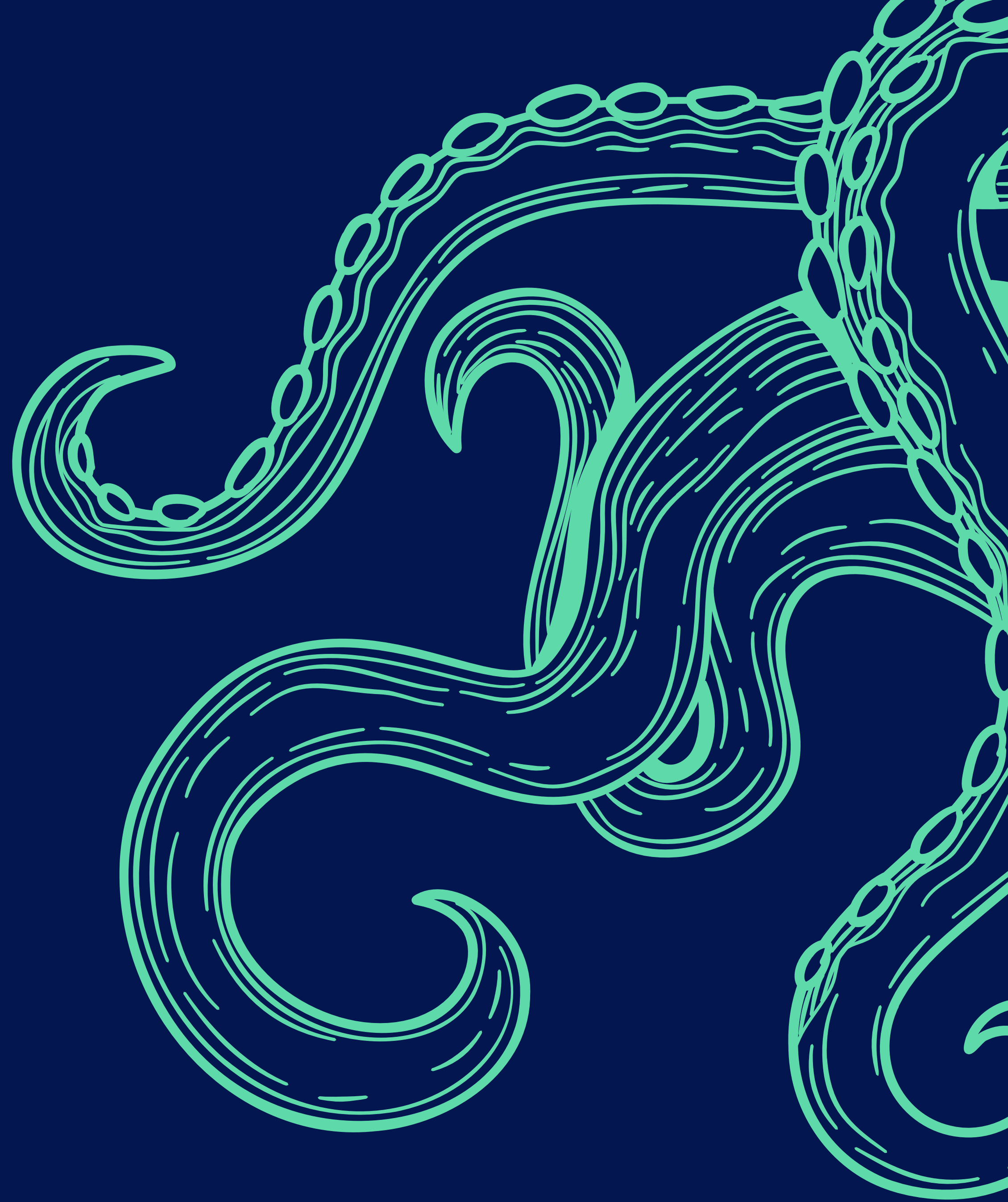




Cyber Asset Attack Surface Management





What is OctoXLabs?

1 Comprehensive **Cyber Visibility**

Founded in **2021**, OctoXLabs provides full visibility into IT infrastructure, enhancing governance and control over cyber assets.

2 **Proactive** Threat Management

Our platform helps security teams manage and protect their attack surface, identifying and mitigating threats before they emerge.

3 **Real-Time** Risk Response

With instant cyber asset insights, teams can isolate risks and take corrective action swiftly.

4 **Automated** Security & Compliance

OctoXLabs enables organizations to build a reliable asset inventory, detect security gaps, and automate policy enforcement.

5 **Seamless** Integration

Supporting **450+** IT security solutions, OctoXLabs deploys in minutes, optimizing operations, incident response, patch management, and more.



Mind the (Visibility) Gap

**69% of
CISOs**

say they lack complete
visibility over their IT
assets (Gartner, 2024)

**63% of
breaches**

are linked to unmanaged
or unknown assets
(IBM Cost of a Data
Breach Report)

**27% of
organizations**

continuously monitor asset
changes in real time
(Forrester, 2023)



Everything Began with a Question?



Jim Schwar
@jimiDFIR

CISO: How many windows hosts do we have?

AV Guy: 7864

Desktop Management: 6321

EDR Team: 6722

CMDB Team: 4848

SIEM Team: 9342

4:55 pm · 8 Feb 2018

33

579

993

20

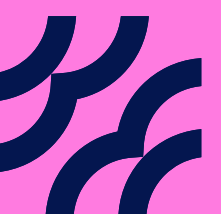
Security teams spend

37%

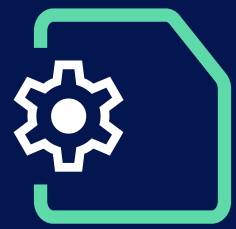
of their time reporting.

