ZERO TRUST

Zurich - CSA & SIGS Special Event

Erik Faassen
Principal Architect, Director

WHO AM I?

- DUTCH - LIVING IN THE NETHERLANDS
- PRINCIPAL ARCHITECT, DIRECTOR
- NORTHERN AND CENTRAL EUROPE
- 5.5 YEARS AT PALO ALTO NETWORKS
  - 3.5 YEARS AS SALES ENGINEER
- BACKGROUND:
  - ROYAL DUTCH NAVY
  - SALES ENGINEERING AND ARCHITECT ROLES
  - PLATFORM SYSTEMS ENGINEER
  - 19+ YEARS IT & SECURITY EXPERIENCE

What's on the agenda

1

The Cybersecurity Forces

Get to know all 5 … or 6?

2

Zero Trust

What we're all doing vs. what should be done

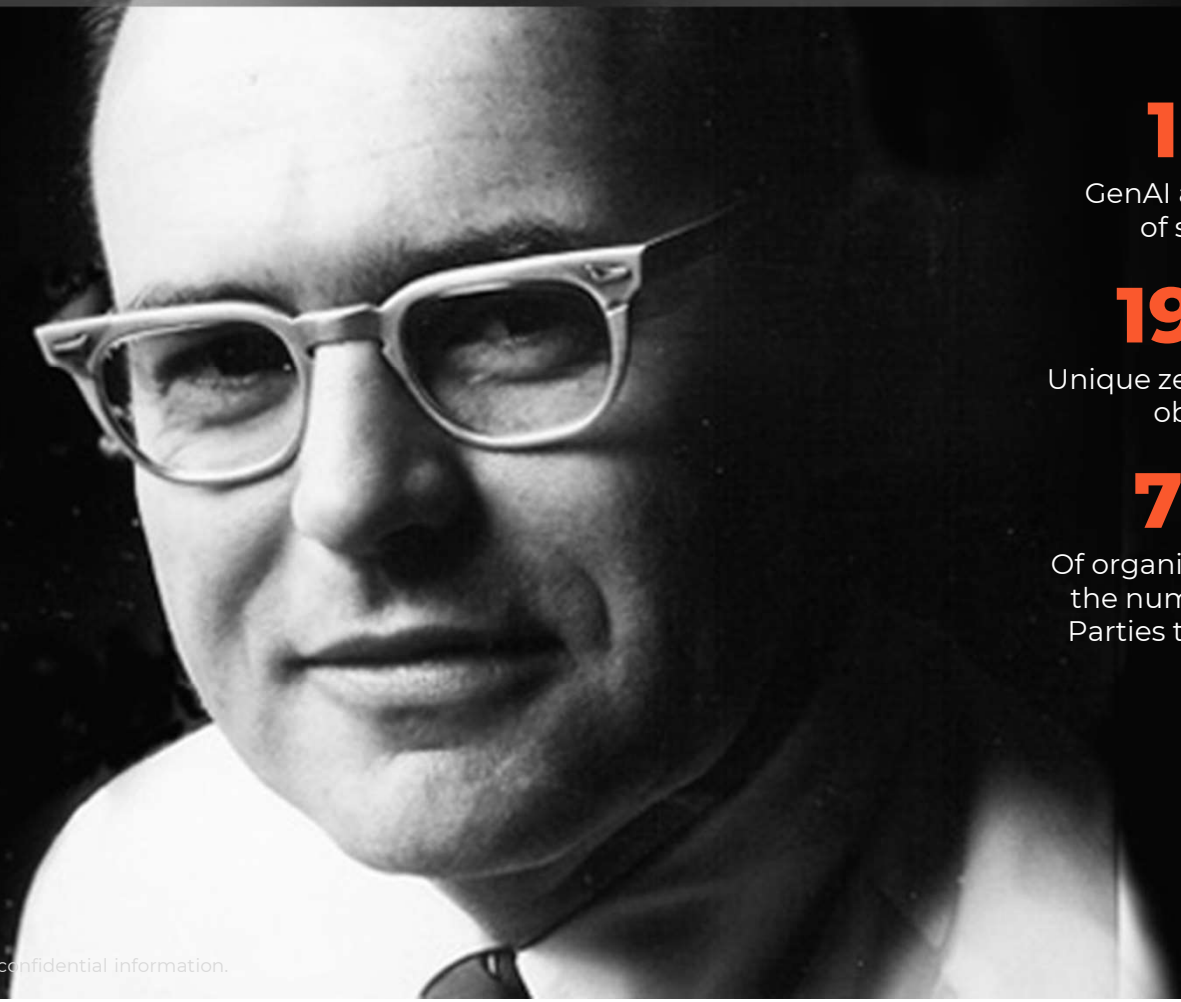
3

Takeaways

For you to take, absorb and share

paloalto NETWORKS

MOORE'S FORCE:
Attack surface wants to grow exponentially



10X
GenAI acceleration of software

19M+
Unique zero-day attacks observed

79%
Of organizations expect the number of Third-Parties to Increase by 2026

Sources: Gartner, McKinsey, The Register, Palo Alto Networks

paloalto NETWORKS

100%

Of business have digital ambitions

89%

Boards agree that Digital is now an implicit part of all business growth strategies

145

hours to resolve a security alert

DARWIN'S FORCE

Cybersecurity can't restrict the speed of innovation

Sources: Gartner, Unit 42 Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface, Palo Alto Networks

paloalto NETWORKS

TERMINATOR'S FORCE:
Attackers will continue to innovate

Average Days from "Compromise" to "Exfil"[1]

2021	2022	2023	Latest
44 days	30 days	5 days	hours

Sources:
1) Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience;

paloalto NETWORKS

~32

Average number of Security Tools deployed by organizations

22%

Have more than 50+ Security Tools deployed in EMEA

6 DAYS

Is the industry average to remediate

FRANKENSTEIN'S FORCE

Disjoint, uninstrumented controls fail over time

Source: Palo Alto Networks What's Next in Cyber Survey & Business Value Consulting analysis

