

BUYERS GUIDE

# Meeting and Exceeding Cybersecurity Compliance Standards and Regulations for Optimal Outcomes

VECTRA®

# Cybersecurity Compliance is your ally for high performance and integrity

You can rely on Vectra AI to always meet or exceed all cybersecurity compliance requirements and regulations so you can perform your operations with safety and confidence.



## What compliance means to Vectra AI and our clients:

Adhering all laws & regulations

---

Meeting all industry standards

---

Monitoring and enforcing internal policies that govern the security & privacy of data & systems



## Compliance requirements vary based on:

Your industry

---

Your geographical region

---

The nature of your organization's operations



## Vectra AI compliance ensures that your organization meets specific:

Security, privacy, and data protection requirements

---

Data encryption, access controls & incident response procedures

---

Regulatory reporting

Adhering to compliance standards helps you mitigate risks, protect sensitive information, and demonstrate your commitment to security and privacy best practices.

# Vectra AI SOC 2 Type 2 Compliance Certified

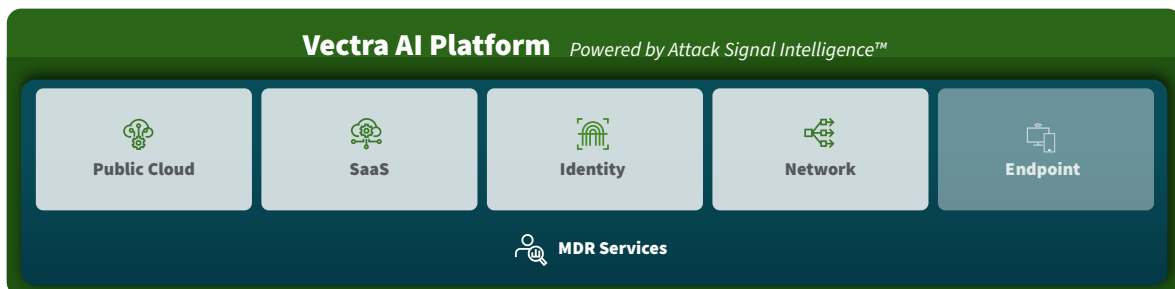
Our commitment to data privacy and protection means peace of mind for your team.

Certification for the Vectra AI Platform (formerly Cognito Detect and Cognito Recall cloud & enterprise software) is a milestone for the company and the NDR industry.

**The SOC 2 certification** is the industry standard for testing and verifying security controls so you can be assured that our internal security policies, procedures, standards, and guidelines have been formally validated by an independent auditing firm.

**Type 2 designation** includes detailed testing of the design and operating effectiveness of a company's controls over a period of time, which helps instill trust and confidence that its systems and data in scope are secured appropriately.

## The Vectra AI Platform:



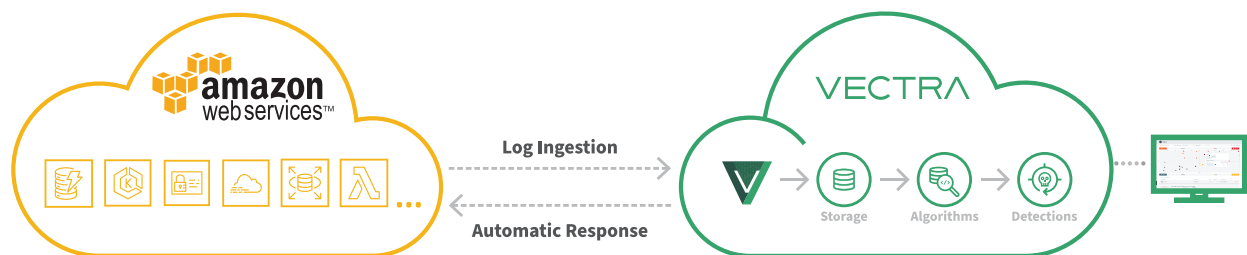
- Surfaces attackers who have circumvented preventative security solutions in cloud and on-premises networks before they can access data and cause damage
- Gives organizations a 360-degree view of historical metadata to spot threats, investigate incidents, and determine common threads between compromised host devices, accounts, and assets

# Vectra AI Detect for Amazon Web Service (AWS)

Vectra AI Detect for Amazon Web Services (AWS) sees and stops attacks targeting an enterprise's AWS footprint in real-time.