89%

of organizations worry that their security investment is not working properly.



Key Challenges Organizations Face Today



Organizational Complexity

Traditional methods fail to manage hybrid IT and security inventories.



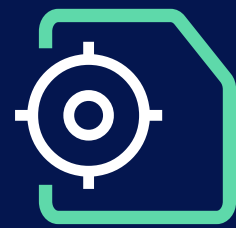
Inefficient Reporting

Teams spend **37%** of their time on reporting.



Lack of Automation

Difficulty in taking automated actions.



Operational Blind Spots

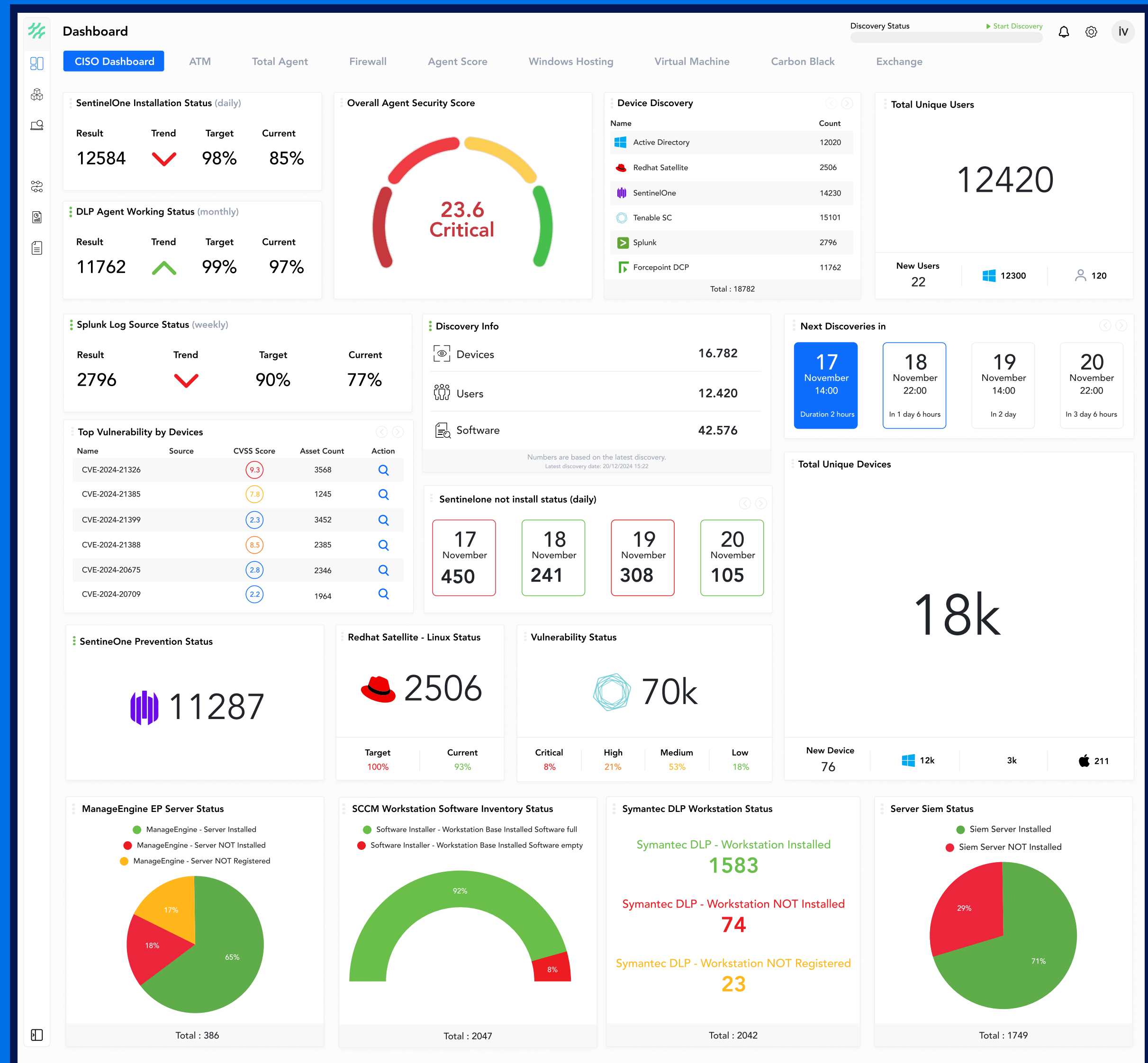
Limited visibility & ineffective gap analysis.



Tracking Difficulties

Identifying security gaps is increasingly challenging.