paloalto NETWORKS

3000+

Regulatory expectations in FSI

75%

World population that will be Covered Under Regulations by 2024

SCULLY'S FORCE

Regulators always want to dig deeper

paloalto NETWORKS

The Five Cybersecurity Forces

are pushing Cybersecurity Teams to their limits

Attack surface wants to grow exponentially

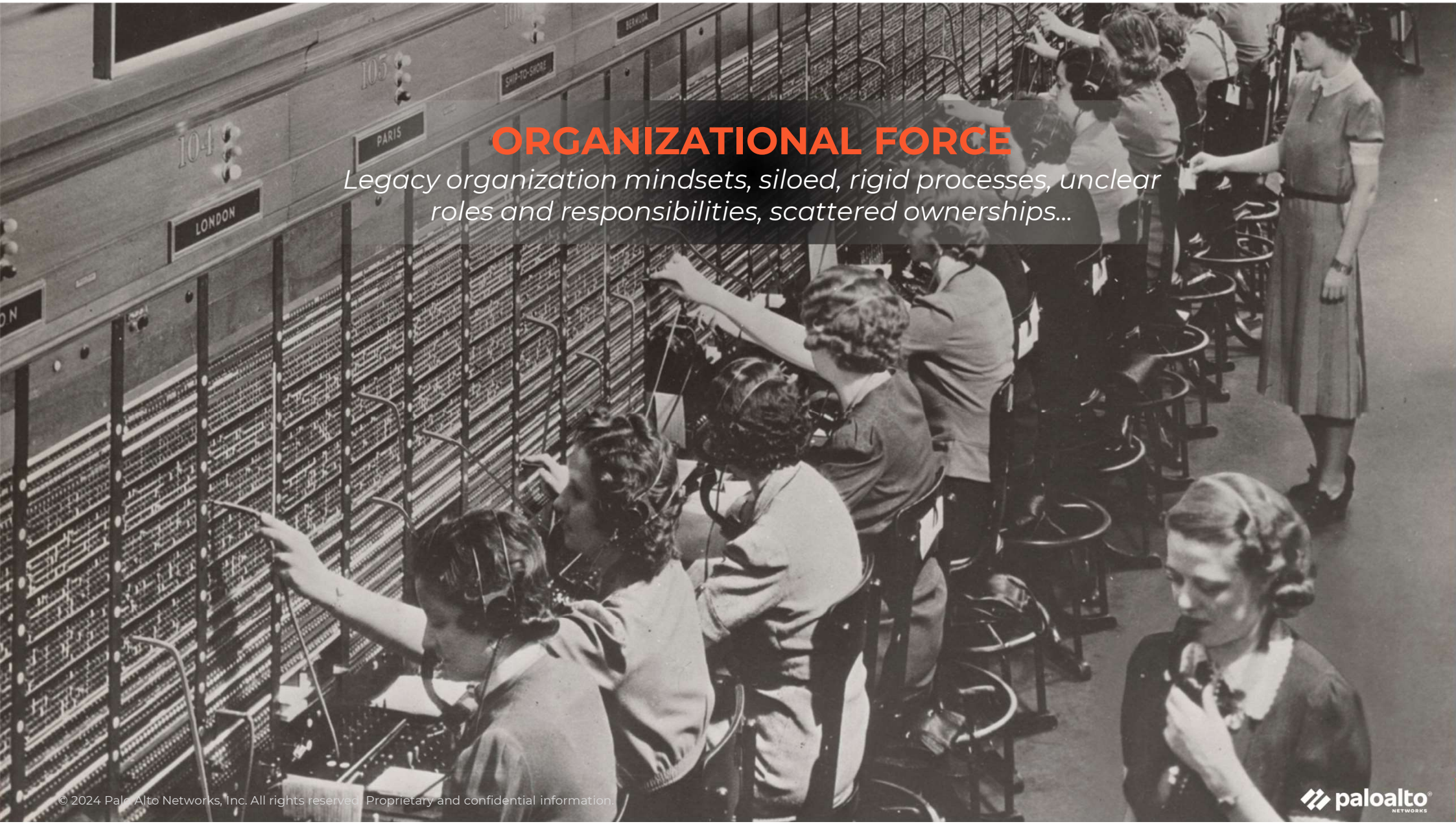
Cybersecurity can't restrict the speed of innovation

Attackers will continue to innovate

Disjoint, uninstrumented controls fail over time

Regulators always want to dig deeper

paloalto NETWORKS



ORGANIZATIONAL FORCE

Legacy organization mindsets, siloed, rigid processes, unclear roles and responsibilities, scattered ownerships...

