Sveiki!

CYBERARK®
The Identity Security Company™

Agentic AI Is Growing And So Are Your Security Risks

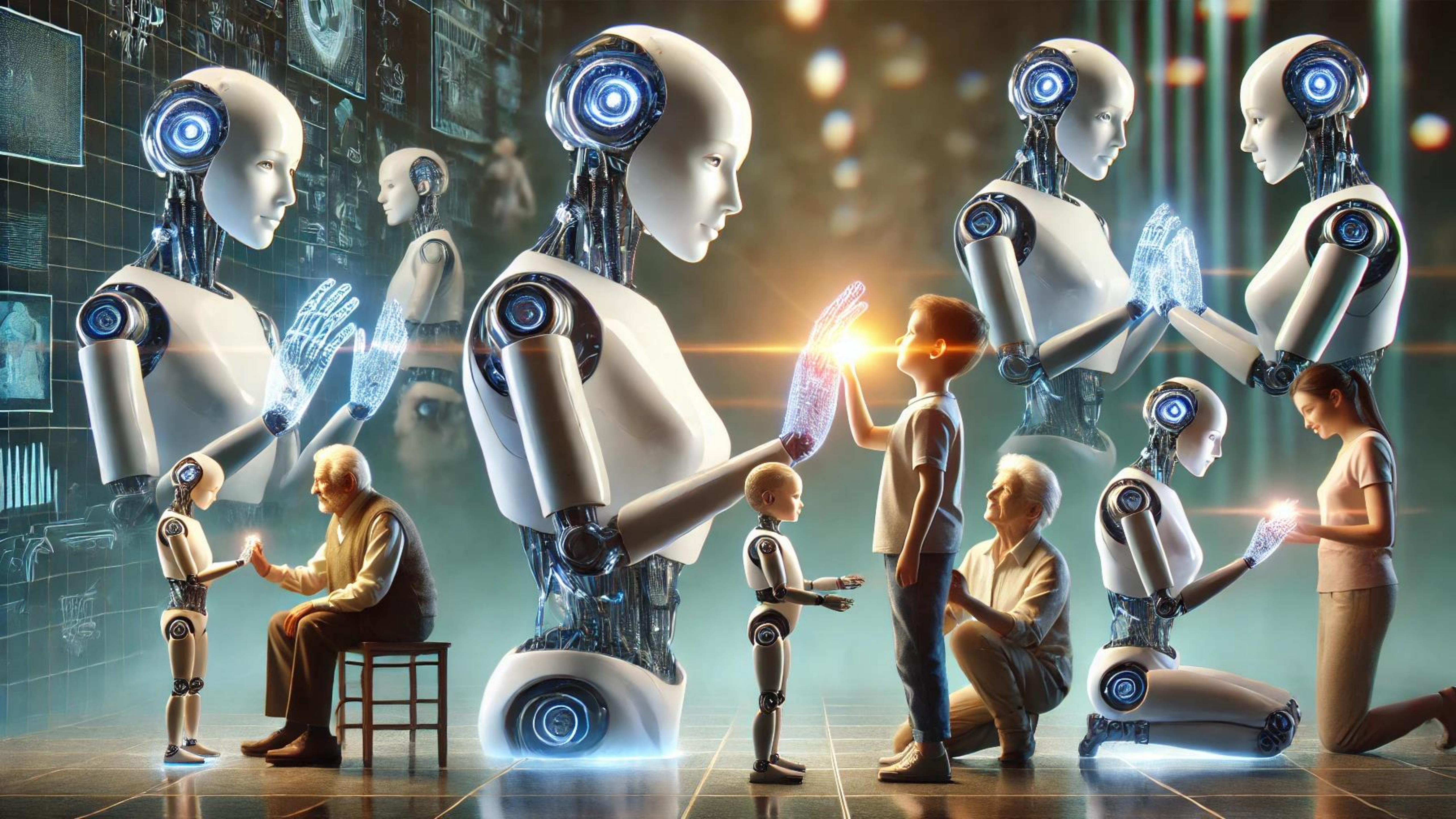
Tomas Janulevicius

Senior Channel Solutions Engineer,

CyberArk

Agenda

1. What is Agentic AI
2. AI Identity security
3. The risks of unsecured AI
4. How does CyberArk use AI
5. Demonstration

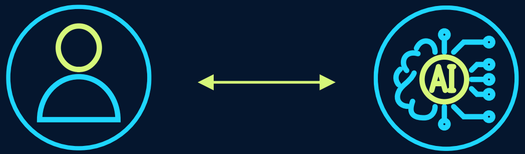


What Is Agentic AI

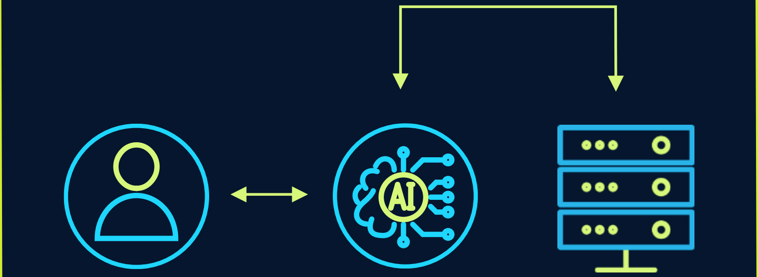
Agentic AI or **AI Agents** refers to artificial intelligence systems that can take autonomous actions to achieve specific goals without constant human direction. They reason, decide, and act independently.