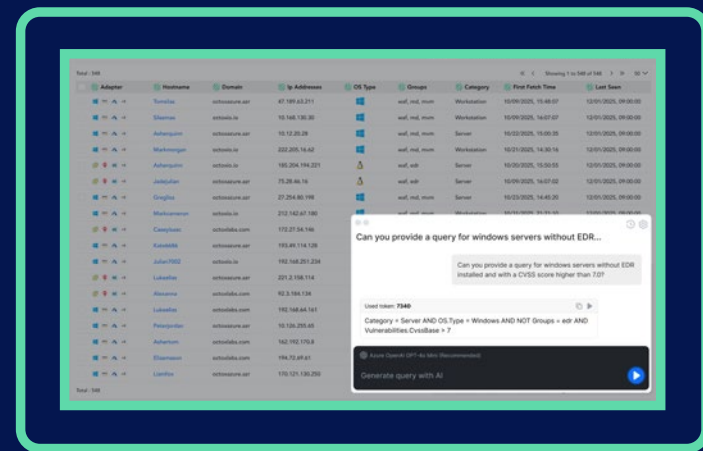


All You Need Is An Aggregator

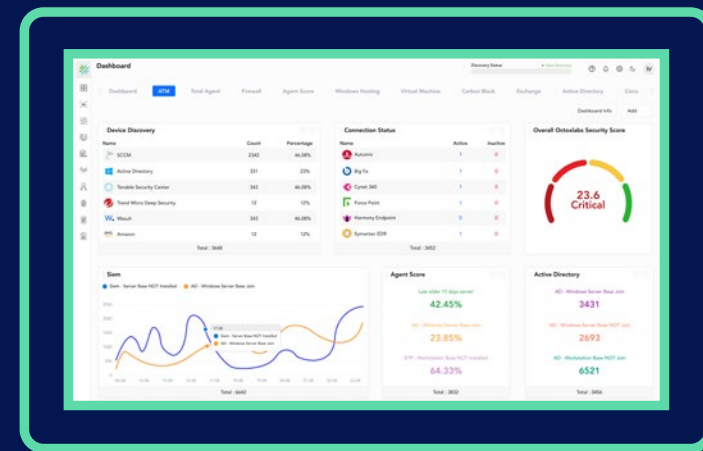
- ✓ Deploy in **15** minutes
- ✓ Agentless
- ✓ **450+** Integrations
- ✓ Get a credible, comprehensive inventory of all devices, users and cloud assets
- ✓ Discover coverage gaps and risk
- ✓ Validate and enforce policies
- ✓ Reporting & Action



