



ZERO TRUST SECURITY

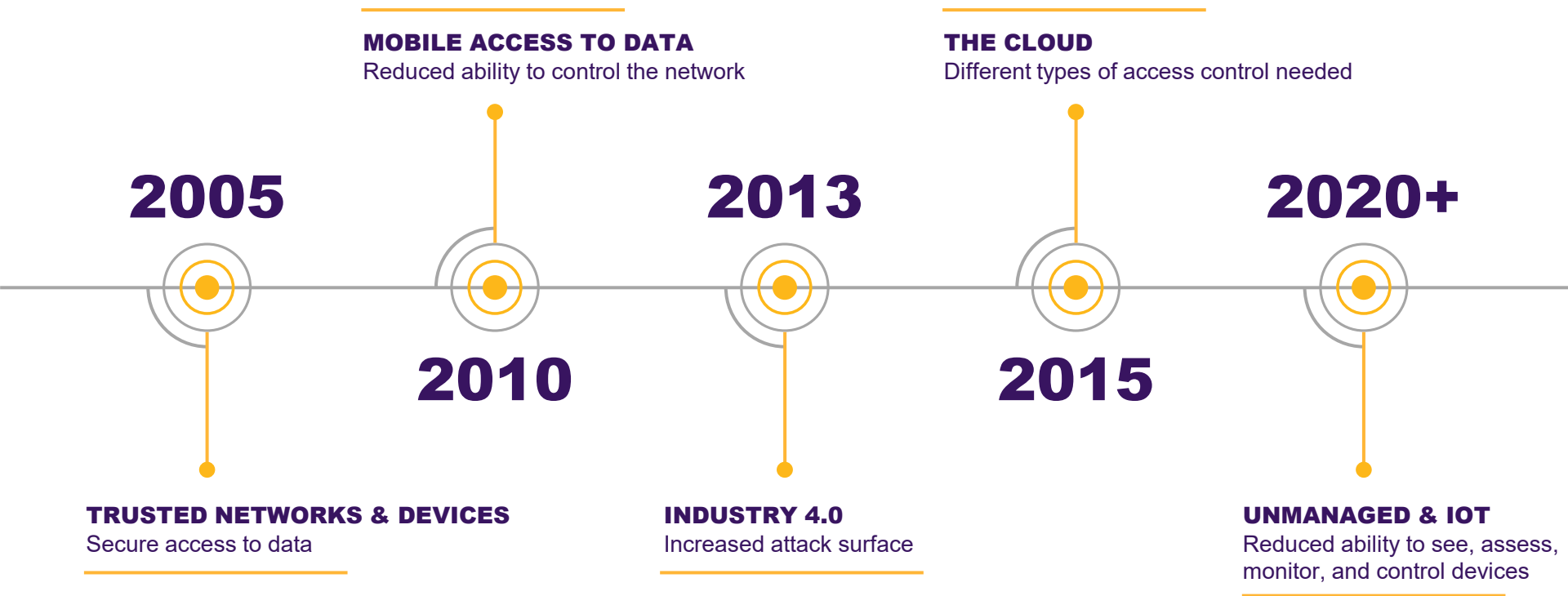
For Unmanaged & IoT Devices

JEFF ZACUTO
Director, Platform Product Marketing

Agenda

- A brief history lesson
- What is Zero Trust?
- How can Armis help?
- Q&A

How did we get here, anyway?



Where'd Zero Trust come from?



**I AM YOUR
FATHER!**

John Kinderbav, Forrester Analyst

- Don't trust any person or device by default either from inside or outside of the network.
- Perform continuous monitoring of user and device behavior to maintain access to resources on the network.

“Never trust. Always Verify.”

Common Zero Trust Approaches for 2021

1

STRONG DEVICE CONTROLS

Policy compliance verification, agent-based endpoint threat detection (EDR) tools.

2

NETWORK SEGMENTATION

Based on the user and device type.

