ZERO TRUST SECURITY

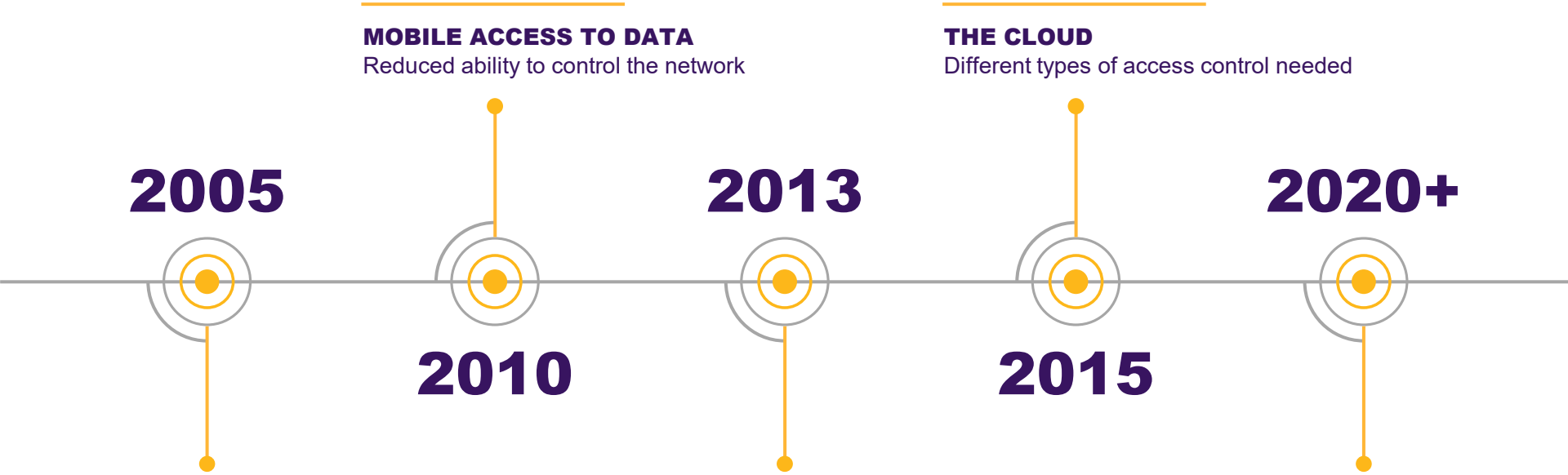
For Unmanaged & IoT Devices

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?

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

1	2	3	4	5	6	7
STRONG DEVICE CONTROLS	NETWORK SEGMENTATION	VISIBILITY & ANALYTICS	STRONG USER CONTROLS	AUTOMATION & SEGMENTATION	DATA SECURITY	WORKLOAD SECURITY







Zero Trust Security Architecture

Users

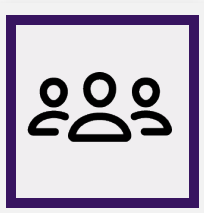
- Identity management
- Strong authentication
- Least privilege, RBAC
- SSO federation
- Behavior monitoring