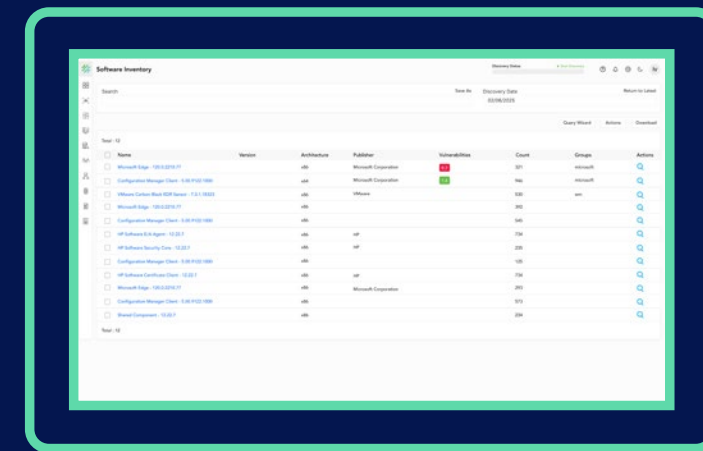
What is OctoX Labs: Solution Overview



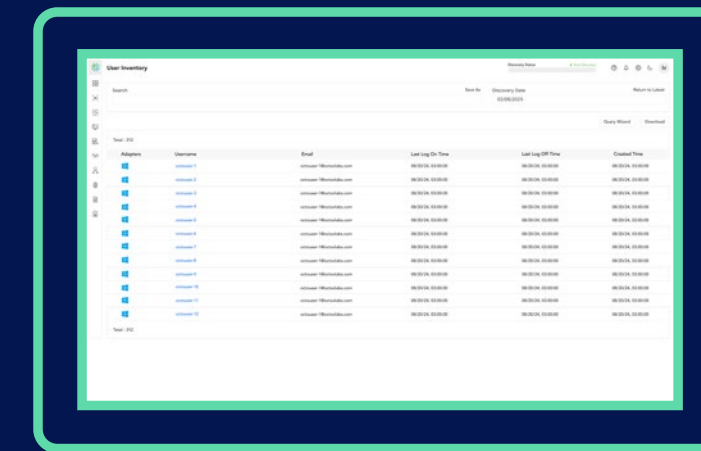
OctoAi



Security Asset Management



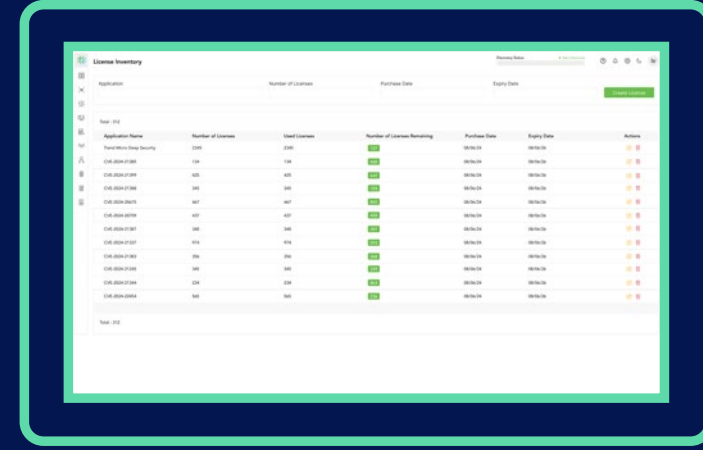
Software Inventory



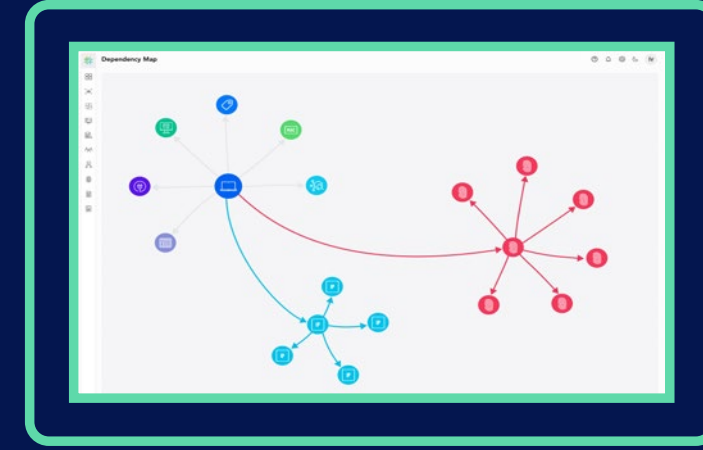
User Management



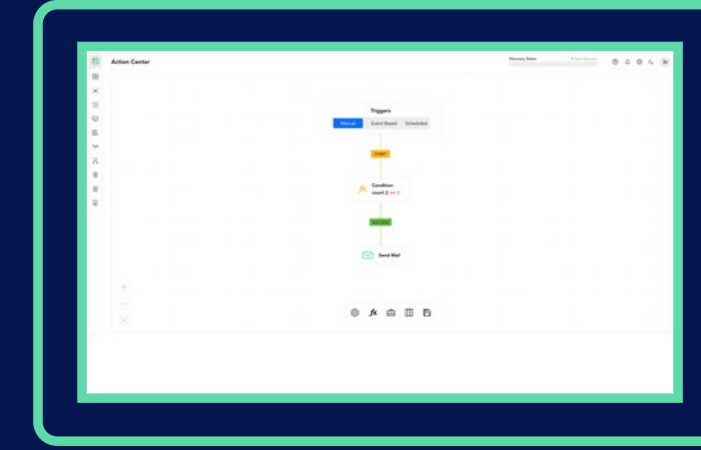
Asset Vulnerability Management



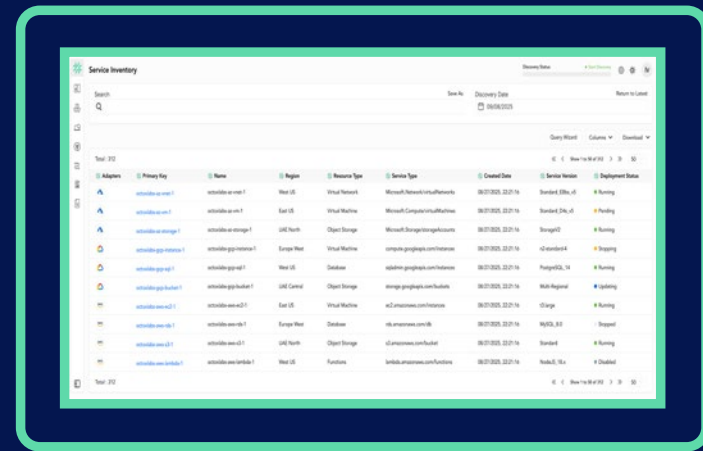
License Management



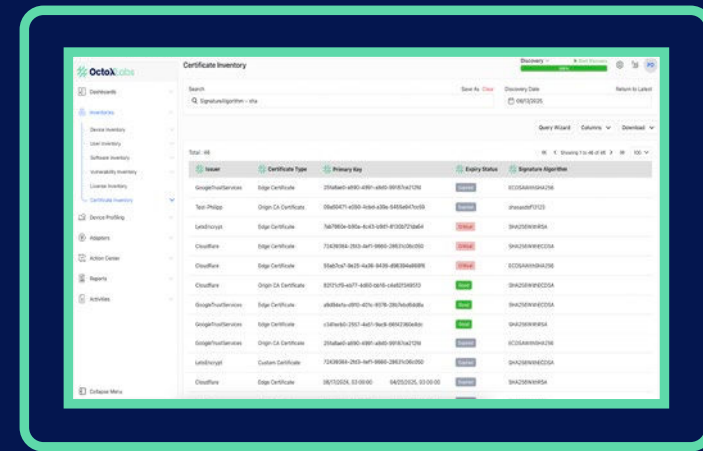
Dependency Map



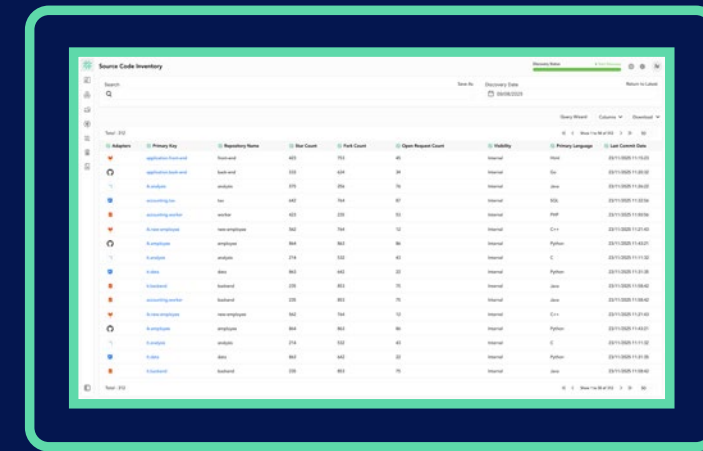
Action Center



