The Relevance Question.

Device Authority is still very relevant?
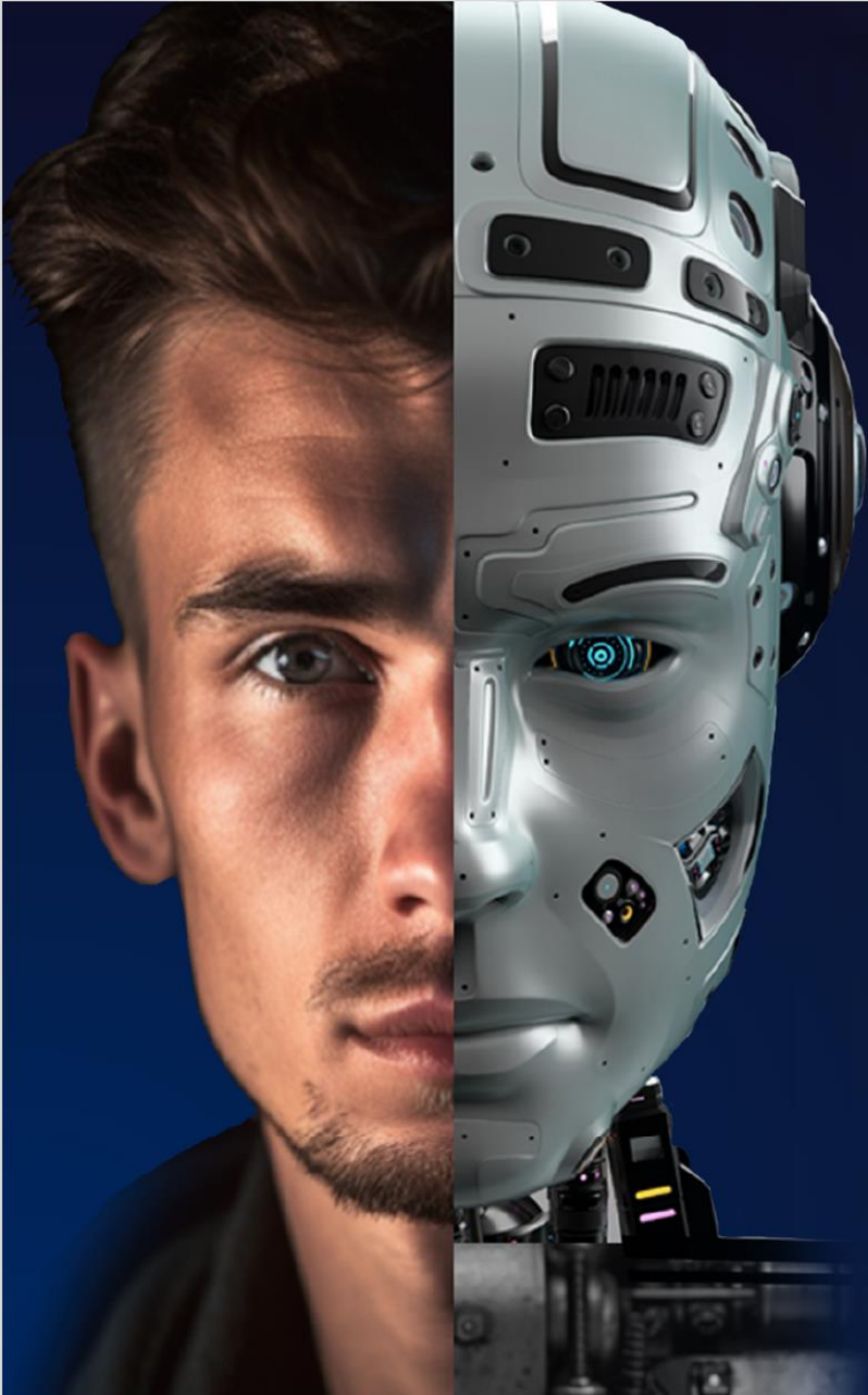