Vectra AI ingests AWS CloudTrail management & data event logs from the entire AWS footprint into the Vectra AI secure cloud. It can then run security-led AI detection models on the data and publish threat detections to a Vectra AI-hosted, per-customer, web portal.

Vectra AI is a SOC2 Type 2 compliant organization with our AI Platform (Detect for Network) product and is currently applying these controls for Detect for AWS.



## Collecting only the required data to secure your AWS Footprint

Vectra AI will only monitor customer-approved CloudTrail Logs\*.

## Minimum coverage includes:

- Management events logged by CloudTrail
- Including S3 Data events is recommended for better coverage
- Logs do not contain any Personally Identifiable Information (PII) aside from user email addresses
- You retain complete control over the events sent to Vectra AI

\*Read about the specific permission requirements here: <https://support.Vectra.AI.ai/s/article/KB-VS-1554>

## Keep Complete Control Over Data Transfer

Logs are ingested from your AWS cloud over secure TLSv1.3-encrypted sessions through the AWS Role created for Vectra AI by your AWS admin. Consent is revocable at any time by deleting this role or removing the role's permissions to access S3 data. Once authorization is revoked, log collection will stop immediately.

Vectra AI Detect for AWS will monitor any AWS CloudTrail logs stored in a specified S3 bucket. The cloud logs consist of:

- Management Events (management activity performed by users and services within your AWS environment)
- Data Events (operations performed against specific resources)

## Your Data At Rest, Encrypted And Segregated

Data is received and stored separately per customer. No direct interfaces to access the data for third parties and only Vectra AI Detect applications are authorized to access this data.

As part of the feed, we only retrieve log event objects, as created by AWS CloudTrail and stored in your S3 bucket; we do not ingest company or user data:

- Data at rest is encrypted with Cryptographic Service Provider (CSP) techniques
- Information is only retained for up to 90 days.

## Your Trusted Hosting Environment

Vectra AI cloud services are deployed within Amazon Web Services (AWS) and certified to the highest standards. Read more about AWS compliance programs here: <https://aws.amazon.com/compliance/programs/>

Vectra AI deploys in multiple regions globally to comply with data sovereignty mandates. For example, a customer in EMEA may choose to store and analyze data out of Vectra AI's EU cloud in Dublin only.

Only authorized Vectra AI employees have access to the production Vectra AI cloud for maintenance purposes.



## Secure User Access For The Modern-Day Cloud

End users will only be able to access data through the Vectra AI cloud. Access is limited to registered users, and Multi-Factor Authentication is strictly enforced.

A secure direct link between the Vectra AI Web Portal and a customer's Vectra AI AWS log receivers (sensor) is maintained. This ensures that the Vectra AI Web Portal can only access detections from logs ingested by its paired sensors. Additionally, Vectra AI Detect connectivity is secured through TLSv1.3-encrypted sessions.

