VECTRA®

COMPLIANCE BRIEF

How the Vectra AI Platform meets PCI DSS 4.0 requirements and security assessment procedures

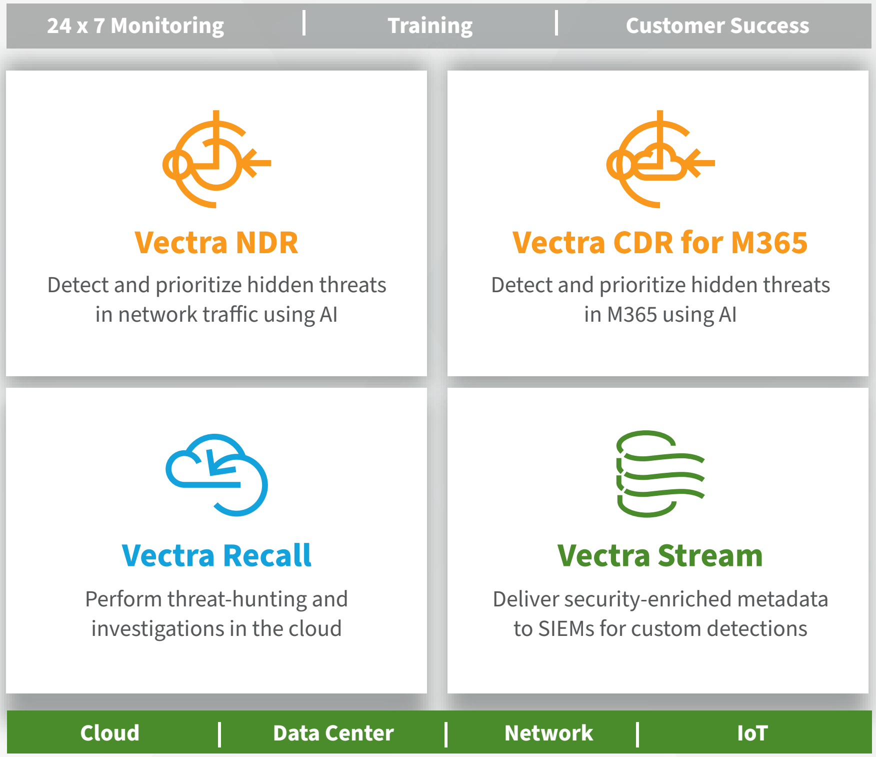
The Vectra® AI platform continuously monitors and analyzes all cloud, data center, IoT and enterprise network traffic to detect and stop in-progress cyberattacks as criminals attempt to steal payment card data, personally identifiable information, and other in-scope assets.

By using data science, machine learning and behavioral traffic analysis, the Vectra AI platform reveals the hidden, fundamental attack behaviors that criminals must perform in order to succeed. Vectra AI-driven Attack Signal Intelligence™ learns normal network traffic patterns host, and account behaviors, which makes malicious attack behaviors stand out – even in encrypted traffic.

Continuously listening and thinking, the Vectra AI platform detects malicious attack behaviors automatically and in real time over hours, days and weeks, correlates those behaviors with hosts and accounts that are under attack, and anticipates the next move of attackers and stops them dead in their tracks.

Cyberattacks are a fact of life. It has become routine to hear about massive credit card number thefts in the news. That's because organizations have multiple vulnerability points:

- Credit card readers
- Point-of-sale systems
- Network and wireless access routers
- Payment card data storage
- Online payment apps and shopping carts
- Shared connections with vendors and partners



24 x 7 Monitoring | Training | Customer Success

Vectra NDR
Detect and prioritize hidden threats in network traffic using AI

Vectra CDR for M365
Detect and prioritize hidden threats in M365 using AI

Vectra Recall
Perform threat-hunting and investigations in the cloud

Vectra Stream
Deliver security-enriched metadata to SIEMs for custom detections

Cloud | Data Center | Network | IoT

With the Vectra AI platform monitoring all network, cloud, and IoT traffic 24x7, organizations can protect their in-scope assets, while demonstrating compliance with Payment Card Industry Data Security Standard (PCI DSS) 4.0 and Payment Application Data Security Standard (PA-DSS) across physical and virtual networks and their individual hosts.

The Vectra AI platform provides real-time insight into advanced persistent threats (APTs). This insight is fully automated with clear, intuitive reports that enable organizations to create a compliance audit trail as they take immediate, decisive action to stop attacks and mitigate their impact.

> Deployed inside the network perimeter and in the cloud, Vectra AI monitors internal (east-west) and internet- bound (north-south) traffic to identify malicious attack behaviors that put in-scope assets at risk.

PCI compliance through real-time, automated threat detection and response

Instead of periodically scanning, Vectra AI continuously monitors all network and cloud traffic. Deployed inside the network perimeter and in the cloud, Vectra AI monitors internal (east-west) and internet- bound (north-south) traffic to identify malicious attack behaviors that put in-scope assets at risk.

Vectra AI uses the network and relevant logs to gain high-fidelity visibility into the actions of all devices and identities – from cloud and data center workloads to user and IoT devices – leaving attackers with nowhere to hide.

Vectra AI also detects attack behaviors in all phases of the attack kill chain – command and control (C&C), internal reconnaissance, lateral movement, ransomware activity, data exfiltration, and botnet monetization behaviors – and across all applications, operating systems and devices.