Service Inventory



Certificate Inventory

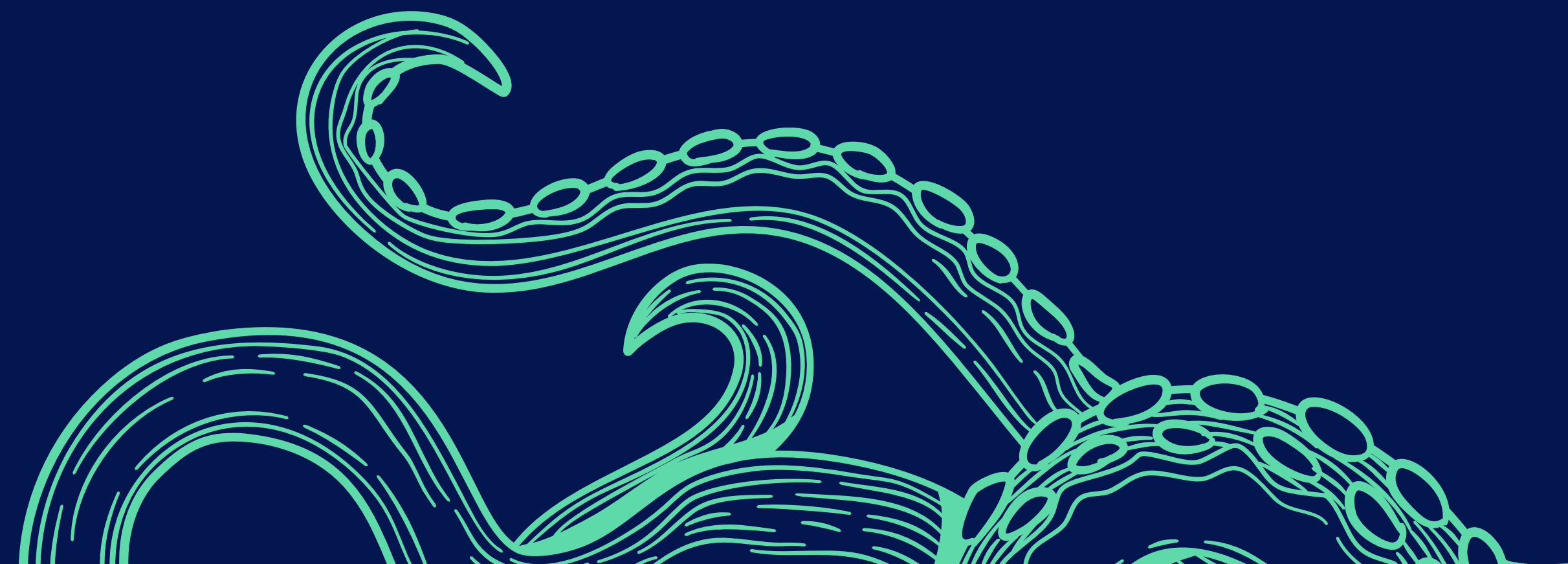


Source Code Inventory



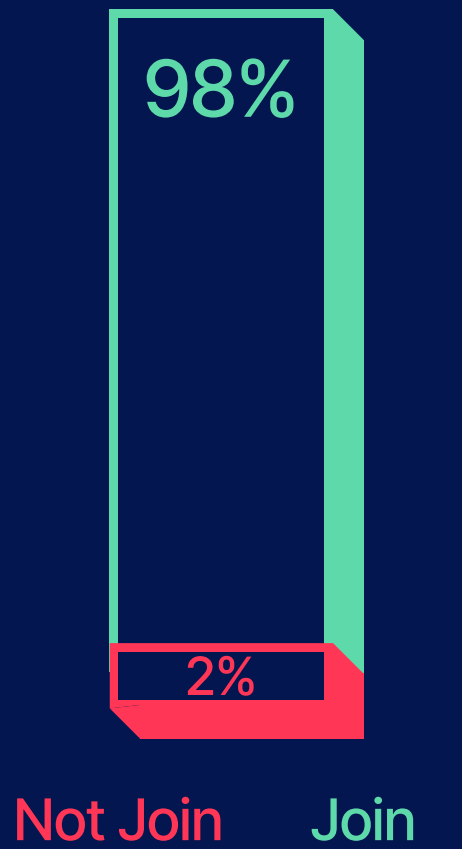
Core Capabilities & Unique Value Proposition

- 1 Unified asset visibility across **all environments**
- 2 **Continuous and automated** asset discovery
- 3 Risk-based prioritization of **security gaps**
- 4 Bridging IT and **security teams**
- 5 **Faster** incident response and **investigation**
- 6 Enhancing **security posture management**
- 7 Api-driven integration with security and **IT ecosystem**

