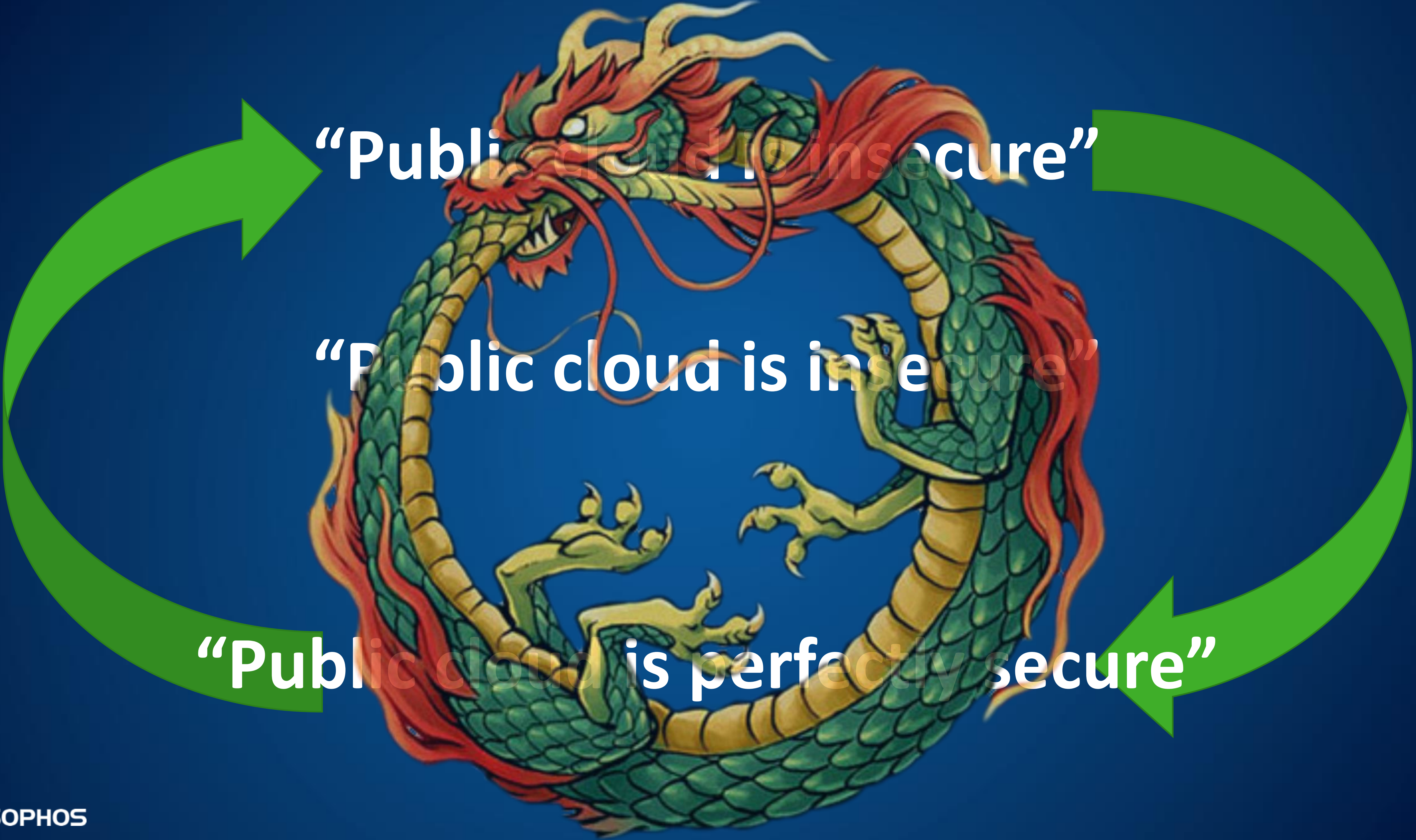
SOPHOS



OLD MAN YELLS AT CLOUD

[illegible]

Oldster Abraham Simpson [illegible]



“Public cloud is insecure”

“Public cloud is insecure”

“Public cloud is perfectly secure”

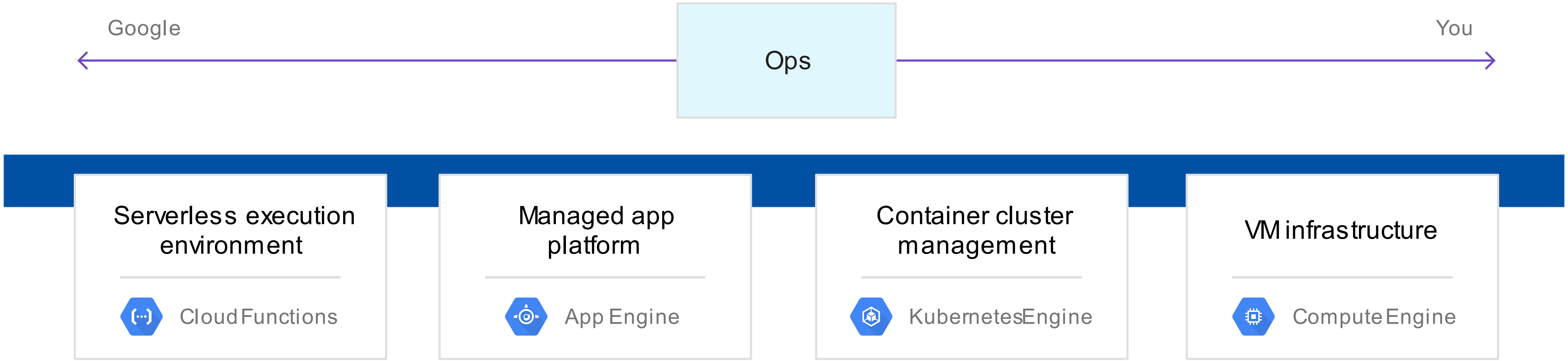
Public cloud is perfectly secure

?