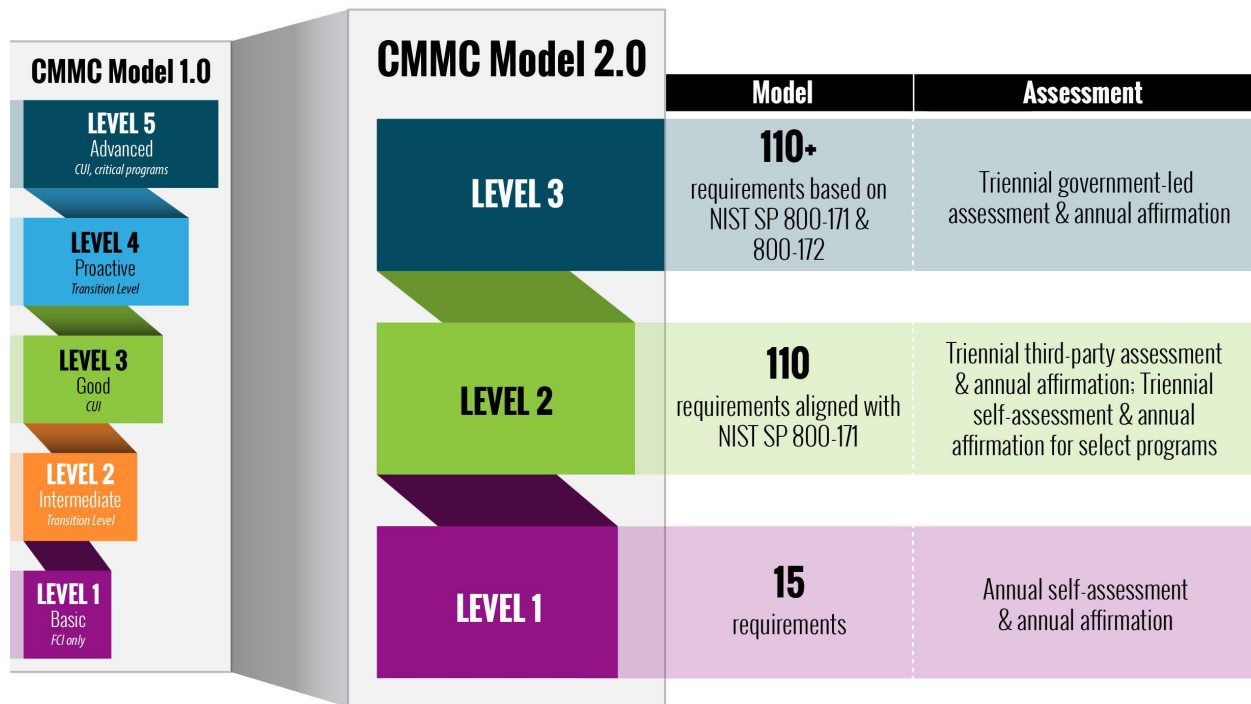
Authorized access to the Vectra AI Detect Web Portal is entirely under the customer's control. No user, including Vectra AI employees, will access the customer web portal or any data within it without explicitly being added as a user to the portal by the customer.

## Maintain Your Privacy & Protecting PII

Vectra AI acts as a data processor for PII on behalf of its customer – the data controller:


- Collects the minimum PII required to discharge its cybersecurity obligations on behalf of the data controller – in this case, the user account name (email ID)
- Does not transfer any PII out of the EU or to any 3rd party organization
- Retains detections and relevant evidence logs for six months, then data is permanently deleted
- Makes all detections and relevant logs available through the product UI in the Vectra AI Web Portal

# Cybersecurity Maturity Model Certification



The Cybersecurity Maturity Model Certification (CMMC) program is aligned to DoD’s information security requirements for DIB partners. It is designed to enforce protection of sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program provides the Department increased assurance that contractors and subcontractors are meeting the cybersecurity requirements that apply to acquisition programs and systems that process controlled unclassified information.

<https://dodcio.defense.gov/CMMC/about/>



# Network and Information Security 2 (NIS2) Compliance Certification

## The NIS (Network and Information Security) Directive

The NIS was the first EU-wide law on cybersecurity (2016) and was intended to achieve a higher and more harmonized level of security for network and information systems across the EU (European Union). Given the ongoing digitalization expansion, the NIS2 is a much-needed update to help organizations become cyber security resilient, and update reporting rules and the costs of not doing so correctly.

**1** **The NIS2 enhances cooperation across the EU.** The establishment of the European Cyber Crises Liaison Organization Network (EU-CyCLONe) supports coordinated management of large-scale cybersecurity incidents at the EU level, strengthening security requirements and focused measures sectors, including:

- Incident response and crisis management
- Vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk management measures
- Basic computer hygiene practices and cybersecurity training
- Effective use of cryptography
- Human resource security
- Access control policies and asset management

## 2 The NIS2 has expanded to eight added sectors, bringing the total to 15.



Providers of public electronic communications networks or services



Food



Postal and courier services



Waste water and waste management



Digital services such as social networking services platforms and data center services



Public administration



Manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals)



Space

## 3 Timeline – Member states have until the end of 2025 to incorporate NIS2 requirements into national law.

## 4 Summary of NIS2

- NIS2 compliance helps to ensure the security and resilience of critical EU information infrastructure, such as energy, transport, and healthcare systems
- The NIS2 directive helps organizations protect themselves against cyberattacks and improve the overall security of the EU's digital landscape
- Failure to comply with NIS2 can result in financial penalties and reputational damage

