SECUR-SERV ⊕ cynomi

Visibility on the Road to Compliance

Secur-Serv & Cynomi

October 16, 2025

Presenters

SECUR-SERV

Brian Edwards

Secur -Serv Director
Security & Compliance

Yoel Platt

Cynomi VP Partnerships
and Business Development

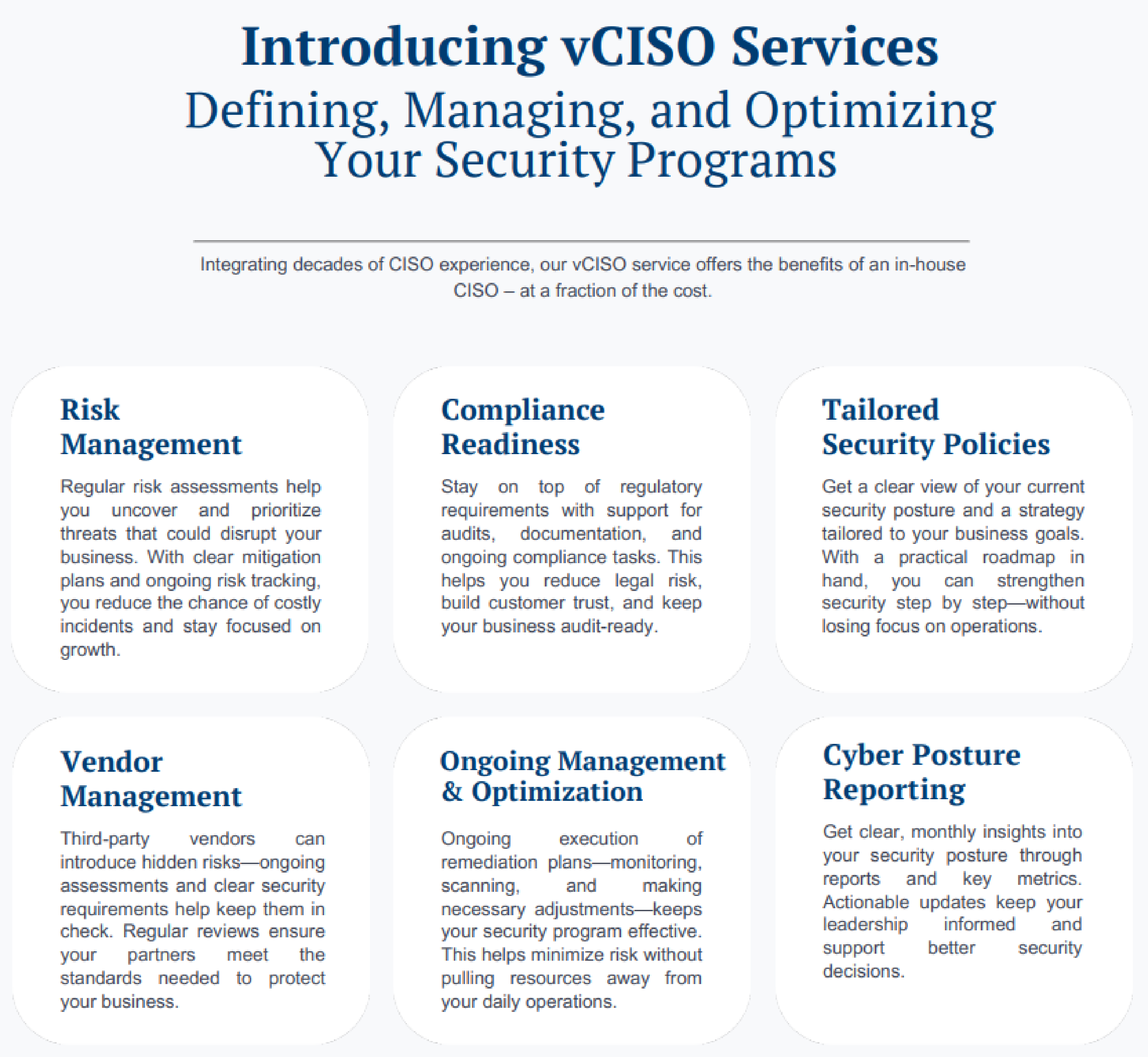
Agenda

1. Secur-Serv vCISO Services
2. Cynomi vCISO Platform
3. Compliance Challenges & Solutions
4. Cynomi Demo

Secur-Serv vCISO Services

vCISO services leverage an AI powered vCISO platform to manage your organization's security posture, risk level and compliance readiness, allowing you to get full visibility into the existing gaps and progress made.

- Risk Management
- Compliance Readiness
- Vendor Management
- Tailored Security Policies
- Ongoing Management & Optimization
- Cyber Posture Reporting



Introducing vCISO Services

Defining, Managing, and Optimizing Your Security Programs

Integrating decades of CISO experience, our vCISO service offers the benefits of an in-house CISO – at a fraction of the cost.

Risk Management

Regular risk assessments help you uncover and prioritize threats that could disrupt your business. With clear mitigation plans and ongoing risk tracking, you reduce the chance of costly incidents and stay focused on growth.

Compliance Readiness

Stay on top of regulatory requirements with support for audits, documentation, and ongoing compliance tasks. This helps you reduce legal risk, build customer trust, and keep your business audit-ready.

Tailored Security Policies

Get a clear view of your current security posture and a strategy tailored to your business goals. With a practical roadmap in hand, you can strengthen security step by step—without losing focus on operations.