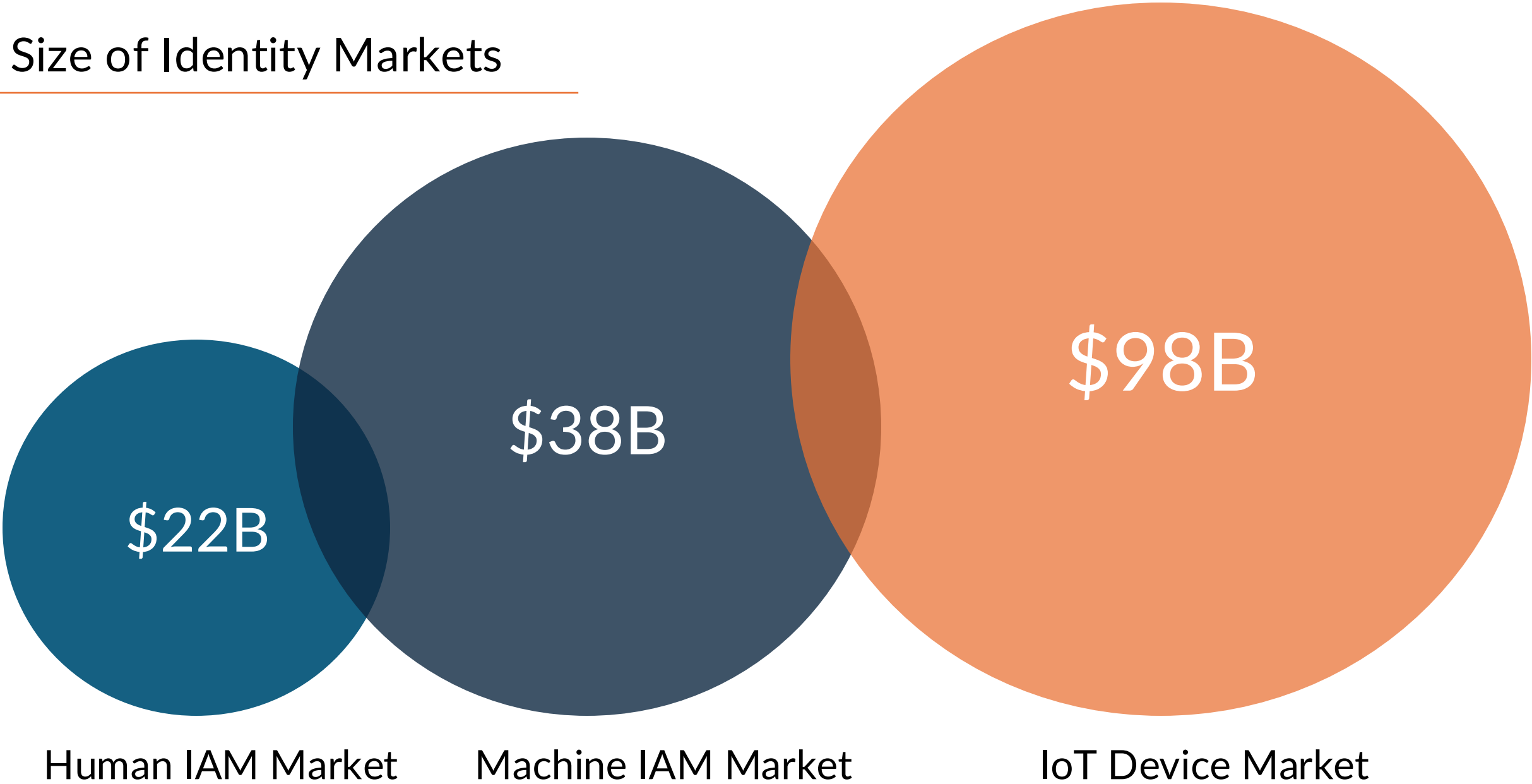# Identity Growth and Impact