What's on the agenda

1

The Five Cybersecurity Forces

Get to know them and their challenges

2

Zero Trust

What we're all doing vs. what should be done

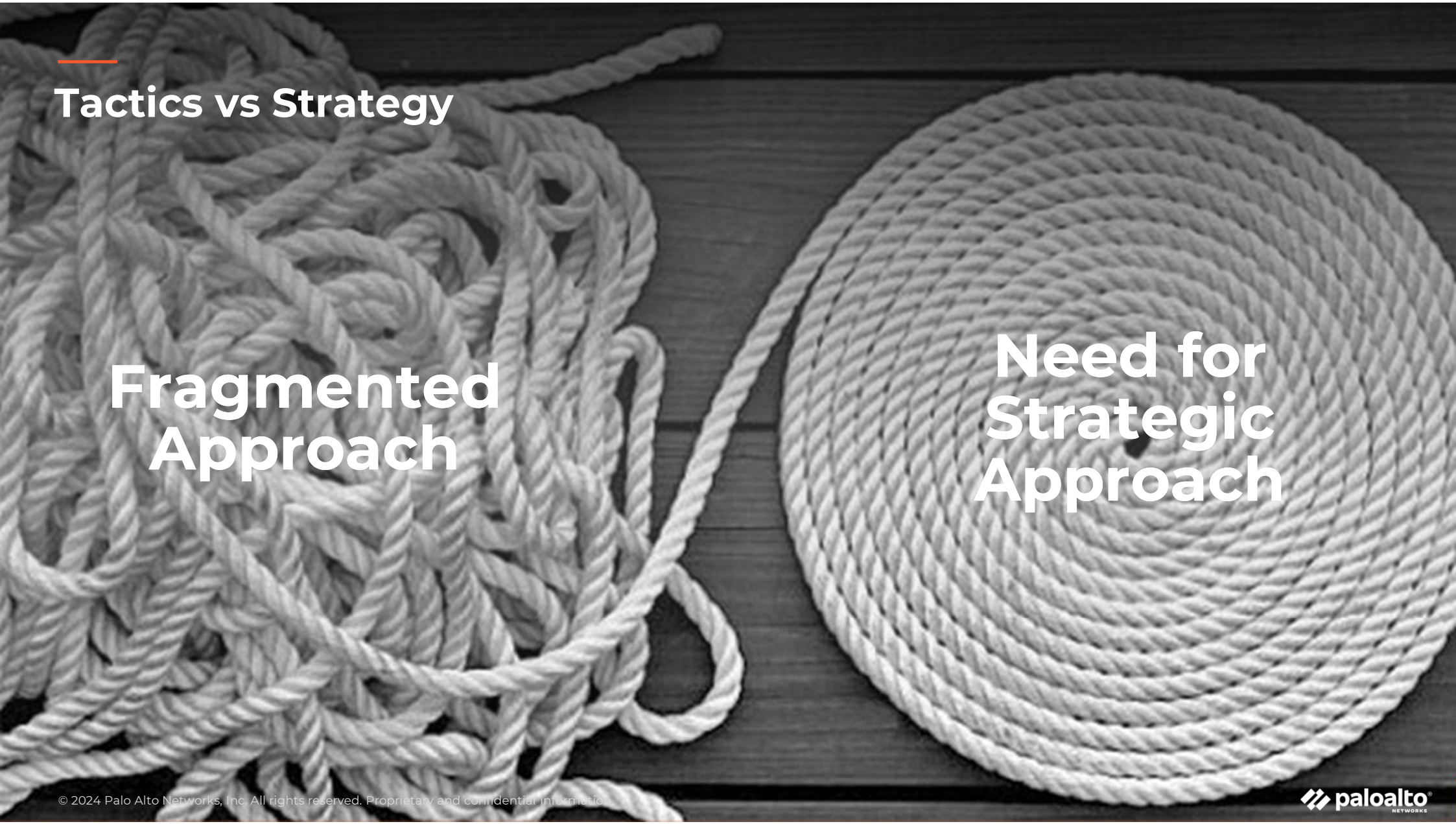
3

Takeaways

For you to take, absorb and share

paloalto NETWORKS

Tactics vs Strategy



ZERO TRUST STRATEGY

Is more than just technology

PEOPLE

PROCESS

TECHNOLOGY

What is Zero Trust?

A strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

Today's security challenges require Zero Trust adoption

Overly Permissive Access

Overly permissive access to applications either because it is unclear what the correct policy should be or mistakes in network and policy configuration, allowing attackers to get a foothold

Large Blast Radius

Internal segmentation largely unrestricted, allowing malicious users and attackers to easily move laterally once they have a foothold

Stolen Credentials Reuse

Attackers accessing sensitive applications and data using stolen credentials

Inconsistent Security

Security scanning only applied to select traffic, creates a significant risk leading to credential theft, data loss, and attackers gaining an opportunity to move laterally

Bad User Experience

End users get a highly fragmented experience based on where they're working from, and operations are overly complex for admins

Unmanaged Devices

Employees accessing sensitive applications and data from unmanaged devices results in data leaving the enterprise's security perimeter

paloalto NETWORKS

And in terms of principles?

Identify & verify all users, devices, applications

Enforce least privilege policy

Apply holistic security inspection

Enforce all data access & movement policies

Optimize user and operational experience

Five widely accepted principles of Zero Trust

paloalto NETWORKS

Five widely accepted principles of Zero Trust

Identify & verify all users, devices, applications

All context gathered

All **users consistently identified**, globally

All **devices & apps** secured

Continuous **passwordless** verification everywhere

Enforce least privilege policy

Contextual policies based on user, device, and apps

Connections allowed based on **business needs**

Default deny all else

Apply holistic security inspection

Core attacks prevention everywhere (e.g., malware)

Adtl. prevention applied by use case (e.g., IoT)

Log detection **analytics**

Enforce all data access & movement policies

Data context used for policies

Controlled data movement to **undesired locations**

Optimize user and operational experience

Performing **architecture** to preserve experience

AI Powered user to app visibility for quick **troubleshooting**

Unified management with consistent policies and data

paloalto NETWORKS

Enterprise Zero Trust

	Identity	Device/Workload	Access	Transaction
Zero Trust for Users	Validate users with strong authentication	Verify user device integrity	Enforce least-privilege user access to data and applications	Scan all content for malicious activity and data theft
Zero Trust for Applications	Validate developers, devops, and admins with strong authentication	Verify workload integrity	Enforce least-privilege access for workloads accessing other workloads	Scan all content for malicious activity and data theft
Zero Trust for Infrastructure	Validate all users with access to the infrastructure	Identify all devices including IoT	Least-privilege access segmentation for native and third-party infrastructure	Scan all content within the infrastructure for malicious activity and data theft