Types of AI

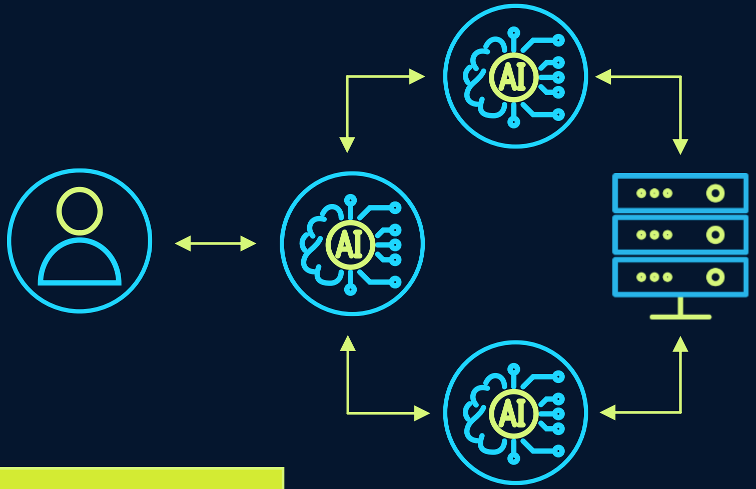
Chat Bot



Agent



Agentic Architecture



Autonomy

Proactivity

AI Identity Security

AI is as good as the information it gets

AI Needs to access data – data you have already got

Query Data Libraries

AI agent Identities are much like human Identities – both need securing

What Makes AI Agents Stand Out

Reasoning

Automation

Decision Making

Action taking

Volume and variety

The Risks of Unsecured AI

Masses of Agents

Credentials Concentration

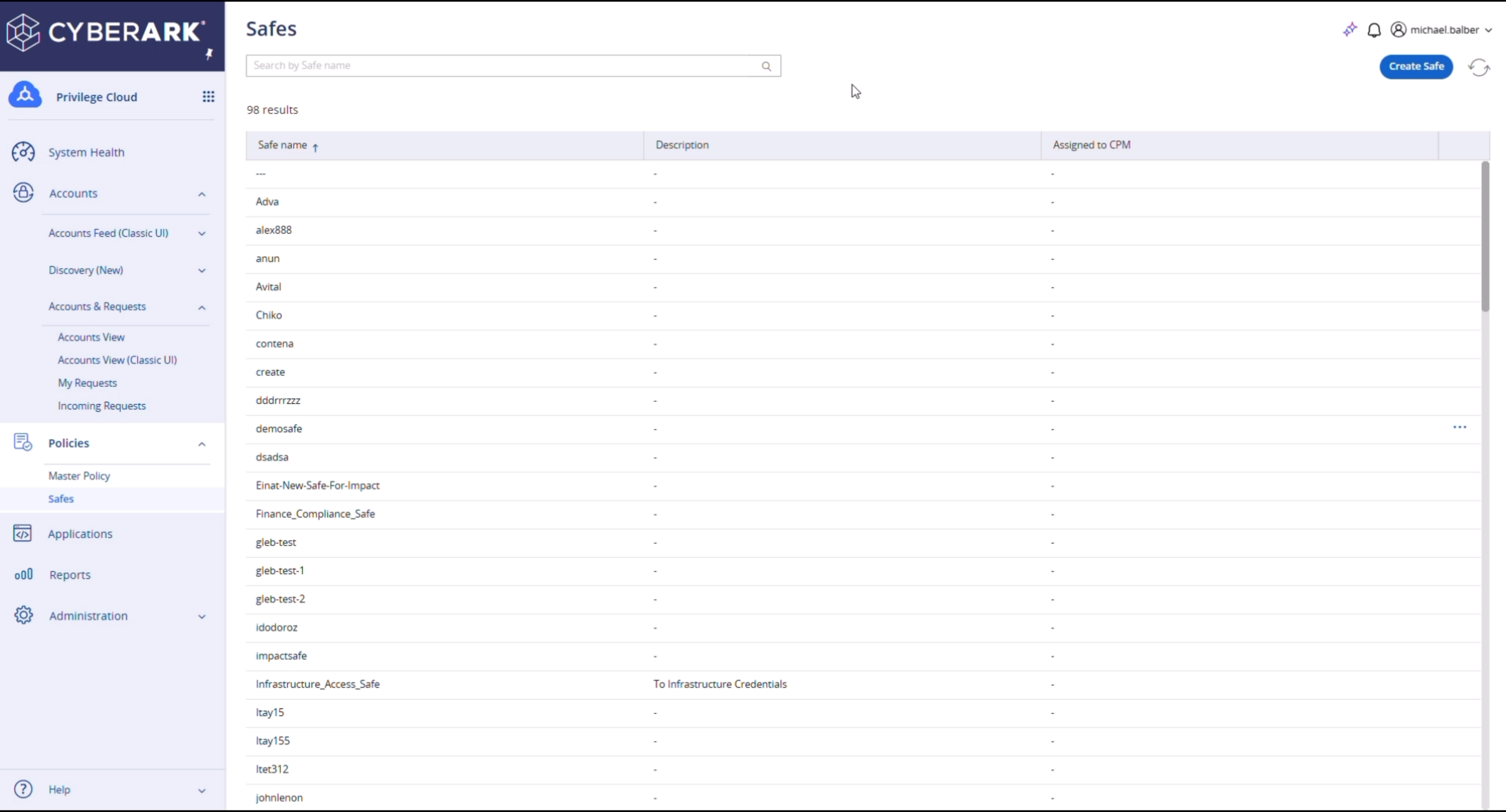
Lack of Controls