52% of human identities have access to sensitive data

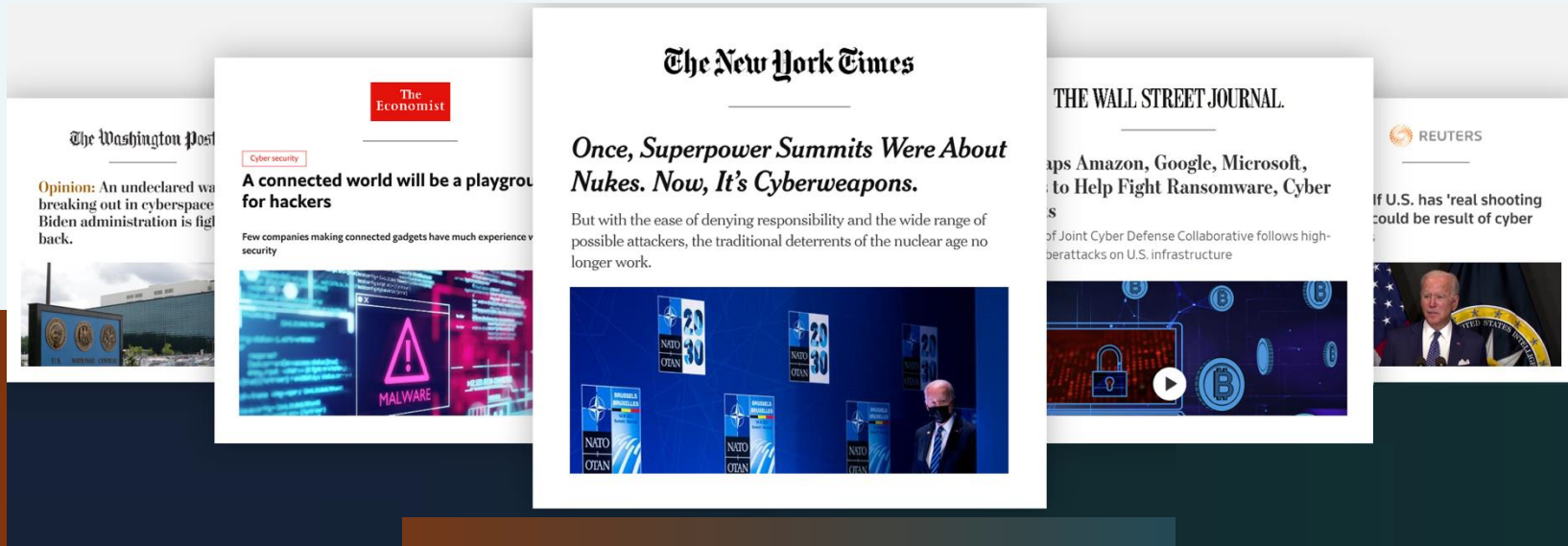**68%** of non-human identities have access to sensitive data and they outnumber humans **45:1**

The average staff member has access to **30** different accounts and applications

There's been a **2.4x** increase in the number of identities this year

CyberArk Identity Security Threat Landscape 2022 and 2023

Size of Identity Markets

$22B

$38B

$98B

Human IAM Market

Machine IAM Market

IoT Device Market

Security Is a Defining Challenge Of Our Time

Cybercrime Today Equals The 3rd Largest Economy In The World And Growing Fast

Annual GDP
- USA $27T
- China $17.8T
- Cybercrime $8T
- Germany $4.4T
- Japan $4.2T

Source: Statistica

GDP annual growth rate
- Cybercrime 15%
- India 6.3%
- China 5.1%
- USA 4.9%

Source: Statistica

Cost of Cybercrime Is Out Of Control

$3 trillion — 2015
$10.5 trillion — 2025

A Fragmented Industry Can't Keep Pace with Today's Adversaries

People Factor

Sophistication, Speed, And Scale Of Cyber Attacks Are Increasing

Security Culture

- **97%** of the time hackers **"login, not break into"** the IT systems.

- **~70%** of people open their phishing emails, and **~50%** of people are tricked by them.

4M
Open jobs worldwide

Source: (ISC)²

28%
Business leaders concerned about data or IP loss due to improper use of AI

Source: IDC

Password attacks per month

30B
2023

3B
2022

Source: Microsoft

Threat actors tracked by Microsoft

300+
2023

200
2022

Source: Microsoft

300+
Unique Threat Actors

160+
Nation State Actors

50+
Ransome Ware Groups

80
Organizations use an average of 80 security tools

Source: Microsoft

CYBER SCAPE   2023

Industry Fragmentation

Today's security leaders have to manage a full spectrum of identities to meet Zero Trust standards:

Workforce	IT	Developers	Machines
Contractors, Employees, Application Admins	Traditional IT, 3rd Parties, Cloud Ops, DevSecOps	Engineering Teams, Data Scientists	Bots, Workloads, Apps, IoT/OT