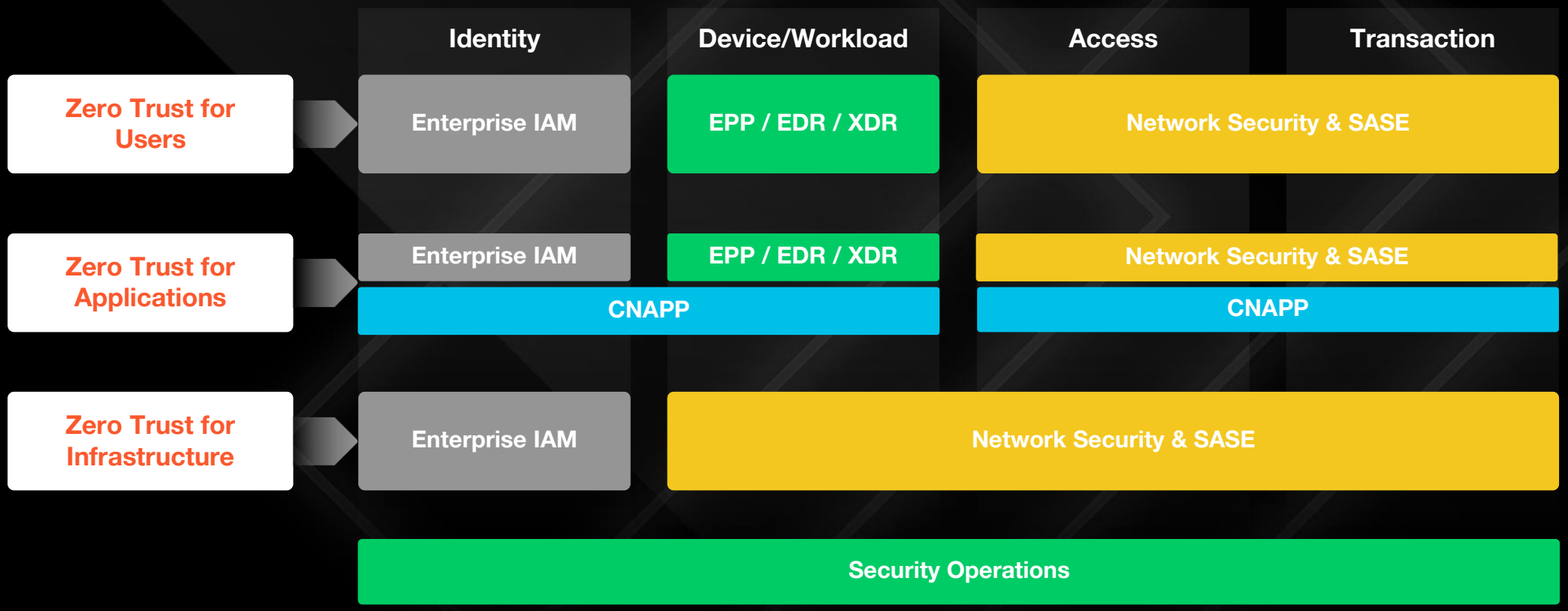
paloalto NETWORKS

The typical approach = Point Product Purchases

~$210 B

to “solve” the problem

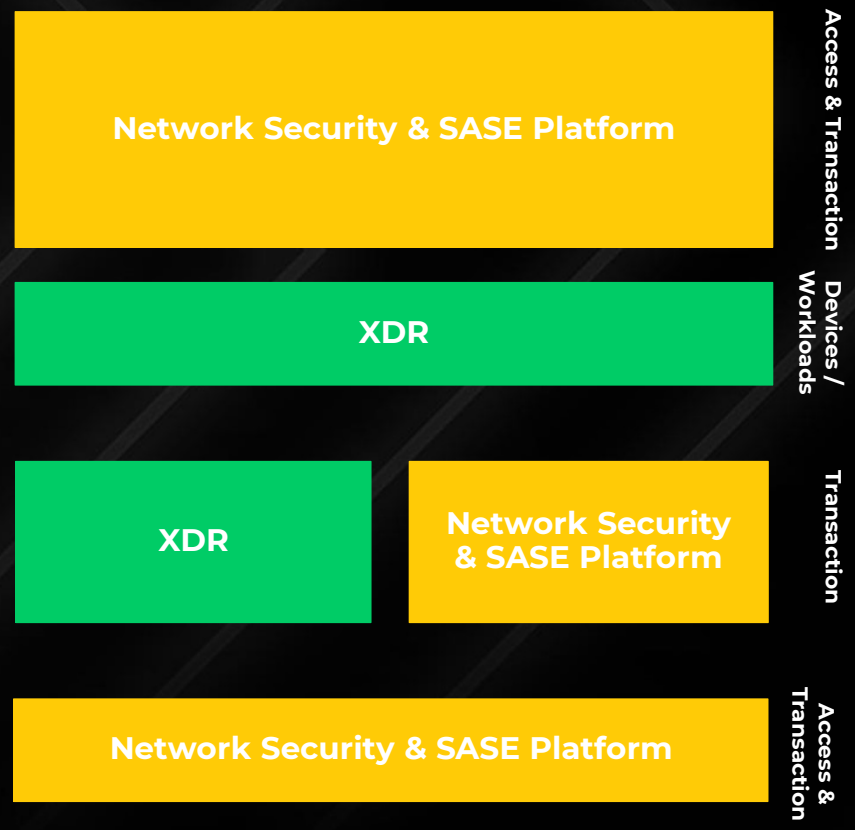
Enterprise Zero Trust



Scenario 1:

How Zero Trust Breaks the Ransomware Attack Chain

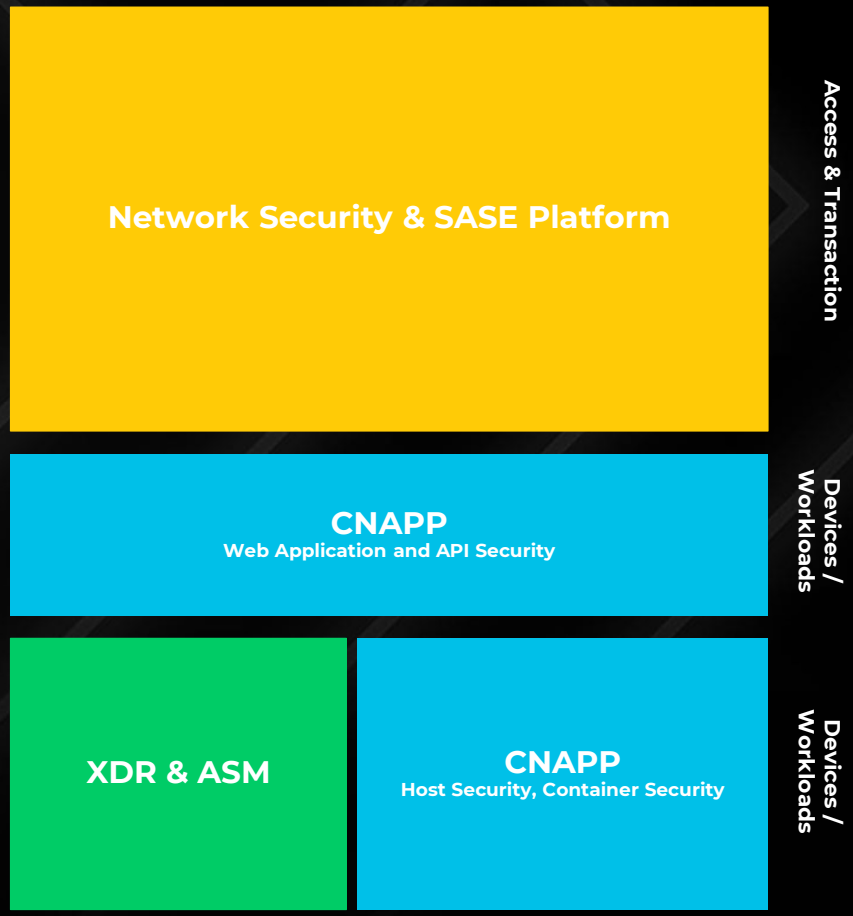
1. **Hacker sends email to CEO**; Email may be blocked via Phishing product.
2. If email reaches user and an email link is clicked, phishing site blocked upon clicking via **DNS Security & Advanced URL Filtering**.
3. If user reaches Phishing site, Ransomware installation is blocked.
4. If initial software is installed, command and control is blocked by **XDR** and **Sandboxing** technology for attachment scanning.
5. If installation successful, expansion is limited / blocked via network segmentation / behavior, C2 detection and exfiltration



paloalto NETWORKS

Scenario 2:
How Zero Trust Breaks the Log4j Attack

1. **Supply chain threat published;** NGFW via Advanced Threat Prevention stops inbound Log4J attacks via Regular Expressions (RegEx) and real-time updates
2. **NGFW** App-ID block LDAP egress to untrusted networks
3. **CNAPP** Web Application API Security (WAAS) rule to block attacks via Regular Expressions (RegEx)
4. Walking internet-facing assets to identify exposures
5. Walk assets (VMs/Containers) to assess impact



= Private = Public

paloalto NETWORKS

Scenario 3:

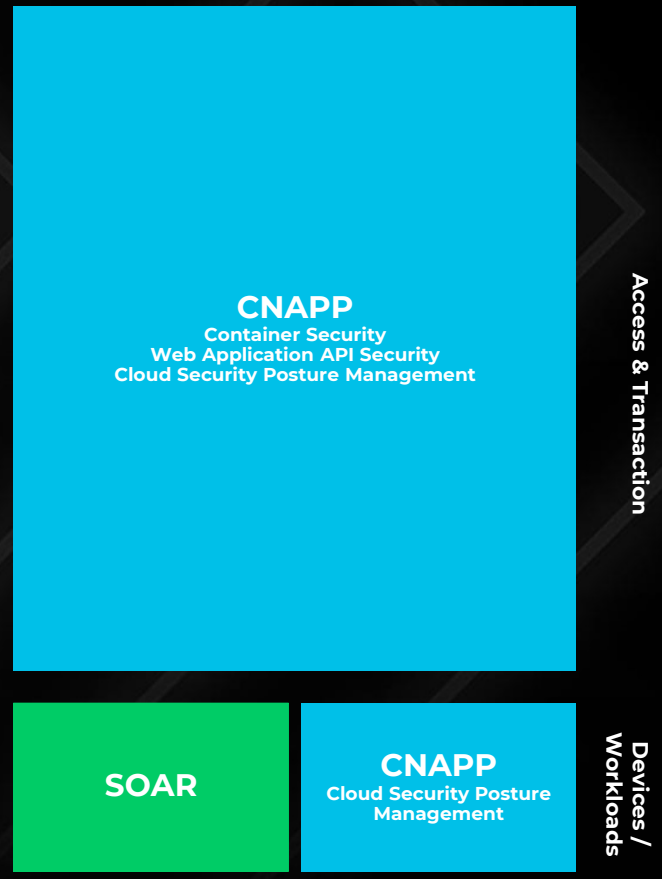
How Zero Trust Breaks Lateral Movement in Containers

1. **Web application in a container is attacked;** **CNAPP** Web Application API Security (WAAS) identifies attack and blocks invalid requests.

2. If attack reaches web application and obtains shell access on container: **CNAPP** **Cloud Security Posture Management (CSPM)** policy for AWS Elastic Kubernetes Service (EKS) will restrict access to Kubernetes API, so as to block reconnaissance. **CWPP** to prevent any unknown behavior

3. If attacker probes Kubernetes Pod for IAM roles which could be exposed: **CNAPP CSPM** policy for AWS Virtual Private Cloud (VPC) would enforce least privilege for users traversing it.

4. If attacker identifies IAM credentials and dumps them to local environment: **CNAPP CSPM** policy for EKS will log that high risk activity and share with the SOC for immediate action



Scenario 4 - integration example:

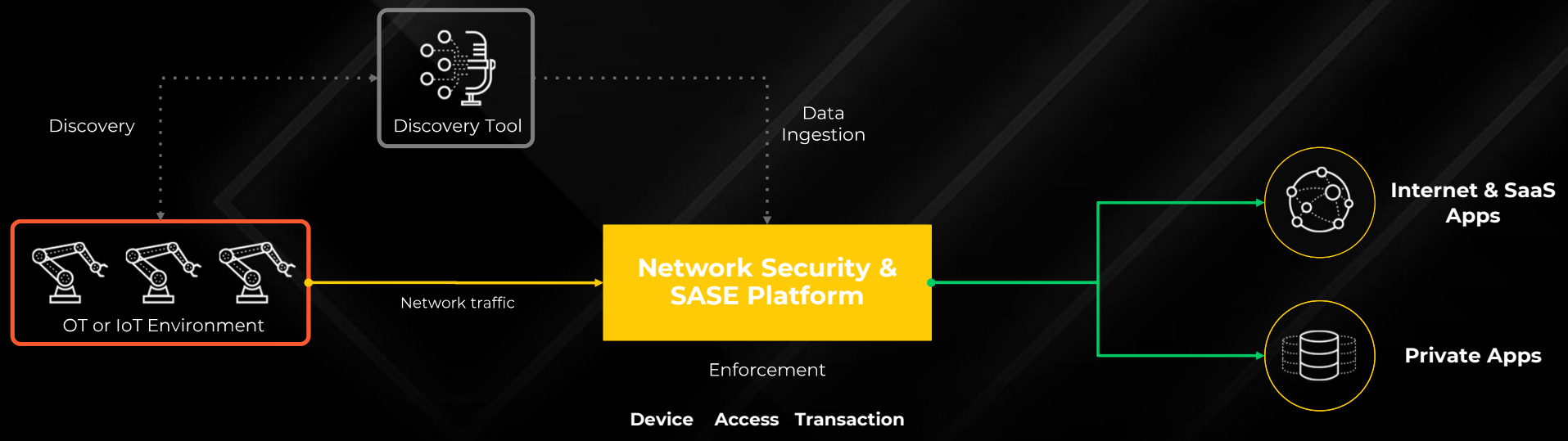
How Zero Trust secures IoT/OT environments in brownfield scenario

1. IoT and OT equipment in manufacturing facilities or offices (IoT) are being discovered with a **3rd party security tool**.

2. After discovery the IoT and OT information is ingested into Network Security Platform for categorization

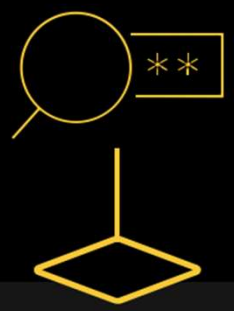
3. **Network Security Platform** contains policies to **enforce security inspection** on the individual or categorized IoT and OT equipment

4. With visibility and security enforcement, IT and Security teams have full visibility and **automated security enforcement.**



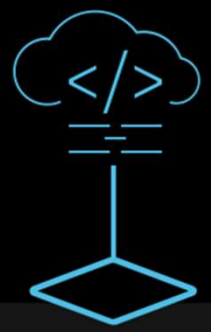
paloalto NETWORKS

Platforms Always Prevail



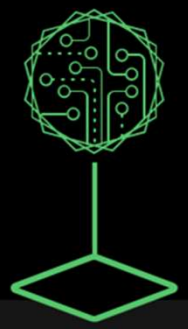
Zero Trust Platform

Network security that ensures every connection is secure



Code to Cloud Platform

Cloud security that ensures every cloud application is secure



AI-Driven Security Operations Platform

SecOps that is powered by a real-time security engine

paloalto NETWORKS

Looking Ahead

Organizations will require
Real-time and Autonomous Security
to Achieve Cyber Resilience

Ubiquitous Platformization will Deliver
Real-Time Security Outcomes

paloalto NETWORKS

Example Outcomes From AI-Enabled Platforms

Reimagined Products

Good Data Drives Great AI

Each day we analyze
750M
new and unique events

AI + ML Deliver Zero-Day Detection

Each day we detect
1.5M
new and unique attacks that weren't there the day before

Attack Prevention Happens Inline

Each day we block
8.6B
attacks

Operational Efficiency

Stronger Cybersecurity Outcomes

10
SECONDS
Mean Time to Detect

15
MINUTE
Mean Time to Respond
(automated & manual)

paloalto NETWORKS

What's on the agenda

1

The Five Cybersecurity Forces

Get to know them and their challenges

2

Zero Trust

What we're all doing vs. what should be done

3

Takeaways

For you to take, absorb and share

paloalto NETWORKS

Palo Alto Networks Recommendation

Zero Trust

A strategy that removes implicit trust and builds on continuous validation. Covering people, process and technology.

