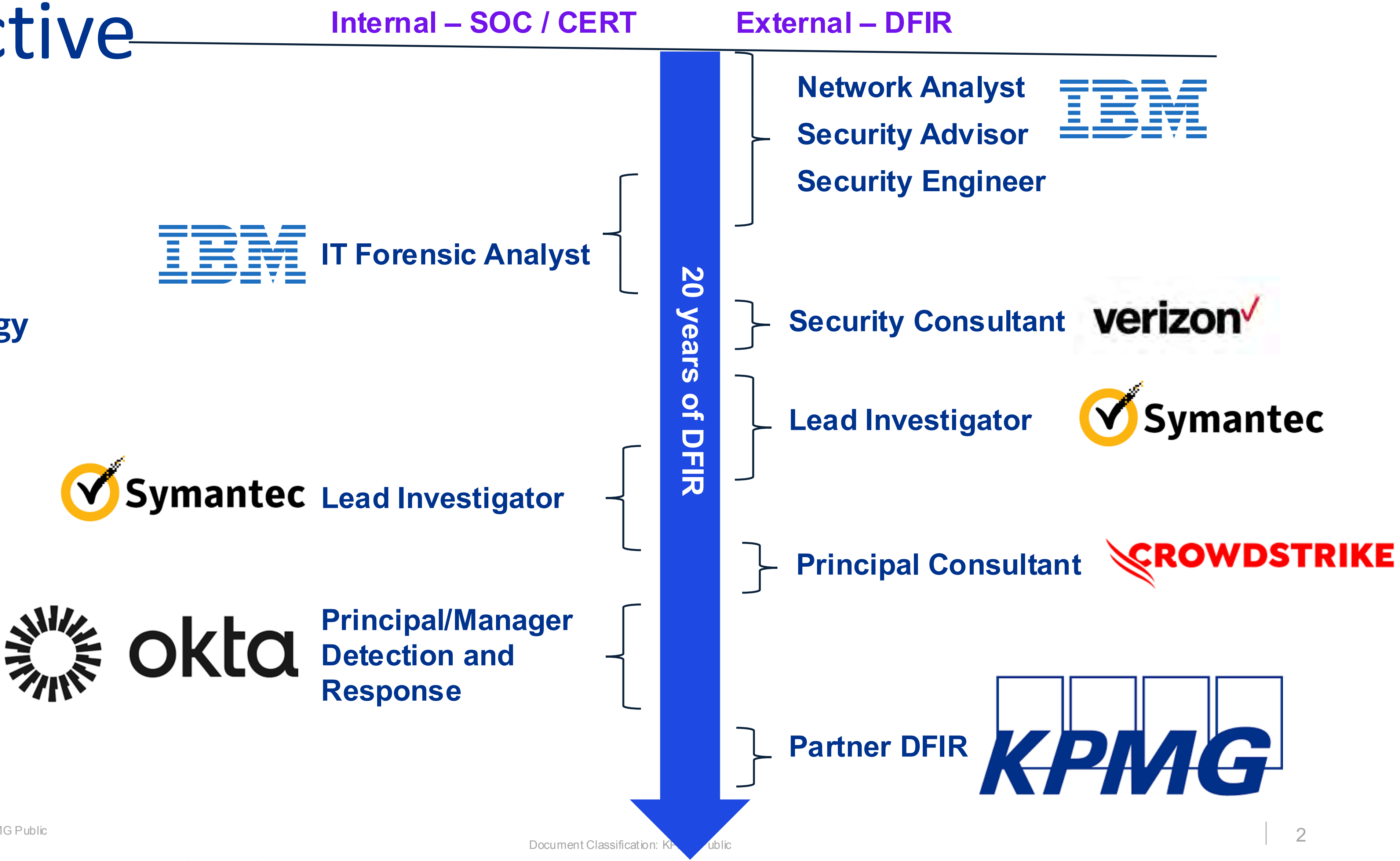
CYBER CHECKLIST

Preventing the need for cyber response

My Perspective

Partner
Cyber Response & Forensic Technology
KPMG Australia



Internal – SOC / CERT

External – DFIR

20 years of DFIR

Network Analyst
Security Advisor
Security Engineer
IBM

IBM
IT Forensic Analyst

Security Consultant
verizon

Lead Investigator
Symantec

Symantec
Lead Investigator

Principal Consultant
CROWDSTRIKE

okta
Principal/Manager Detection and Response

Partner DFIR
KPMG

PNG FOCUSED CYBER CHECKLIST

1. **Becoming a ghost**
2. **Ticking all the boxes**
3. **Doing your part in the cloud**

Becoming a ghost

Document Classification: KPMG Public

Becoming a ghost

Liability limited by a scheme approved under Professional Standards Legislation.

Document Classification: KPMG Public

Becoming a ghost

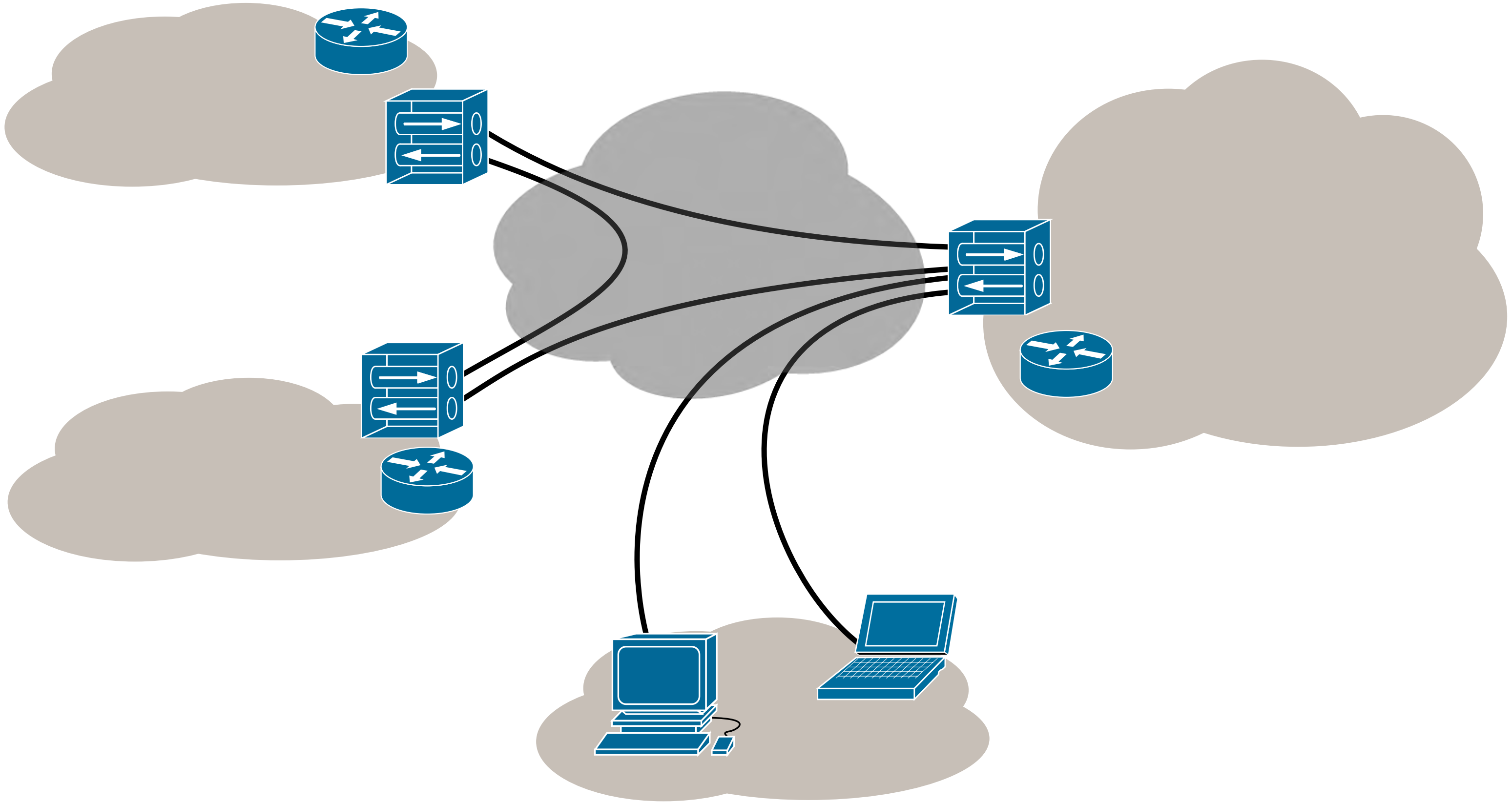
[redacted]

Becoming a ghost

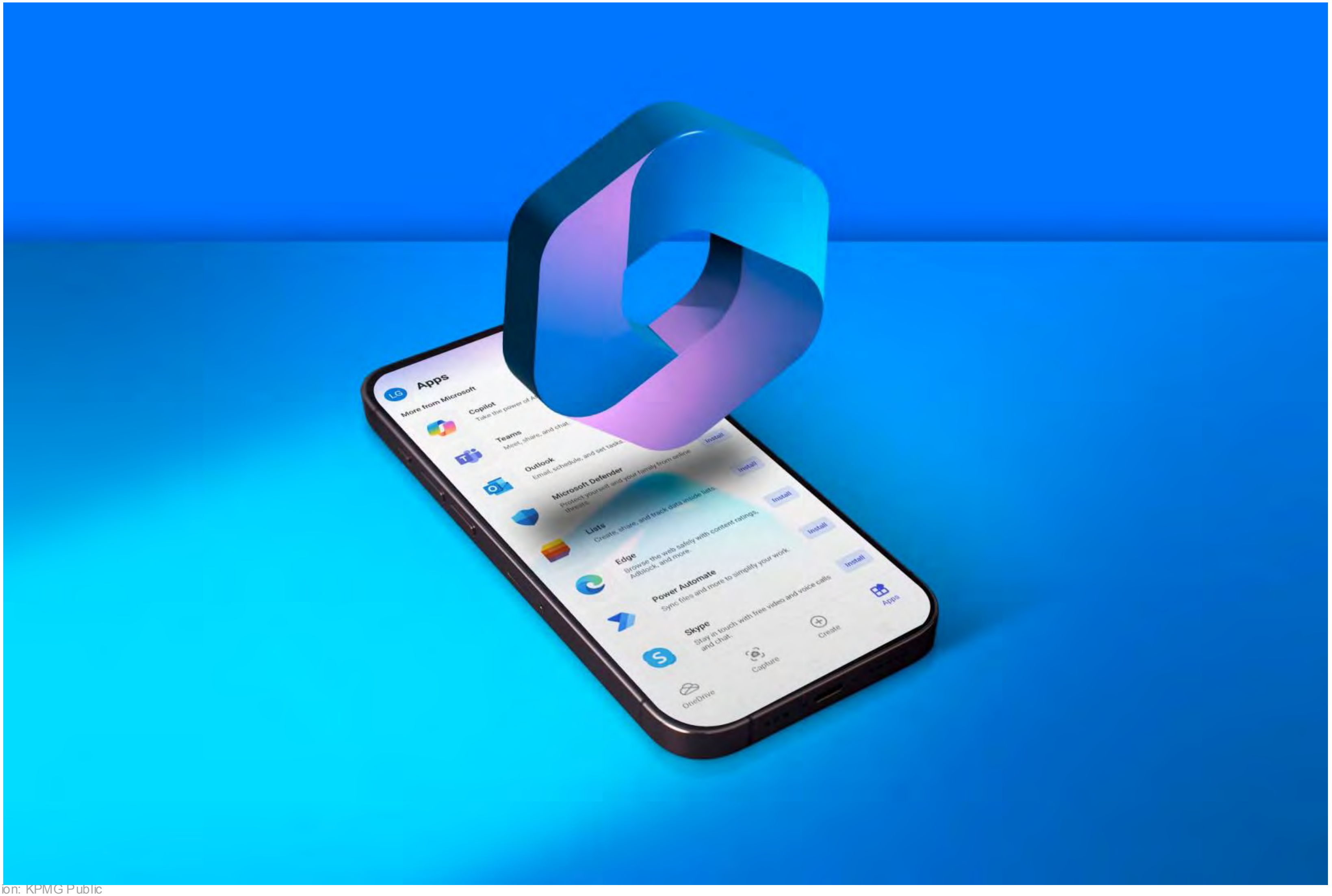
Liability limited by a scheme approved under Professional Standards Legislation.