Vendor Management

Third-party vendors can introduce hidden risks—ongoing assessments and clear security requirements help keep them in check. Regular reviews ensure your partners meet the standards needed to protect your business.

Ongoing Management & Optimization

Ongoing execution of remediation plans—monitoring, scanning, and making necessary adjustments—keeps your security program effective. This helps minimize risk without pulling resources away from your daily operations.

Cyber Posture Reporting

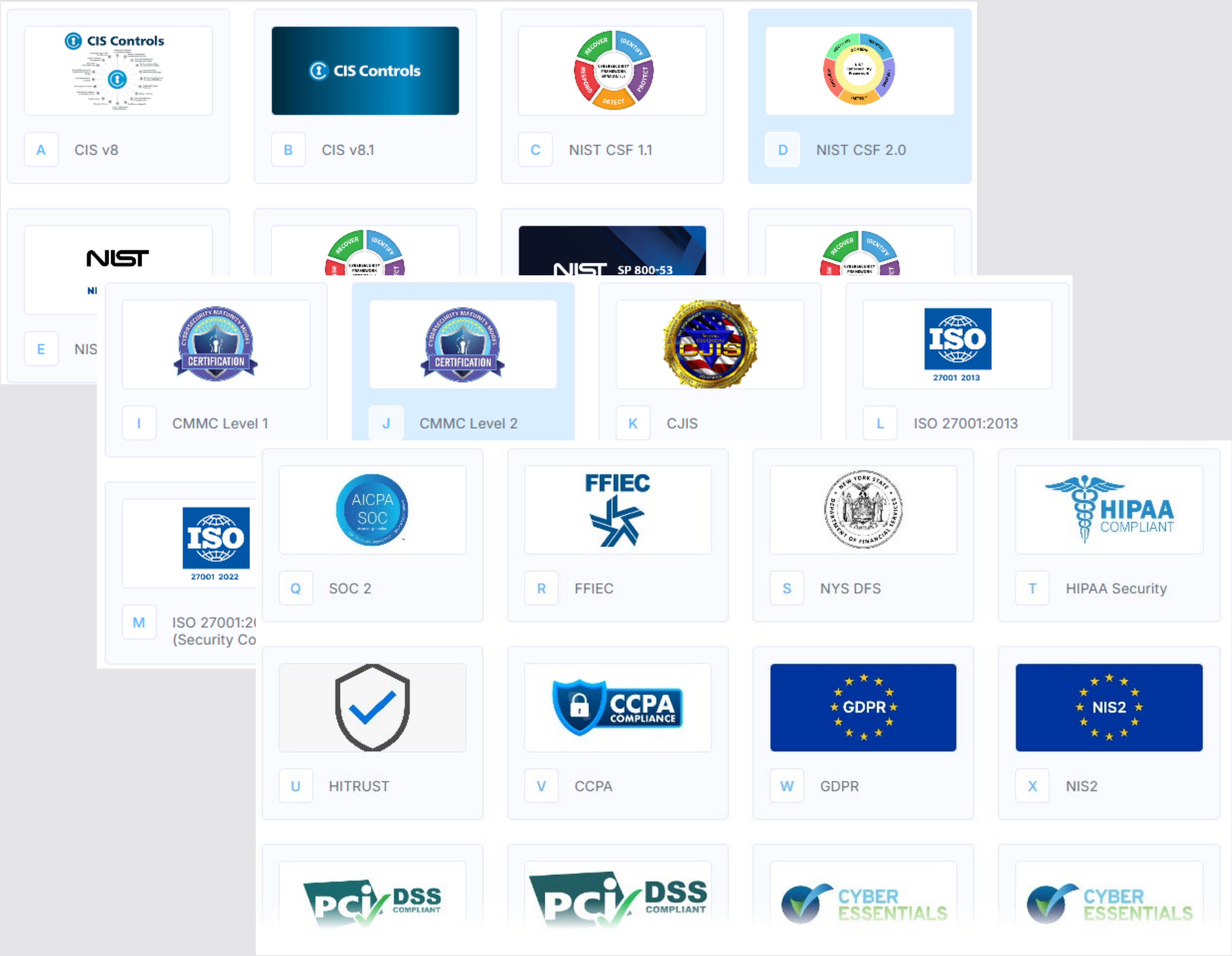
Get clear, monthly insights into your security posture through reports and key metrics. Actionable updates keep your leadership informed and support better security decisions.