Workforce / Development / IT

CYBERARK®
The Identity Security Company™

How Does CyberArk Use AI

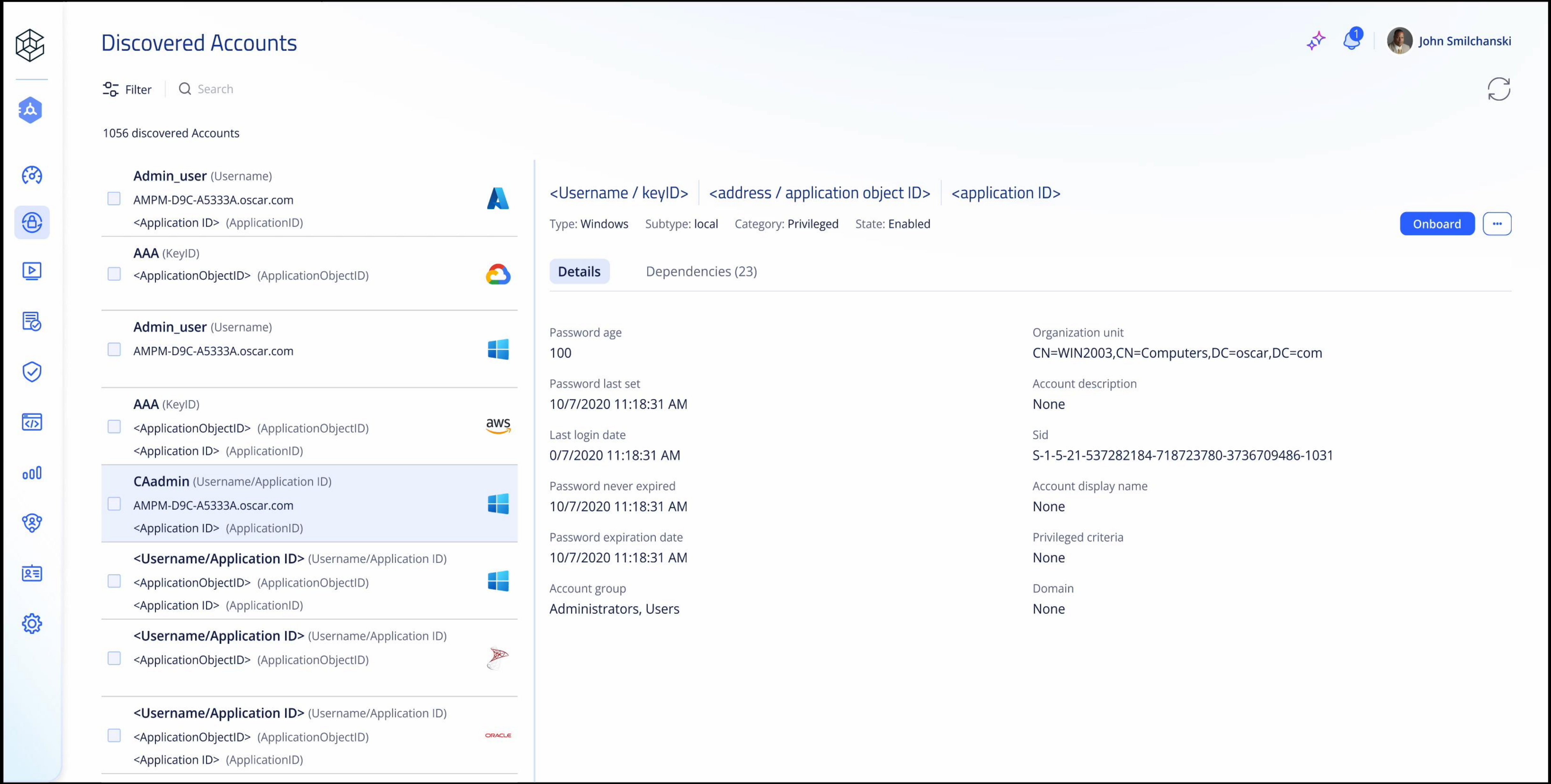
CORA AI™



Safes

98 results

Safe name ↑	Description	Assigned to CPM
---	-	-
Adva	-	-
alex888	-	-
anun	-	-
Avital	-	-
Chiko	-	-
contena	-	-
create	-	-
dddrrrzzz	-	-
demosafe	-	-
dsadsa	-	-
Einat-New-Safe-For-Impact	-	-
Finance_Compliance_Safe	-	-
gleb-test	-	-
gleb-test-1	-	-
gleb-test-2	-	-
idodoroz	-	-
impactsafe	-	-
Infrastructure_Access_Safe	To Infrastructure Credentials	-
Itay15	-	-
Itay155	-	-
Itet312	-	-
johnlenon	-	-