Managed Devices

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

Unmanaged Devices

- Device discovery

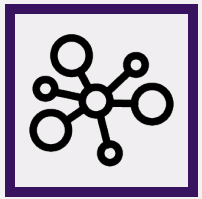


Zero Trust Enforcement

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

Anomaly Response

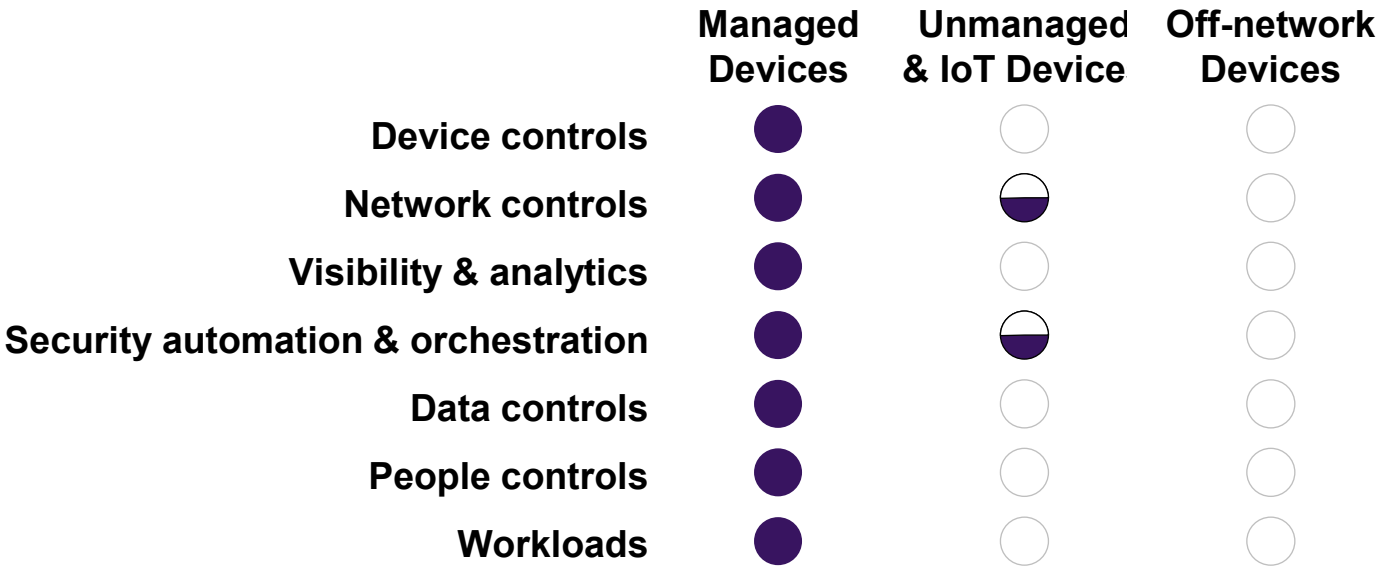
- SOAR
- EDR

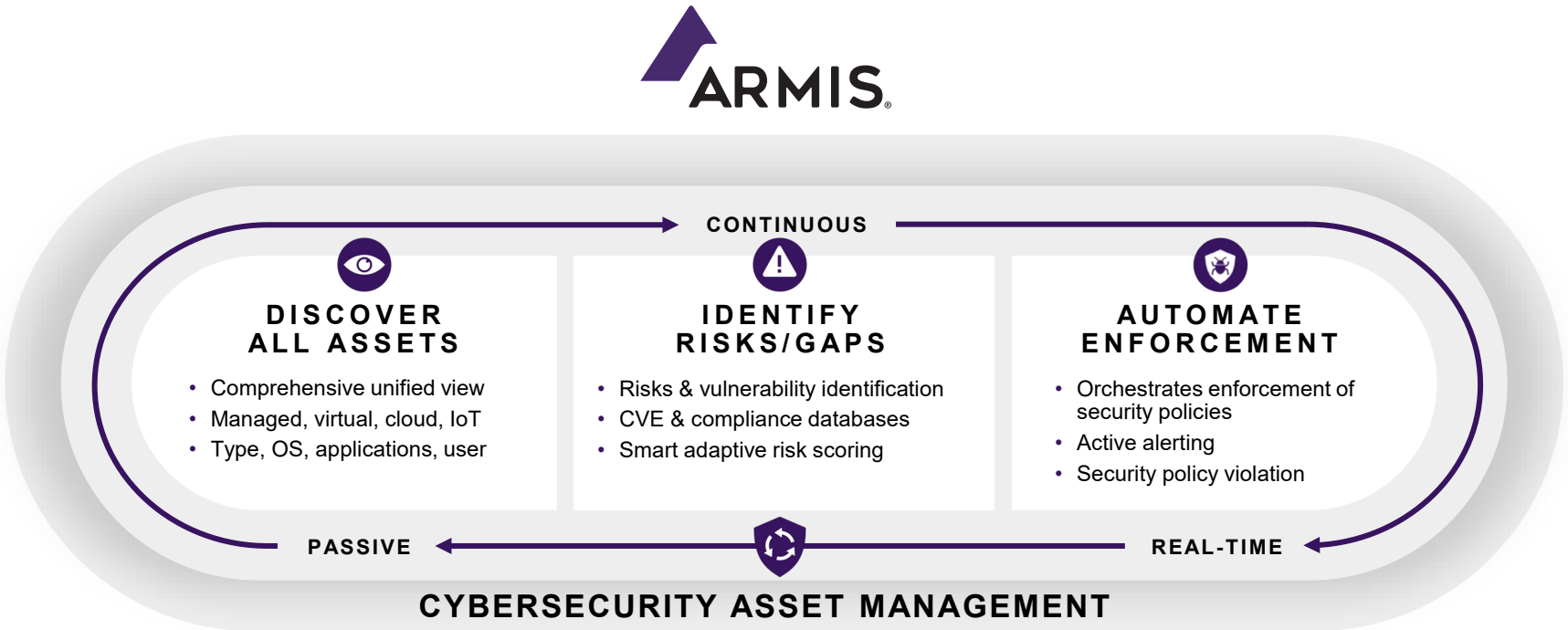


Security Analytics

- SIEM
- Threat Intel
- AI

Zero Trust Security Gaps





ORACLE DocuSign Mondelēz International flex Allergan Sysco The Home Depot CLEAREnt Intelligent Processing PerkinElmer MATTRESSFIRM