Cynomi vCISO Platform

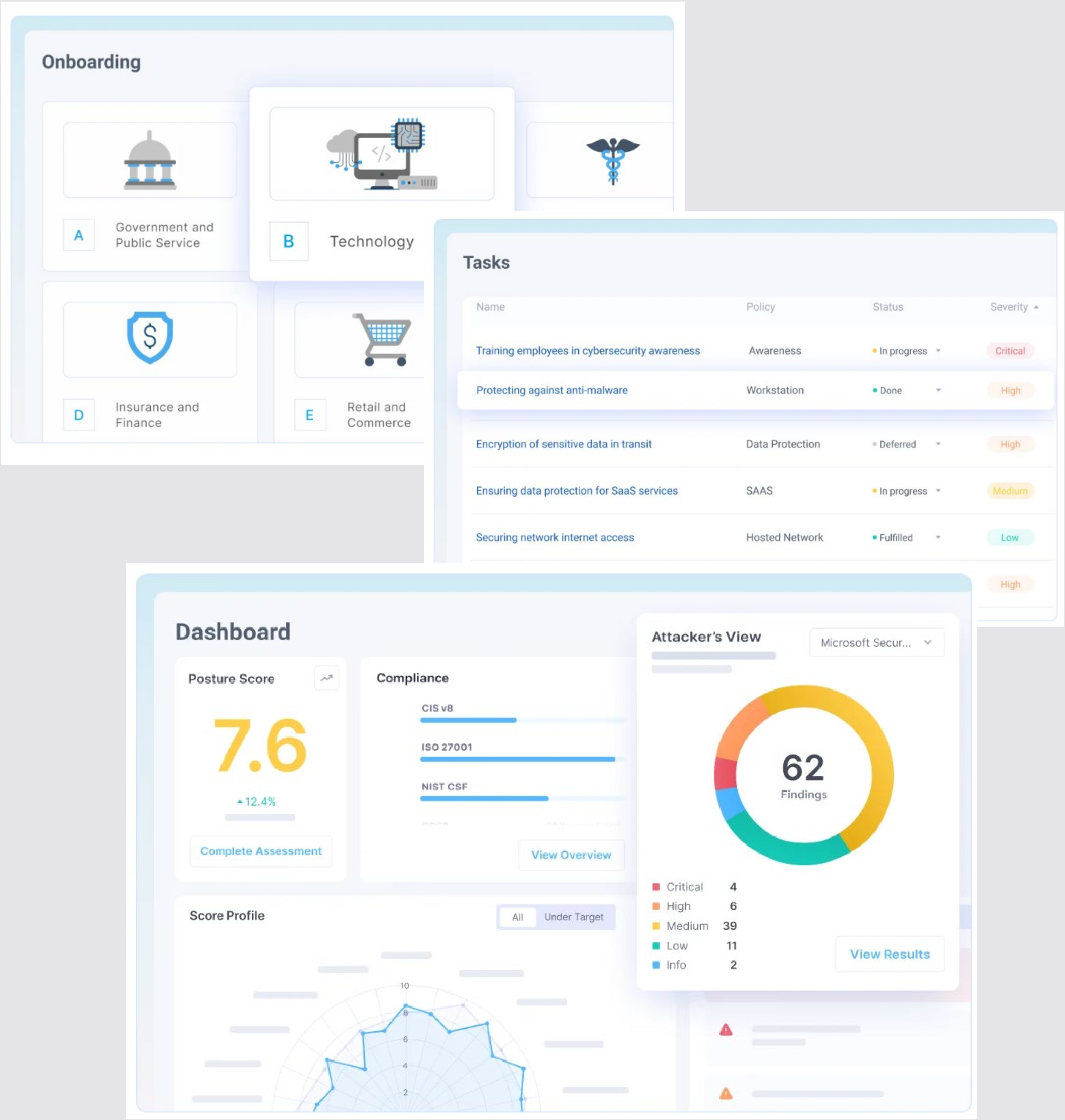
SECUR-SERV

Cynomi Process

- Assess & Identify
- Establish & Plan
- Optimize & Track Progress



A	CIS v8
B	CIS v8.1
C	NIST CSF 1.1
D	NIST CSF 2.0
E	NIS
I	CMMC Level 1
J	CMMC Level 2
K	CJIS
L	ISO 27001:2013
M	ISO 27001:2 (Security Co
Q	SOC 2
R	FFIEC
S	NYS DFS
T	HIPAA Security
U	HITRUST
V	CCPA
W	GDPR
X	NIS2



Onboarding

A	Government and Public Service
B	Technology
D	Insurance and Finance
E	Retail and Commerce

Tasks

Name	Policy	Status	Severity
Training employees in cybersecurity awareness	Awareness	In progress	Critical
Protecting against anti-malware	Workstation	Done	High
Encryption of sensitive data in transit	Data Protection	Deferred	High
Ensuring data protection for SaaS services	SAAS	In progress	Medium
Securing network internet access	Hosted Network	Fulfilled	Low
			High

Dashboard

Posture Score

7.6

▲12.4%

Complete Assessment

Compliance

CIS v8

ISO 27001

NIST CSF

View Overview

Attacker's View

Microsoft Secur...