## 5 How Vectra AI helps you become and stay NIS2 compliant

We make the world a safer place by erasing the unknown with the best [Attack Signal Intelligence™](#) on the planet. We continue to focus our attention on three main deliverables that help organizations like yours rapidly and efficiently detect and respond to cyber threats:

- **Attack Signal Intelligence** – artificial intelligence and algorithms are at the heart of our offering
- **Security Operations Transformation** – helping organizations to meet the challenges of today and tomorrow
- **An AI security platform that's easy to use** – highly automated, integrates with cybersecurity ecosystem partners



# NIS2 (Network and Information Security 2) – A Best Practices Guide

NIS2 is a set of cybersecurity regulations designed to improve the resilience and security of network and information systems across the EU. The law requires organizations that provide essential services, such as energy, finance, healthcare, and transportation, to implement robust cybersecurity measures and report certain types of security incidents. The directive also establishes a cooperation framework between EU member states to share information and coordinate responses to cyber incidents.

## What steps can you take to achieve NIS2 compliance?

### 1 Identify your critical infrastructure:

- Determine which assets are critical to your business operations
- Assess the risks to those critical assets
- Use automated threat detection to identify potential risks and vulnerabilities in real-time

Vectra AI can help you identify your critical infrastructure by continuously monitoring your network and cloud environments, providing real-time visibility into the security posture of your entire infrastructure. Learn more about the [Vectra AI Platform](#).

## 2 Develop an incident response plan to minimize the impact of a security breach:

- Define roles and responsibilities for responding to security incidents
- Establish procedures for reporting and investigating security incidents
- Use threat intelligence to prioritize response efforts and minimize the impact of security incidents

Vectra AI can help you develop an incident response plan by providing real-time threat detection for both known (with Suricata) and unknown threats, automated incident response capabilities, and metadata for forensic analysis to help you quickly detect and respond to security incidents. Learn more about [Vectra AI Attack Signal Intelligence™](#) and Vectra AI Match.

## 3 Conduct regular security assessments to resolve vulnerabilities before they're exploited

- Use vulnerability scanning tools or penetration tests to identify vulnerabilities in your systems
- Conduct red team exercises to identify potential weaknesses in your security defense
- Use automated vulnerability management and patch management tools to quickly remediate identified vulnerabilities

Vectra AI can also assist with security assessments by running regular blue team workshops to identify potential weaknesses. You can also engage other third parties to provide dedicated pen-test services. You can register for a [Vectra AI Blue Team Training Workshop](#).

## 4 Keep your software up to date to protect your systems against known vulnerabilities

- Use automated patch management tools to ensure that all software is up to date
- Use vulnerability management tools to identify and remediate known vulnerabilities
- Implement software whitelisting to prevent unauthorized software from being installed on company devices

Vectra AI regularly releases updates to ensure that the platform is always up to date and protects you against known and unknown threats. Visit the [Vectra AI Support Page](#).

## 5 Train your employees—they're your first line of defense against cyberattacks

- Provide regular cybersecurity training to all employees
- Conduct phishing simulations to test employees' susceptibility to social engineering attacks
- Implement a strong password policy and educate employees on password hygiene

Vectra AI hosts regular webinars focused on informing customers on the latest cyber tech trends and delivers red and blue team workshops to help security professionals hone their cyber defense skills. Visit the [Vectra AI Blog Posts](#).

## 6 Monitor your network for anomalies to detect security breaches as early as possible

- Use behavioral analytics to detect anomalous activity on your network
- Implement intrusion detection and prevention systems to prevent and respond to security incidents Use machine learning algorithms to quickly identify and respond to threats in real-time

Vectra AI can help you monitor your network for anomalies by providing industry-leading Attack Signal Intelligence™, automated incident response capabilities, and behavioral analytics to identify anomalies that may indicate a security breach. Vectra AI can provide coverage for networks, the cloud, SaaS (software as a service), and identity environments. With native integrations to leading EDR (Endpoint Detection and Response) providers, Vectra AI can provide coverage for all five attack surfaces. Vectra AI Extended Managed Detection and Response services are available to help organizations who lack the required resources and skills to deliver a comprehensive internal service.