Public cloud is insecure

SOPHOS

Shared responsibility



Google

Ops

You

Serverless execution environment

Cloud Functions

Managed app platform

App Engine

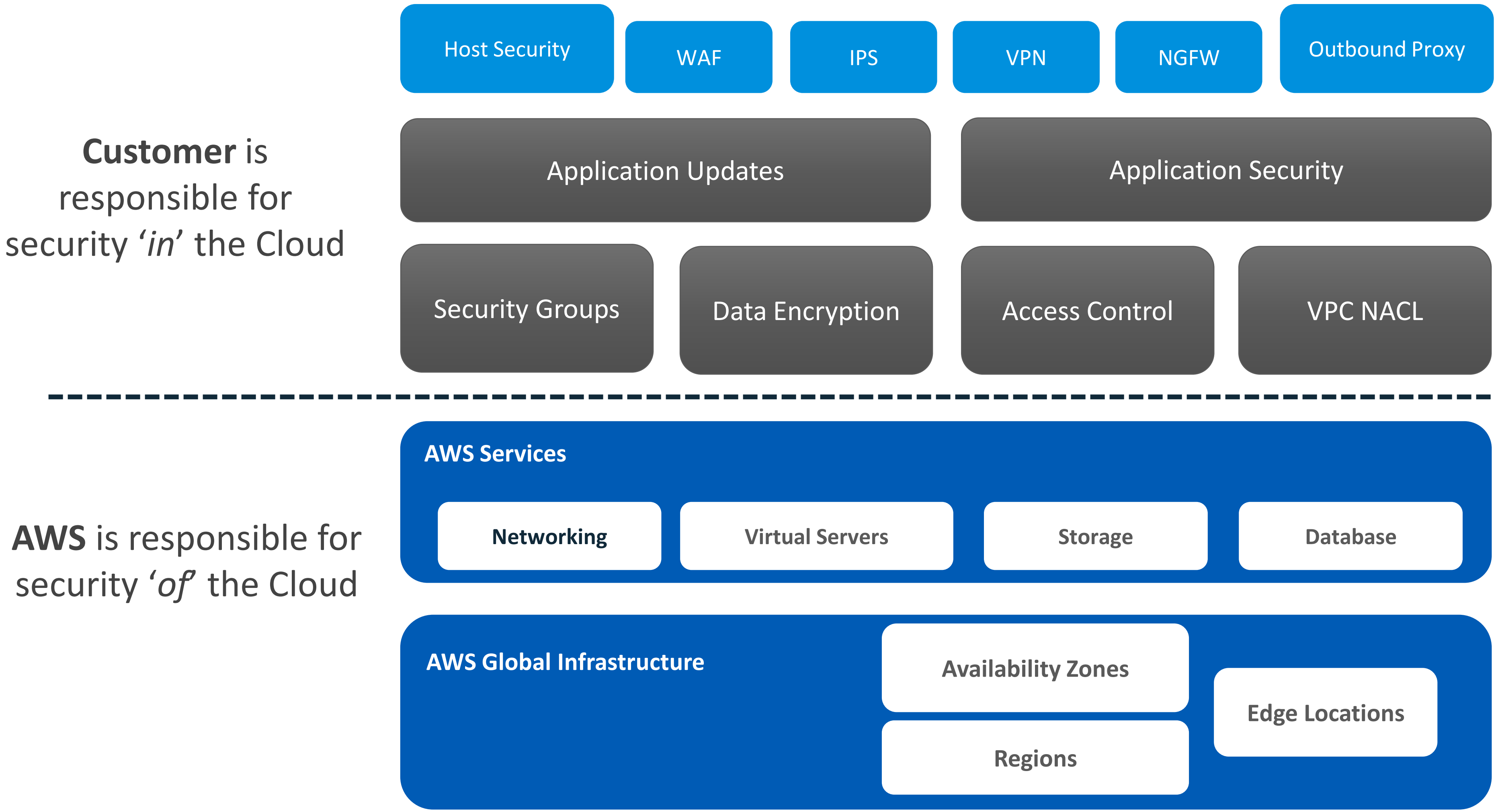
Container cluster management

Kubernetes Engine

VM infrastructure

Compute Engine

Source: https://cloud.google.com/docs/overview/cloud-platform-services



Customer is responsible for security *'in'* the Cloud

Host Security

WAF

IPS

VPN

NGFW

Outbound Proxy

Application Updates

Application Security

Security Groups

Data Encryption

Access Control