62 Findings

Critical	4
High	6
Medium	39
Low	11
Info	2

View Results

Score Profile

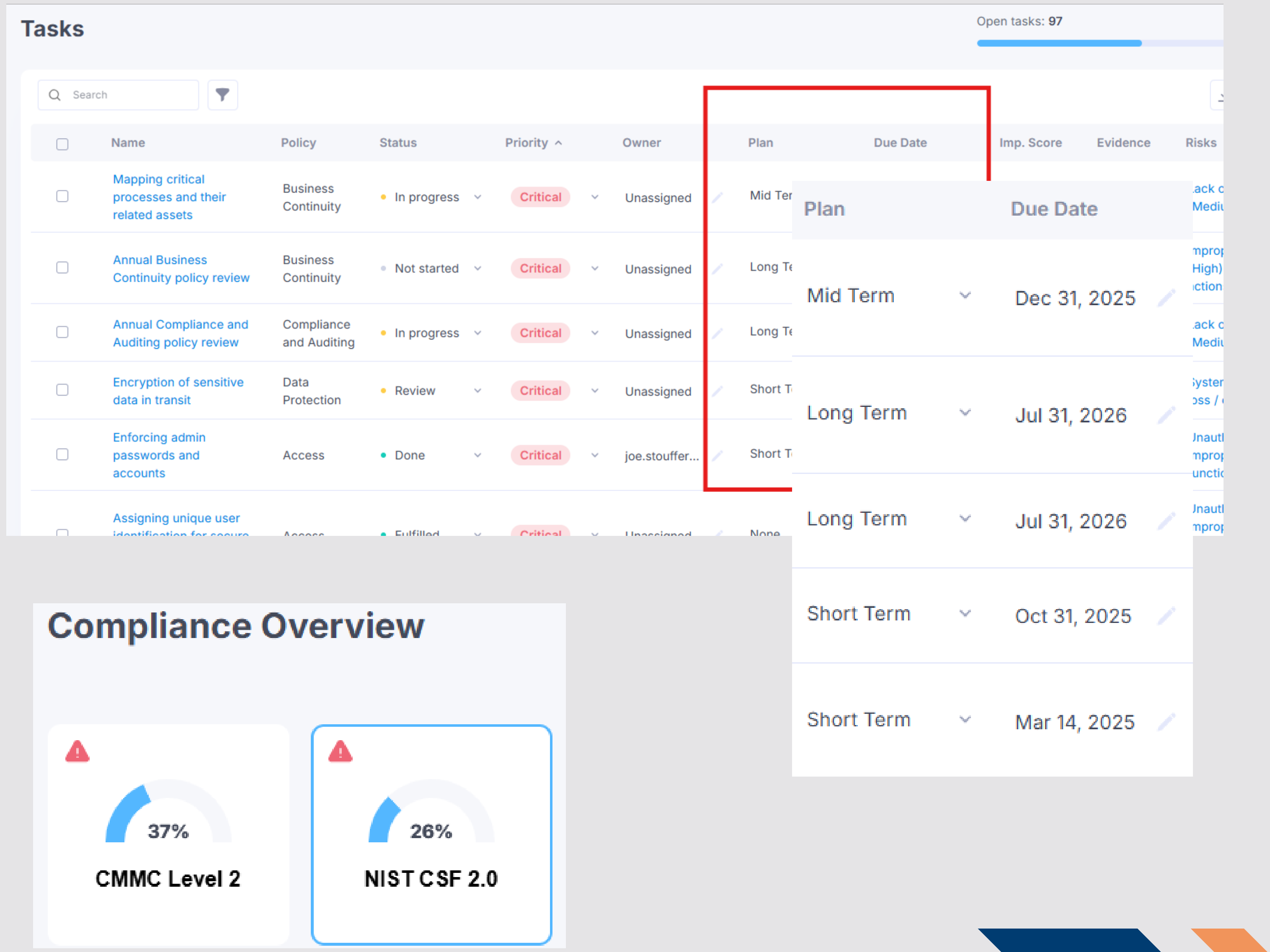
All | Under Target

cynomi

Compliance Challenges & Solutions

Preparing for audits can strain already limited staff and resources.
Stressful exam cycles with short prep windows.

- Your vCISO is available each month for dedicated consulting hours and regular check-ins, giving you direct access to strategic guidance, expert answers, and hands-on support.
- Working with your vCISO or independently, quickly onboard and complete discovery by answering a series of short interactive risk assessments.
- Easily track compliance readiness in real-time, identify gaps and manage all tasks from a single centralized dashboard.



Tasks

Open tasks: **97**

□	Name	Policy	Status	Priority	Owner	Plan
□	Mapping critical processes and their related assets	Business Continuity	● In progress	Critical	Unassigned	Mid Ter
□	Annual Business Continuity policy review	Business Continuity	● Not started	Critical	Unassigned	Long Te
□	Annual Compliance and Auditing policy review	Compliance and Auditing	● In progress	Critical	Unassigned	Long Te
□	Encryption of sensitive data in transit	Data Protection	● Review	Critical	Unassigned	Short T
□	Enforcing admin passwords and accounts	Access	● Done	Critical	joe.stouffer...	Short T
□	Assigning unique user identification for secure	Access	● Fulfilled	Critical	Unassigned	None

Plan	Due Date
Mid Term	Dec 31, 2025
Long Term	Jul 31, 2026
Long Term	Jul 31, 2026
Short Term	Oct 31, 2025
Short Term	Mar 14, 2025