ARMIS

Armis Device Controls: Asset Inventory

Device Information

- Device type
- Manufacturer
- IP address
- MAC address
- Computer name
- User name

Endpoint Behavior

- Stationary vs. moving
- Communication timing
- Communication volume
- Cloud services accessed
- Tunnels utilized
- Encryption usage

Connection Information

- Connection type *(Wired, Wi-Fi, Bluetooth, etc.)*
- Connection point *(corp, guest, rogue, etc.)*
- Traffic volume and timing
- Internet domains accessed

Software Information

- OS type and version
- Applications

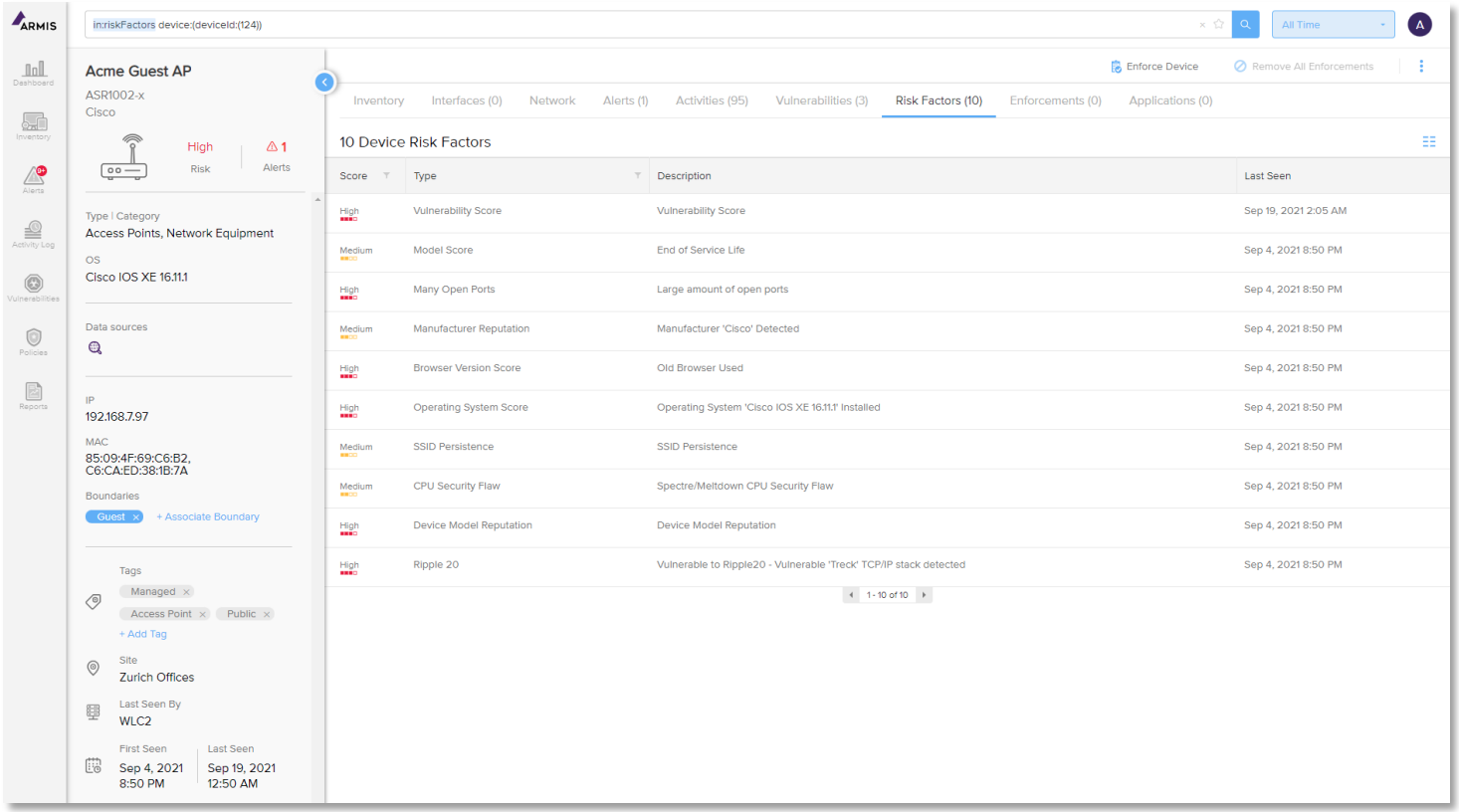
Wi-Fi Information

- AP name
- AP CPU utilization
- AP bandwidth utilization
- AP OS version

Switch Information

- Switch name and location
- Switch CPU utilization
- Switch configuration
- Internet domains accessed