Document Classification: KPMG Public

Becoming a ghost



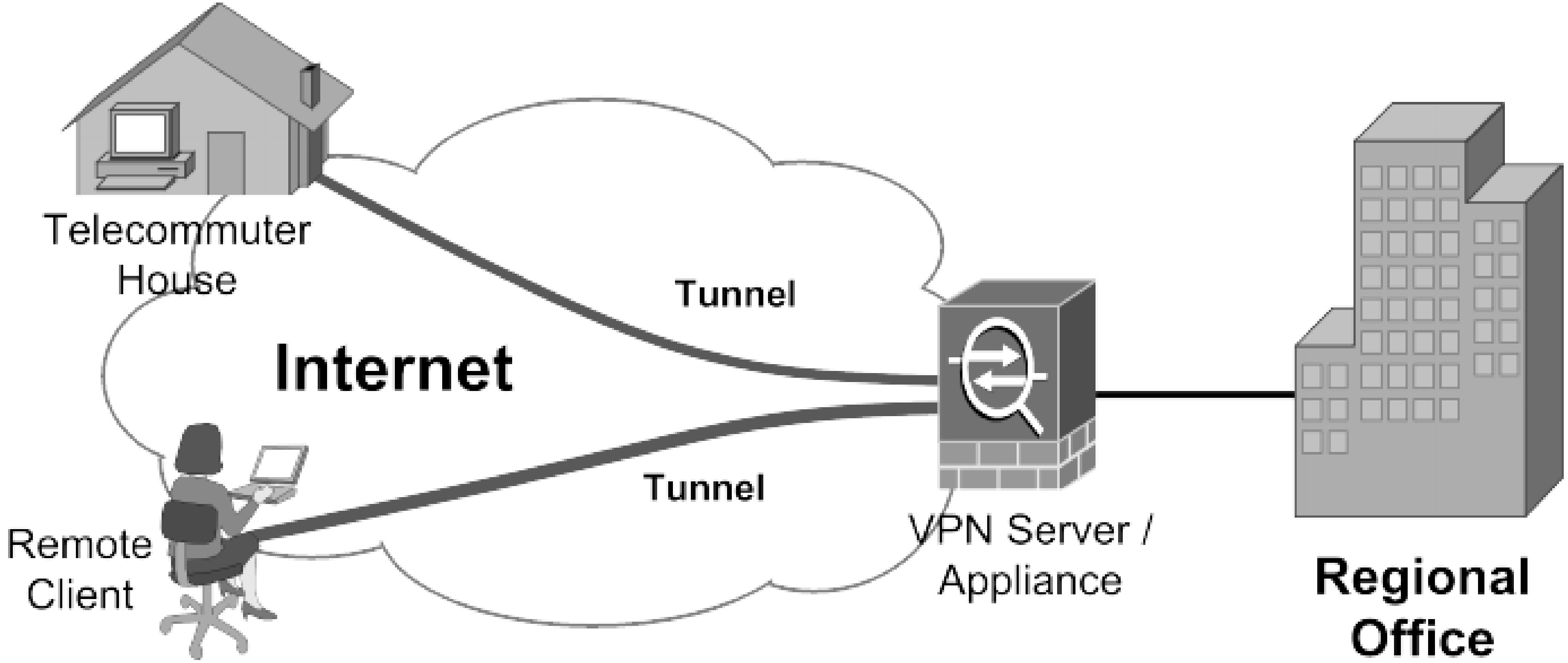
Becoming a ghost



Document Classification: KPMG Public

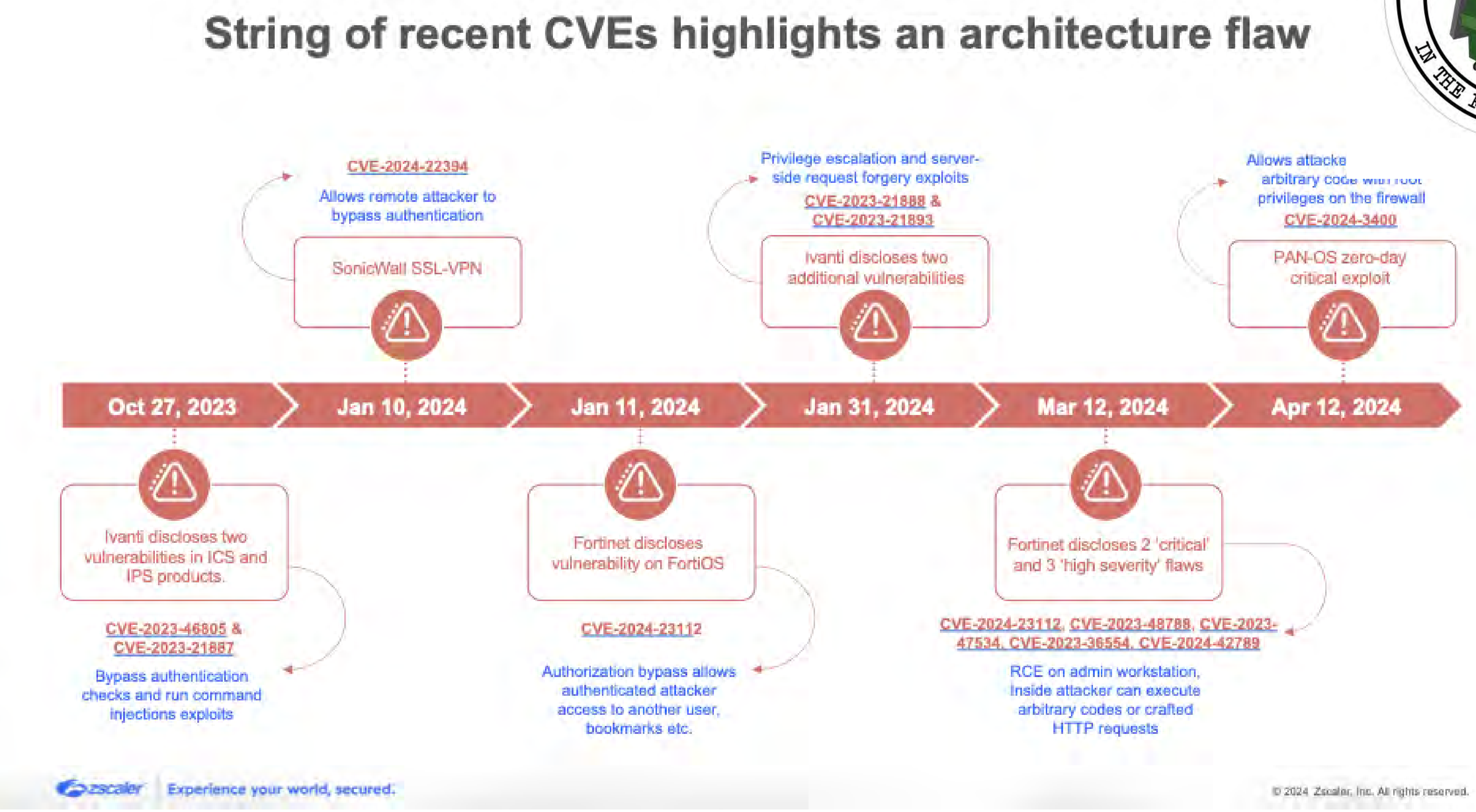
Becoming a ghost

Becoming a ghost



Becoming a ghost

THE STRONGEST STEEL IS FORGED IN THE FIRE OF A DUMPSTER



String of recent CVEs highlights an architecture flaw

Oct 27, 2023 — Ivanti discloses two vulnerabilities in ICS and IPS products.

CVE-2023-46805 & CVE-2023-21887

Bypass authentication checks and run command injections exploits

Jan 10, 2024 — SonicWall SSL-VPN

CVE-2024-22394

Allows remote attacker to bypass authentication

Jan 11, 2024 — Fortinet discloses vulnerability on FortiOS

CVE-2024-23112

Authorization bypass allows authenticated attacker access to another user, bookmarks etc.

Jan 31, 2024 — Ivanti discloses two additional vulnerabilities

Privilege escalation and server-side request forgery exploits

CVE-2023-21888 & CVE-2023-21893

Mar 12, 2024 — Fortinet discloses 2 'critical' and 3 'high severity' flaws

CVE-2024-23112, CVE-2023-48788, CVE-2023-47534, CVE-2023-36554, CVE-2024-42789

RCE on admin workstation, Inside attacker can execute arbitrary codes or crafted HTTP requests

Apr 12, 2024 — PAN-OS zero-day critical exploit

Allows attacke arbitrary code with root privileges on the firewall

CVE-2024-3400

zscaler | Experience your world, secured.

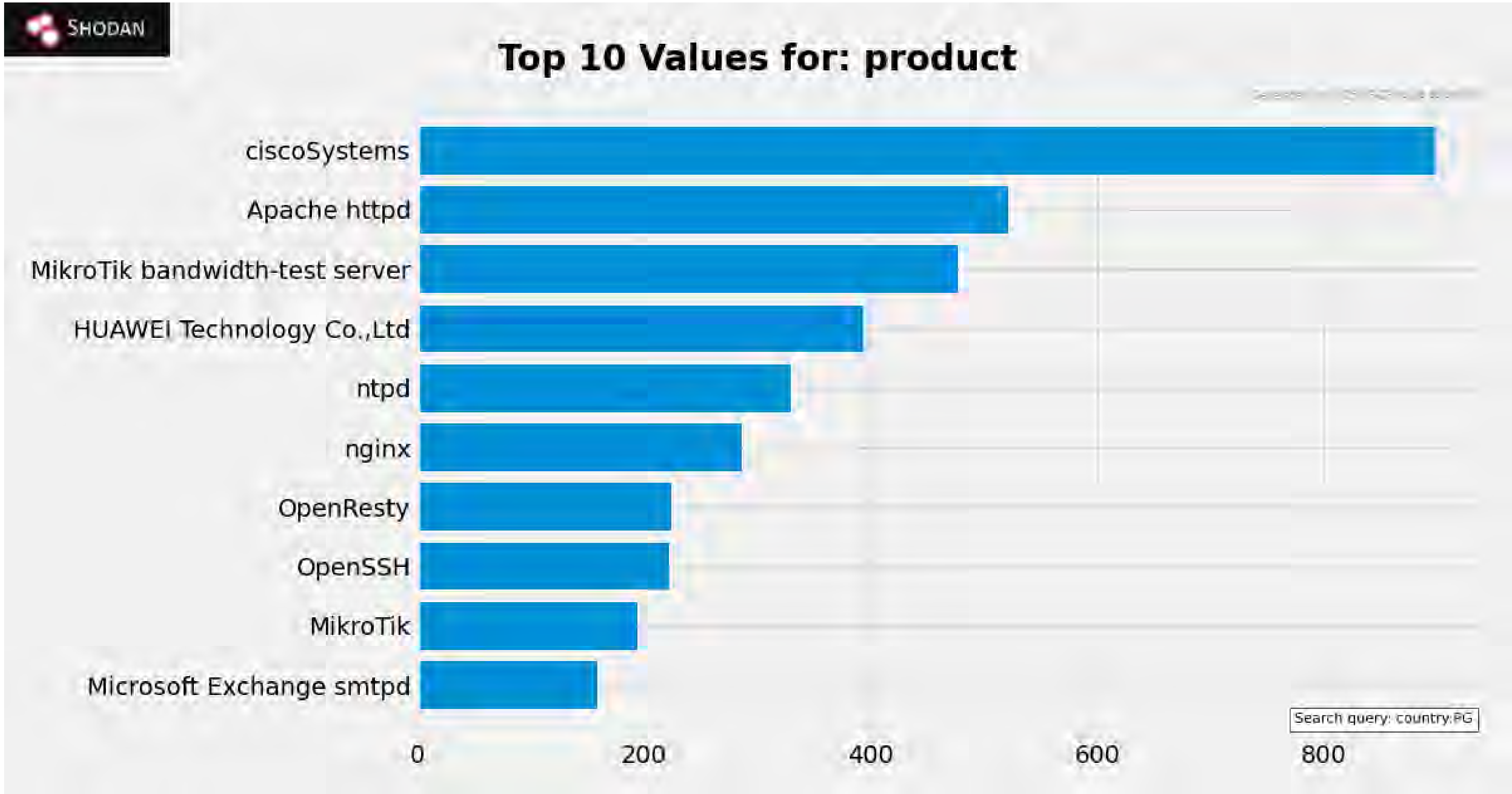
© 2024 Zscaler, Inc. All rights reserved.