VPC NACL

AWS is responsible for security *'of'* the Cloud

AWS Services

Networking

Virtual Servers

Storage

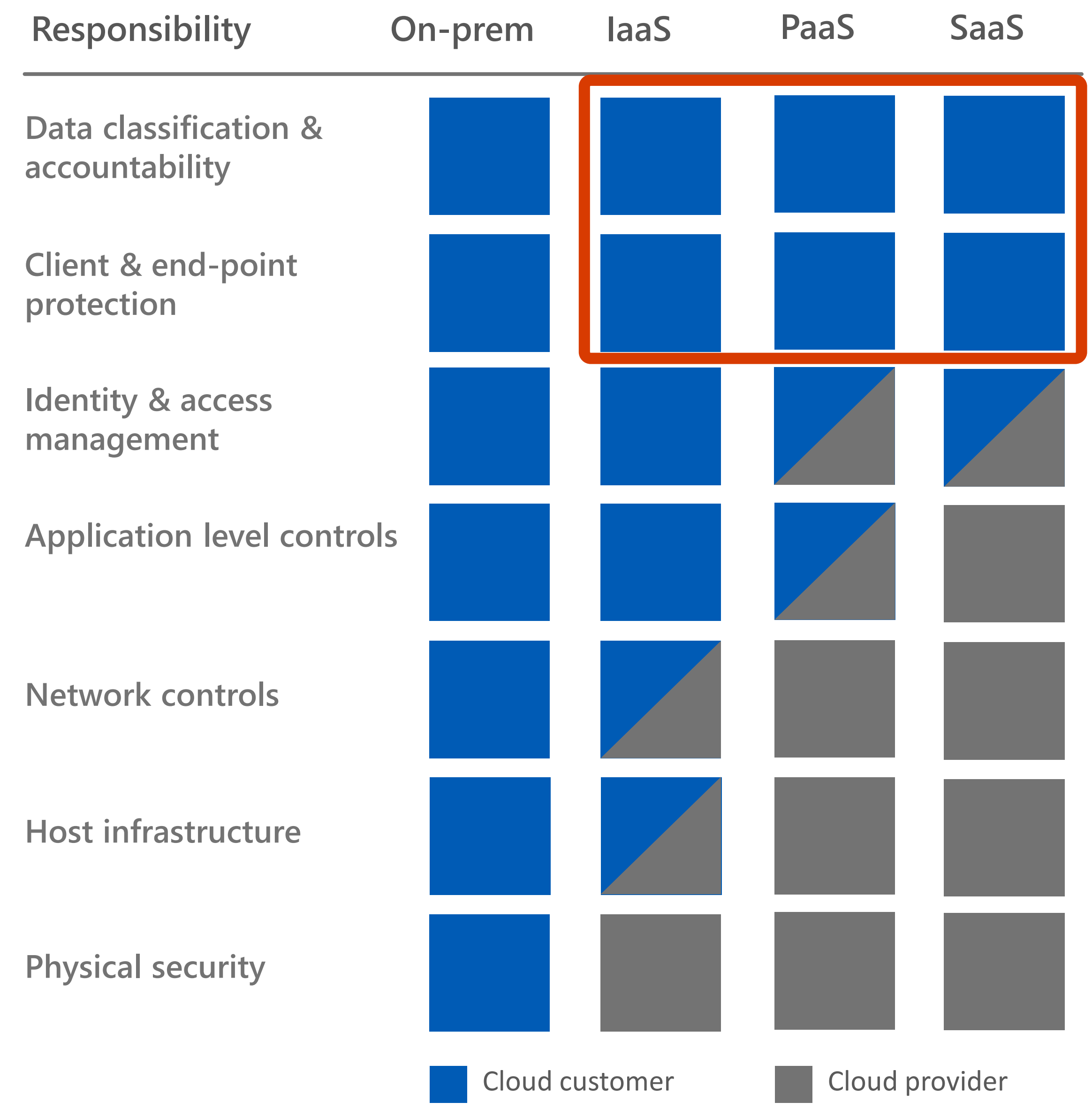
Database

AWS Global Infrastructure

Availability Zones

Regions

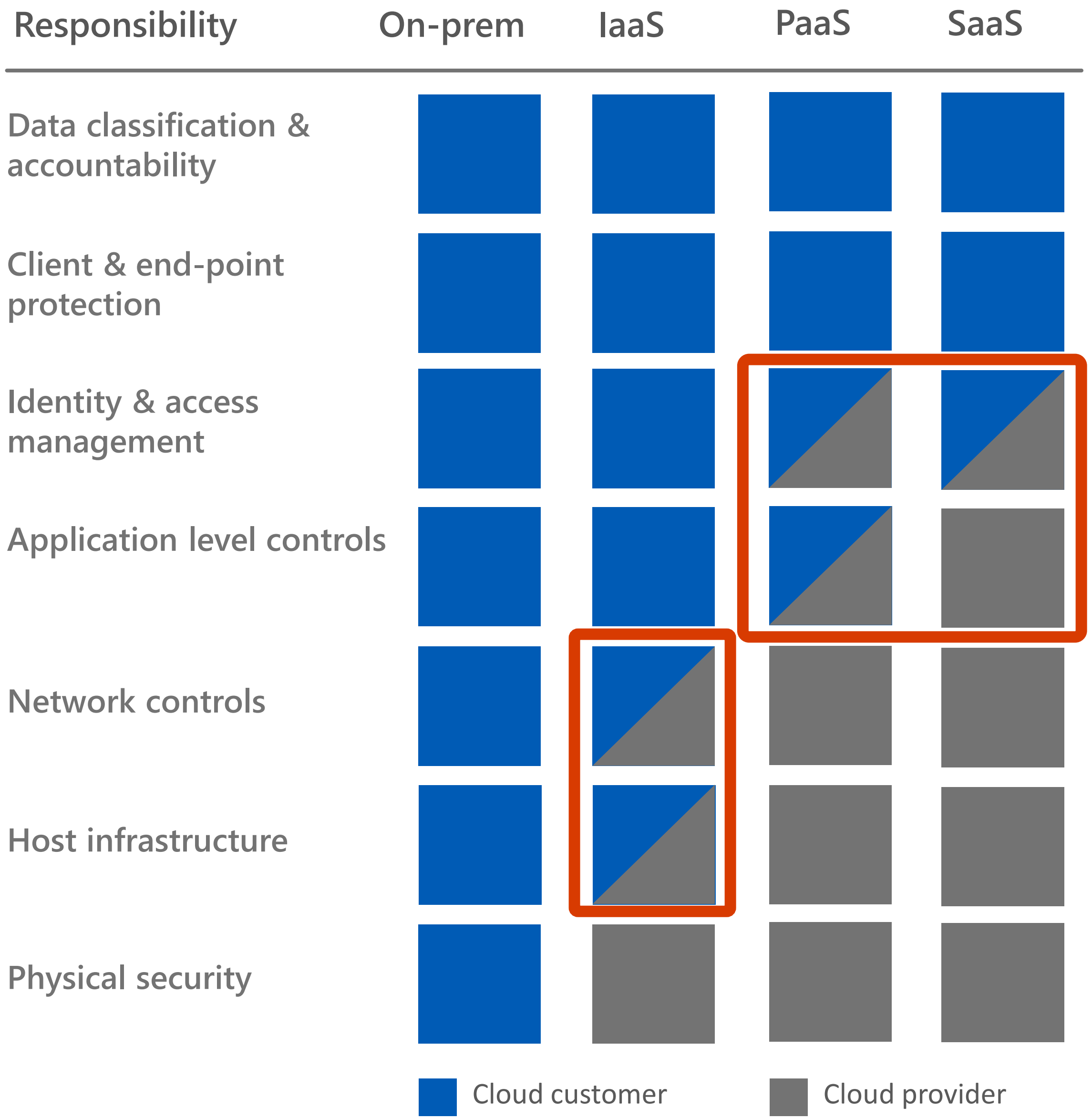
Edge Locations



Responsibility	On-prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	🟦
Identity & access management	🟦	🟦	🟦/⬛	🟦/⬛
Application level controls	🟦	🟦	🟦/⬛	⬛
Network controls	🟦	🟦/⬛	⬛	⬛
Host infrastructure	🟦	🟦/⬛	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud customer ⬛ Cloud provider