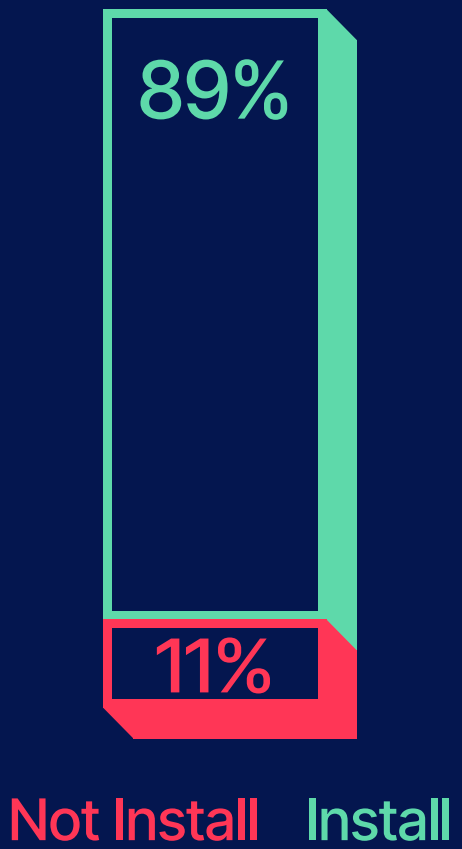


Our Findings

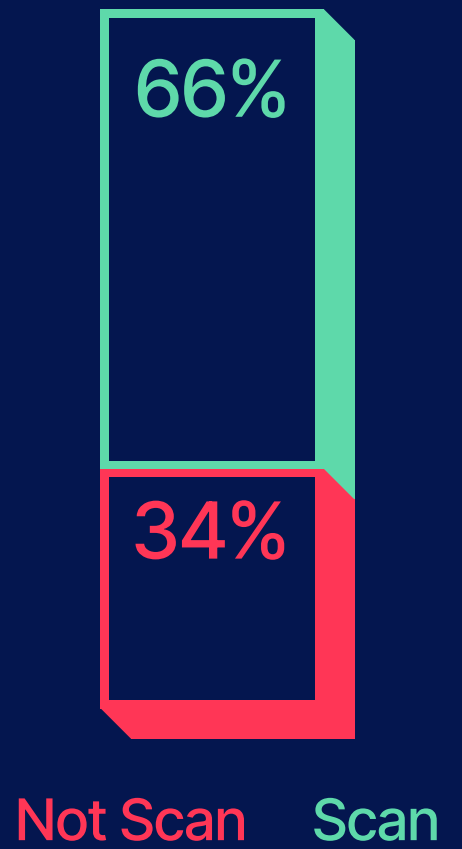
Microsoft Active Directory



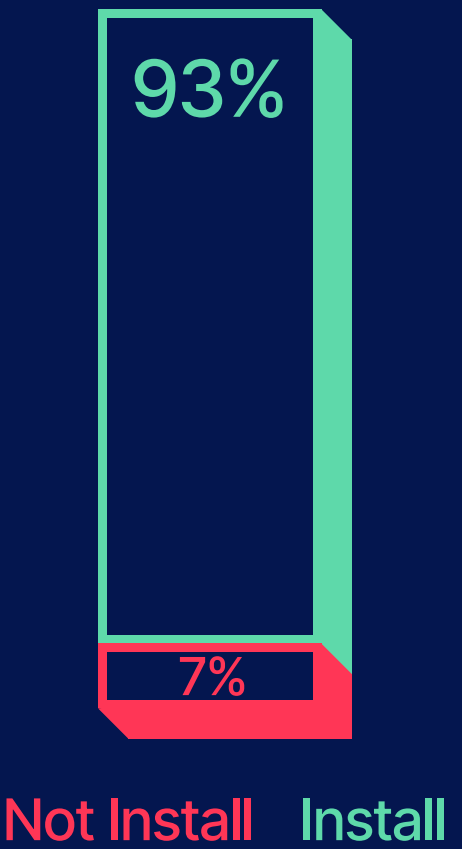
EDR



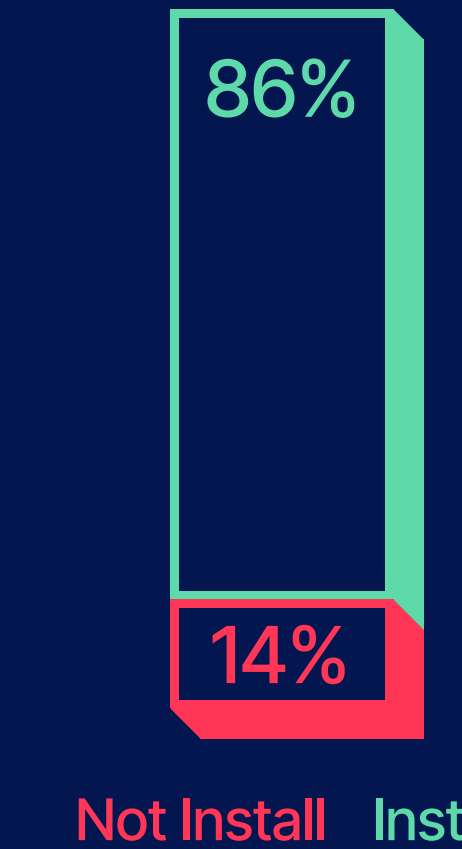
Vulnerability Management



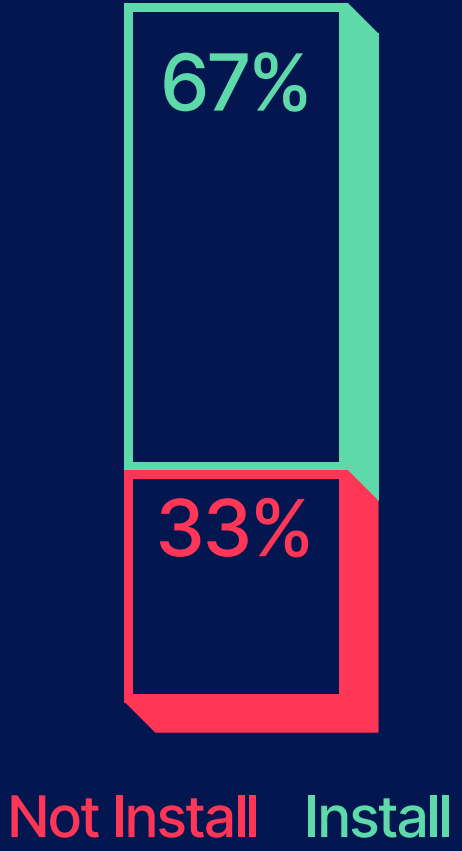
EPP



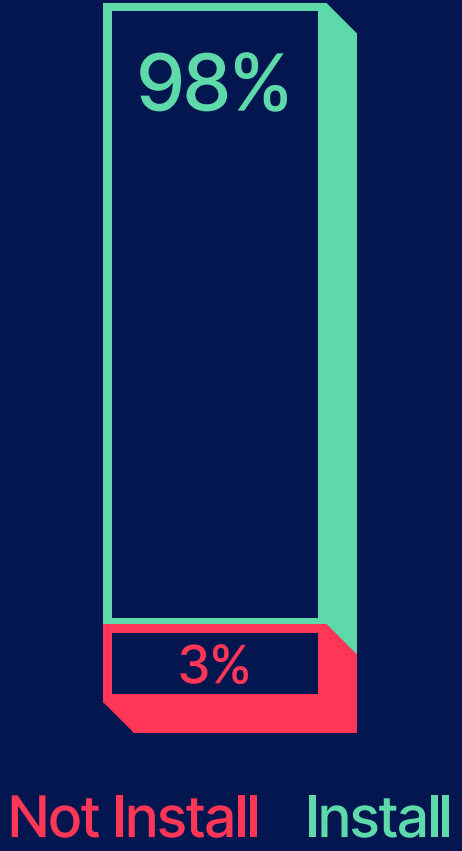
Database Activity Monitoring



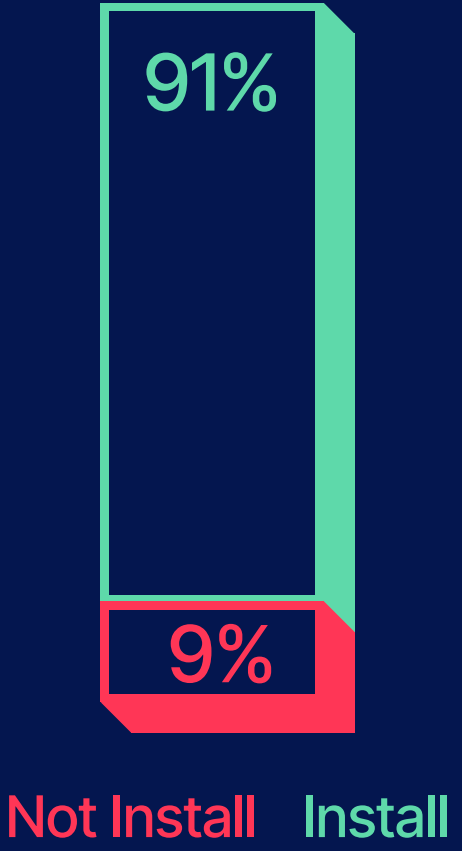
DLP



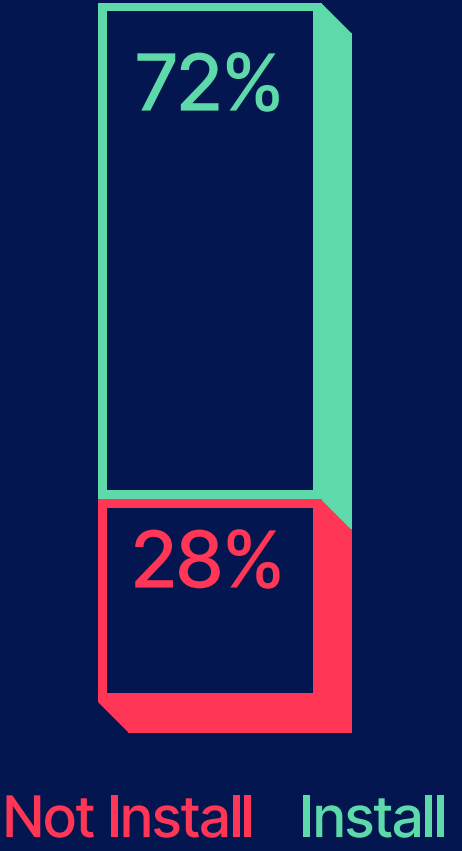
NAC



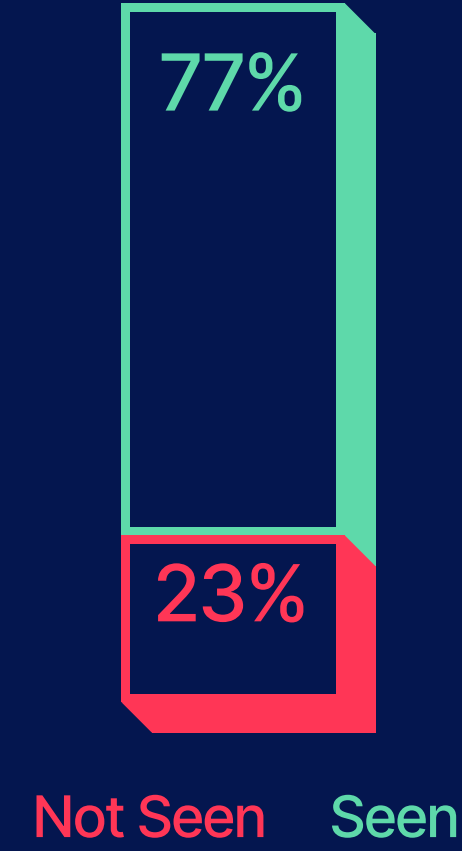
SIEM



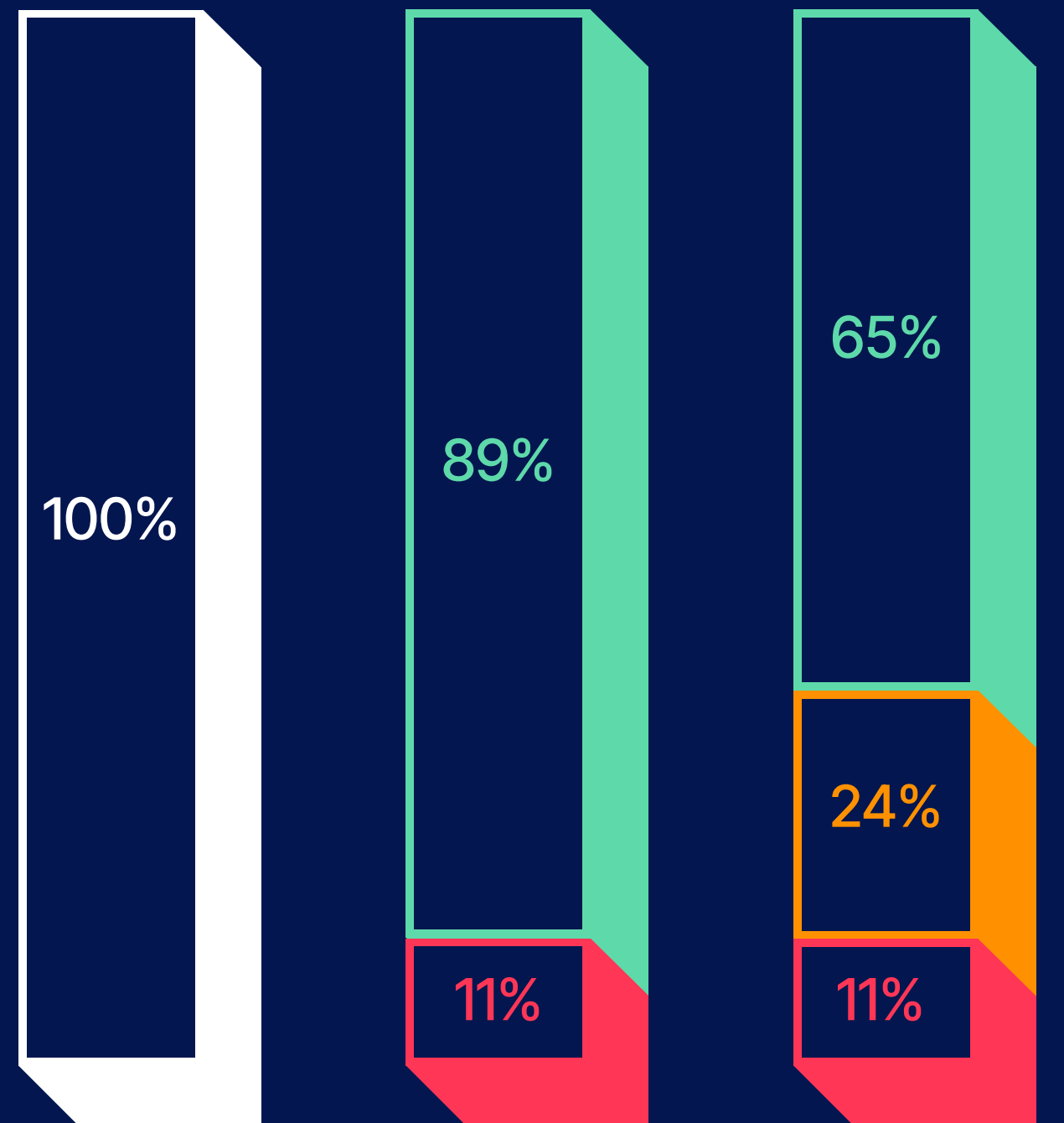
Software Deployment



CMDB



XDR in Details



All Inventory

XDR Agent Installed

XDR Agent Not Installed

Agent Installed/Prevention Mod

Agent Installed/Detection Mod