Becoming a ghost

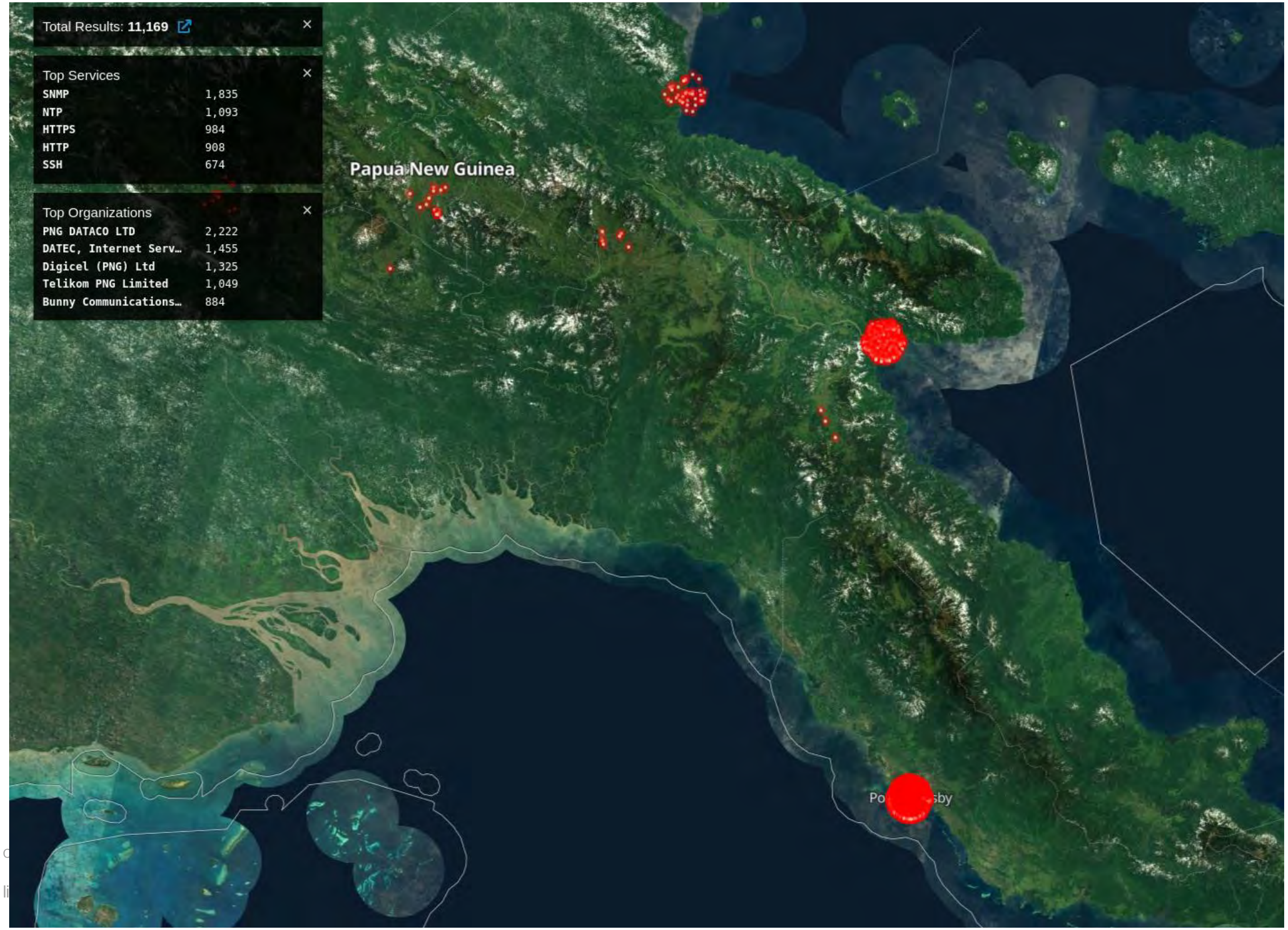
Liability limited by a scheme approved under Professional Standards Legislation.

Document Classification: KPMG Public

Becoming a ghost



Becoming a ghost



Total Results: **11,169**

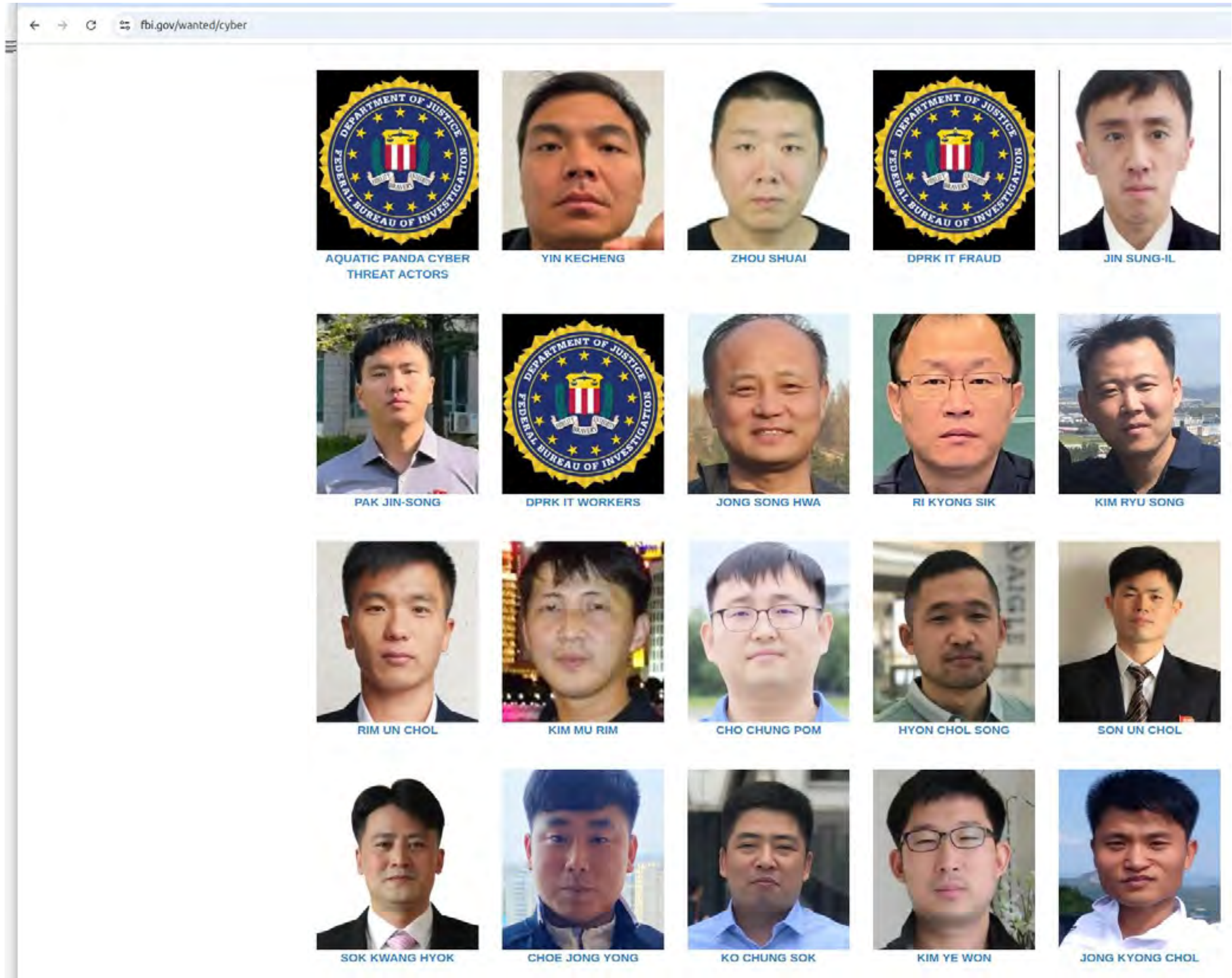
Top Services

SNMP	1,835
NTP	1,093
HTTPS	984
HTTP	908
SSH	674

Top Organizations

PNG DATACO LTD	2,222
DATEC, Internet Serv…	1,455
Digicel (PNG) Ltd	1,325
Telikom PNG Limited	1,049
Bunny Communications…	884

Ticking all the boxes



fbi.gov/wanted/cyber

AQUATIC PANDA CYBER THREAT ACTORS

YIN KECHENG

ZHOU SHUAI

DPRK IT FRAUD

JIN SUNG-IL

PAK JIN-SONG

DPRK IT WORKERS

JONG SONG HWA

RI KYONG SIK

KIM RYU SONG

RIM UN CHOL

KIM MU RIM

CHO CHUNG POM

HYON CHOL SONG

SON UN CHOL

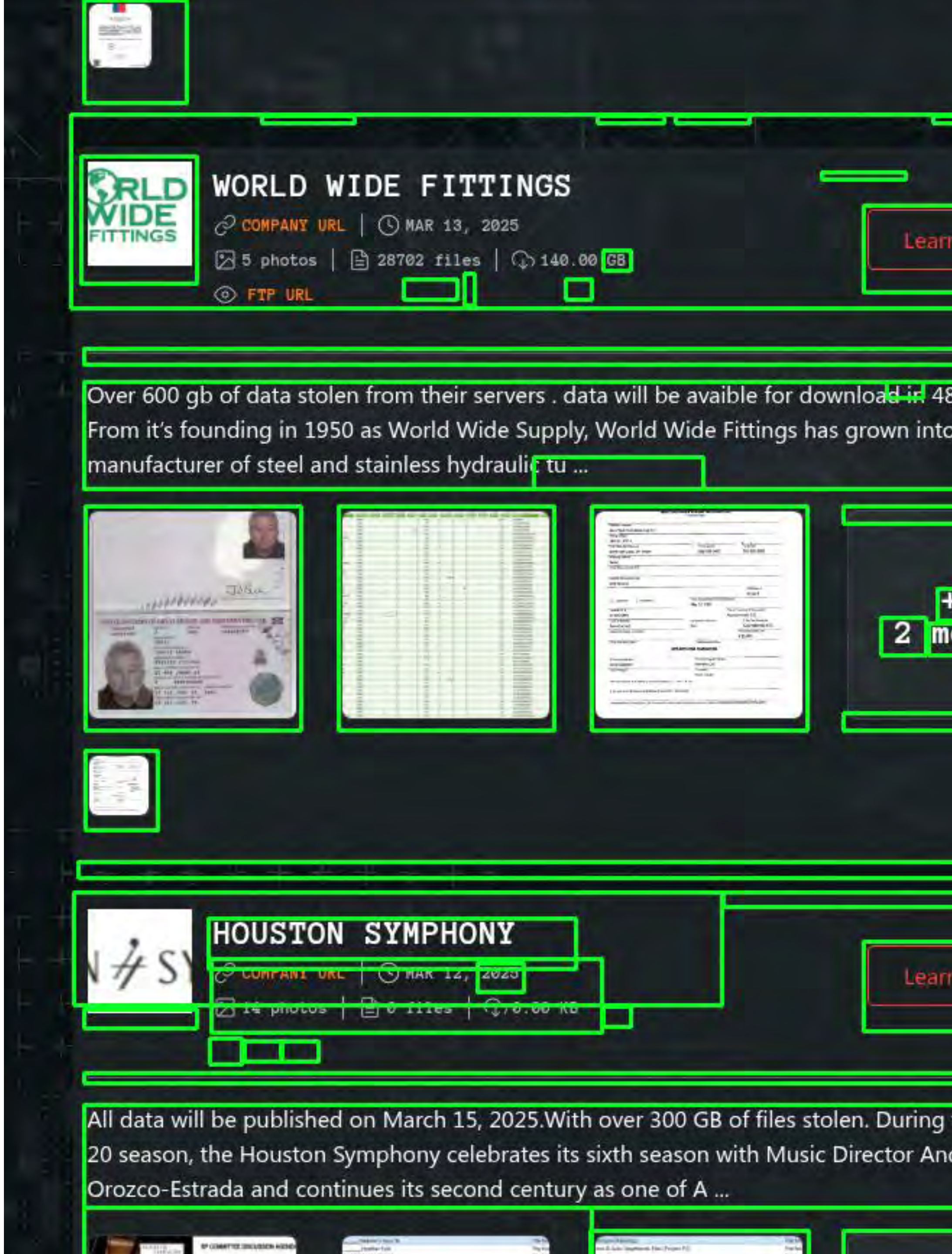
SOK KWANG HYOK

CHOE JONG YONG

KO CHUNG SOK

KIM YE WON

JONG KYONG CHOL



WORLD WIDE FITTINGS

COMPANY URL | MAR 13, 2025

5 photos | 28702 files | 140.00 GB

FTP URL

Over 600 gb of data stolen from their servers . data will be avaible for download in 48

From it's founding in 1950 as World Wide Supply, World Wide Fittings has grown into

manufacturer of steel and stainless hydraulic tu ...