CYBERARK **VENAFI** **DEVICE AUTHORITY**

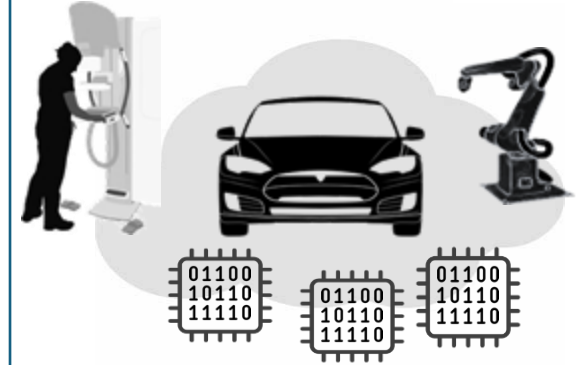**Target Resources**

Endpoints, Data, Biz Apps	Data, Apps, Workloads, CI/CD Tools	Data, Apps, Workloads, Code Repos, Cloud Services	Devices, Data, Apps, Workloads, Code

Access to Data | Access and ability to change data and infrastructure | Access and ability to change data, infrastructure, and code

Risk of Access Level

Complexity of Access

Low ——————————————→ High
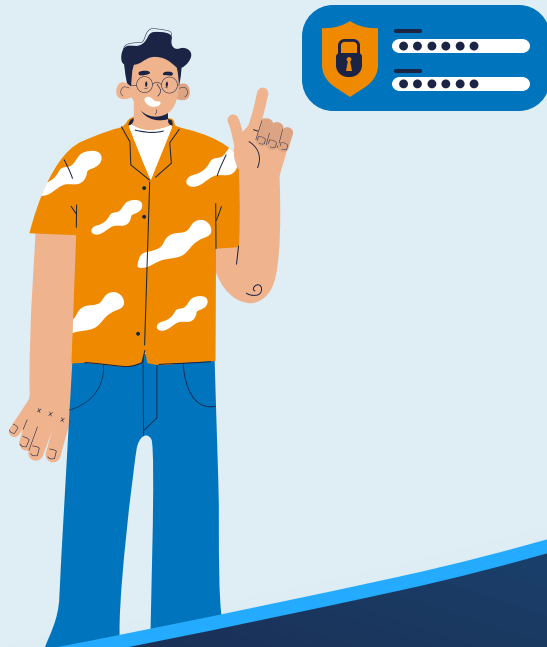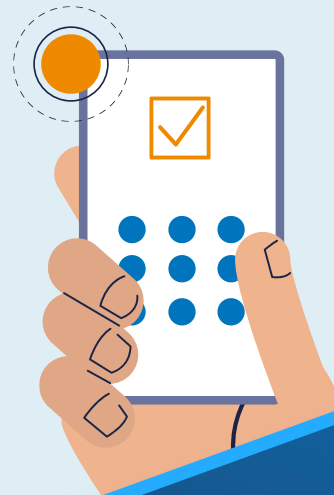
Which Translate into 3 Broad Management Strategies:

Human Identities
augmented by Multi-Factor Auth

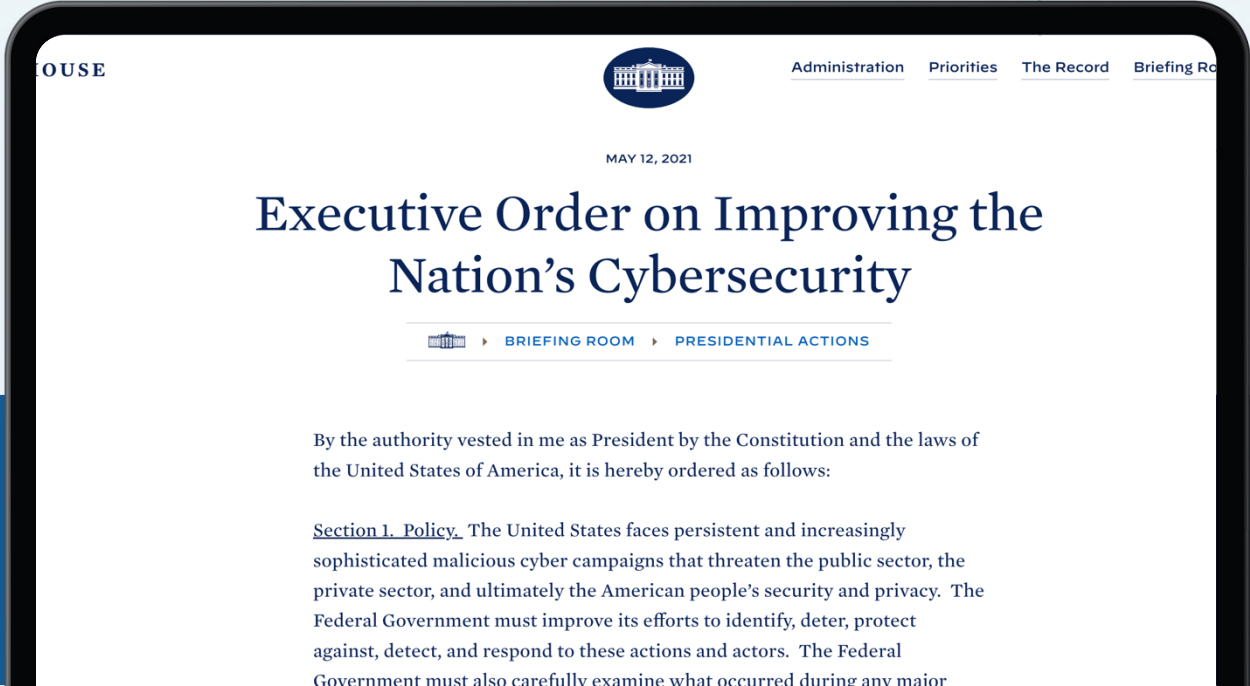**Machine Identities**
using keys and certificates

IoT/OT Device Identities
requiring Zero-Touch Automation

**Complexity of Access
X Volume of Identities**

=

**Potential for
Human Error**

Global regulations and standards are raising the game

The Challenges of Securing IoT in the Supply Chain

Going beyond PKI to manage the full device lifecycle

End-to-End Data Security
is a big challenge and unencrypted data is a favourite target for hackers

Applications need device trust
to make the data valid and deliver an ROI for IoT

Security Lifecycle Management
is a huge challenge when devices at scale change their state over time

AIoT
leverages the Intelligence of Things to drive actionable insights

A Certificate based identity model
is critical for devices but not the only challenge

Identity is the new perimeter
Can't just rely on network security layers when devices are outside the firewall

A universal trusted method is required
to deliver secure updates to devices in the field

Evolving Legislation
EO14028 (Zero Trust, SBOM), ETSI 303 645, EU Cyber Act, SEC Regulation