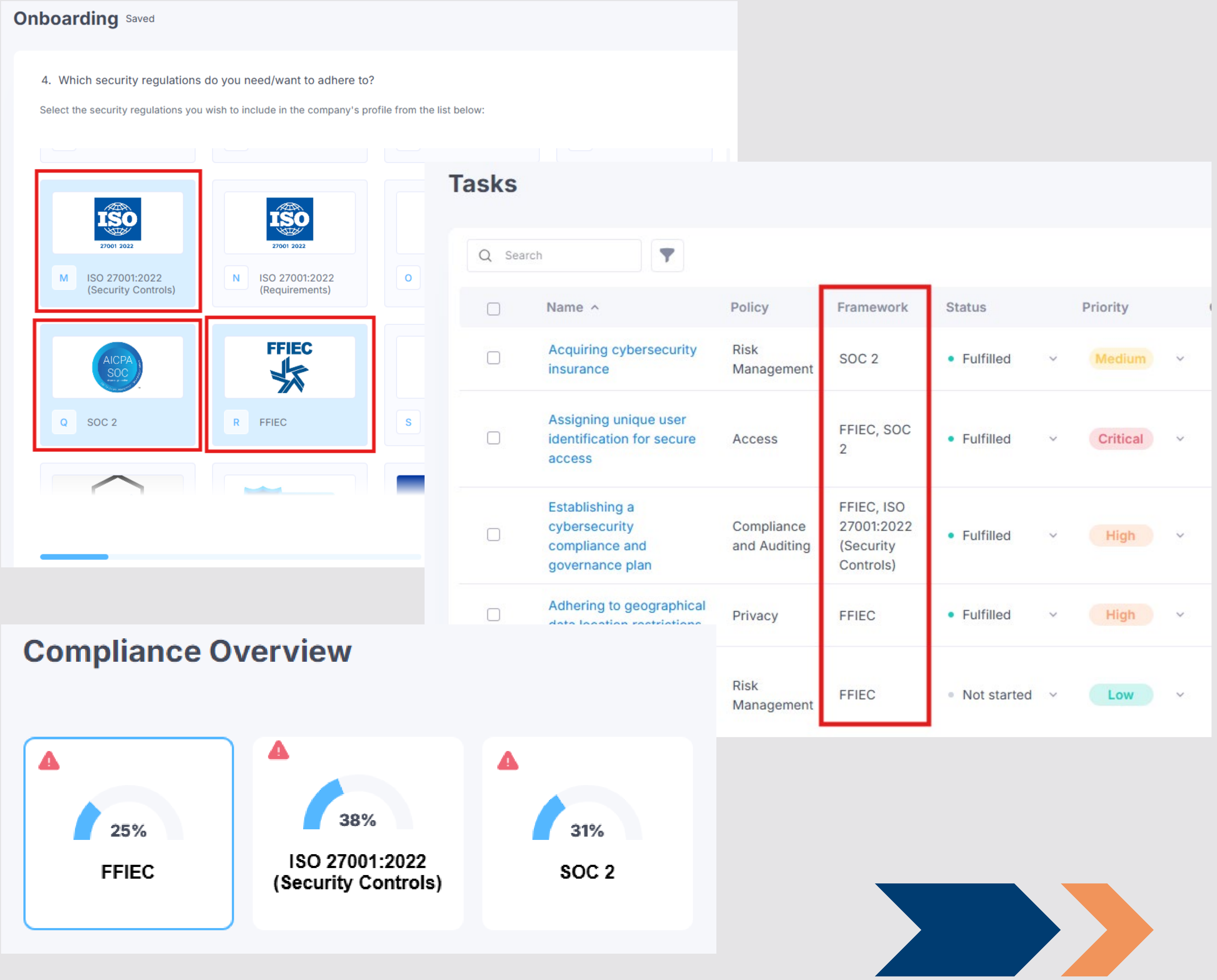
Compliance Overview

37%	26%
CMMC Level 2	NIST CSF 2.0

Compliance Challenges & Solutions

Requirement to comply with multiple evolving regulations and cybersecurity frameworks. Staying current with updates from agencies like FDIC, OCC and NCUA.

- Assess your security posture and track compliance readiness for one or more cybersecurity frameworks.
- Tasks, responses and evidence automatically mapped to framework(s) and controls.
- Over 30 frameworks available in the vCISO platform, automatically tracking changes and flagging new compliance gaps.



Onboarding Saved

4. Which security regulations do you need/want to adhere to?

Select the security regulations you wish to include in the company's profile from the list below:

ISO 27001 2022
M ISO 27001:2022 (Security Controls)
ISO 27001 2022
N ISO 27001:2022 (Requirements)
O
AICPA SOC
Q SOC 2
FFIEC
R FFIEC
S

Tasks

□	Name ^	Policy	Framework	Status	Priority
□	Acquiring cybersecurity insurance	Risk Management	SOC 2	● Fulfilled	Medium
□	Assigning unique user identification for secure access	Access	FFIEC, SOC 2	● Fulfilled	Critical
□	Establishing a cybersecurity compliance and governance plan	Compliance and Auditing	FFIEC, ISO 27001:2022 (Security Controls)	● Fulfilled	High
□	Adhering to geographical	Privacy	FFIEC	● Fulfilled	High
		Risk Management	FFIEC	● Not started	Low