HOUSTON SYMPHONY

COMPANY URL | MAR 12, 2025

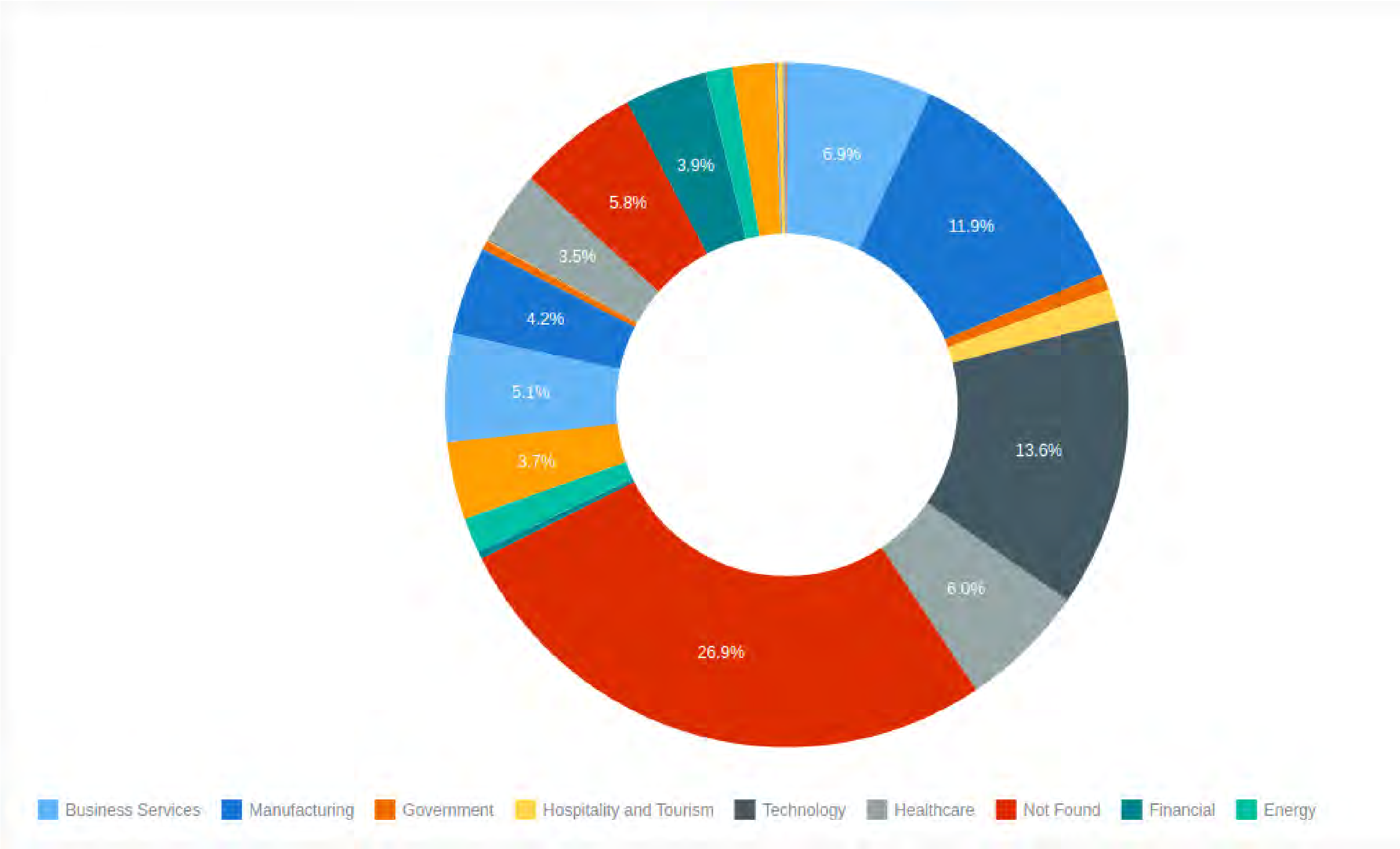
14 photos | 0 files | 0.00 KB

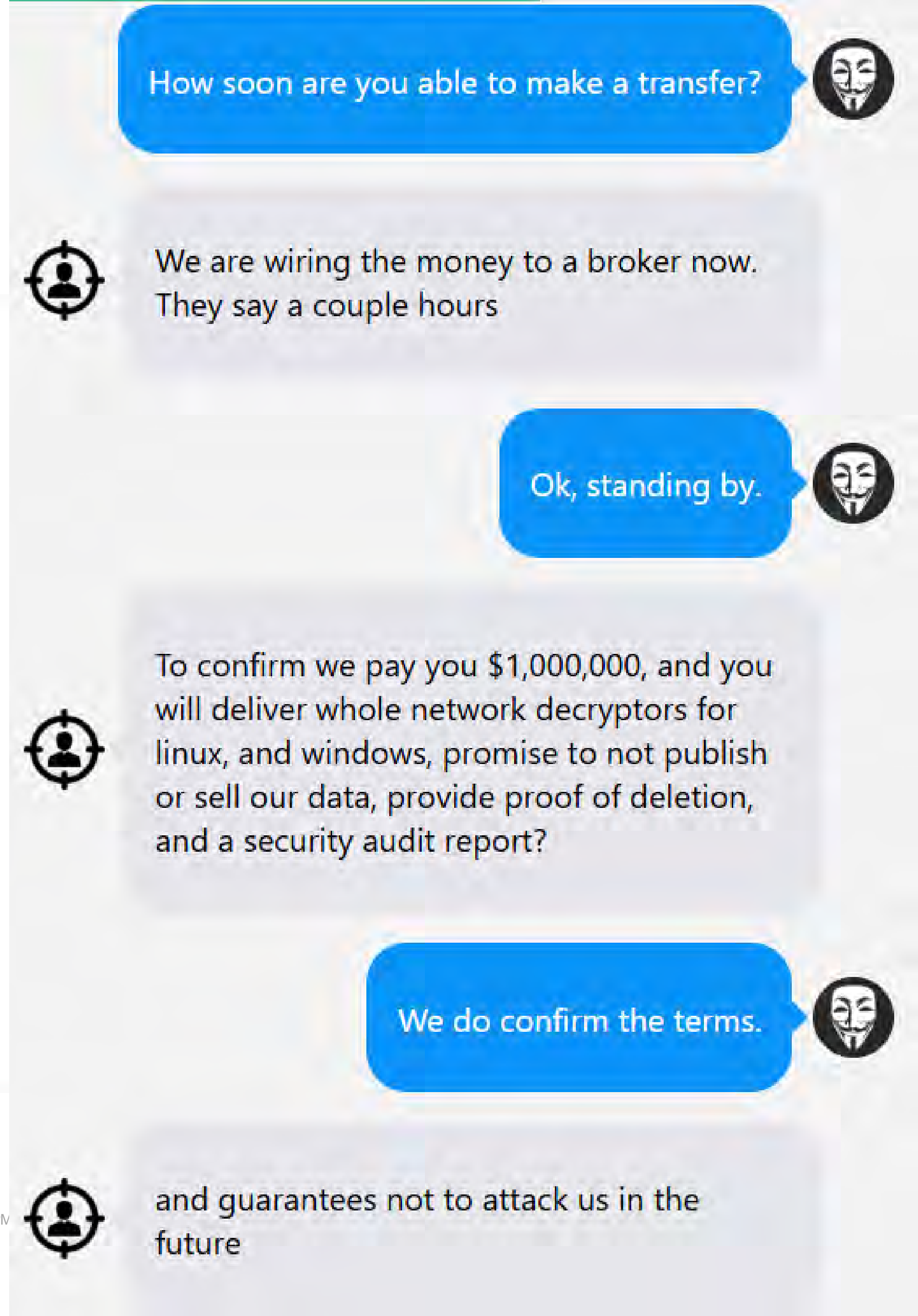
All data will be published on March 15, 2025.With over 300 GB of files stolen. During

20 season, the Houston Symphony celebrates its sixth season with Music Director And

Orozco-Estrada and continues its second century as one of A ...

Ticking all the boxes





How soon are you able to make a transfer?

We are wiring the money to a broker now. They say a couple hours

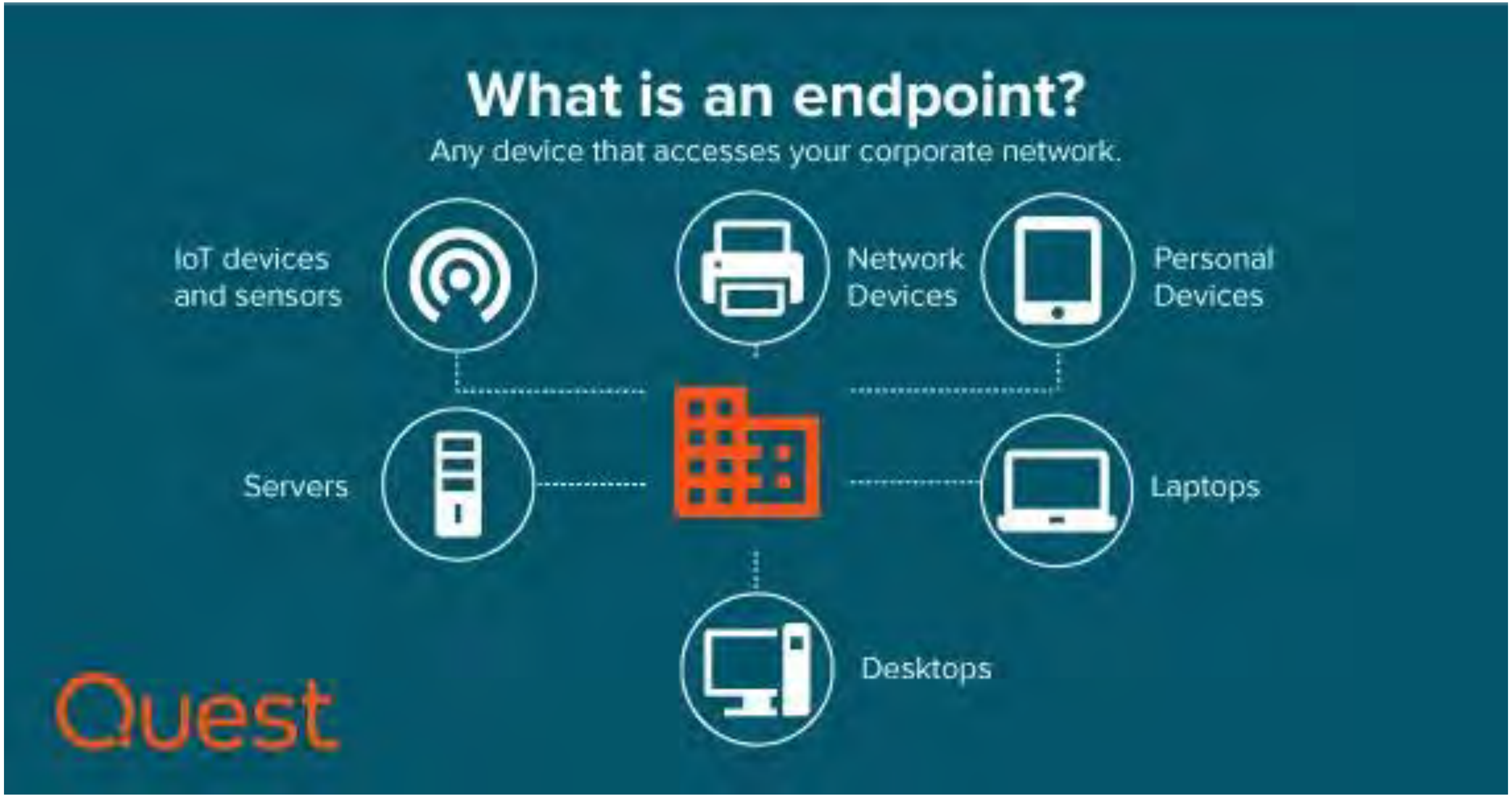
Ok, standing by.

To confirm we pay you $1,000,000, and you will deliver whole network decryptors for linux, and windows, promise to not publish or sell our data, provide proof of deletion, and a security audit report?