Discovered Accounts

1056 discovered Accounts

Admin_user (Username)
AMPM-D9C-A5333A.oscar.com
<Application ID> (ApplicationID)

AAA (KeyID)
<ApplicationObjectID> (ApplicationObjectID)

Admin_user (Username)
AMPM-D9C-A5333A.oscar.com

AAA (KeyID)
<ApplicationObjectID> (ApplicationObjectID)
<Application ID> (ApplicationID)

CAadmin (Username/Application ID)
AMPM-D9C-A5333A.oscar.com
<Application ID> (ApplicationID)

<Username/Application ID> (Username/Application ID)
<ApplicationObjectID> (ApplicationObjectID)
<Application ID> (ApplicationID)

<Username/Application ID> (Username/Application ID)
<ApplicationObjectID> (ApplicationObjectID)

<Username/Application ID> (Username/Application ID)
<ApplicationObjectID> (ApplicationObjectID)
<Application ID> (ApplicationID)

<Username / keyID> <address / application object ID> <application ID>

Type: Windows Subtype: local Category: Privileged State: Enabled

Password age
100

Password last set
10/7/2020 11:18:31 AM

Last login date
0/7/2020 11:18:31 AM

Password never expired
10/7/2020 11:18:31 AM

Password expiration date
10/7/2020 11:18:31 AM

Account group
Administrators, Users

Organization unit
CN=WIN2003,CN=Computers,DC=oscar,DC=com

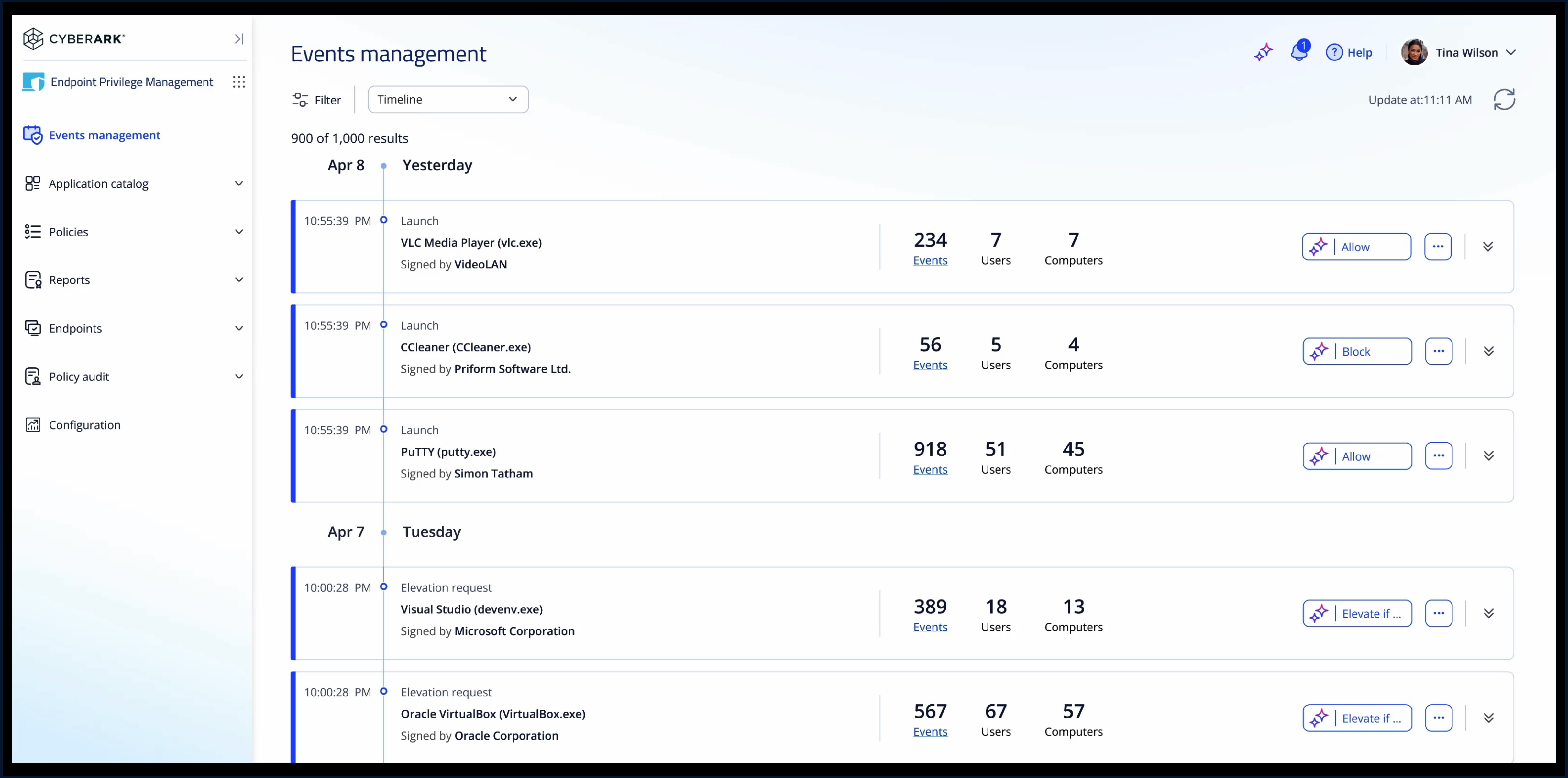
Account description
None

Sid
S-1-5-21-537282184-718723780-3736709486-1031

Account display name
None

Privileged criteria
None

Domain
None



Events management

Update at:11:11 AM

900 of 1,000 results

Apr 8 Yesterday

10:55:39 PM
Launch
VLC Media Player (vlc.exe)
Signed by **VideoLAN**
234 Events · 7 Users · 7 Computers
Allow