+

AI Driven Platform(s)

Best-in-breed capabilities connected where needed for the greatest visibility, control, and efficiency. **Enable real-time, autonomous security.**

=

Future Proof

Frees you to operate and innovate with speed and safety—easing your secure transformation

To deliver cybersecurity that stays ahead of threats rather than just reacts to them!

paloalto NETWORKS

THANK YOU

paloaltonetworks.com

Erik Faassen
Principal Architect, Director

AI-Driven Platforms
Enable Real-Time & Autonomous Security

Zero Trust SASE Platform
Infused with AI for Real-Time Protection

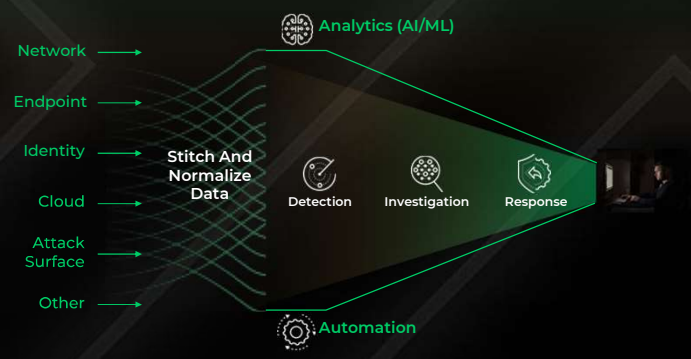
- Unified Management & AIOps
- Cloud-Delivered Security Services
- Hardware NGFW
- Software NGFW
- SASE

Code to Cloud Platform
AI Powered Code-to-Cloud Experience

- Code
- Cloud Infrastructure
- Cloud Runtime

Code To Cloud Platform

AI Security Operations
AI Delivers the Autonomous SOC



Legacy Security

Hyper Innovation

Cloud adoption, mobility, API mesh, IoT and even the metaverse drive our new digital economy in **breakneck pace**.

+

Evolved Attackers

Attackers are evolving their methods to exploit gaps created by the pace of innovation**.**

>

Legacy Security

Perimeter based security that **relies on implicit trust,** is highly **manual** and **inaccurate** due to **fragmented** security tools.

Many organisations are still trying to defend evolved attacks with old tools and tactics.


MOORE
DARWIN
TERMINATOR
FRANKENSTEIN
SCULLY
The Five Cybersecurity Forces
are pushing Cybersecurity Teams to their limits
Attack surface wants to grow exponentially
Cybersecurity can't restrict the speed of innovation
Attackers will continue to innovate
Disjoint, uninstrumented controls fail over time
Regulators always want to dig deeper
paloalto NETWORKS

Adding tools becomes chaos

1,300

Executives (CIOs, CISOs, CTOs, COOs)

400
NAM

500
EMEA

100
LATAM

300
JAPAC

DID YOU KNOW

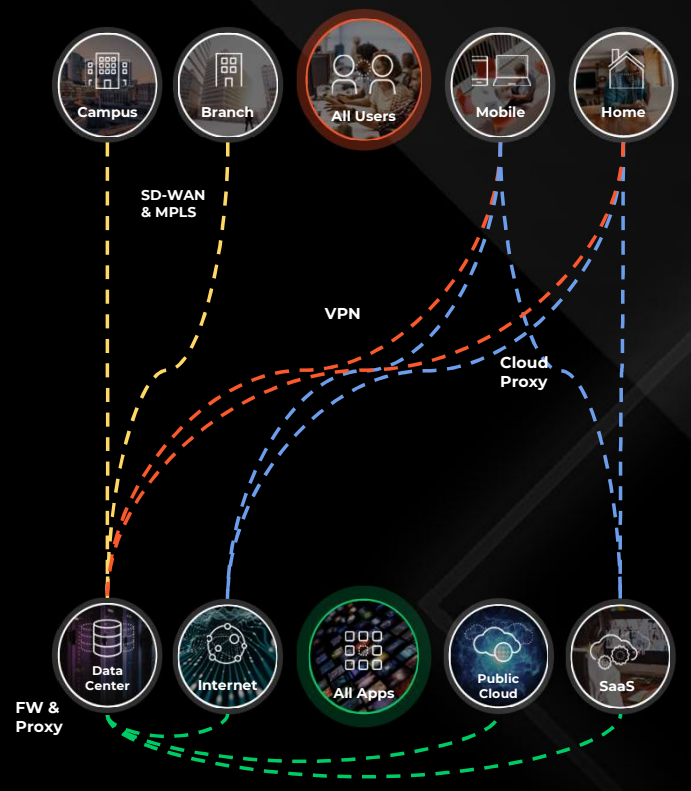
96%
of all respondents experienced **at least 1 Incident** in the last 12 months

57%
experienced **3 or more Incidents** in the last 12 months

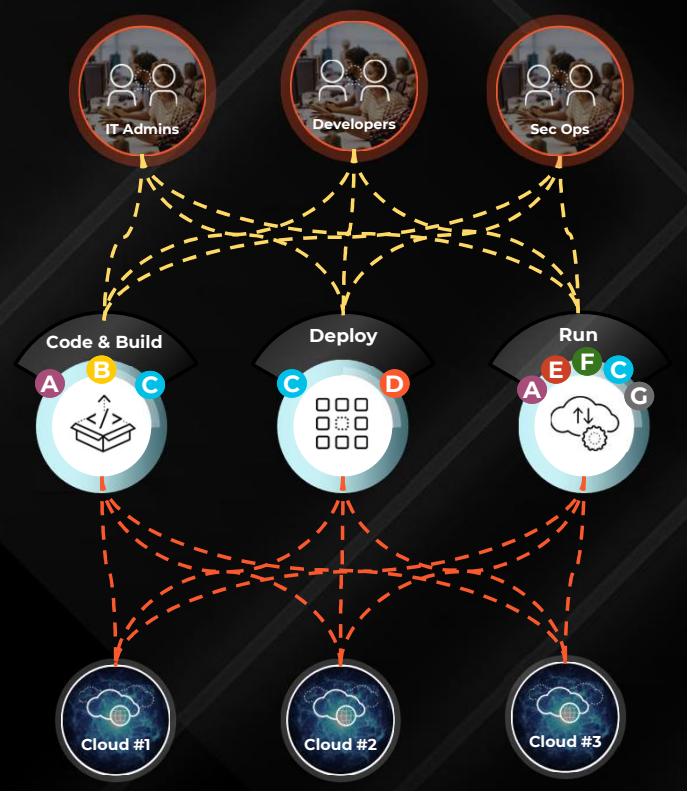
33%
of CXOs said they **experienced an operational disruption** as a result of a breach in the past year