3

VISIBILITY AND ANALYTICS

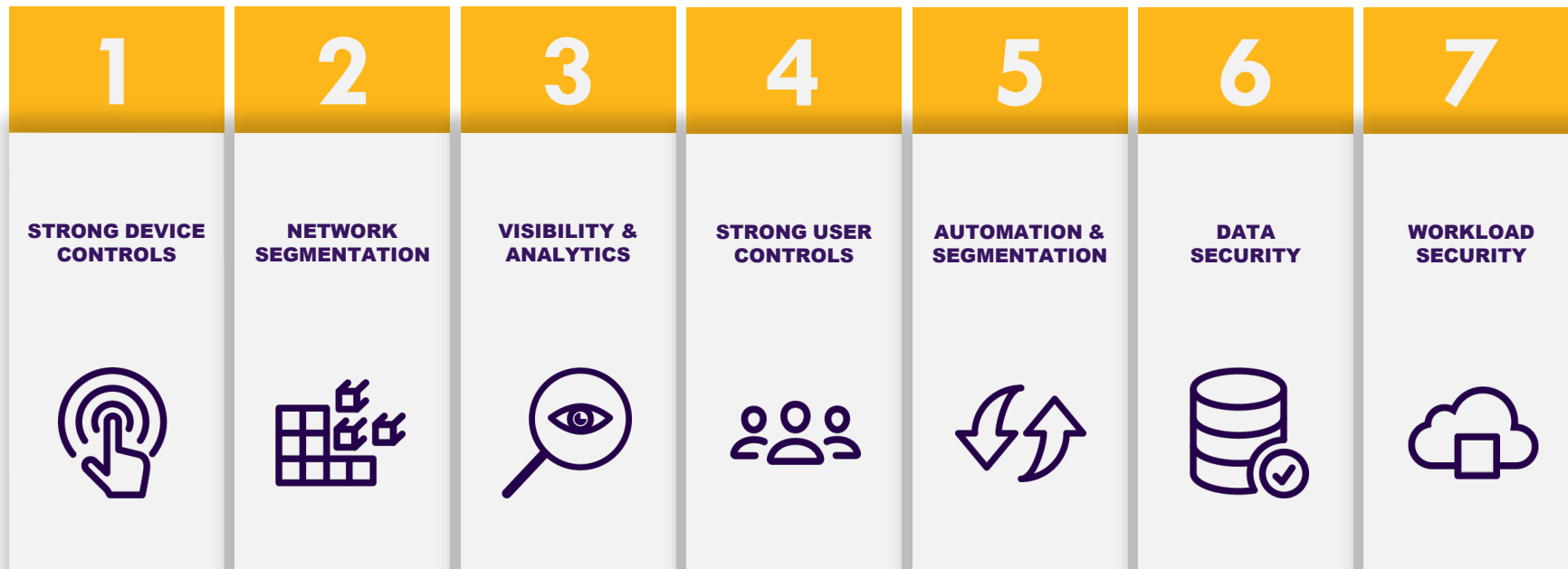
Based on the analysis of logs and user behavior.

4

STRONG USER CONTROLS

MFA, SSO, IAM, least privilege access, behavior monitoring, risk-based authentication.

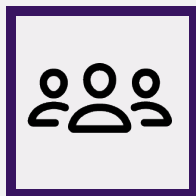
The Seven Zero Trust Pillars



Zero Trust Security Architecture

Users

- Identity management
- Strong authentication
- Least privilege, RBAC
- SSO federation
- Behavior monitoring



Managed Devices

- Certificates
- Configurations
- Vulnerabilities
- Data encryption
- Behavior monitoring



Unmanaged Devices

- Device discovery



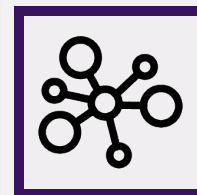
Zero Trust Enforcement

- Network Access Control
- Application Access Broker
- VPN
- Network ACLs
- SSO/MFA
- PAM