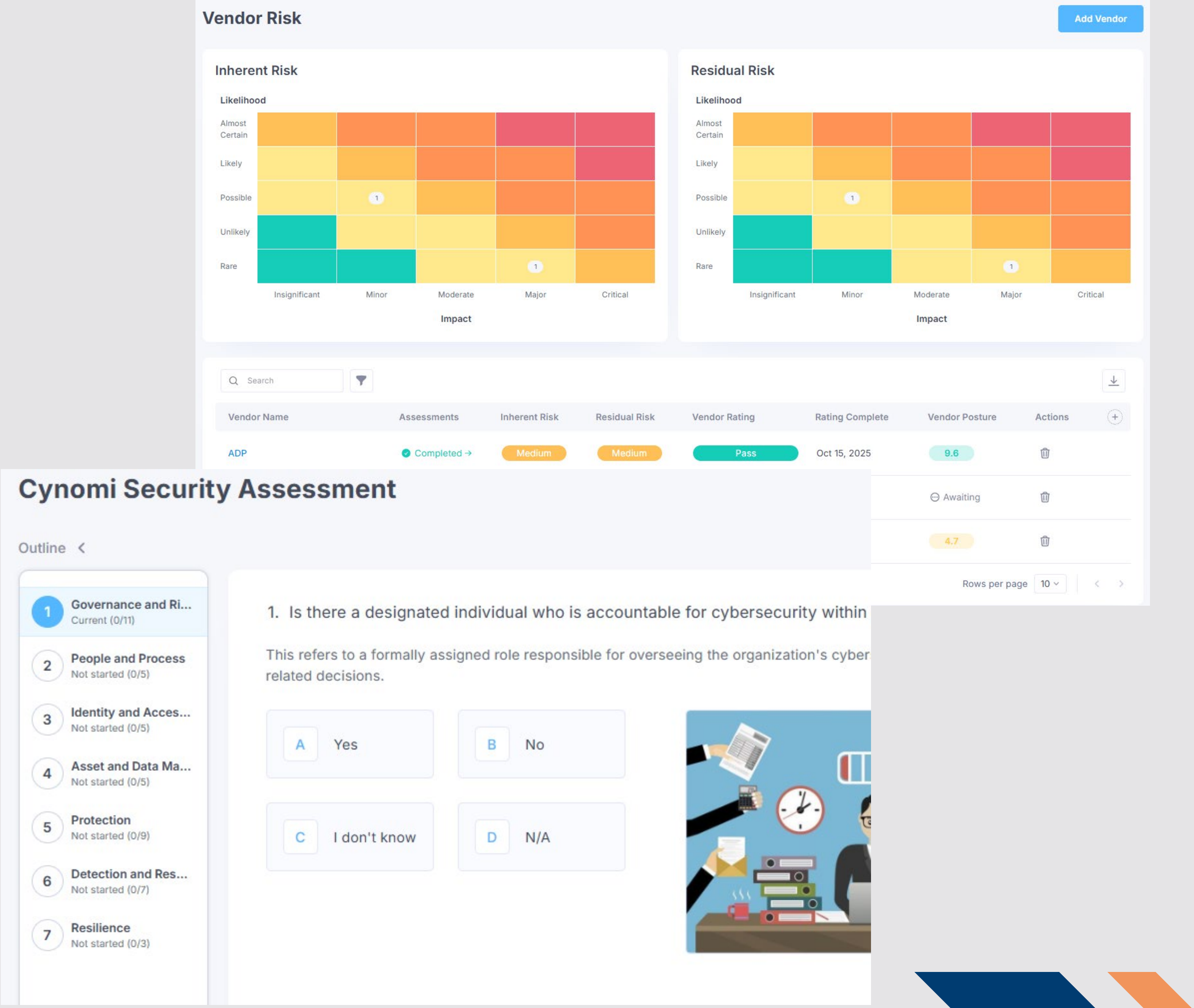
Compliance Overview

Compliance Challenges & Solutions

SECUR-SERV

Third-party vendor oversight and due diligence requirements.

- Impact Assessment – assess the potential impact if the vendor’s security is compromised.
- Security Assessment - streamlined security questionnaire evaluates a vendor’s cybersecurity posture across key areas such as access controls, processes, system management, and incident response.
- Consistent, efficient third-party risk assessments.



Vendor Name	Assessments	Inherent Risk	Residual Risk	Vendor Rating	Rating Complete	Vendor Posture	Actions
ADP	Completed →	Medium	Medium	Pass	Oct 15, 2025	9.6	
						Awaiting	
						4.7	

Rows per page 10

Cynomi Security Assessment

Outline

1 Governance and Ri...
Current (0/11)

2 People and Process
Not started (0/5)

3 Identity and Acces...
Not started (0/5)

4 Asset and Data Ma...
Not started (0/5)

5 Protection
Not started (0/9)

6 Detection and Res...
Not started (0/7)

7 Resilience
Not started (0/3)

1. Is there a designated individual who is accountable for cybersecurity within

This refers to a formally assigned role responsible for overseeing the organization's cyber related decisions.