We do confirm the terms.

and guarantees not to attack us in the future

Ticking all the boxes



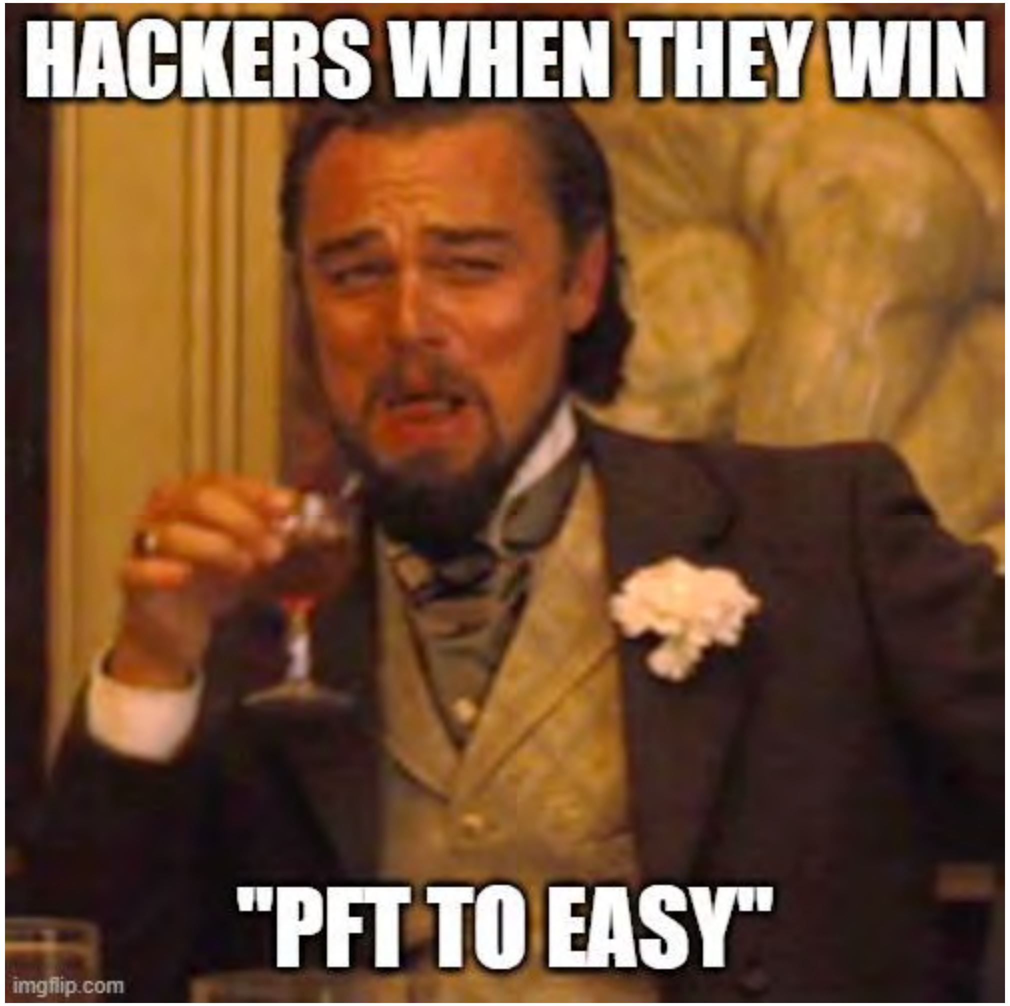
What is an endpoint?

Any device that accesses your corporate network.

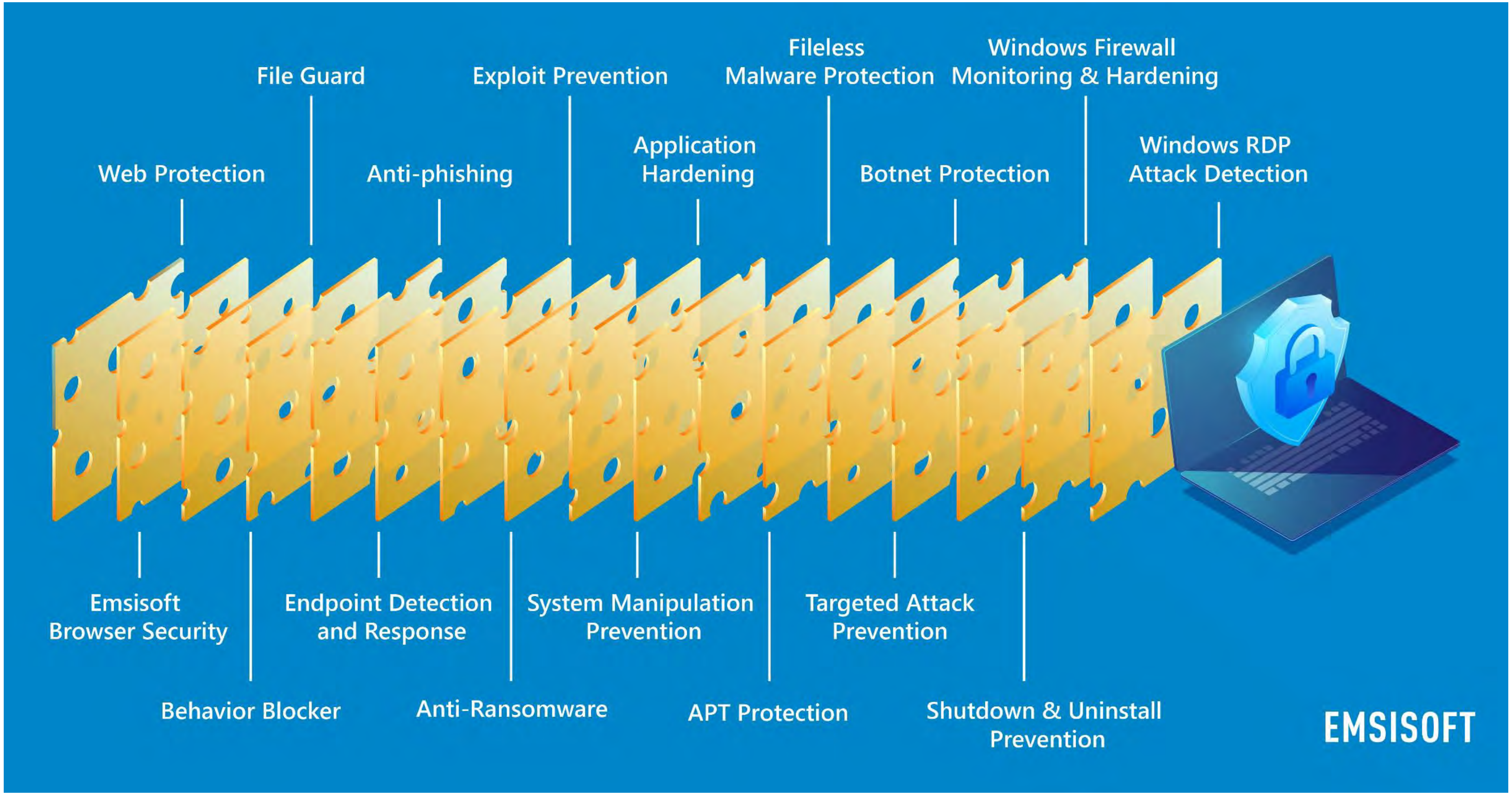
Document Classification: KPMG Public

Liability limited by a scheme approved under Professional Standards Legislation.

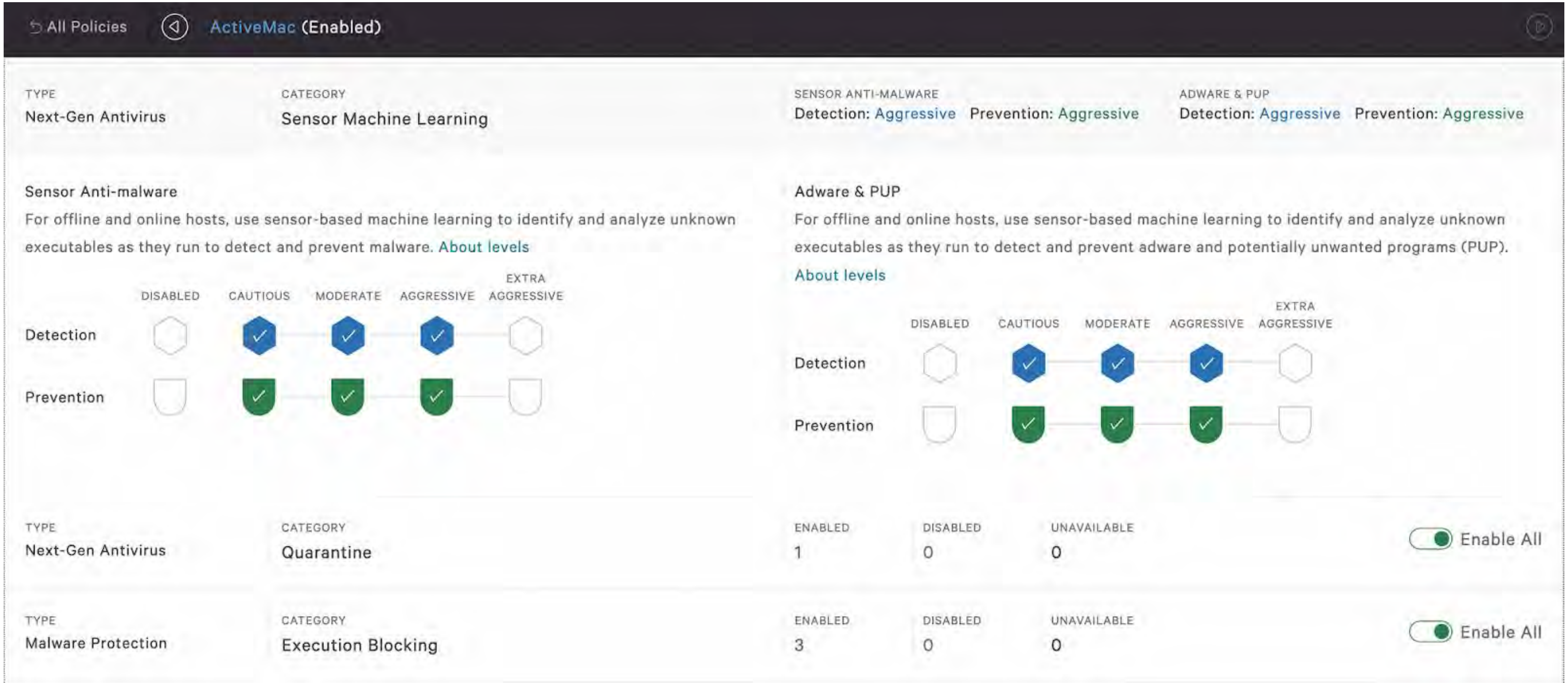
Ticking all the boxes



Ticking all the boxes



Ticking all the boxes



ActiveMac (Enabled)

TYPE	CATEGORY	SENSOR ANTI-MALWARE	ADWARE & PUP
Next-Gen Antivirus	Sensor Machine Learning	Detection: Aggressive Prevention: Aggressive	Detection: Aggressive Prevention: Aggressive

Sensor Anti-malware

For offline and online hosts, use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent malware. About levels

	DISABLED	CAUTIOUS	MODERATE	AGGRESSIVE	EXTRA AGGRESSIVE
Detection		✓	✓	✓	
Prevention		✓	✓	✓	