10:55:39 PM
Launch
CCleaner (CCleaner.exe)
Signed by **Priform Software Ltd.**
56 Events · 5 Users · 4 Computers
Block

10:55:39 PM
Launch
PuTTY (putty.exe)
Signed by **Simon Tatham**
918 Events · 51 Users · 45 Computers
Allow

Apr 7 Tuesday

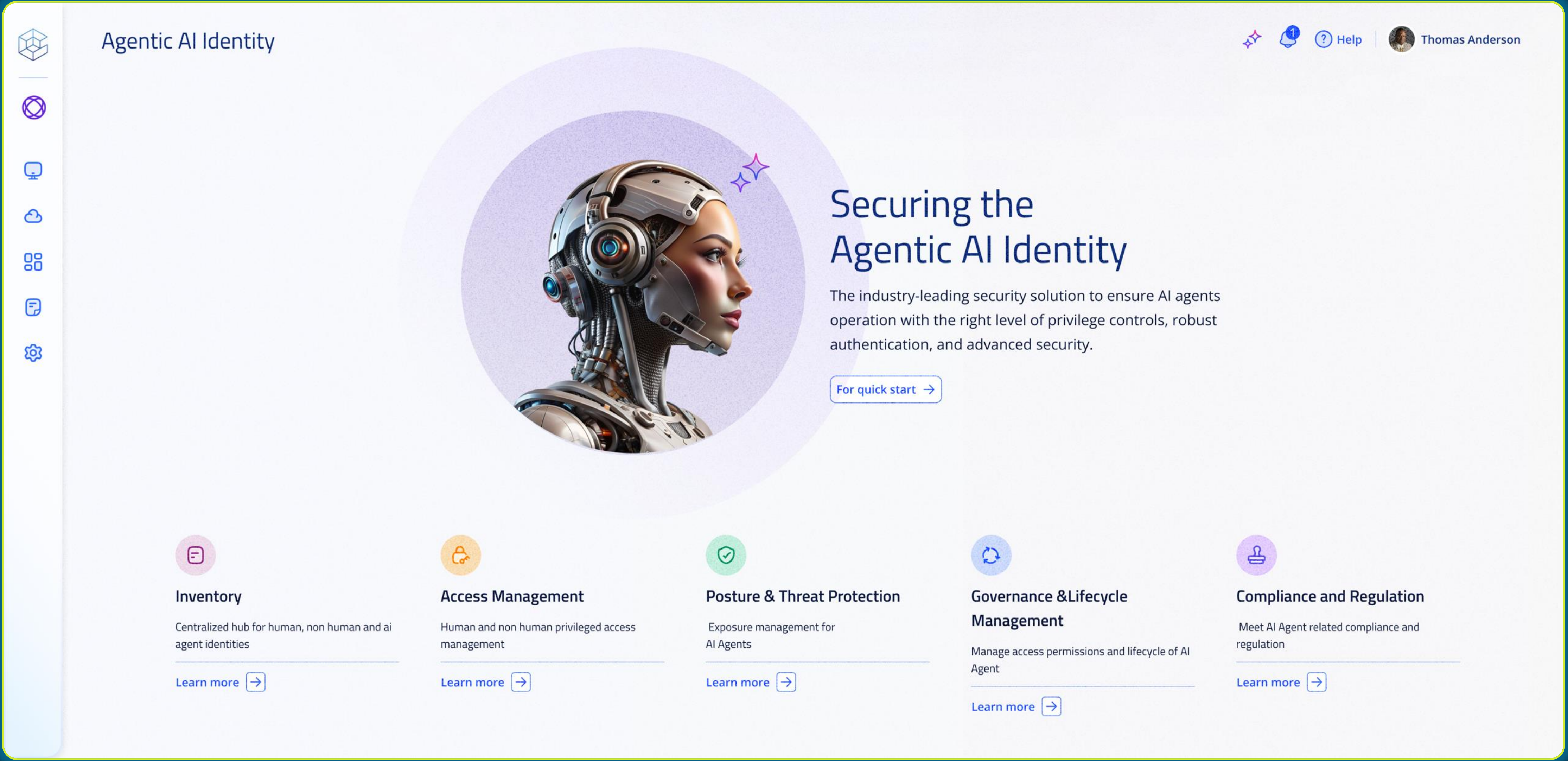
10:00:28 PM
Elevation request
Visual Studio (devenv.exe)
Signed by **Microsoft Corporation**
389 Events · 18 Users · 13 Computers
Elevate if ...

10:00:28 PM
Elevation request
Oracle VirtualBox (VirtualBox.exe)
Signed by **Oracle Corporation**
567 Events · 67 Users · 57 Computers
Elevate if ...