Zero Trust
Is only achievable when you account for all of these steps

Reference Architecture Microsoft is launching Jan 2025. DA in the Security piece.
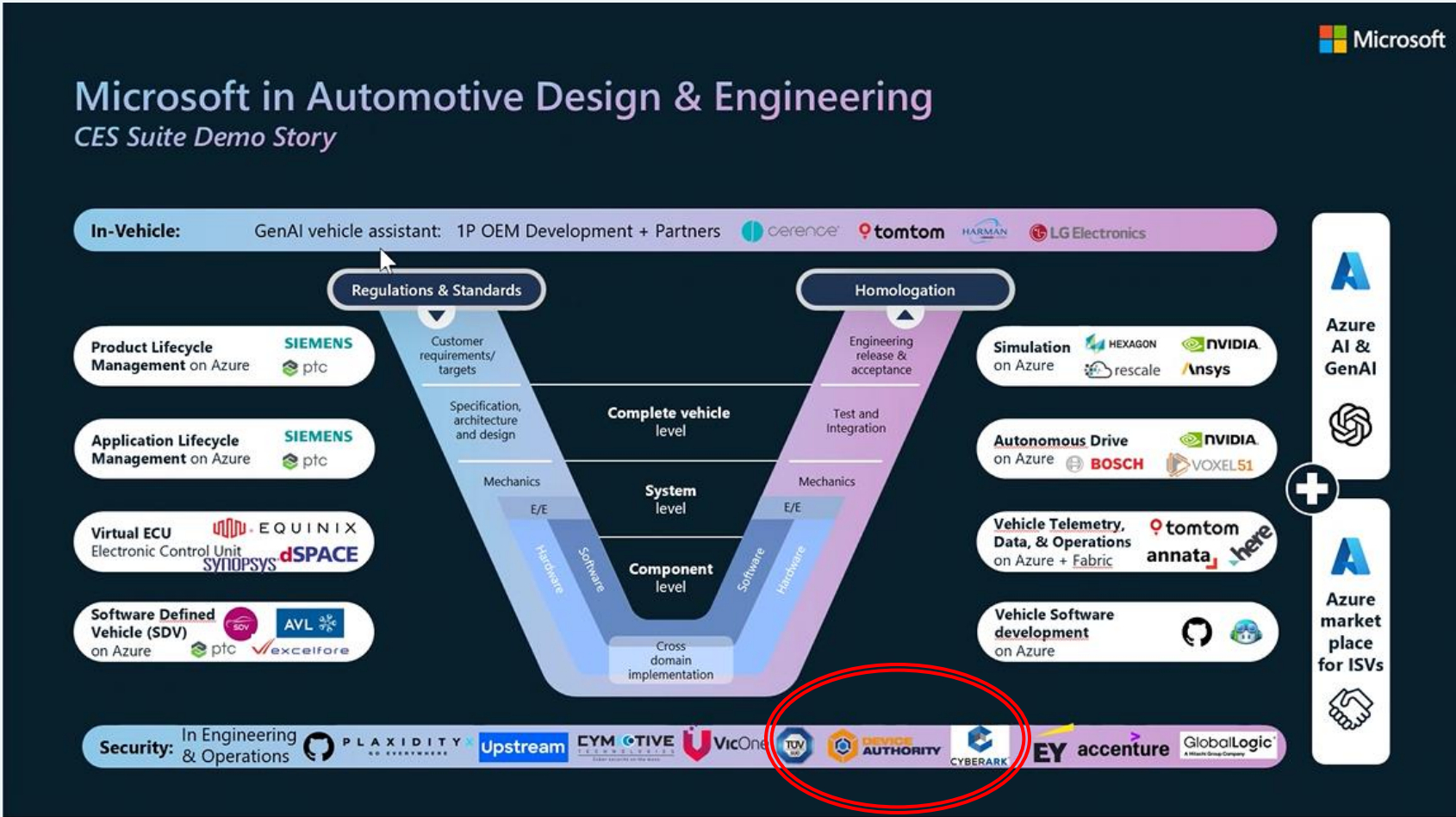
2025: Automotive Manufacturing with CyberArk and Microsoft

Strategic Partnerships – Drive Forward

Strategic Importance -
- Pathway to Government business model through Federal and State funding vehicles
- Collaboration with foreign government agencies including UK, Australia, Germany, etc.
- Influence over critical infrastructure device manufacturers (e.g. sensors, gateways, eSim)

GTM -
- Embedded in VIPC testbed initiative with DHS funding
- Crossroads Innovation Group is strategic consultant leading sales initia
- Government contracts available via strategic reseller partner Carahsoft
- Existing opportunities with US Air Force and VA DOT

Marketing Assets
- Public Sector demo via Testbed
- Joint value presentations

SI/Channel GTM Initiatives

carahsoft. →
- Outbound lead gen campaign underway
- Focus on existing CyberArk accounts and PAM for IoT

CYBERARK
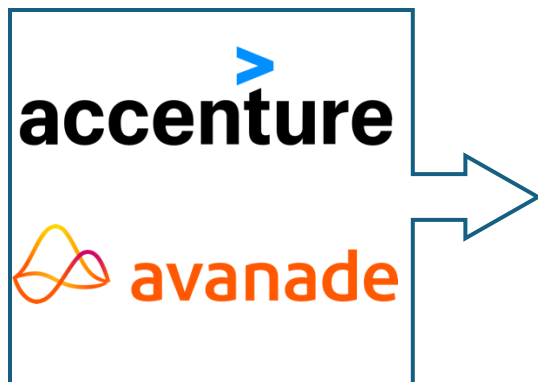
accenture
avanade →
- Utilize Microsoft to gain access to North American contacts
- Build on success in EMEA to drive engagement

snam

GRUPPO HERA

minsait
An Indra company

MSP's →
- Trial the Discovery Tool
- Mid size MSP's and regional reach – focus in North America
- Richey May, Legato, explore others