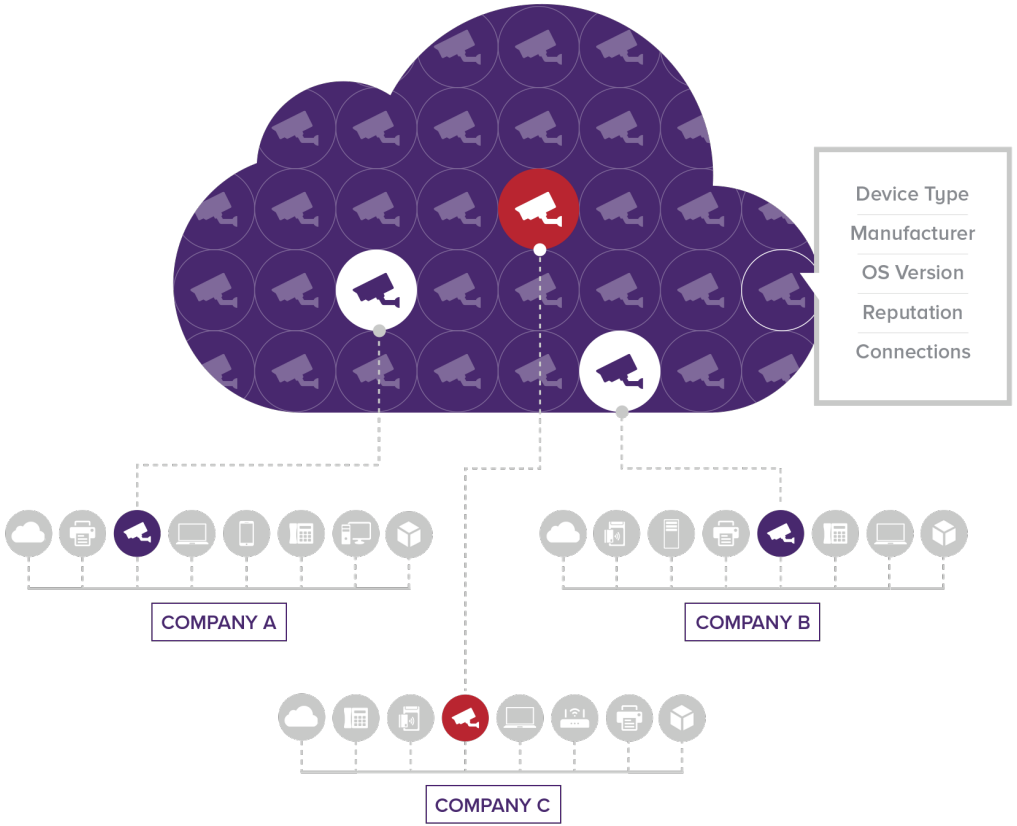
Armis Device Controls: Risk Assessment



Armis Network Controls: Proactive Segentation

Armis Threat Detection

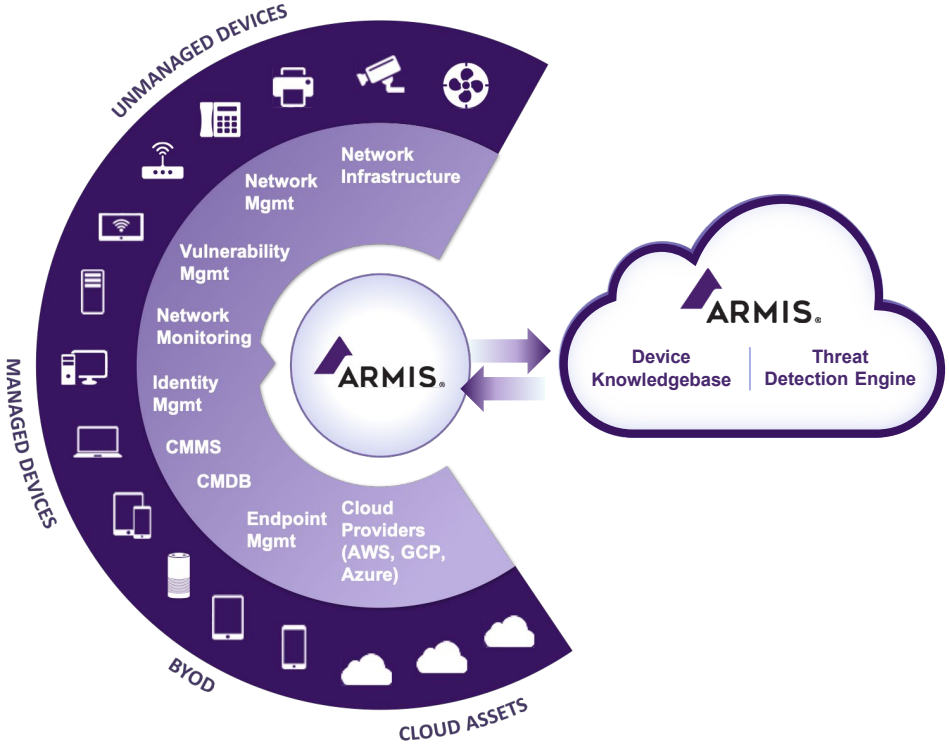
Armis: Zero Trust Visibility and Analytics



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.



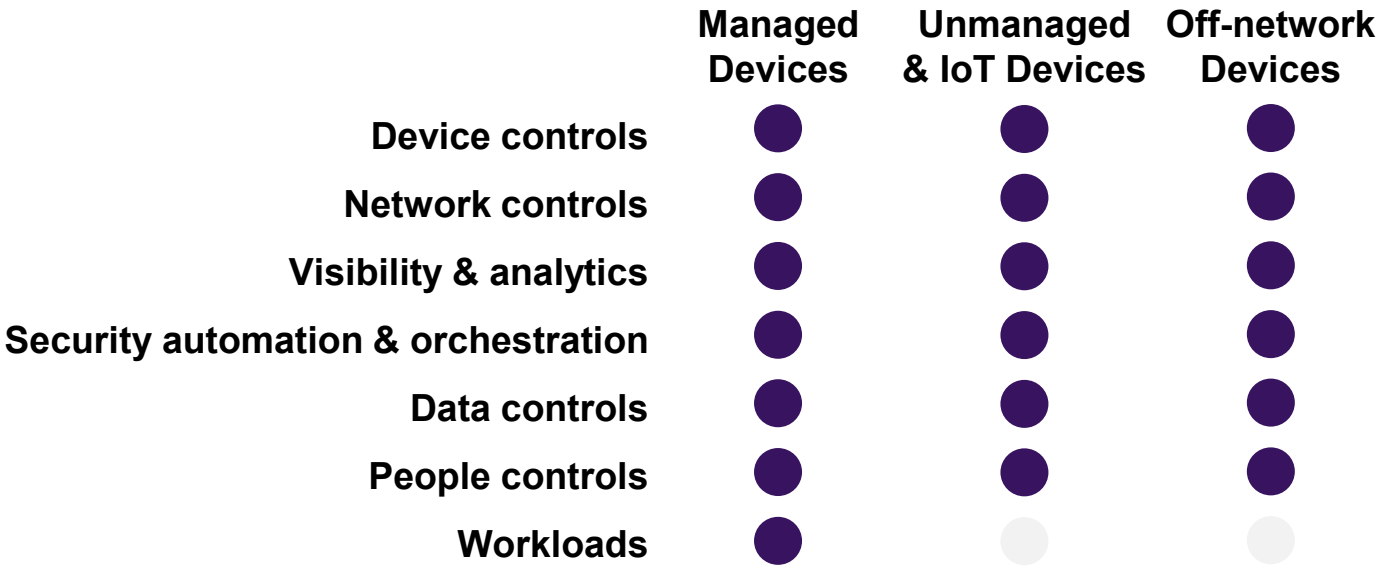
Fast to deploy

- 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



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

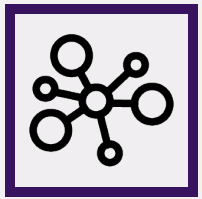
- Device discovery
- Asset inventory
- Device risk assessment
- Behavior monitoring
- Treat detection
- Security Orchestration

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

ARMIS

Q&A

THANK YOU