Source: Microsoft TechNet – Shared Responsibilities for Cloud Computing



Responsibility	On-prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	🟦
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	◩	⬛	⬛
Host infrastructure	🟦	◩	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud customer ⬛ Cloud provider

Source: Microsoft TechNet – Shared Responsibilities for Cloud Computing

Security posture

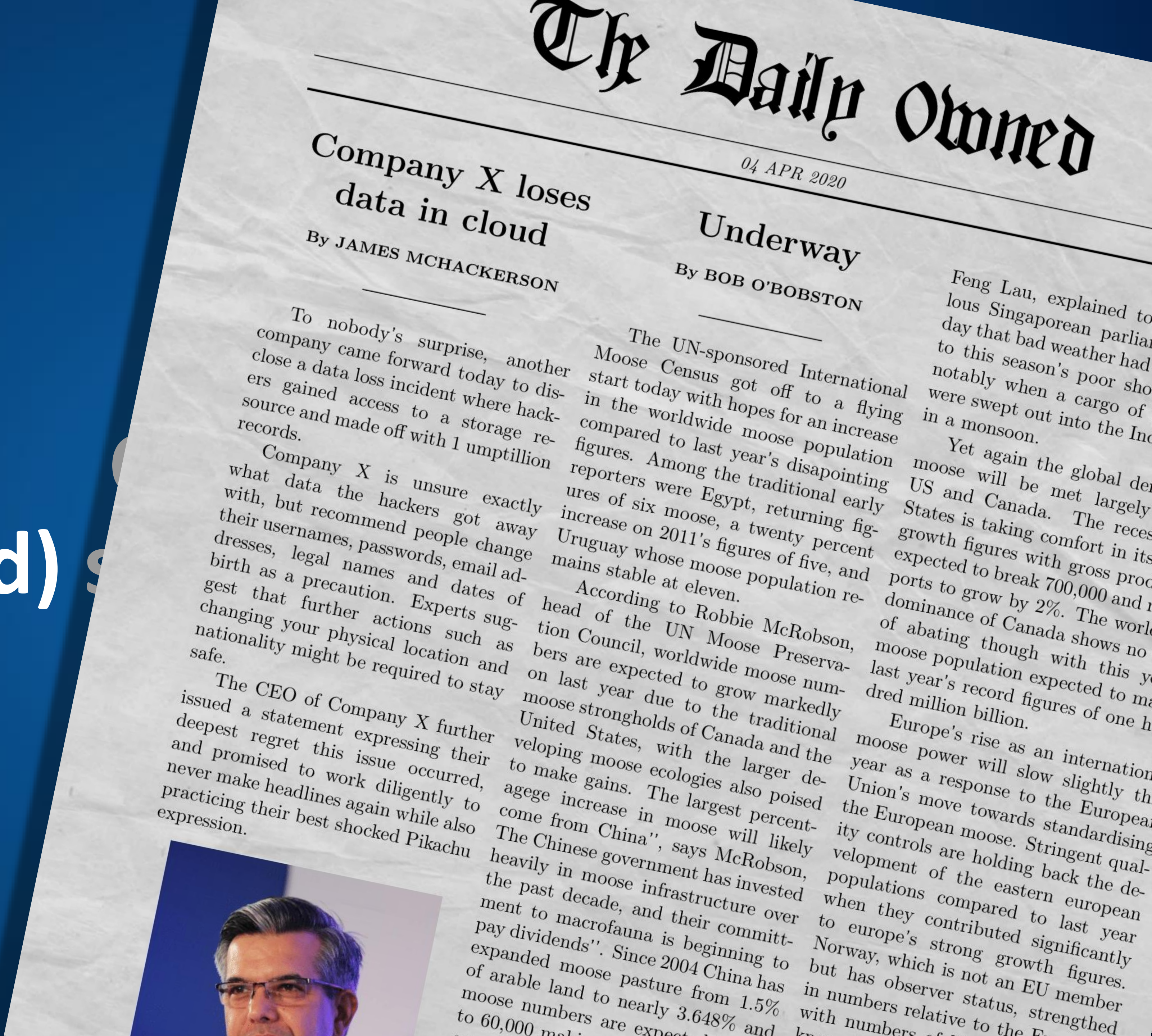
Source: Photo by Ylanite Koppens from Pexels

“The greatest teacher, failure is”

How (not) to secure your cloud environment

- Yoda

(Shared) s



The Daily Owned

04 APR 2020

Company X loses data in cloud

By JAMES MCHACKERSON

To nobody's surprise, another company came forward today to disclose a data loss incident where hackers gained access to a storage resource and made off with 1 umptillion records.

Company X is unsure exactly what data the hackers got away with, but recommend people change their usernames, passwords, email addresses, legal names and dates of birth as a precaution. Experts suggest that further actions such as changing your physical location and nationality might be required to stay safe.

The CEO of Company X further issued a statement expressing their deepest regret this issue occurred, and promised to work diligently to never make headlines again while also practicing their best shocked Pikachu expression.

Underway

By BOB O'BOBSTON

The UN-sponsored International Moose Census got off to a flying start today with hopes for an increase in the worldwide moose population compared to last year's disapointing figures. Among the traditional early reporters were Egypt, returning figures of six moose, a twenty percent increase on 2011's figures of five, and Uruguay whose moose population remains stable at eleven.