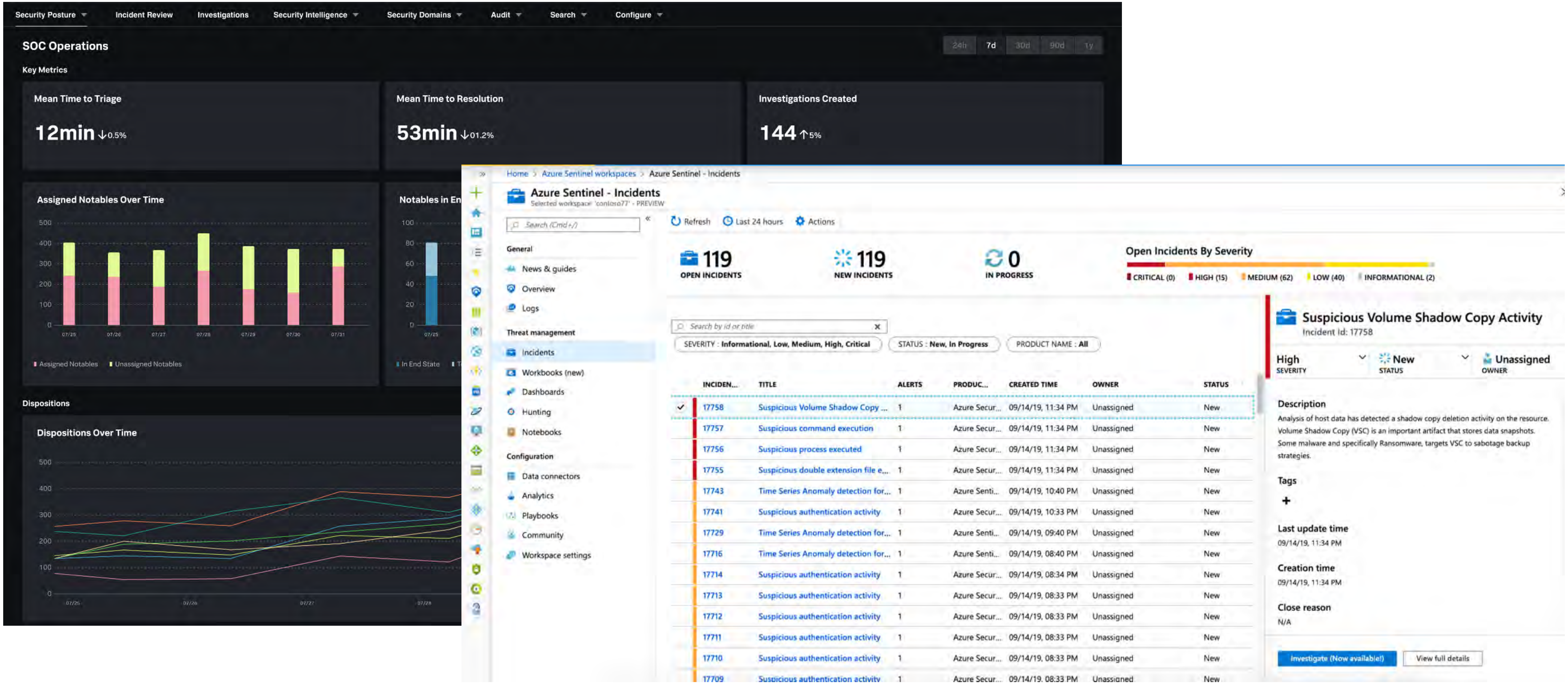
Adware & PUP

For offline and online hosts, use sensor-based machine learning to identify and analyze unknown executables as they run to detect and prevent adware and potentially unwanted programs (PUP). About levels

	DISABLED	CAUTIOUS	MODERATE	AGGRESSIVE	EXTRA AGGRESSIVE
Detection		✓	✓	✓	
Prevention		✓	✓	✓	

TYPE	CATEGORY	ENABLED	DISABLED	UNAVAILABLE	
Next-Gen Antivirus	Quarantine	1	0	0	● Enable All
Malware Protection	Execution Blocking	3	0	0	● Enable All

Ticking all the boxes



SOC Operations

Key Metrics

Mean Time to Triage	Mean Time to Resolution	Investigations Created
12min ↓0.5%	53min ↓01.2%	144 ↑5%

Dispositions

Azure Sentinel - Incidents

Selected workspace: 'contoso77' - PREVIEW

119 OPEN INCIDENTS

119 NEW INCIDENTS

0 IN PROGRESS

Open Incidents By Severity

CRITICAL (0) HIGH (15) MEDIUM (62) LOW (40) INFORMATIONAL (2)

SEVERITY : Informational, Low, Medium, High, Critical

STATUS : New, In Progress

PRODUCT NAME : All

	INCIDEN...	TITLE	ALERTS	PRODUC...	CREATED TIME	OWNER	STATUS
✓	17758	Suspicious Volume Shadow Copy ...	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17757	Suspicious command execution	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17756	Suspicious process executed	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17755	Suspicious double extension file e...	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17743	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 10:40 PM	Unassigned	New
	17741	Suspicious authentication activity	1	Azure Secur...	09/14/19, 10:33 PM	Unassigned	New
	17729	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 09:40 PM	Unassigned	New
	17716	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 08:40 PM	Unassigned	New
	17714	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:34 PM	Unassigned	New
	17713	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17712	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17711	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17710	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17709	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New

Suspicious Volume Shadow Copy Activity

Incident Id: 17758

High SEVERITY — New STATUS — Unassigned OWNER

Description

Analysis of host data has detected a shadow copy deletion activity on the resource. Volume Shadow Copy (VSC) is an important artifact that stores data snapshots. Some malware and specifically Ransomware, targets VSC to sabotage backup strategies.

Last update time

09/14/19, 11:34 PM

Creation time

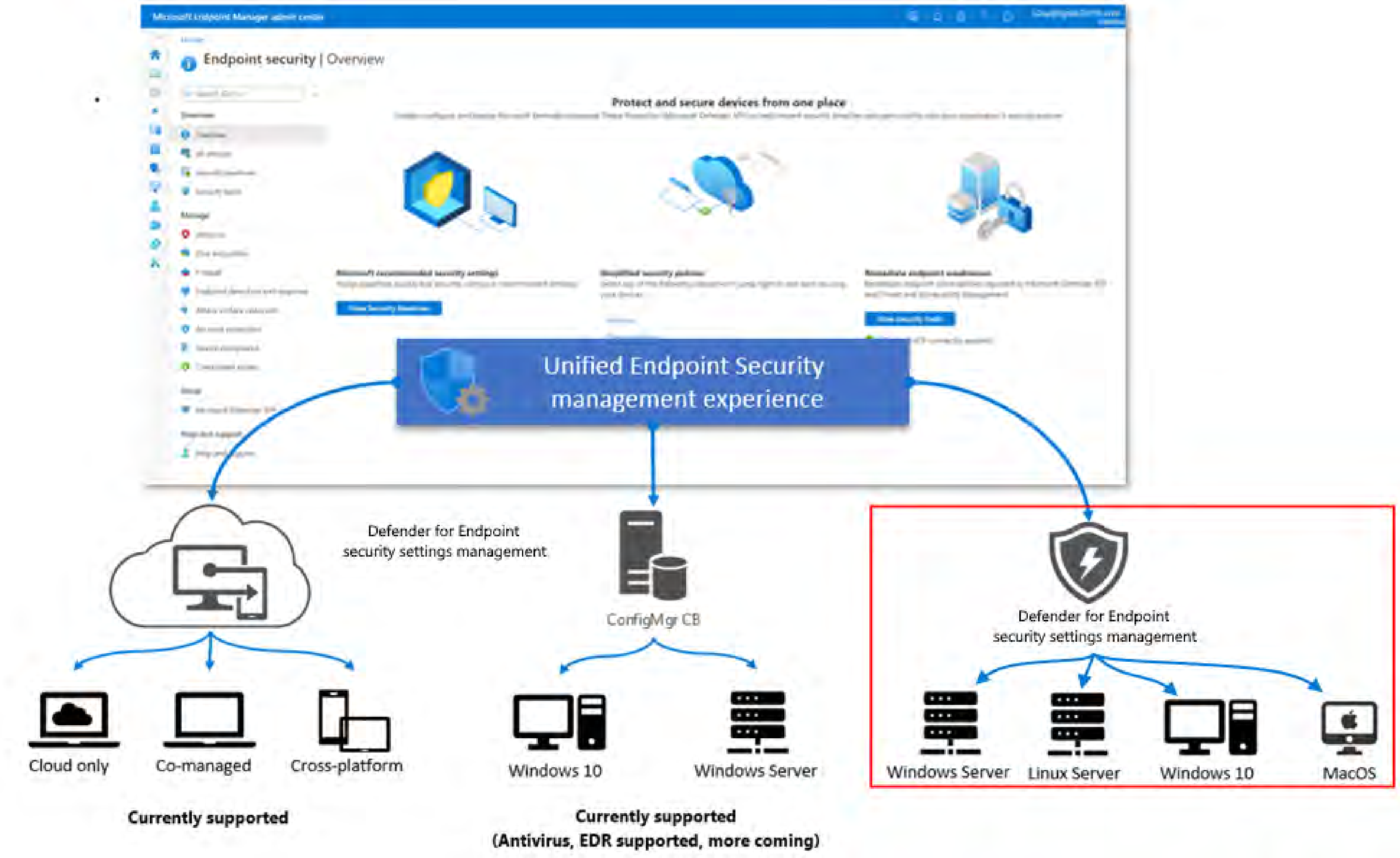
09/14/19, 11:34 PM

Close reason

N/A

Document Classification: KPMG Public

Ticking all the boxes



Microsoft Endpoint Manager admin center

Endpoint security | Overview

Protect and secure devices from one place

Unified Endpoint Security management experience

Defender for Endpoint security settings management

ConfigMgr CB

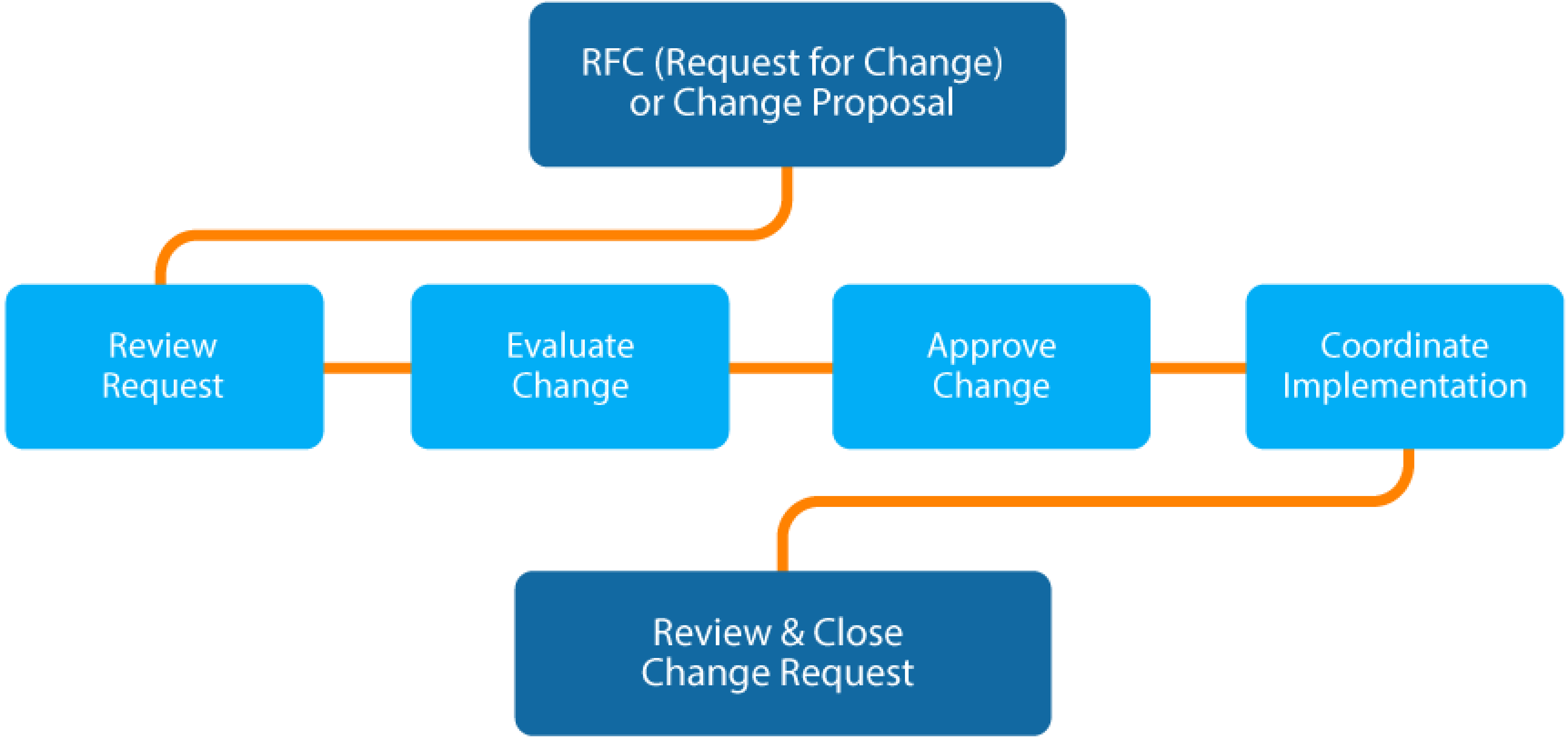
Defender for Endpoint security settings management

Currently supported

Currently supported
(Antivirus, EDR supported, more coming)