A Yes

B No

C I don't know

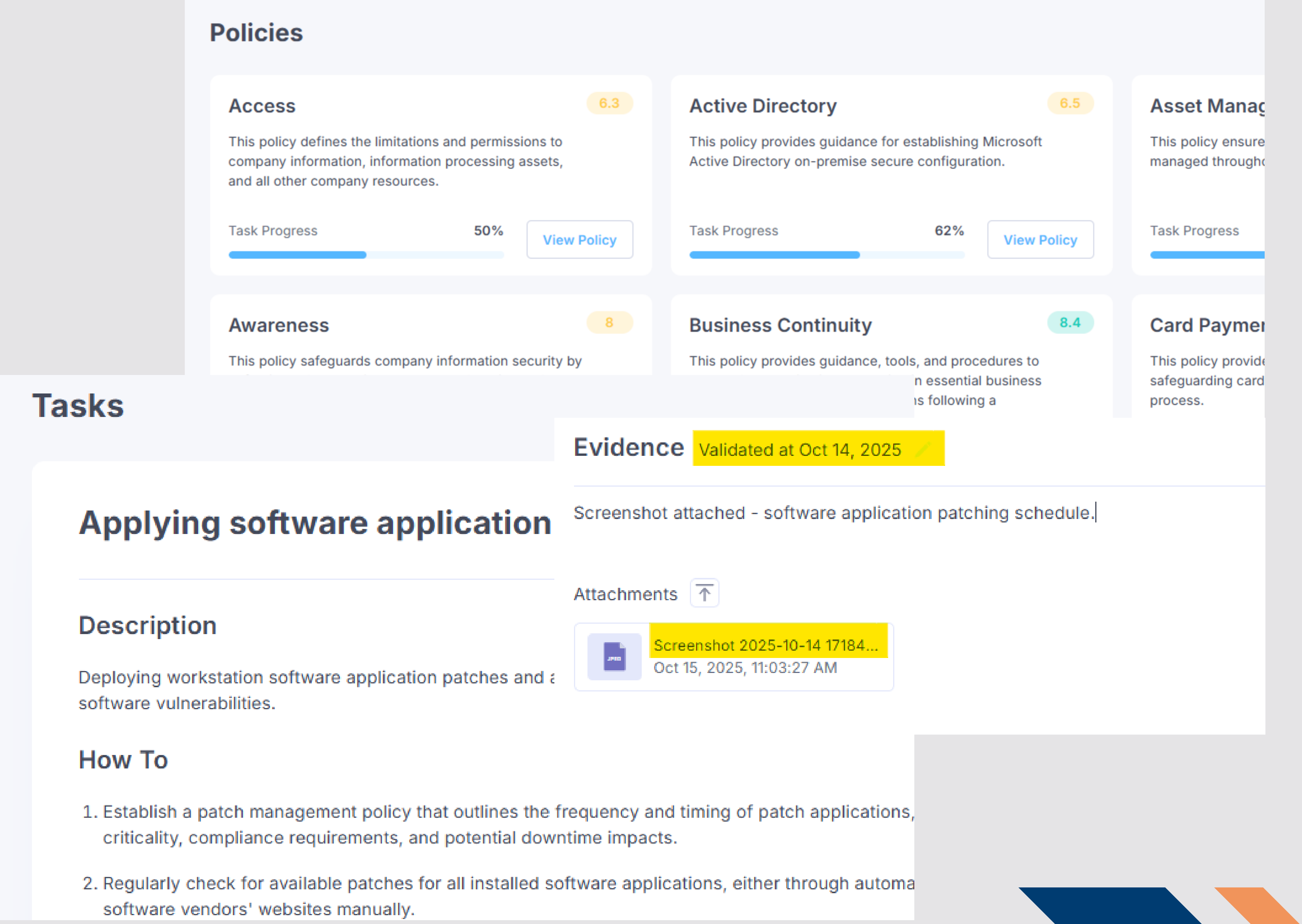
D N/A

Compliance Challenges & Solutions

SECUR-SERV

Inconsistent documentation leading to audit findings or regulatory scrutiny. Regulators expect detailed documentation of cybersecurity policies, risk assessments and controls.

- Policies are automatically generated from answers to assessment questions, linked to supporting tasks and progress is tracked as tasks are completed.
- Add Standard Operating Procedures and organization-specific notes to tasks while tracking status, due dates and dependencies.
- Easily capture and document evidence for any Task by uploading screenshots or other files and providing a validation date.



Policies

Access 6.3
This policy defines the limitations and permissions to company information, information processing assets, and all other company resources.
Task Progress 50% View Policy

Active Directory 6.5
This policy provides guidance for establishing Microsoft Active Directory on-premise secure configuration.
Task Progress 62% View Policy

Asset Manag
This policy ensure
managed through
Task Progress

Awareness 8
This policy safeguards company information security by

Business Continuity 8.4
This policy provides guidance, tools, and procedures to
n essential business
is following a

Card Paymer
This policy provide
safeguarding card
process.

Tasks

Applying software application

Description

Deploying workstation software application patches and a
software vulnerabilities.

How To

1. Establish a patch management policy that outlines the frequency and timing of patch applications, criticality, compliance requirements, and potential downtime impacts.
2. Regularly check for available patches for all installed software applications, either through automa software vendors' websites manually.

Evidence Validated at Oct 14, 2025

Screenshot attached - software application patching schedule.

Attachments

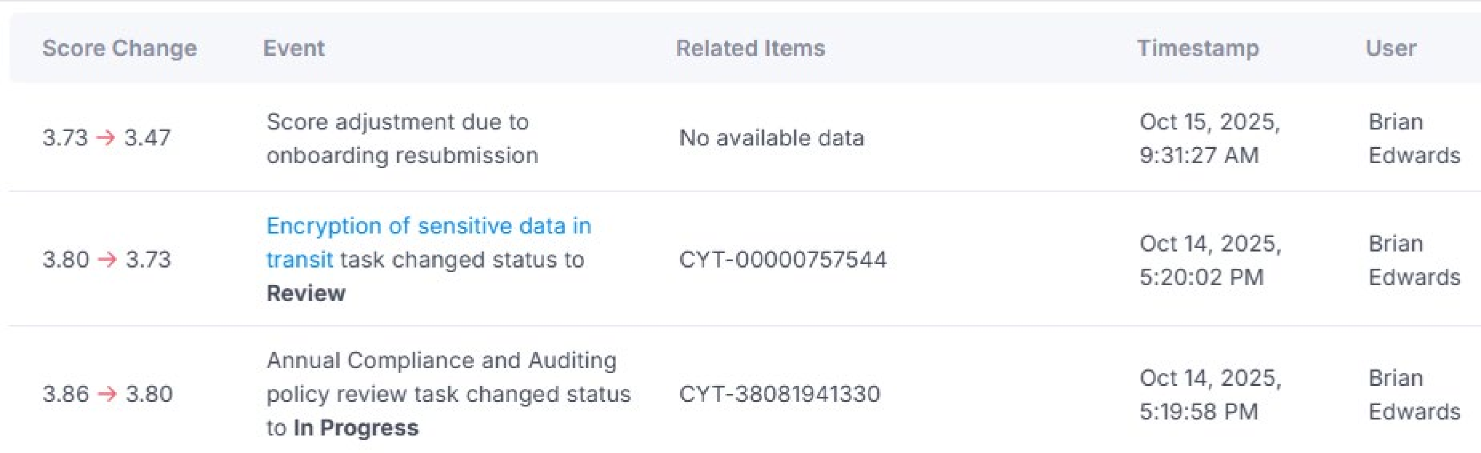
Screenshot 2025-10-14 17184...
Oct 15, 2025, 11:03:27 AM