Anomaly Response

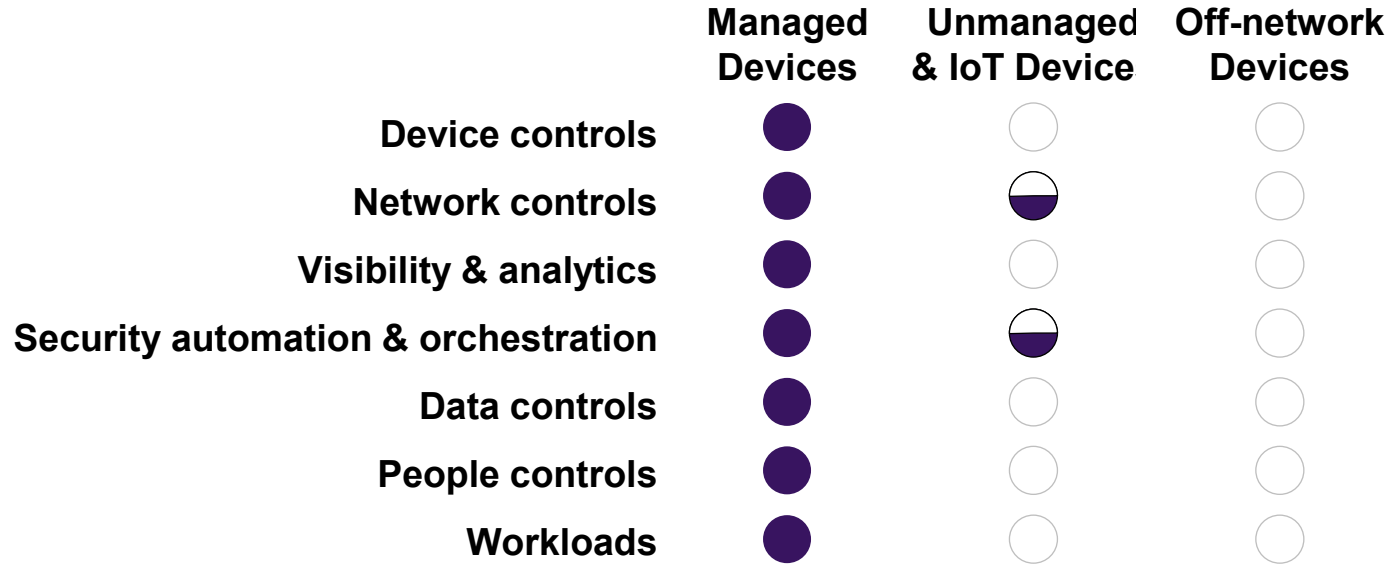
- SOAR
- EDR

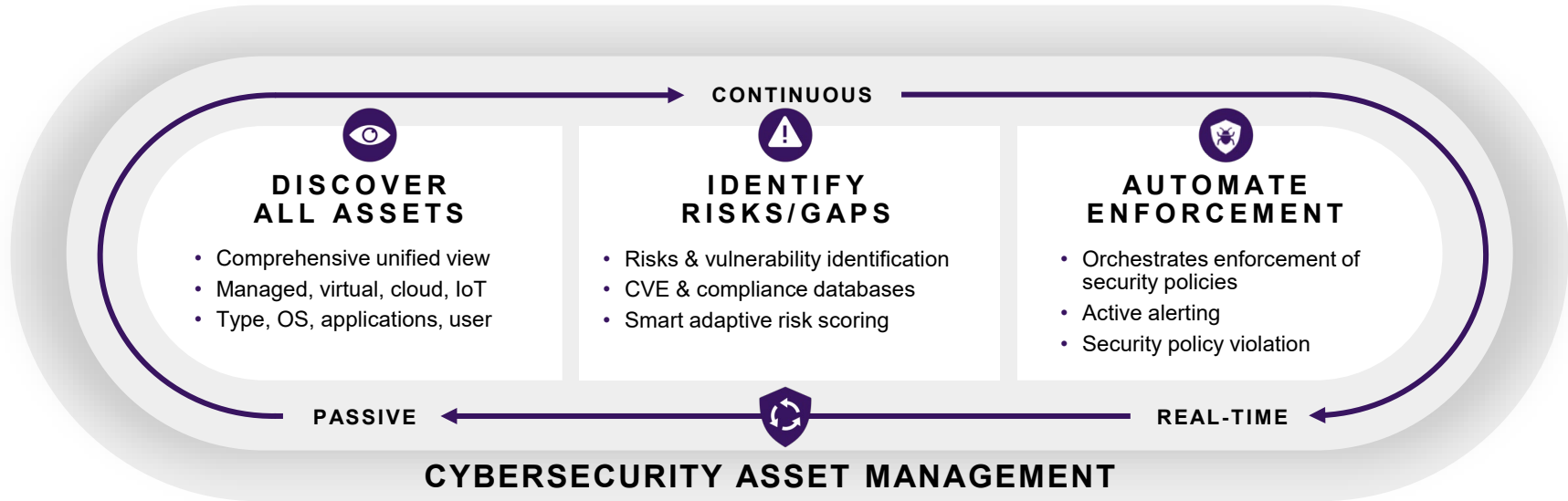


Security Analytics

- SIEM
- Threat Intel
- AI

Zero Trust Security Gaps





ORACLE® DocuSign®

Mondelēz International

flex

Allergan

Sysco



CLEARRENT™ INTELLIGENT PROCESSING

PerkinElmer

MATTRESSFIRM



Armis Device Controls: Asset Inventory

Device Information <ul style="list-style-type: none">• Device type• Manufacturer• IP address• MAC address• Computer name• User name	Endpoint Behavior <ul style="list-style-type: none">• Stationary vs. moving• Communication timing• Communication volume• Cloud services accessed• Tunnels utilized• Encryption usage	Connection Information <ul style="list-style-type: none">• Connection type <i>(Wired, Wi-Fi, Bluetooth, etc.)</i>• Connection point <i>(corp, guest, rogue, etc.)</i>• Traffic volume and timing• Internet domains accessed
Software Information <ul style="list-style-type: none">• OS type and version• Applications	Wi-Fi Information <ul style="list-style-type: none">• AP name• AP CPU utilization• AP bandwidth utilization• AP OS version	Switch Information <ul style="list-style-type: none">• Switch name and location• Switch CPU utilization• Switch configuration• Internet domains accessed