Document Classification: KPMG Public

Ticking all the boxes



RFC (Request for Change) or Change Proposal

Review Request

Evaluate Change

Approve Change

Coordinate Implementation

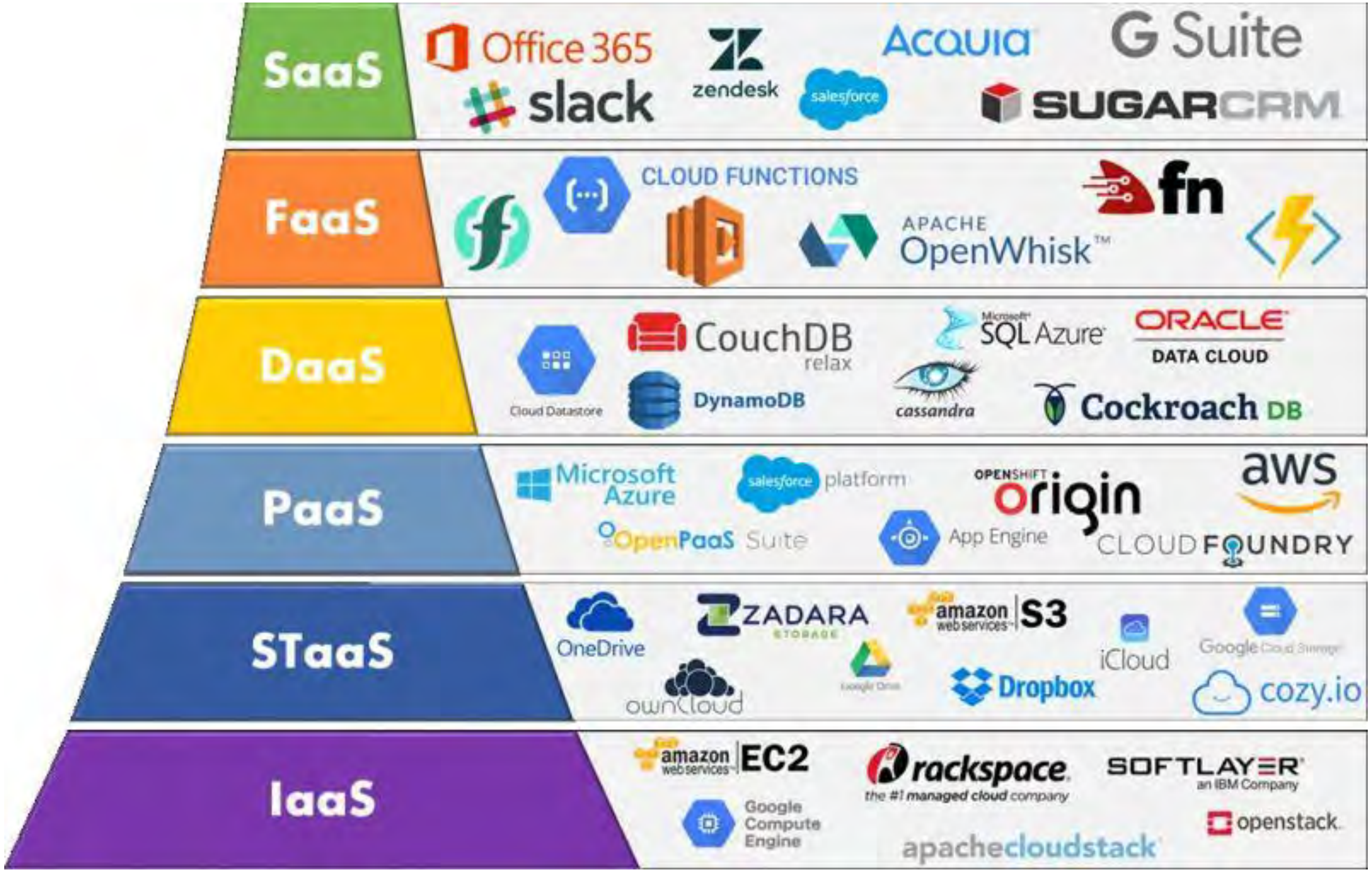
Review & Close Change Request

Ticking all the boxes

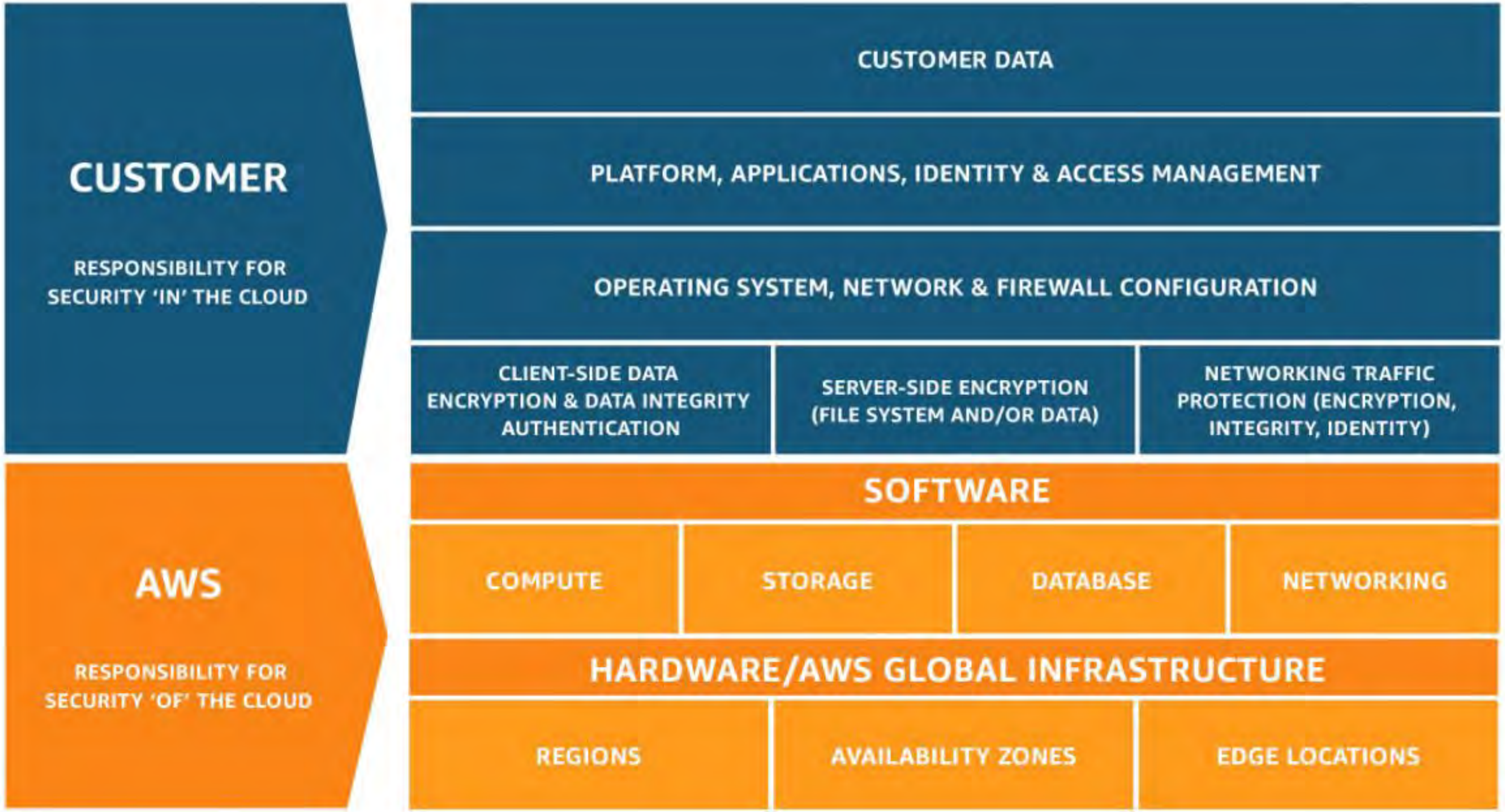
Prevent
Threat Alert
Threat Alert
Respond
Detect

Document Classification: KPMG Public

Doing your part in the cloud



Doing your part in the cloud



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

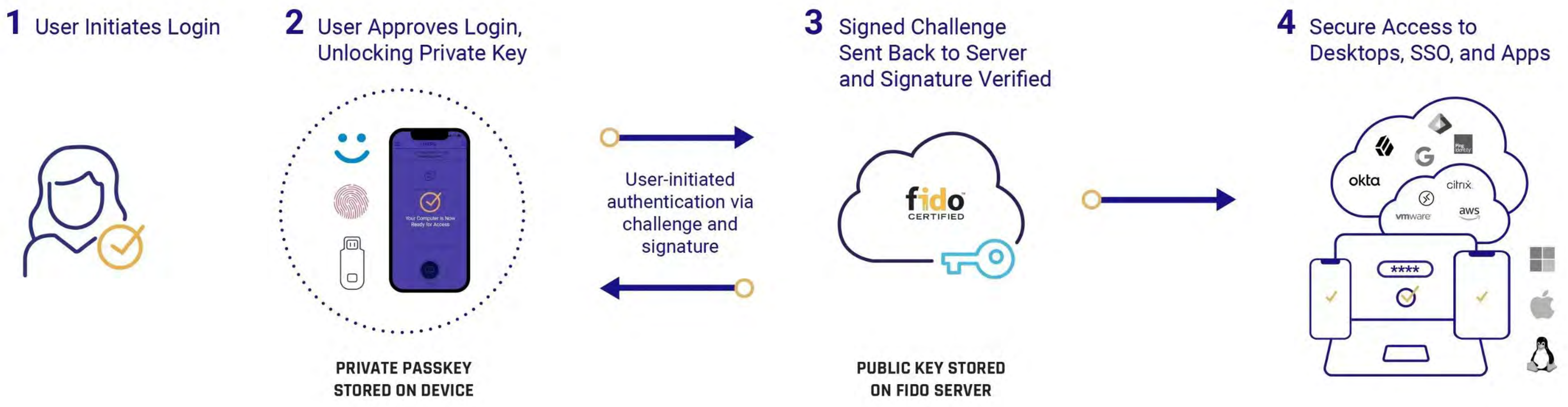
SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

Doing your part in the cloud



1 User Initiates Login

2 User Approves Login, Unlocking Private Key

PRIVATE PASSKEY STORED ON DEVICE

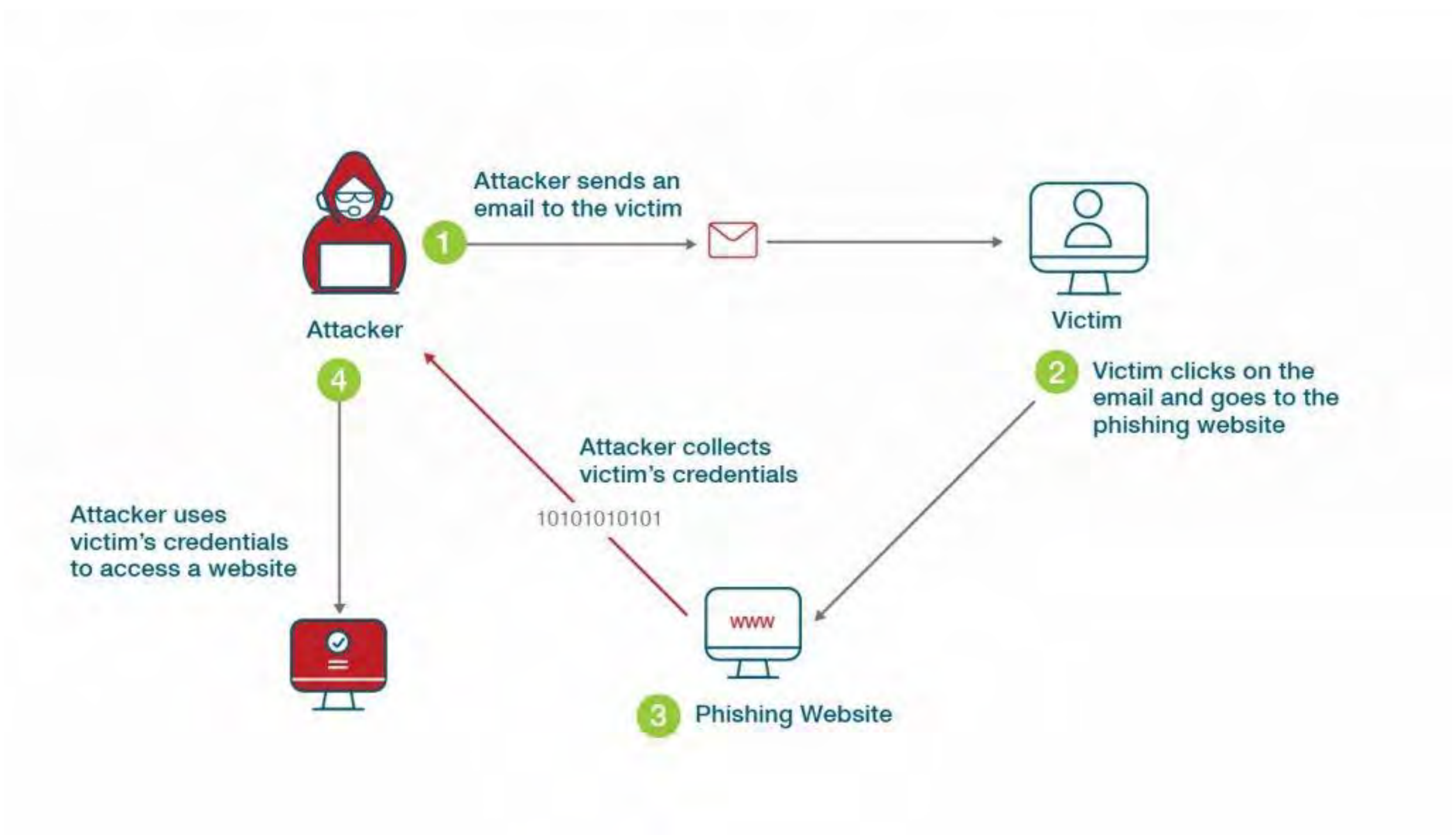
User-initiated authentication via challenge and signature