## 7 Develop a disaster recovery plan to minimize the impact of a security breach

- Define recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical systems.
- Implement data backup and restoration procedures to ensure that critical data can be recovered in the event of a security incident.
- Test your disaster recovery plan regularly to ensure that it is effective and up to date.

Vectra AI can help disaster recovery by providing automated incident response capabilities and forensic analysis to help you quickly detect and respond to security incidents.

Implementing NIS2 requires a comprehensive approach to cybersecurity that includes identifying critical infrastructure, developing an incident response plan, conducting regular security assessments, keeping software up to date, training employees, monitoring the network for anomalies, and developing a disaster recovery plan.

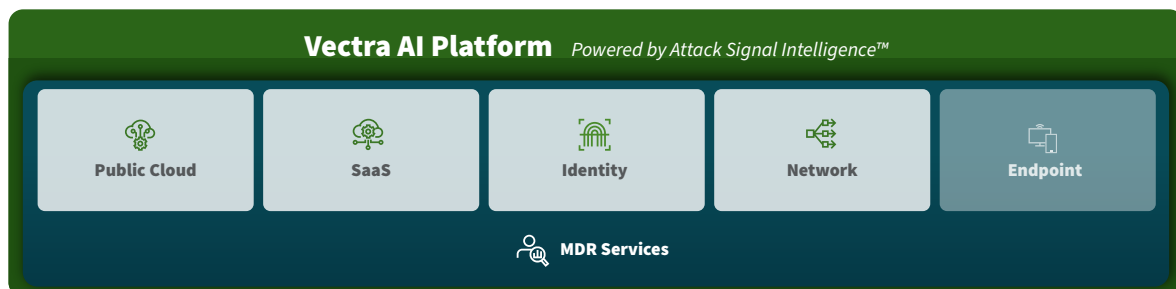
Vectra AI can help your company succeed in implementing NIS2 by providing coverage, clarity, and intelligent control aligned with native integrations with other leading cybersecurity solution vendors such as Microsoft, CrowdStrike, SentinelOne, Splunk, IBM QRadar, Amazon Security Lake, Palo Alto Cortex XSOAR, and many others.

Vectra AI solutions are also available via KPMG, Capgemini, Orange Cyber Defense, AT&T, NTT Data, and Dell technologies.

# The Vectra AI Platform keeps your financial firm in compliance with the NYSDFS Cybersecurity Regulation

The NYSDFS Cybersecurity Regulation, 23 New York Codes, Rules and Regulations (NYCRR) 500 requires New York banks, financial services companies, and insurance companies, including non-New York insurance companies who do business in New York, to perform a cybersecurity risk assessment and to create and maintain a cybersecurity program based on the risk assessment.

The Vectra AI Platform helps your financial firm comply with the 23 NYCRR 500 financial regulations in all the required assessment categories.



The Vectra AI Platform uses a risk-based approach to protect the confidentiality, integrity, and availability of information systems, ultimately protecting consumers and the New York state financial services industry.



# Vectra AI keeps your organization in compliance with GDPR requirements

The Vectra AI platform enhances your cybersecurity team's technical capabilities to comply with the GDPR

- **Deterministic identification of attack behaviors**—such as remote access Trojans, encrypted tunnels, botnet behaviors, ransomware, insider attackers, and targeted advance threats
- **Threat tracking across all phases of an attack**—ranging from command and control (C&C), internal reconnaissance, lateral movement, and, critically for GDPR, data exfiltration behaviors
- **Automated correlation of threats**—with host devices under attack and threat detection details that include host context, packet captures, the seriousness of the threat, and certainty scores
- **Support adaptive cybersecurity**—through an iterative process from the Vectra AI Threat Labs™, a group of highly skilled security researchers
- **Behavioral detection algorithms** that constantly learn from the local environment and global trends
- **Continuous network traffic monitoring**—real-time threat detection, triage, and incident reporting using artificial intelligence and attacker behavior analytics
- **Automated threat detection**—across the enterprise network, from cloud and data center workloads to user and IoT devices

## Key capabilities of the Vectra AI-driven platform include:

- **Continuous monitoring and analysis of all network traffic**—including Internet-bound traffic and internal network traffic between physical and virtual hosts with an IP address – such as laptops, servers, printers, BYOD, and IoT devices – regardless of the device type, operating system or application
- **Real-time visibility into network traffic**—extract metadata from packets rather than performing deep packet inspection allows protection without prying into personal or sensitive payload information
- **Analyze metadata from captured packets**—behavioral detection algorithms spot hidden and unknown attackers, whether traffic is encrypted or not

# Vectra AI Detect for Entra ID (formerly Azure AD) and M365: Security, Privacy, and Compliance

[Vectra AI Detect for Entra ID \(formerly Azure AD\) and M365](#) lets you see and stop threats to your SaaS apps, Entra ID backend, and M365 data to remain in compliance.