Compliance Challenges & Solutions

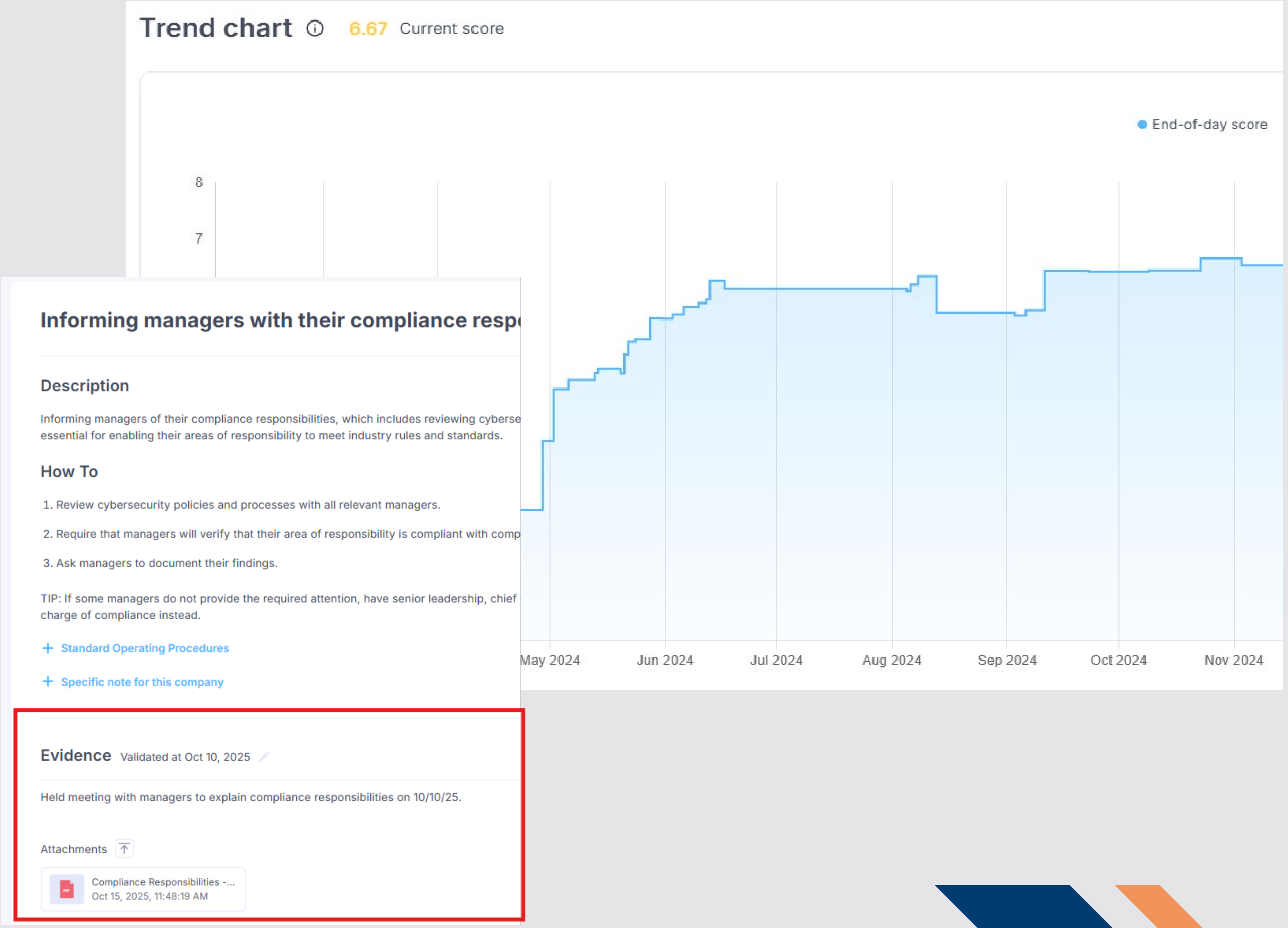
SECUR-SERV

Difficulty retrieving historical data or demonstrating corrective actions.

- View impacts to Posture Score over time, pinpoint date and time and identify details of changes in the event log.
- Update status and record details of work done on each task.



Score Change	Event	Related Items	Timestamp	User
3.73 → 3.47	Score adjustment due to onboarding resubmission	No available data	Oct 15, 2025, 9:31:27 AM	Brian Edwards
3.80 → 3.73	Encryption of sensitive data in transit task changed status to **Review**	CYT-00000757544	Oct 14, 2025, 5:20:02 PM	Brian Edwards
3.86 → 3.80	Annual Compliance and Auditing policy review task changed status to **In Progress**	CYT-38081941330	Oct 14, 2025, 5:19:58 PM	Brian Edwards



Informing managers with their compliance resp

Description

Informing managers of their compliance responsibilities, which includes reviewing cyberse
essential for enabling their areas of responsibility to meet industry rules and standards.

How To

1. Review cybersecurity policies and processes with all relevant managers.
2. Require that managers will verify that their area of responsibility is compliant with comp
3. Ask managers to document their findings.

TIP: If some managers do not provide the required attention, have senior leadership, chief
charge of compliance instead.

+ Standard Operating Procedures

+ Specific note for this company

Evidence Validated at Oct 10, 2025

Held meeting with managers to explain compliance responsibilities on 10/10/25.

Attachments

Compliance Responsibilities -...
Oct 15, 2025, 11:48:19 AM

Cynomi Demonstration

- Report Samples

SECUR-SERV

THANK YOU

SECUR-SERV

Address	2020 S 156th Circle, Omaha, NE
Contact	800-228-3628

www.secur-serv.com