CYBERARK

New - Value of the Discovery Tool
Empowering Strategic Insights for IoT Environments

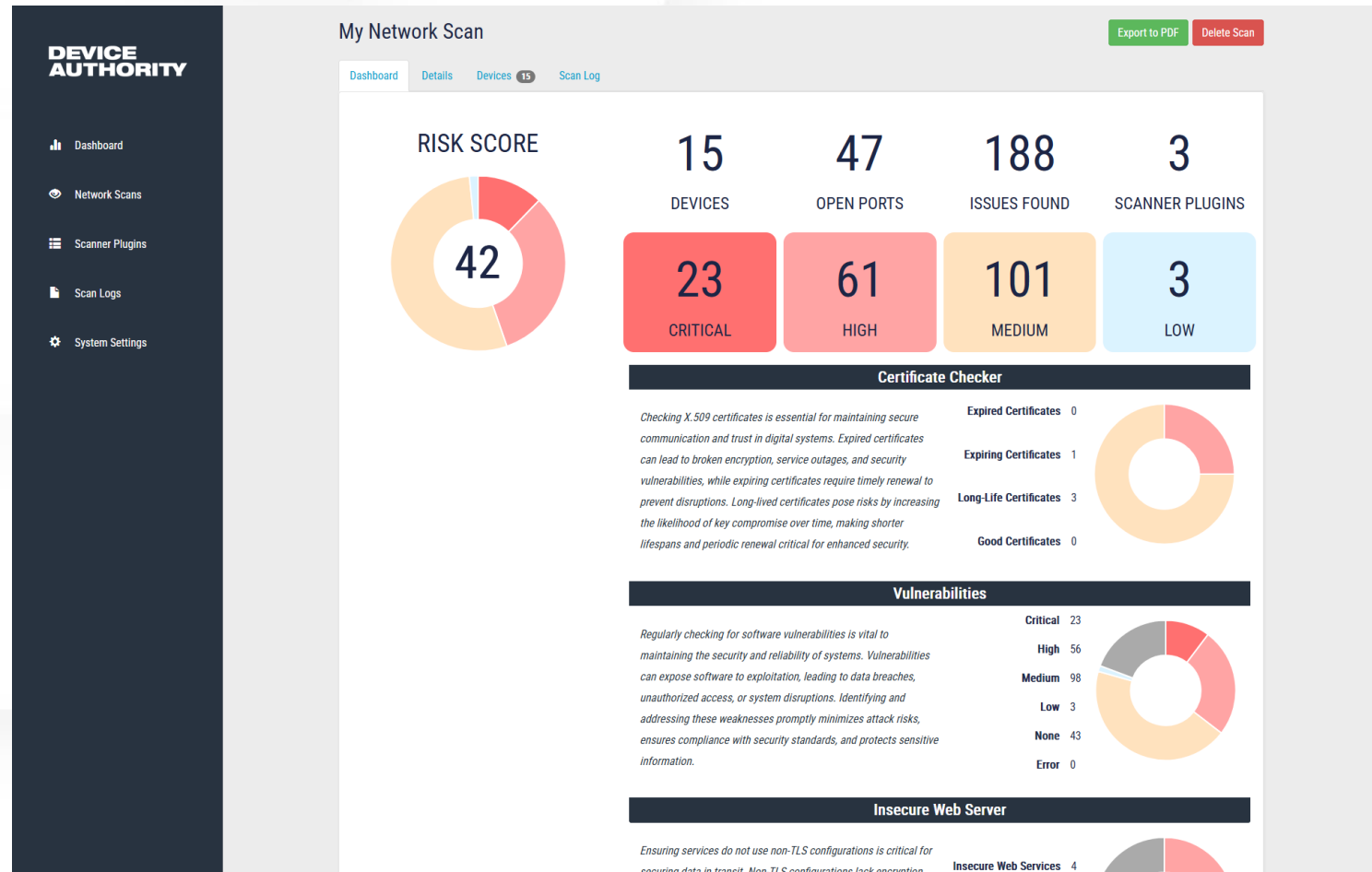**Rapid Insights**: Uncover hidden risks and fortify IoT network security

Enhanced Decision-Making: Provides critical tailored reporting to inform high-stakes IoT strategies and compliance

Zero-Trust Alignment: Built with a zero-trust framework to ensure robust security and integrity