CyberArk’s Vision on Securing AI

AI Agents as privileged Identities

Securing The Agentic AI Identity



Agentic AI Identity

Securing the Agentic AI Identity

The industry-leading security solution to ensure AI agents operation with the right level of privilege controls, robust authentication, and advanced security.

Inventory

Centralized hub for human, non human and ai agent identities

Access Management

Human and non human privileged access management

Posture & Threat Protection

Exposure management for AI Agents

Governance &Lifecycle Management

Manage access permissions and lifecycle of AI Agent

Compliance and Regulation

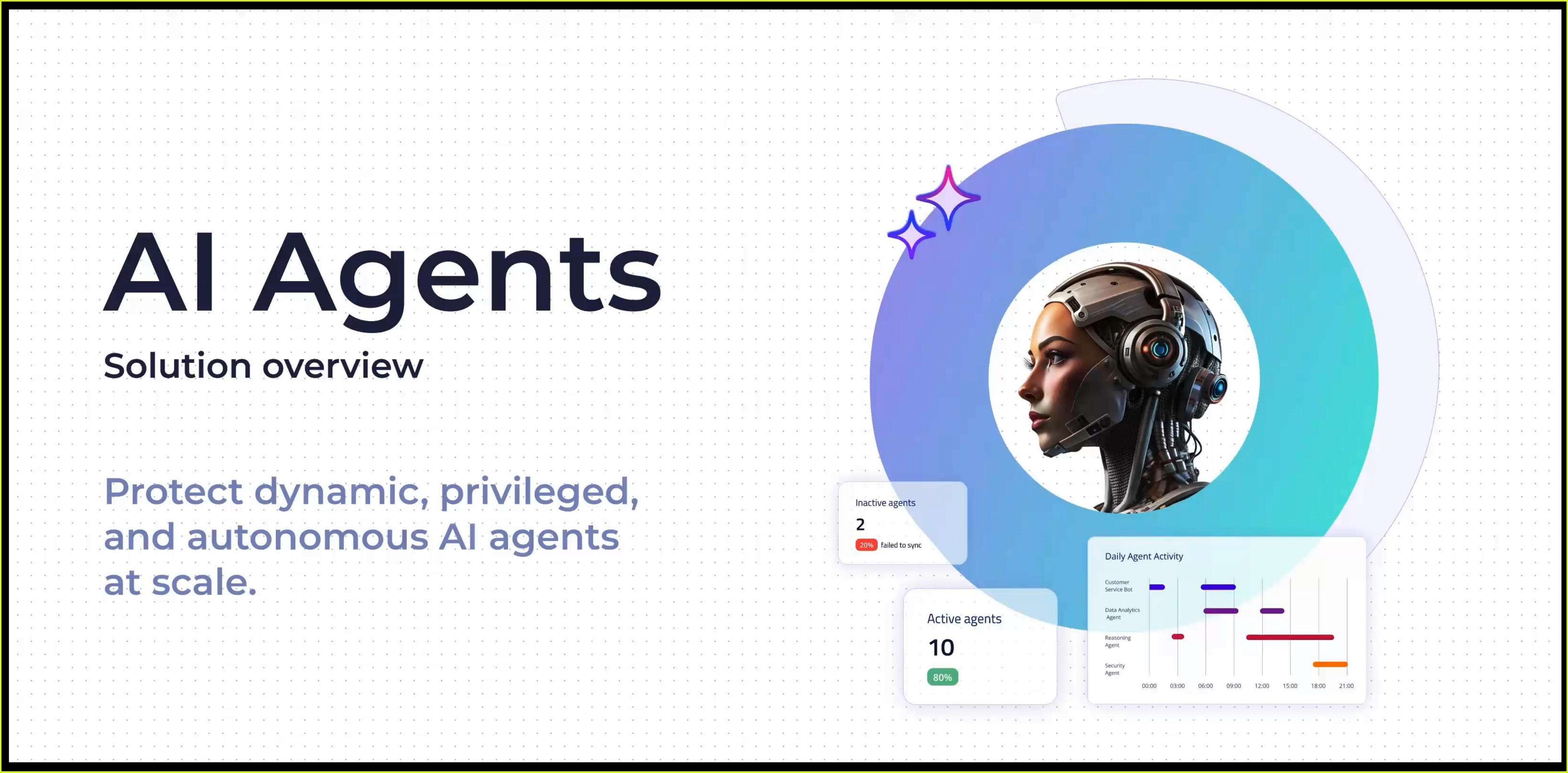
Meet AI Agent related compliance and regulation

CyberArk’s Vision on Securing AI

AI Agents as privileged Identities

Discovery & Lifecycle Management

Discovery & Context Demo (Inventory)



AI Agents

Solution overview

Protect dynamic, privileged, and autonomous AI agents at scale.