Source: What's Next in Cyber Survey by Palo Alto Networks

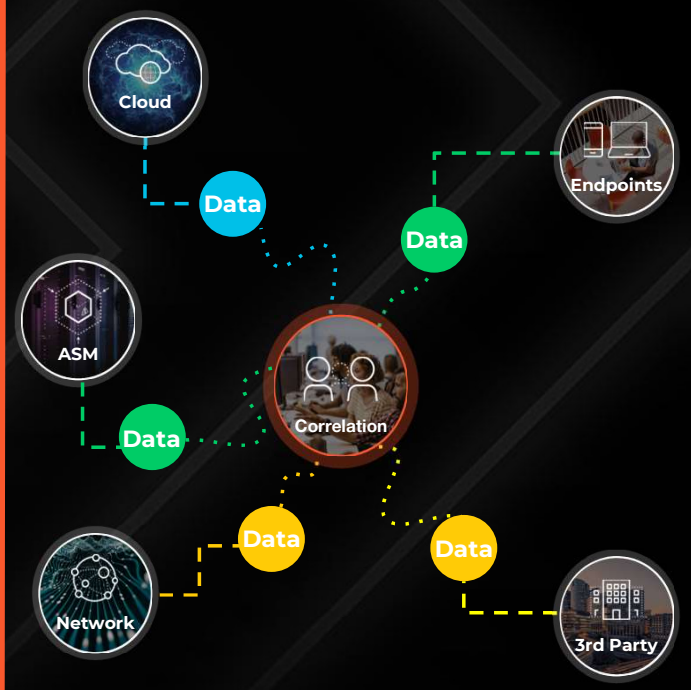
Security chaos proved it doesn't work



Network Security Chaos



Cloud Security Chaos



Security Ops Chaos

Scenario 4: integration example

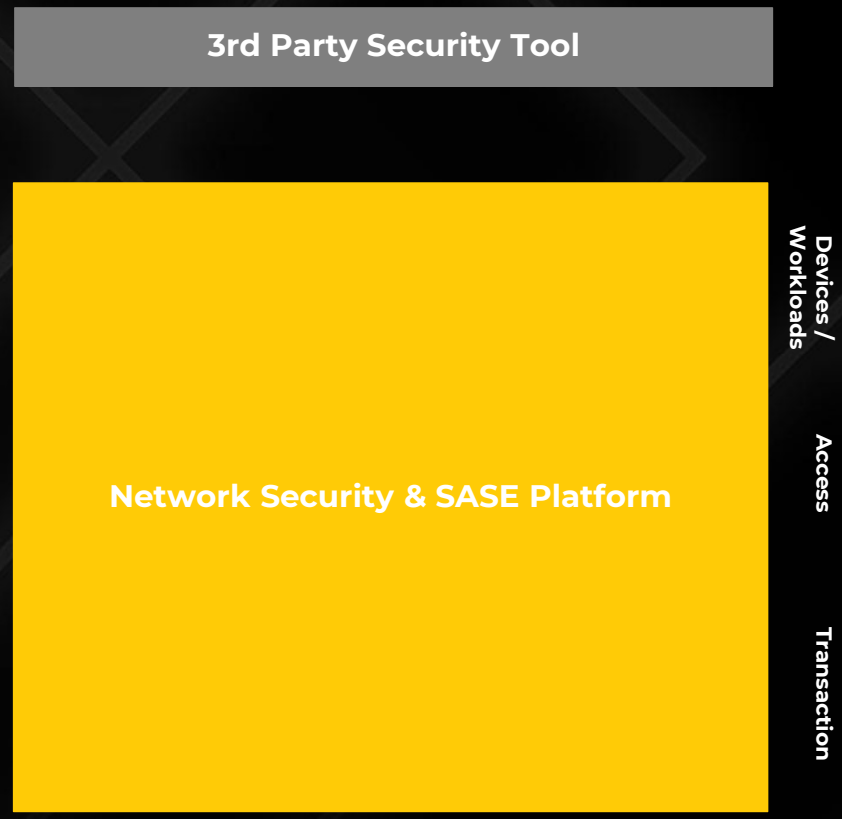
How Zero Trust secures IoT/OT environments in a brownfield scenario

1. IoT and OT equipment in manufacturing facilities or offices (IoT) are being discovered with a 3rd party security tool.

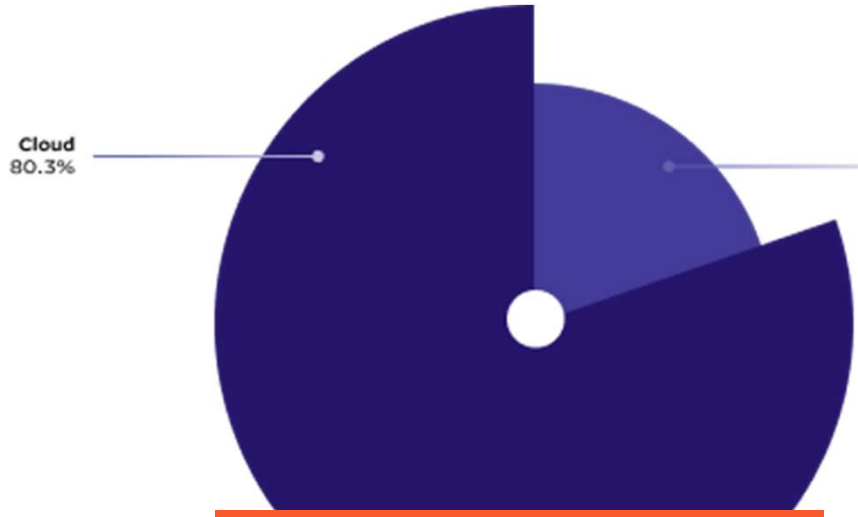
2. After discovery the IoT and OT information is ingested into Network Security Platform for categorization

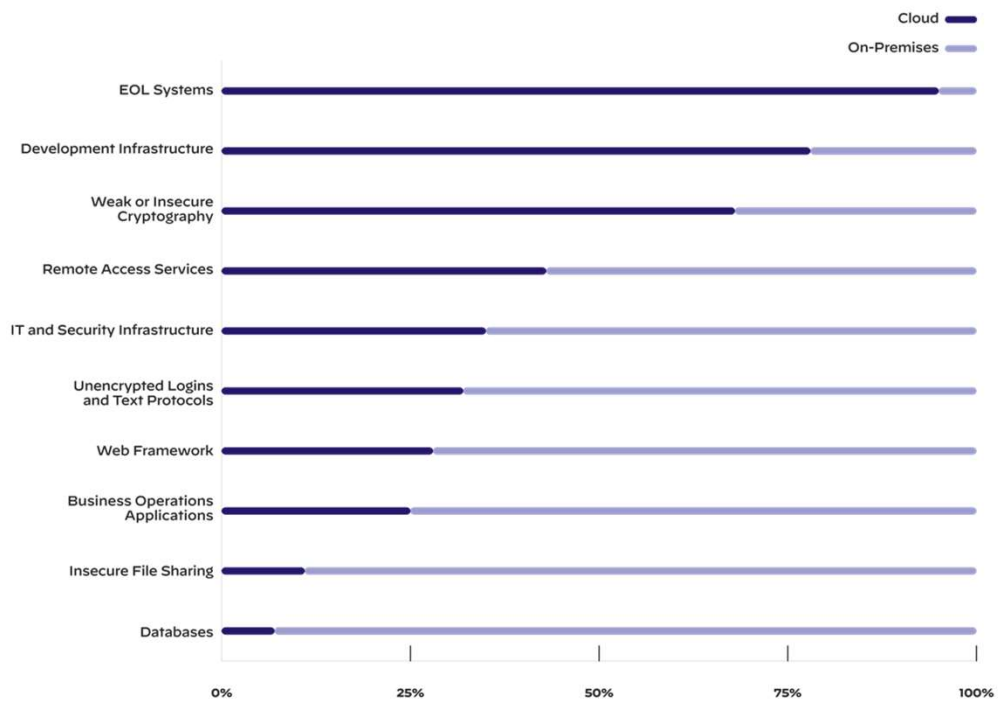
3. Network Security Platform contains policies to enforce security inspection on the individual or categorized IoT and OT equipment