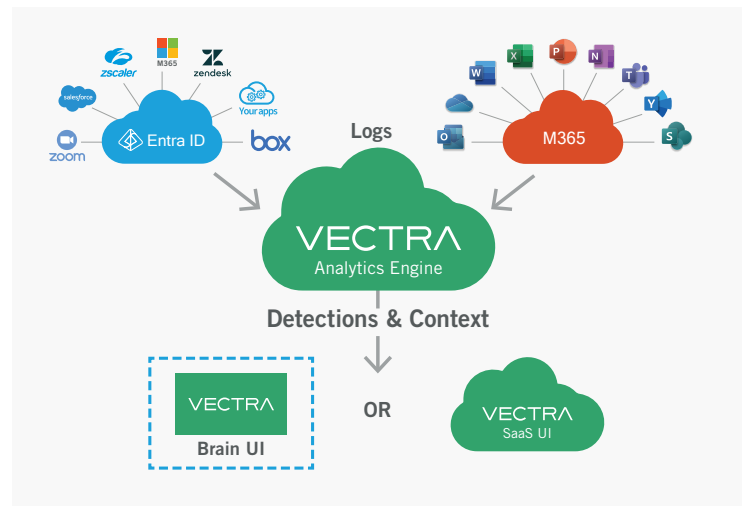
## Vectra AI keeps you in compliance:

- Securely collect Entra ID and M365 logs from the customer's tenant into Vectra AI's secure cloud
  - Run detection models on those logs in Vectra AI's cloud
  - Publish detection events and context into the customer's Vectra AI UI, located on a customer-managed brain (on-premises or virtual) or in Vectra AI's SaaS UI
- Vectra AI cloud services are deployed in the most widely used public cloud providers – namely Microsoft Entra ID and Amazon Web Services (AWS), whose facilities and services are certified to the high standards documented below:

- AWS
- Entra ID

To comply with customers' data sovereignty mandates, Vectra AI deploys in multiple regions globally. For example, a customer may choose to store and analyze data out of Vectra AI's EU cloud in Dublin only.

- Only specific, authorized Vectra AI personnel have access to the production Vectra AI cloud for management purposes
- Vectra AI is a SOC2 Type 2 compliant organization with our Detect for Network product and is currently applying these controls to Detect for Entra ID and M365



## Privacy

Vectra AI acts as a data processor for PII on behalf of its customer – the data controller:

- Collects only the minimum PII required to discharge its cyber-security obligations on behalf of the data controller – in this case, the user account name (email ID)
- Does not transfer any PII out of the EU or to any 3rd party organization
- Retains detections and relevant evidence logs for six months, after which the data is permanently deleted
- Makes all detections and relevant logs available through the Vectra AI UI

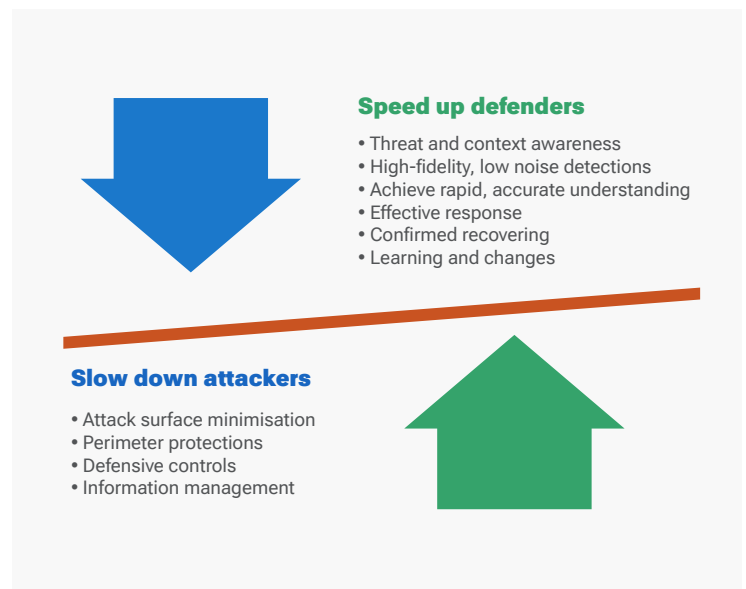
# Pass the (Pen) Test: NDR Insights and Value for Financial Services