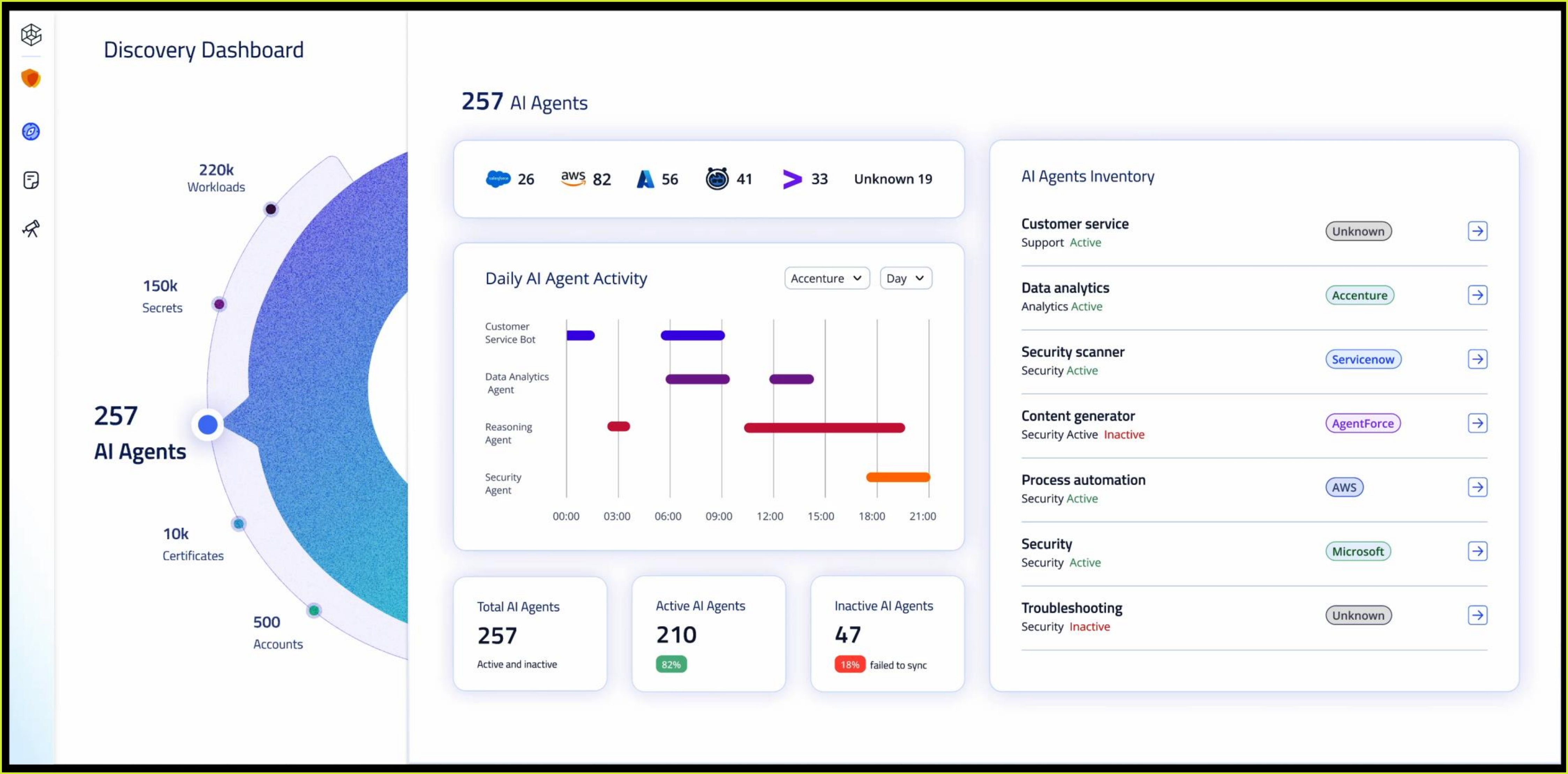
CyberArk's Vision on Securing AI

AI Agents as privileged Identities

Discovery & Lifecycle Management

Policy-based access controls (Zero Trust Enforcement)

Discovery & Context Demo



Discovery Dashboard

257 AI Agents

26 aws 82 56 41 33 Unknown 19

Daily AI Agent Activity

Accenture ⌄ Day ⌄

Total AI Agents
257
Active and inactive

Active AI Agents
210
82%

Inactive AI Agents
47
18% failed to sync

AI Agents Inventory

Customer service Support Active	Unknown	→
Data analytics Analytics Active	Accenture	→
Security scanner Security Active	Servicenow	→
Content generator Security Active Inactive	AgentForce	→
Process automation Security Active	AWS	→
Security Security Active	Microsoft	→
Troubleshooting Security Inactive	Unknown	→