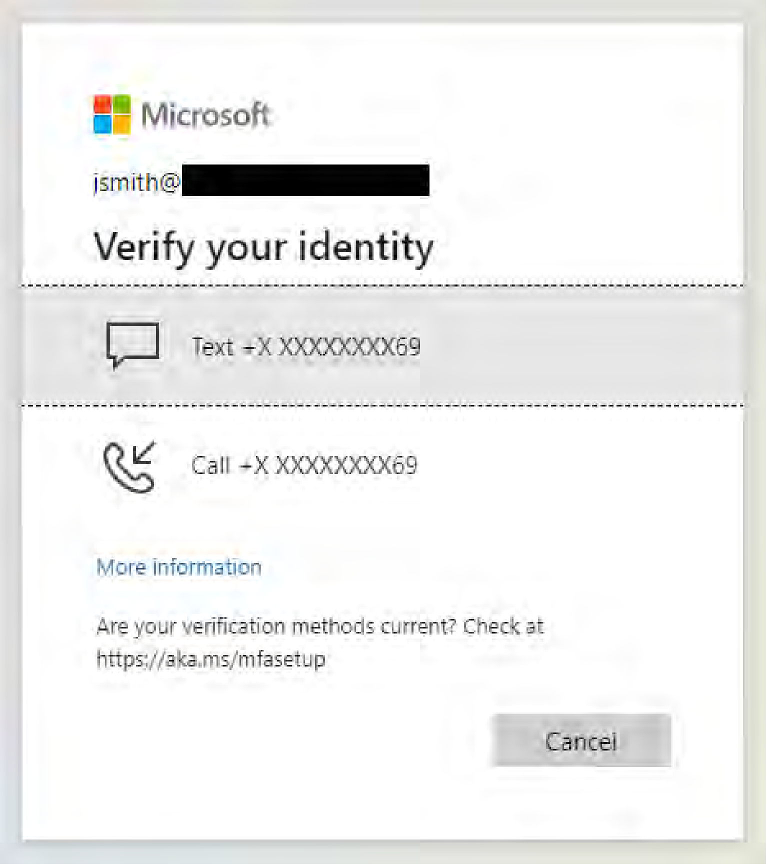
3 Signed Challenge Sent Back to Server and Signature Verified

PUBLIC KEY STORED ON FIDO SERVER

4 Secure Access to Desktops, SSO, and Apps

Doing your part in the cloud


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker collects victim's credentials
10101010101
Attacker uses victim's credentials to access a website
www
3
Phishing Website


Microsoft

jsmith@[redacted]

Verify your identity

Text +X XXXXXXXX69

Call +X XXXXXXXX69

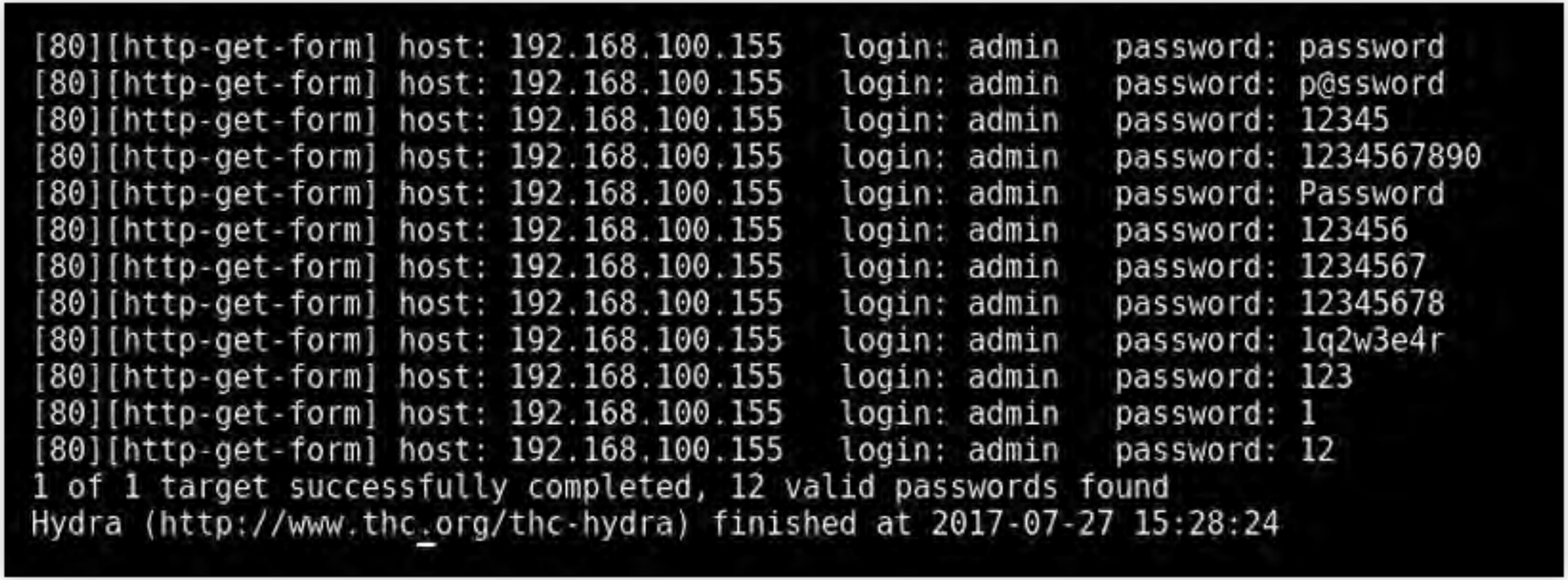
More information

Are your verification methods current? Check at https://aka.ms/mfasetup

Cancel

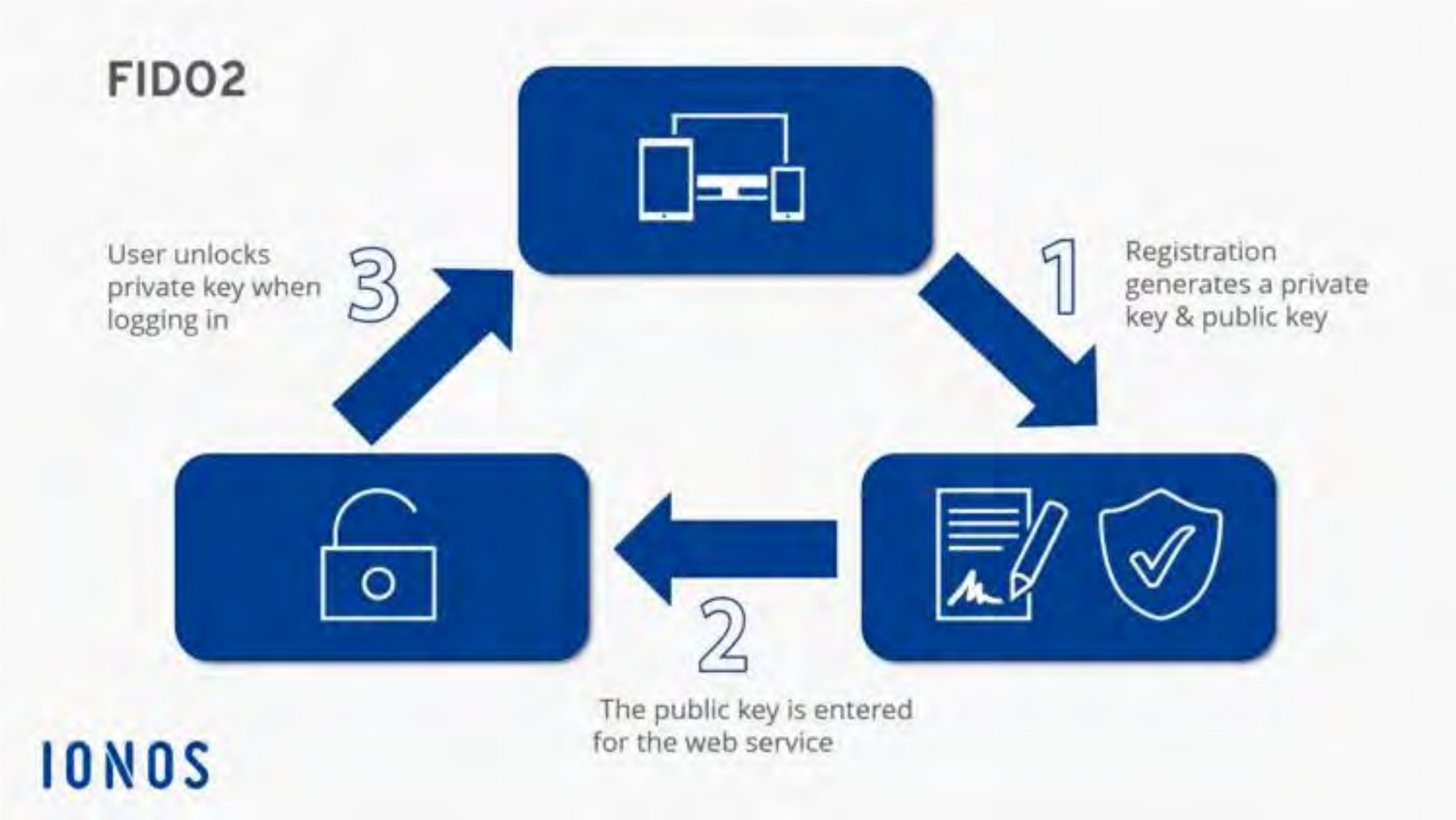
Document Classification: KPMG Public

Doing your part in the cloud



```
[80][http-get-form] host: 192.168.100.155   login: admin   password: password
[80][http-get-form] host: 192.168.100.155   login: admin   password: p@ssword
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567890
[80][http-get-form] host: 192.168.100.155   login: admin   password: Password
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123456
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345678
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```

Doing your part in the cloud



1 Registration generates a private key & public key

2 The public key is entered for the web service

3 User unlocks private key when logging in

Document Classification: KPMG Public

Liability limited by a scheme approved under Professional Standards Legislation.

Doing your part in the cloud

Liability limited by a scheme approved under Professional Standards Legislation.

QUESTIONS FOR IT

1. **Becoming a ghost**
   - **What services do we have that are Internet facing?**
   - **What happens if we turn them off?**
2. **Ticking all the boxes**
   - **What is our IT inventory, computers, servers, network?**
   - **What is the patch level on everything?**
   - **What security alerts have we seen and why?**
   - **Have we enabled all the security features we have?**
   - **Could a hacker damage our backups?**
3. **Doing your part in the cloud**
   - **What cloud services do we have?**
   - **Do all accounts use phishing resistant MFA?**
   - **What security alerts have we seen and why?**

Verify

Penetration test

Threat Hunt

Purple team

Cloud-Native Application Protection Platform (CNAPP)

Cloud Security Posture Management (CSPM)

Change control review