According to Robbie McRobson, head of the UN Moose Preservation Council, worldwide moose numbers are expected to grow markedly on last year due to the traditional moose strongholds of Canada and the United States, with the larger developing moose ecologies also poised to make gains. The largest percentagege increase in moose will likely come from China'', says McRobson, The Chinese government has invested heavily in moose infrastructure over the past decade, and their committment to macrofauna is beginning to pay dividends''. Since 2004 China has expanded moose pasture from 1.5% of arable land to nearly 3.648% and moose numbers are expect

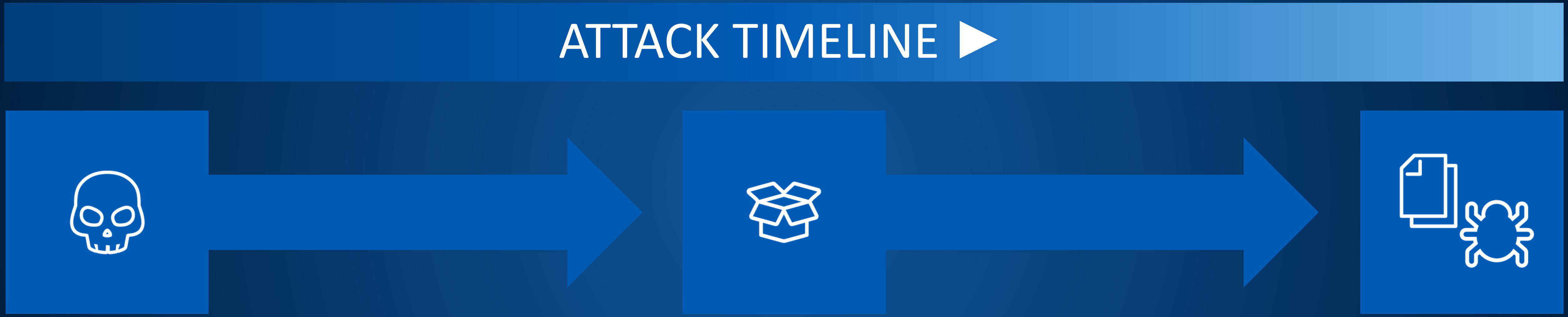
to 60,000 mal

Feng Lau, explained to
lous Singaporean parliam
day that bad weather had
to this season's poor sho
notably when a cargo of
were swept out into the Ind
in a monsoon.

Yet again the global de
moose will be met largely
US and Canada. The reces
States is taking comfort in its
growth figures with gross proc
expected to break 700,000 and r
ports to grow by 2%. The worl
dominance of Canada shows no
of abating though with this y
moose population expected to ma
last year's record figures of one h
dred million billion.

Europe's rise as an internation
moose power will slow slightly th
year as a response to the Europea
Union's move towards standardising
the European moose. Stringent quality controls are holding back the development of the eastern european populations compared to last year when they contributed significantly to europe's strong growth figures. Norway, which is not an EU member but has observer status, strengthed
in numbers relative to the E
with numbers

(Shared) storage data loss



ATTACK TIMELINE ▶

Scan cloud provider environment for resources

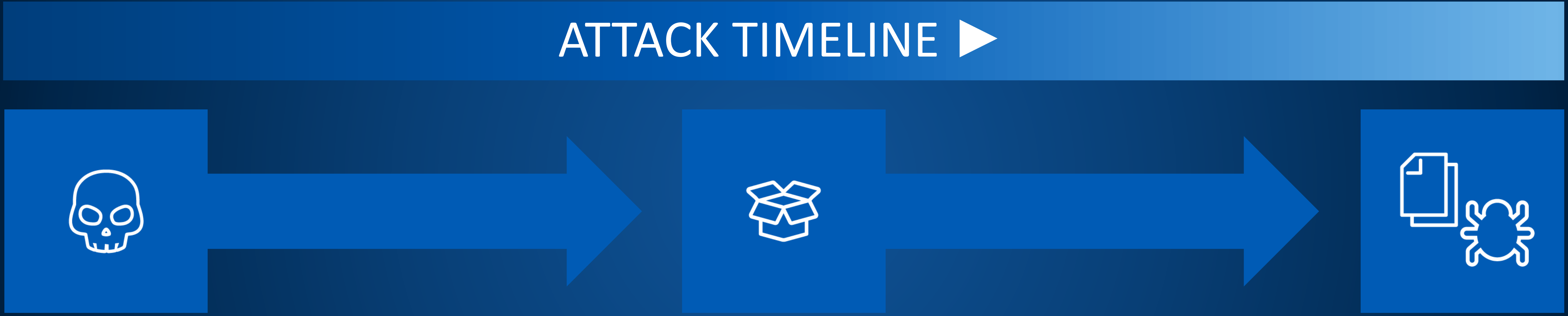
Connect to unprotected resource

Exfiltrate data and / or ransom company

> Human error such as misconfigured cloud servers, unsecured cloud databases, and improperly secured rsync backups were responsible for 43% of publicly disclosed misconfiguration incidents, resulting in a more than 20% increase since last year.