Armis Device Controls: Risk Assessment

Acme Guest AP
ASR1002-x
Cisco

High Risk | **1 Alerts**

Type | Category
Access Points, Network Equipment

OS
Cisco IOS XE 16.11.1

Data sources

IP
192.168.7.97

MAC
85:09:4F:69:C6:B2,
C6:CA:ED:38:1B:7A

Boundaries
Guest | + Associate Boundary

Tags
Managed | Access Point | Public
+ Add Tag

Site
Zurich Offices

Last Seen By
WLC2

First Seen | Last Seen
Sep 4, 2021 8:50 PM | Sep 19, 2021 12:50 AM

10 Device Risk Factors

Score	Type	Description	Last Seen
High	Vulnerability Score	Vulnerability Score	Sep 19, 2021 2:05 AM
Medium	Model Score	End of Service Life	Sep 4, 2021 8:50 PM
High	Many Open Ports	Large amount of open ports	Sep 4, 2021 8:50 PM
Medium	Manufacturer Reputation	Manufacturer 'Cisco' Detected	Sep 4, 2021 8:50 PM
High	Browser Version Score	Old Browser Used	Sep 4, 2021 8:50 PM
High	Operating System Score	Operating System 'Cisco IOS XE 16.11.1' Installed	Sep 4, 2021 8:50 PM
Medium	SSID Persistence	SSID Persistence	Sep 4, 2021 8:50 PM
Medium	CPU Security Flaw	Spectre/Meltdown CPU Security Flaw	Sep 4, 2021 8:50 PM
High	Device Model Reputation	Device Model Reputation	Sep 4, 2021 8:50 PM
High	Ripple 20	Vulnerable to Ripple20 - Vulnerable 'Track' TCP/IP stack detected	Sep 4, 2021 8:50 PM

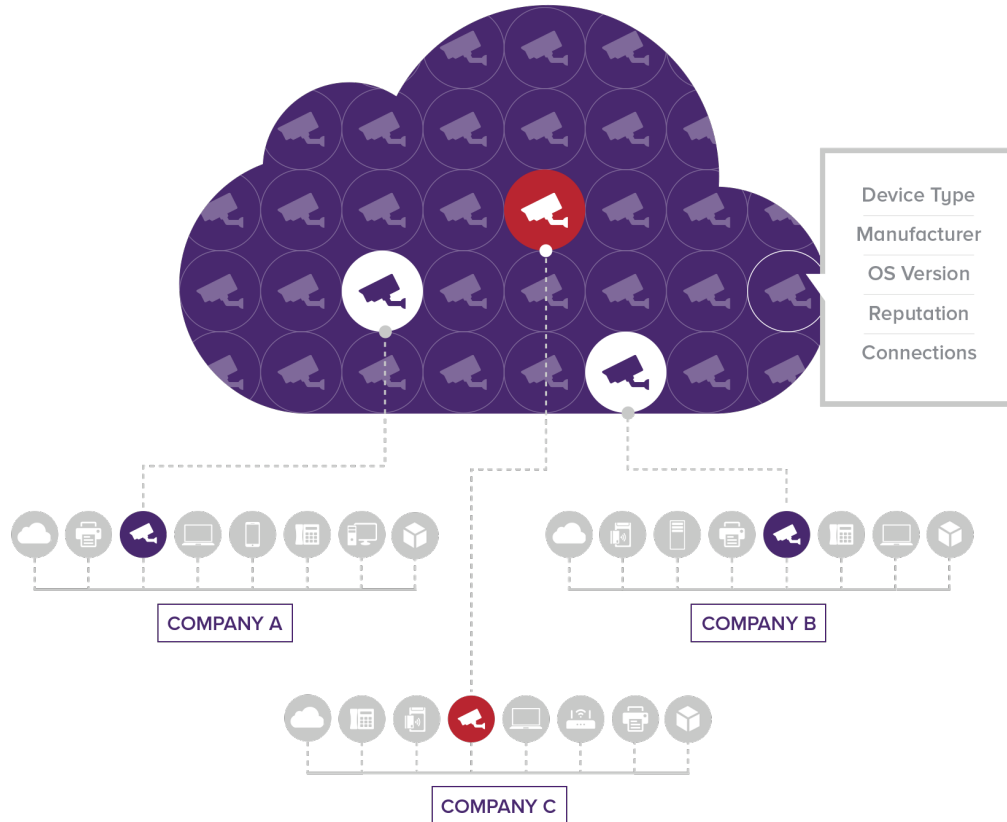
Armis Network Controls: Proactive Segmentation