CYBERARK®

CyberArk's Vision on Securing AI

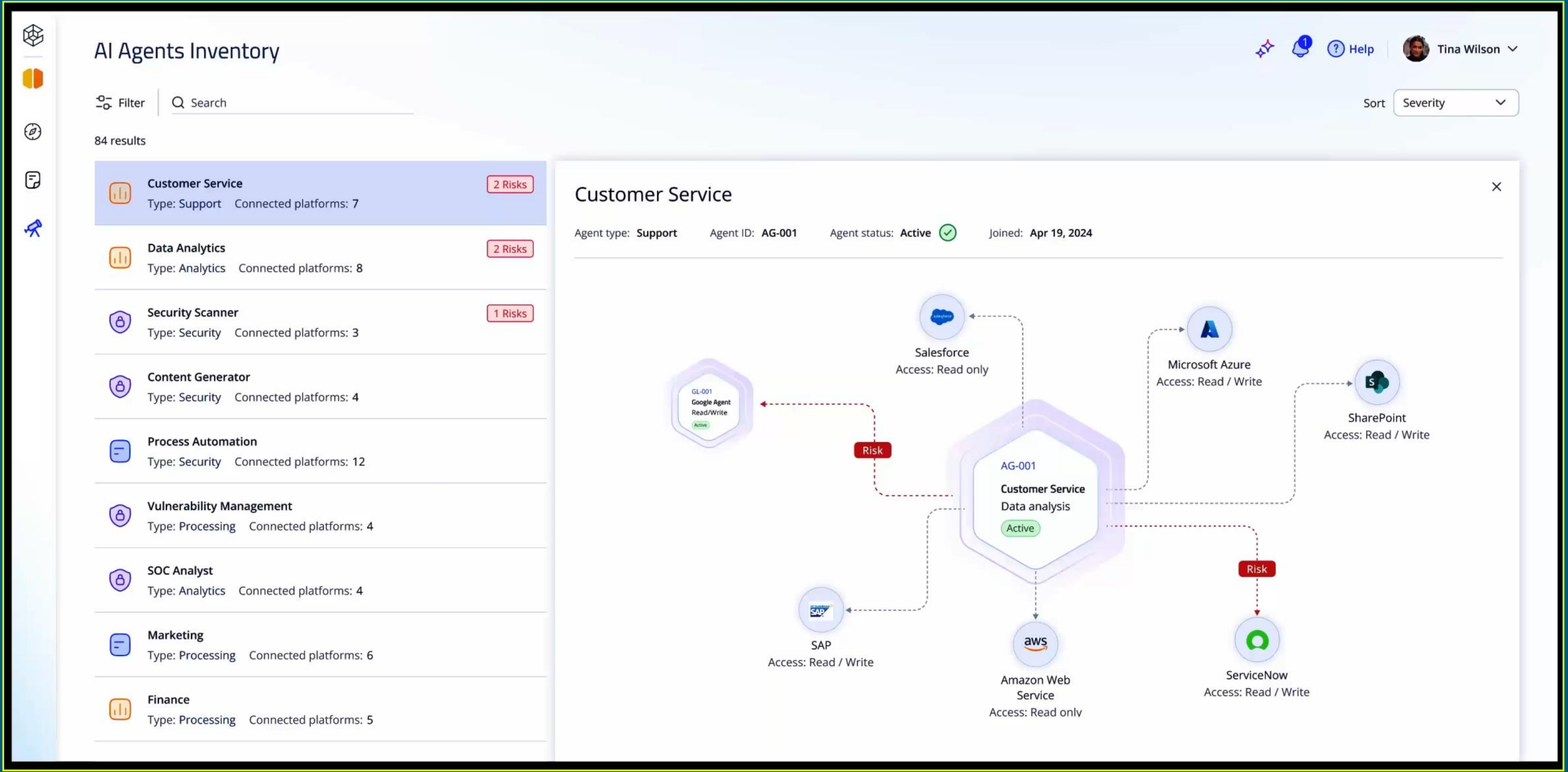
AI Agents as privileged Identities

Discovery & Lifecycle Management

Policy-based access controls (Zero Trust Enforcement)

Behavioral monitoring and anomaly detection

Posture & Threat Detection Demo



AI Agents Inventory

84 results

Customer Service — 2 Risks
Type: Support Connected platforms: 7

Data Analytics — 2 Risks
Type: Analytics Connected platforms: 8

Security Scanner — 1 Risks
Type: Security Connected platforms: 3

Content Generator
Type: Security Connected platforms: 4

Process Automation
Type: Security Connected platforms: 12

Vulnerability Management
Type: Processing Connected platforms: 4

SOC Analyst
Type: Analytics Connected platforms: 4

Marketing
Type: Processing Connected platforms: 6

Finance
Type: Processing Connected platforms: 5

Customer Service

Agent type: **Support** Agent ID: **AG-001** Agent status: **Active** ✓ Joined: **Apr 19, 2024**

AG-001
Customer Service
Data analysis
Active

GL-001
Google Agent
Read/Write
Active

Salesforce
Access: Read only

Microsoft Azure
Access: Read / Write

SharePoint
Access: Read / Write

SAP
Access: Read / Write

Amazon Web Service
Access: Read only

ServiceNow
Access: Read / Write

Spectrum of Secured Identities

	Human			Machines		
Identity Group	App Admins Contractors Employees	Traditional IT 3rd Parties	DevSecOps Data Scientists Cloud Ops Engineering	Models Agents Bots	Applications Code APIs	IT IoT OT
	Workforce	**IT**	**Developers**	**AI**	**Workloads**	**Devices**
Target Resources	Endpoints, Data, Biz Apps	Data, Apps, Workloads, CI/CD Tools	Data, Apps, Workloads, Code Repos, Cloud Services	Devices, Data, Apps, Workloads, Code		
Risk of Access Level	Access to data	Access and ability to change data and infrastructure		Access and ability to change data infrastructure and code		
Complexity of Access	Lower					Higher

Key Takeaways

Agentic AI Security is Identity Security

AI Agents are Machine Identities that behave like Humans

You Should Start Now!

Ačiū!