Source: IBM X-Force Threat Intelligence Index Report - 2019, February 26, 2019

(Shared) storage data loss



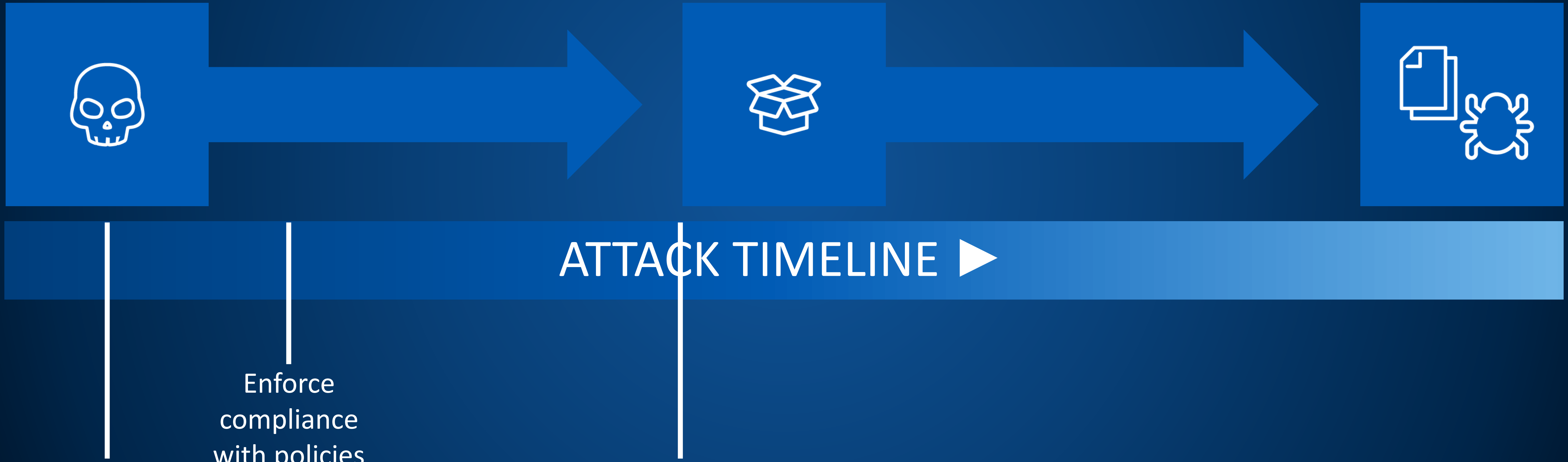
ATTACK TIMELINE ▶

Scan cloud provider environment for resources

Connect to unprotected resource

Exfiltrate data and / or ransom company

How to prevent and defend

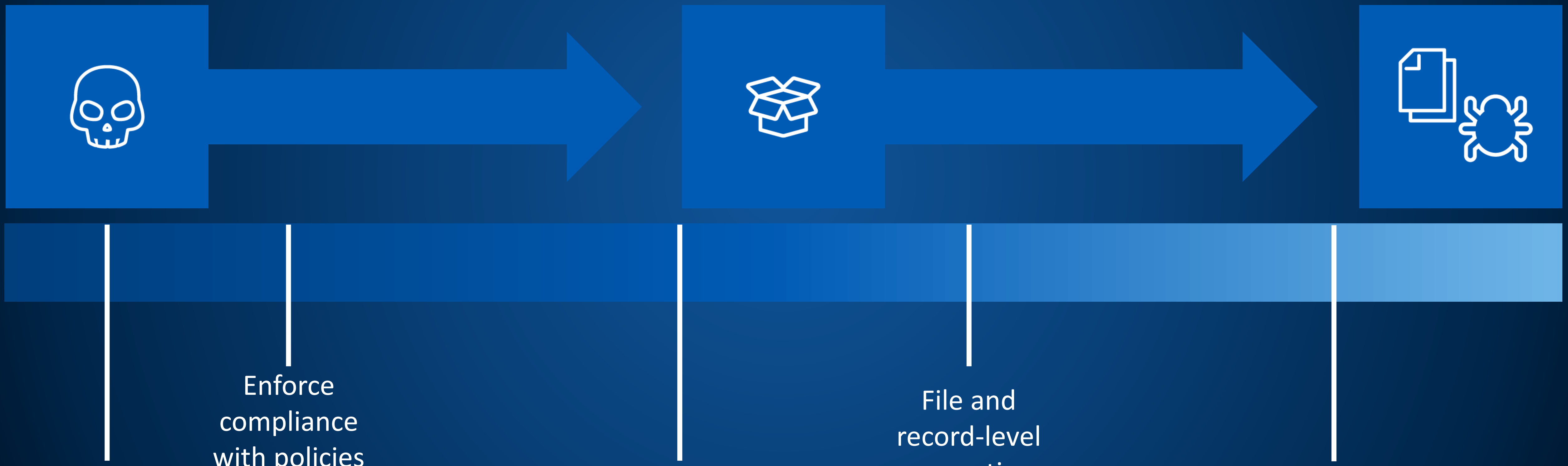


Implement best practices for service

Enforce compliance with policies

Access logging and reporting

How to prevent and defend



Implement best practices for service

Enforce compliance with policies

Access logging and reporting

File and record-level encryption

Implement a backup strategy and regime

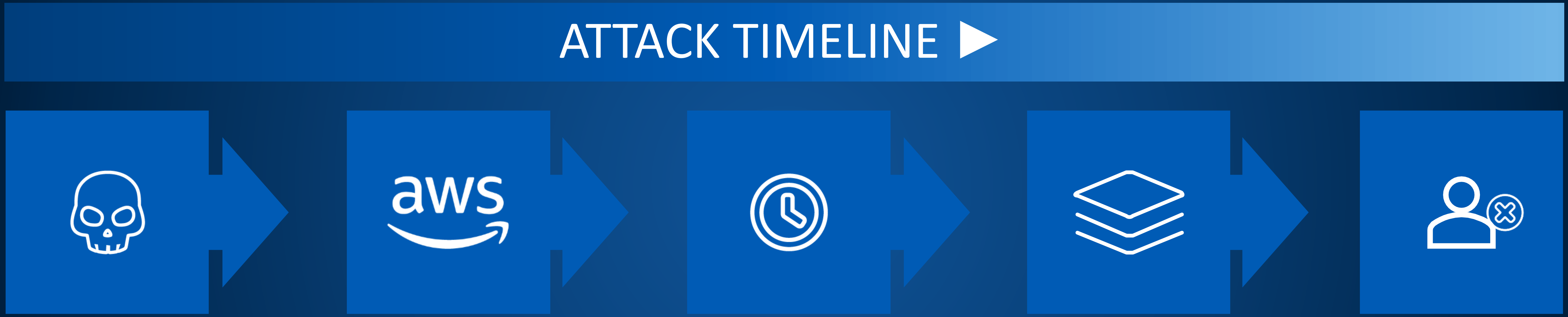
Case 2
Cloud cryptojacking

Cloud cryptojacking

ATTACK TIMELINE ▶

Access keys stolen (from SCM)

Cloud cryptojacking



ATTACK TIMELINE ▶

Access keys stolen (from SCM)