Armis Threat Detection



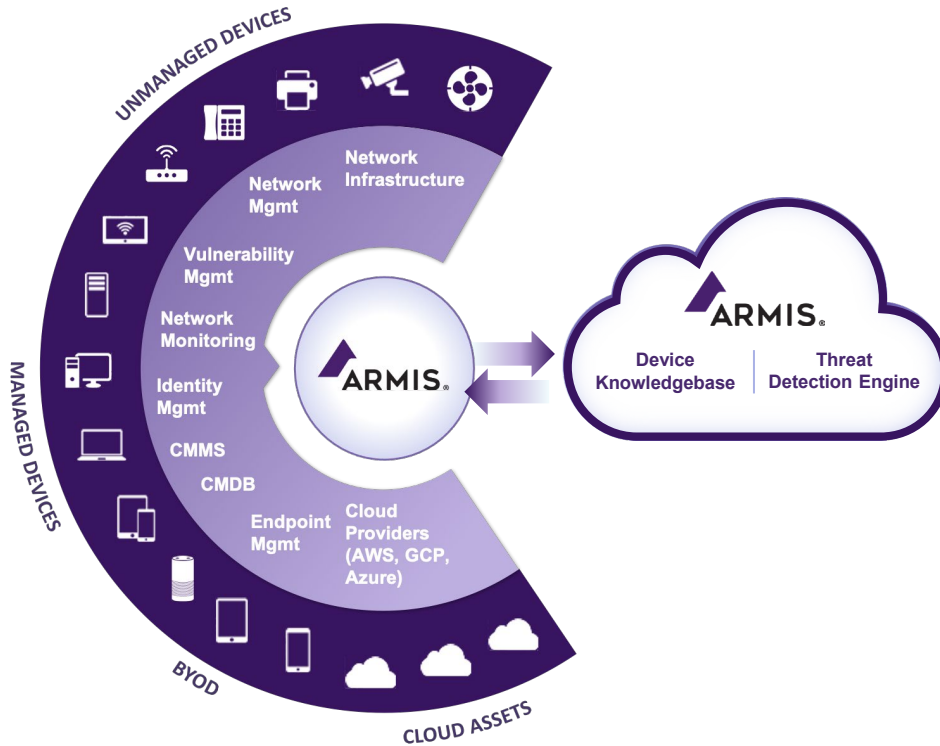
Armis: Zero Trust Visibility and Analytics



Armis Device Knowledgebase

- ✓ 1B+ Devices Tracked (and growing)
- ✓ Largest Cloud-based, crowd sourced, device knowledgebase
- ✓ Enriches the asset insights with even more sources of telemetry data
- ✓ Identifies policy violations, misconfigurations, or abnormal behavior
- ✓ Rapid deployment & operationalization

Complete. Unified. Actionable.



Fast to deploy

- No agents
- Deploys in minutes to hours
- Integrates into existing IT & security solutions
- No network impact
- Saves 100+ person-hours per year

Hundreds of Prebuilt Adapters



Highlighting a few prebuilt adapters

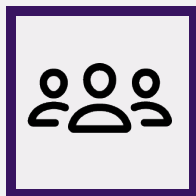
The Zero Trust Security Gap

	Managed Devices	Unmanaged & IoT Devices	Off-network Devices
Device controls	●	●	●
Network controls	●	●	●
Visibility & analytics	●	●	●
Security automation & orchestration	●	●	●
Data controls	●	●	●
People controls	●	●	●
Workloads	●	○	○

Zero Trust Security Architecture

Users

- Identity management
- Strong authentication
- Least privilege, RBAC
- SSO federation
- Behavior monitoring



Managed Devices

- Certificates
- Configurations
- Vulnerabilities
- Data encryption
- Behavior monitoring



Unmanaged Devices

- Device discovery
- Asset inventory
- Device risk assessment
- Behavior monitoring
- Threat detection
- Security Orchestration



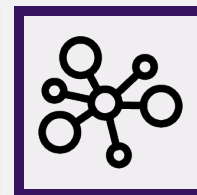
Zero Trust Enforcement

- Network Access Control
- Application Access Broker
- VPN
- Network ACLs
- SSO/MFA
- PAM



Anomaly Response

- SOAR
- EDR



Security Analytics

- SIEM
- Threat Intel
- AI

Q&A

THANK YOU