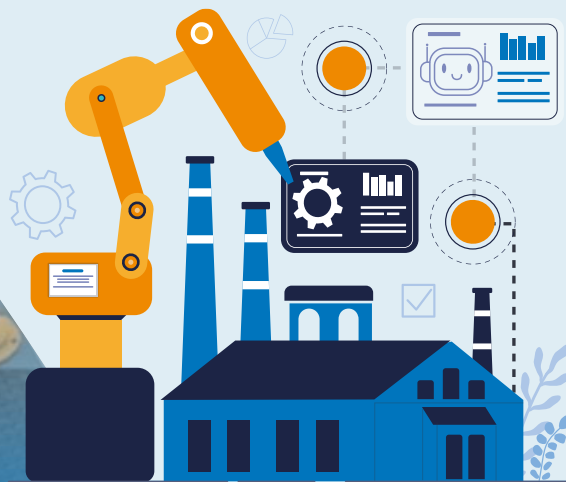**Extensible Architecture**: Rapidly extend and enhance discovery capabilities using the scanner plugin framework

DEVICE AUTHORITY

- Dashboard
- Network Scans
- Scanner Plugins
- Scan Logs
- System Settings

My Network Scan

Export to PDF   Delete Scan

Dashboard | Details | Devices 15 | Scan Log

RISK SCORE
42

| 15 DEVICES | 47 OPEN PORTS | 188 ISSUES FOUND | 3 SCANNER PLUGINS |

| 23 CRITICAL | 61 HIGH | 101 MEDIUM | 3 LOW |

Certificate Checker

Checking X.509 certificates is essential for maintaining secure communication and trust in digital systems. Expired certificates can lead to broken encryption, service outages, and security vulnerabilities, while expiring certificates require timely renewal to prevent disruptions. Long-lived certificates pose risks by increasing the likelihood of key compromise over time, making shorter lifespans and periodic renewal critical for enhanced security.

Expired Certificates 0
Expiring Certificates 1
Long-Life Certificates 3
Good Certificates 0

Vulnerabilities

Regularly checking for software vulnerabilities is vital to maintaining the security and reliability of systems. Vulnerabilities can expose software to exploitation, leading to data breaches, unauthorized access, or system disruptions. Identifying and addressing these weaknesses promptly minimizes attack risks, ensures compliance with security standards, and protects sensitive information.

Critical 23
High 56
Medium 98
Low 3
None 43
Error 0

Insecure Web Server

Ensuring services do not use non-TLS configurations is critical for securing data in transit. Non-TLS configurations lack encryption.

Insecure Web Services 4

Let's see some examples…

DEVICE AUTHORITY

Industrial IoT:
Secure Key Generation, Storage, and Distribution

Situation

A global manufacturer of automotive components has multiple secure manufacturing lines that require a Key Distribution and Management System to securely transport keys from the OEM delivery service to the remote factories.
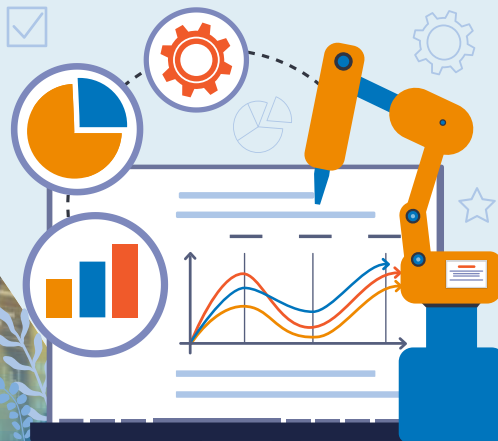
Keys are injected directly into the OEM's vehicle electronic components, which are then distributed to end customers for inclusion in their finished automotive products.

Those finished products need to close the loop with the initial key provider for auditing.

Automotive:
PKI Management for Construction Equipment

Situation

- The next generation of diesel engines feature a new array of options aimed to increase efficiency, lower the cost of operation, and reduce overall lifecycle expense.

- This new technology relies on the exchange of critical performance data between the engine and cloud-based systems to adjust engine parameters in real-time.

- These diesel engines require the use of X.509 certificates from an existing provider for identity, authentication, and encryption to the cloud.

Thank you!

Darron Antill

info@deviceauthority.com