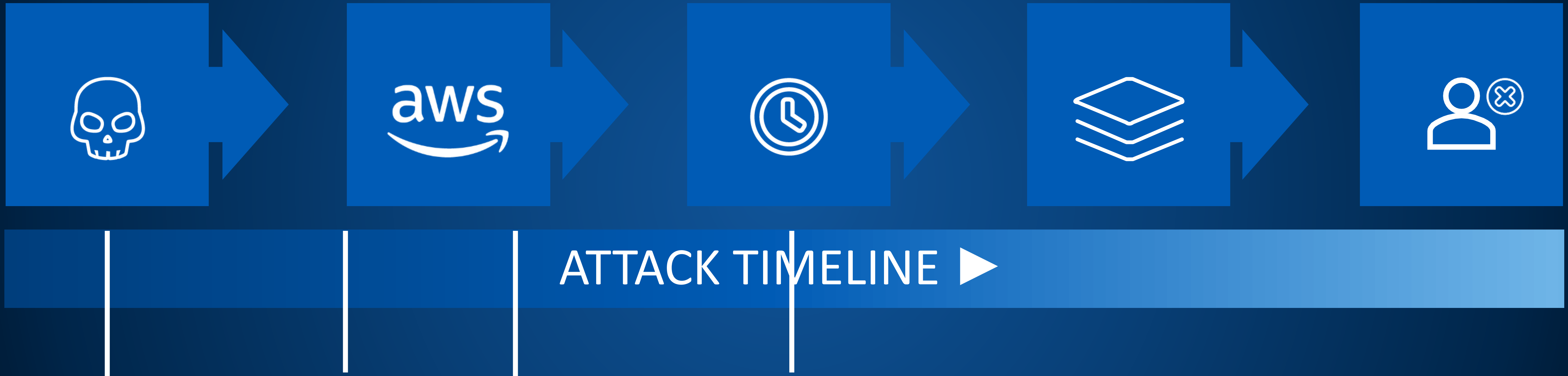
Attacker accesses cloud account

Monitors account activity

Automates provisioning of instances

Hardens settings and revokes access

How to prevent and defend



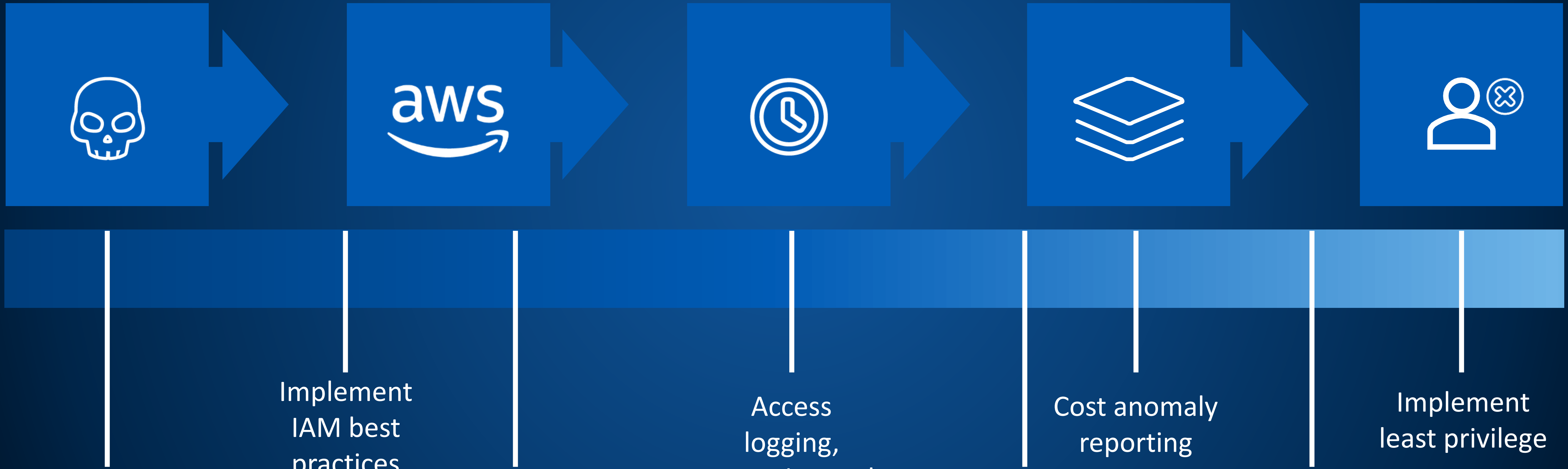
Use private SCM repositories

Implement IAM best practices

Safely store secrets and use secure execution

Access logging, reporting and alerting

How to prevent and defend



Use private SCM repositories

Implement IAM best practices

Safely store secrets and use secure execution

Access logging, reporting and alerting

Administrative event logging and alerting

Cost anomaly reporting

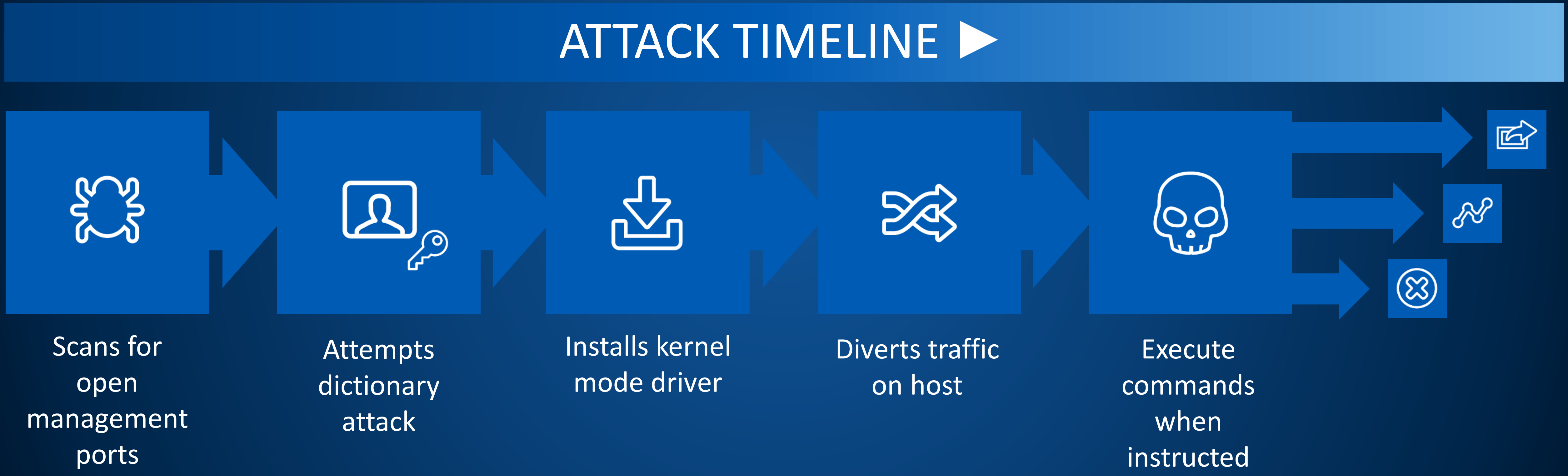
Enforce VM compliance and endpoint security