XDR Agent Not Installed

The screenshot shows a security console interface. At the top, there's a 'Devices' section with a search query: 'Adapters = falcon-crowdstrike AND Specifics.falcon-crowdstrike.device_policies.prevention.policy_type = prevention'. Below this is a table with 106 total devices. The table has columns for Adapters, Hostname, Domain, OS Type, and Prevention Type. Below the table is a 'Query Wizard' dialog box with two rows of search criteria. The first row is 'OctoXLabs' AND 'Adapters' Equal 'Falcon Crowdstrike'. The second row is 'Falcon Crowdstrike' AND 'Device Policies Preventi' Equal 'Prevention'. There are 'Run' and 'Cancel' buttons at the bottom of the wizard.

Adapters	Hostname	Domain	OS Type	Prevention Type
	test-hostname-7026	octoxlabs.com	Windows	Prevention
	dev-host-44018	octoxlabs.local	Windows	Prevention
	test-hostname-3340p	octoxlabs.local	Windows	Prevention
	test-hostname-4984e	octoxlabs.com	Windows	Prevention
	test-hostname-8567	octoxlabs.local	Windows	Prevention
	test-hostname-1482	octoxlabs.com	Windows	Prevention



Key Benefits

Reduce Risk

Increase Efficiency

Save Time



References









Finance / Banking

Insurance

Transportation / Aviation / Automotive

Holding / Investment / Corporate / Services

Energy / Manufacturing / Industry

Retail / E-Commerce / Food & Beverage

Technology / Telecom / Software

Public Sector / Institution / Stock Exchange



Thank You