## Define and cover areas of security responsibility between cloud service providers (CSP) and FSI through appropriate controls:

- Analyze anonymized metadata shared from hundreds of Vectra AI platform deployments and identify attacker behavioral insights to expose tactics that remain open to abuse.
- The Vectra AI Platform augments the defending “blue team” with high-fidelity attacker TTP behavioral detections which are prioritized by risk/Certainty Index™, profiled by attack type, and the totality of the affected hosts and accounts are displayed as an attack campaign

Regulatory assessment tools such as [CBEST](#) in the UK, the European [TIBER-EU](#), Federal Financial Institutions Examination Council ([FFIEC](#)) in the US, and New York State Department of Financial Services ([NYSDDFS](#)) cybersecurity regulations and frameworks take an intelligence-led approach to identifying salient threats to FSI organizations. They are required to demonstrate the use of independently delivered penetration testing and the ability to protect against identified risks.

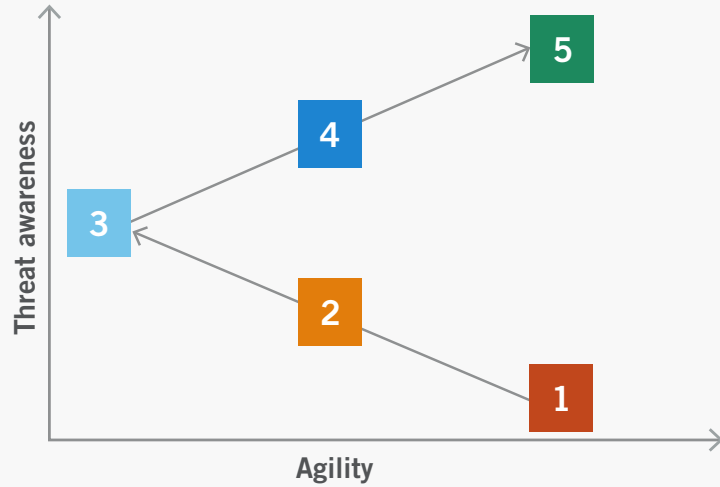
Governments rightly view their financial institutions and systems as part of their nation’s critical national infrastructure (CNI). Additionally, legislative and compliance responsibilities around cybersecurity risk and posture fall on FSI—this includes building and testing organizational resilience.



Identifying potential threats and placing appropriate protective controls are rational first steps but it is important to recognize that persistent, motivated, and skilled attackers will always find a way inside an organization’s digital infrastructure.

The Vectra AI Platform enables financial services security operations and regulatory compliance to:

- Impede the bad, accelerate the good, and prove your capabilities
- Protect shared infrastructures, services, and your digital supply chains
- Detect and defend against Sunburst Supply Chain Attacks
- Accelerate Incident Response maturity
- Enhance threat awareness/visibility
- Accelerate response agility/performance



Maturity	Typical Detection	Typical Response	Risk Awareness
Predictive Defense	Internal (Hunting, Deception) + External	Highly Proactive	Very High
Intelligence Driven	Internal (Hunting) + External	Threat/Adversary Driven	High
Process Driven	Internal (Hunting) + External	Service Driven (SLAs)	Medium
Tool Driven / Signature Based	External	Tool Driven	Low
Reactive / Ad-hoc	External, User Report	Reformat, Reinstall, Restore	Very Low

**About Vectra AI**

Vectra AI is the leader in hybrid attack detection, investigation and response. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Vectra AI’s patented Attack Signal Intelligence empowers security teams to rapidly detect, prioritize, investigate and stop the most advanced hybrid cyber-attacks. With 35 patents in AI-driven detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit [www.vectra.ai](http://www.vectra.ai).