Implement least privilege access

Case 3
Cloud-specific malware

SOPHOS

Cloud-specific malware



ATTACK TIMELINE ▶

Scans for open management ports

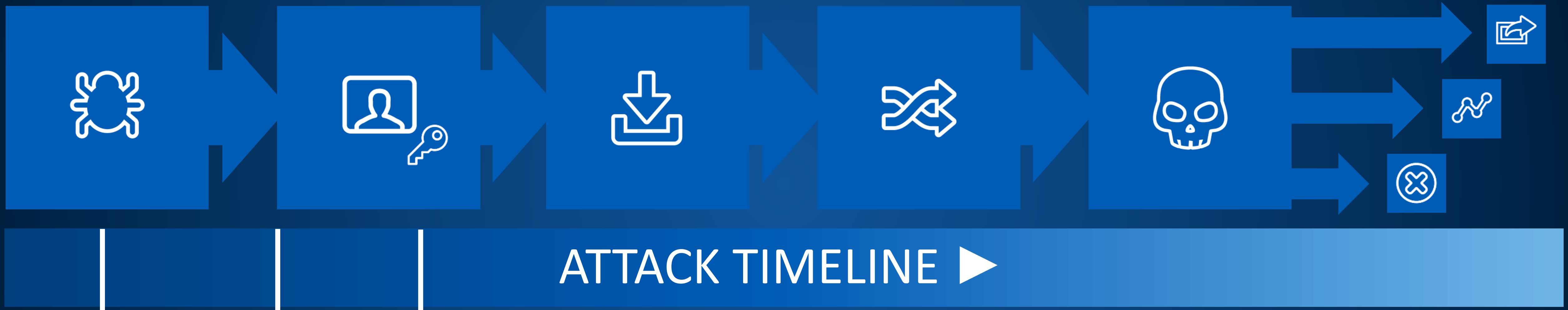
Attempts dictionary attack

Installs kernel mode driver

Diverts traffic on host

Execute commands when instructed

How to prevent and defend

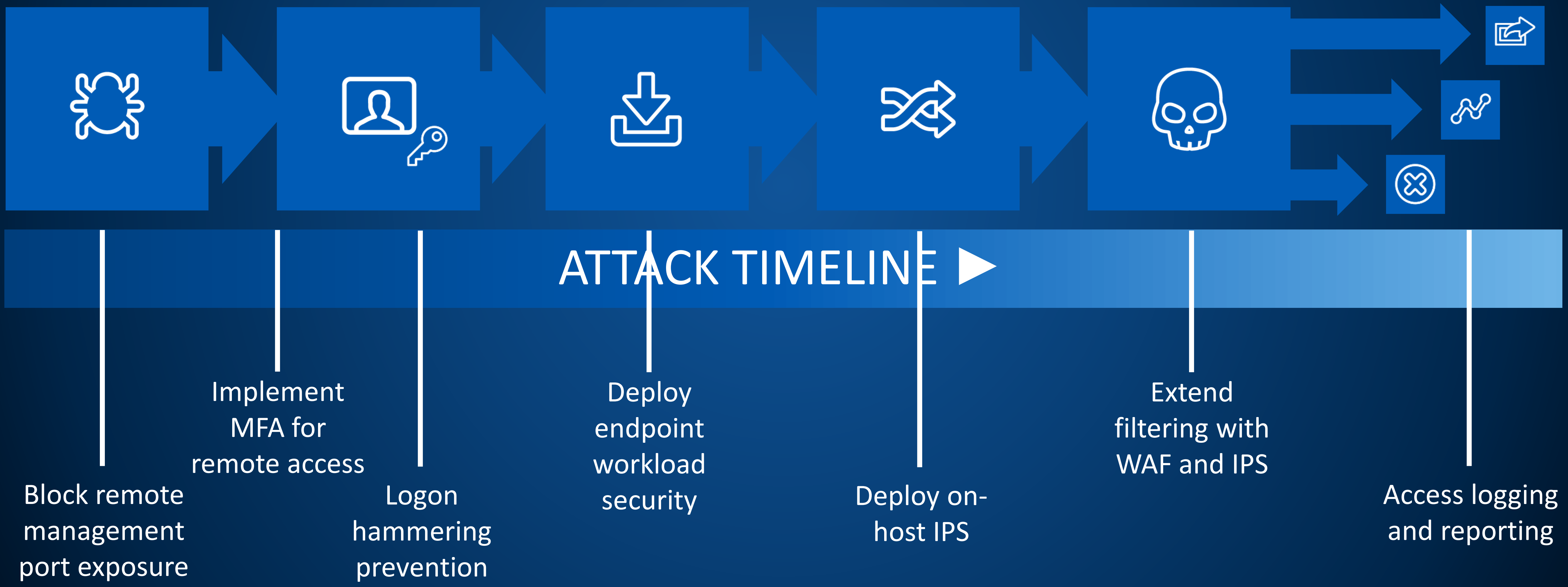


Implement MFA for remote access

Block remote management port exposure

Logon hammering prevention

How to prevent and defend


ATTACK TIMELINE ▶
Block remote management port exposure
Implement MFA for remote access
Logon hammering prevention
Deploy endpoint workload security
Deploy on-host IPS
Extend filtering with WAF and IPS
Access logging and reporting

MISSION: IMPOSSIBLE

Five-point public cloud action plan

1. Define your cloud security posture
2. Enforce and test compliance with your posture
3. Deploy a Cloud Security Posture Management solution
4. Extend platform security tools where needed
5. Continuous monitoring and alerting

SOPHOS

7 BEST PRACTICES FOR SECURING THE PUBLIC CLOUD

www.sophos.com/seven

SOPHOS

Security made simple.