4. With visibility and security enforcement IT and Security teams have full visibility and security enforcement.



Security typically lags behind technological adoption. Example Cloud:

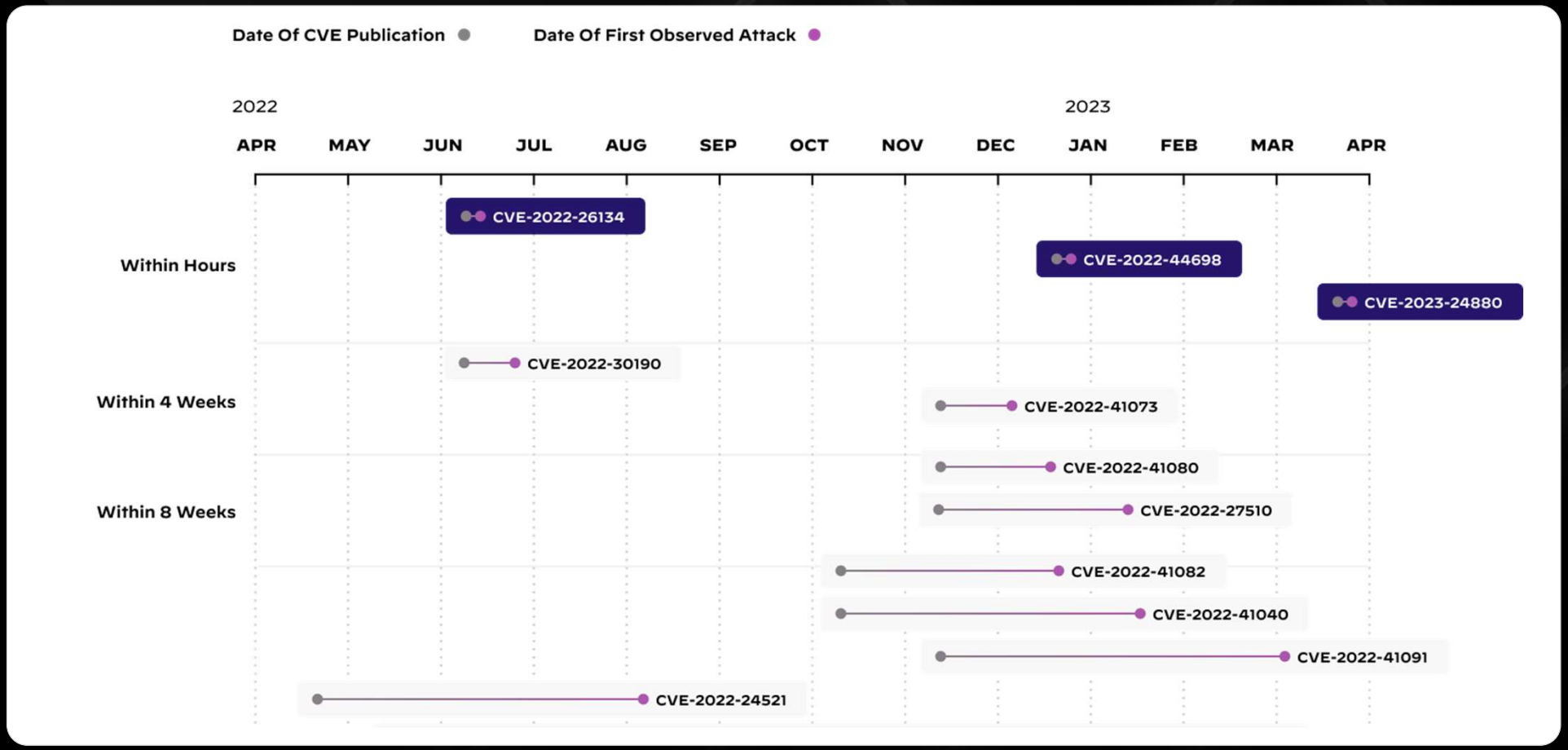




Unit42 (2023): 80% of high exposures were observed on assets hosted in the public cloud

Source: 2023 Unit 42 Attack Surface Report

The speed of “first” attacks …



Source: 2023 Unit 42 Attack Surface Report

Current State of Cybersecurity

Top Challenges Organizations Face Today

Fragmented Vendor Base

~3,500+

Cybersecurity Vendors[1]

Attackers take Advantage of Complexity & Lack of Visibility

Lack of Integration

~32

Average # of security tools organizations use today[2]

Customers are left to Integrate their Security Tools

1. CyberDB, 2023; The Cyber Research Databank
2. What's Next in Cyber Survey, 2022: Palo Alto Networks, Total N=1300
3. IDC Survey: "Current State of SOCs", 2022

Next wave of regulations will put more pressure on cyber security

First attempts
occasional of cyber and privacy regulation

- *Privacy Act* (1974), USA
- *Gramm-Leach-Bliley Act* (1999) for the financial sector

First wave:
personal data protection

- *Sarbanes-Oxley Act* (2002), USA
- *Payment Services Directive* (2007), EU
- *General Data Protection Regulation* (2018), EU
- *California Consumer Privacy Act* (2020), USA
- *Personal Data Protection Law* (2020), Brazil
- *Personal Information Protection Law* (2021), China
- *Personal Data Law* (2022), Russia

Second wave:
critical infrastructure protection

- *National Cyber Security and Critical Infrastructure Protection Act* (2014), USA
- *Network and Information Security NIS 1* (2016), EU
- *Cybersecurity Law*(2017), China
- *NYCRR 500 Cybersecurity Regulations (2017), USA*
- *Network and Information Security NIS 2* (2023)
- Digital Operational Resilience Act (DORA)

New era:
digital products protection

- *Cyber Resilience Act, EU*
- *AI Act, EU*