For example, Vectra AI will detect cyberthieves as they patiently make their way to in-scope assets in the network, persistently track the hosts involved in an attack, and recognize when a specific host or user account is abnormally accessing the cardholder data environment.

Vectra AI detects the presence of remote access tools used in C&C attack communications and recognizes when a host account is abnormally accessing resources such as payment card data.

In addition, Vectra AI tracks normal usage behaviors and detect when a trusted user's credentials are compromised by an attacker.

Vectra AI also provides multiple early-warning opportunities to detect ransomware, other malware variants and malicious activity that precede an attack on any network device, including devices that may not be able to run antivirus software.

This includes the ability to detect malware on mobile smart devices, servers using any operating system, and point-of-sale terminals. Vectra AI learns the traffic patterns and behaviors that are typical to a network, while remembering and correlating anomalous behaviors it has previously seen.

Protect cardholder data with Security that thinks®

It's time for security to get smarter. Attackers are already in your network, looking for an opportunity to steal high-value payment card data. The Vectra AI platform does the hard work by recognizing cyberthreats amid the normal chatter in your network and anticipating the next move of attackers in real time so they can be stopped.

HOW VECTRA ADDRESSES PCI DSS 4.0 COMPLIANCE

Addressing PCI DSS requirements for sections 1 and 2

1.3.2	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**Vectra AI monitors internal traffic to automatically detect signs of data exfiltration to the internet and multistage transfers.**
1.3.2.b	Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	**Vectra AI analysis of outbound traffic provides additional coverage by detecting the use of approved ports protocols, including HTTP, HTTPS and DNS being used as hidden tunnels to exfiltrate data.**
2.2.7	Review services and parameter files on systems to determine that Telnet and other insecure remote login commands are not available for non-console access.	**Vectra AI automatically detects the presence of external remote access, regardless of the type of application, to find unauthorized remote access and malicious remote administration tools.**

Addressing PCI DSS requirements for sections 3 and 5

3.6.1	Restrict access to cryptographic keys to the fewest number of custodians necessary.	**Vectra AI automatically tracks the behavior of physical hosts and recognizes when a specific host or user account is abnormally accessing resources such as cryptographic keys.**
5.2	Deploy anti-virus software on all systems commonly affected by malicious software. Malicious software (malware) is prevented, detected and addressed.	**Vectra AI analyzes all network traffic to reveal the behaviors of all variants of malware – including ransomware – even when the malware is customized to intentionally avoid detection by signature or the malware is new and unknown. Vectra AI detects botnet behavior, hidden command-and-control traffic, the internal propagation of worms, and various attacker tools such as remote administration tools.**
5.2.2	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. Replace anti-virus with anti-malware and malicious software with malware.	
5.2.3	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. Replace malicious software with malware, and anti-virus with anti-malware.	**Vectra AI uses network-based behavioral analysis to detect the presence of malware or malicious activity on any network device, including devices that may not be able to run antivirus software. Vectra AI detects malware on mobile smart devices, servers using any operating system, point-of-sale terminals, and Internet-of-Things devices such as cameras, printers, or control systems.**

HOW VECTRA ADDRESSES PCI DSS 4.0 COMPLIANCE

Addressing PCI DSS requirements for Section 6

6.3.1.a	Examine policies and procedures to verify that processes are defined: • To identify new security vulnerabilities. • To assign a risk ranking to vulnerabilities. • To use reputable outside sources for security vulnerability information.	**Vectra AI monitors the behavior of network traffic to proactively recognize when a device may have been compromised before the vulnerability becomes known to the industry. In addition, Vectra AI can identify the act of an attacker scanning the network or a specific host for vulnerabilities.**
6.5.1	Change control procedures must include: • Documentation of impact • Documented change approval by authorized parties • Functionality testing to verify that the change does not adversely impact the security of the system • Back-out procedures	**Vectra AI automatically identifies hygiene issues in the network that can introduce risk, impair performance or provide opportunities for attackers to hide. Vectra AI alerts IT security teams about unnoticed errors that may have been introduced during a system update.**
6.5.2	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	
6.2.4	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**Vectra AI analyzes internal traffic to recognize the signs of SQL injection attempts, even if the particular exploit or vulnerability is unknown.**

Addressing PCI DSS requirements for Section 7

7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	**Vectra AI automatically tracks the behavior of physical hosts on the network and recognizes when a specific host or user account is abnormally accessing the cardholder data environment.**
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	

HOW VECTRA ADDRESSES PCI DSS 4.0 COMPLIANCE

Addressing PCI DSS requirements for Section 8

8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components	**Vectra AI automatically tracks the behavior of physical hosts on the network and recognizes when a specific host or user account is abnormally accessing resources. This audit trail identifies when a user begins to behave abnormally and signs of credential abuse if an authorized user has been compromised.**
8.2.2	Do not use group, shared, or generic IDs, passwords.	**Vectra AI continuously tracks the internal Kerberos infrastructure to understand normal usage in terms of the physical host, user account and services requested. Kerberos client anomalies can identify when a user's credentials are compromised and when multiple user devices begin sharing access information.**
8.2.2.a	For a sample of system components, examine user ID lists to verify: • Generic user IDs are disabled or removed. • Shared user IDs for system administration activities and other critical functions do not exist. • Shared and generic user IDs are not used to administer any system components.	
8.2.7	Manage IDs used by third parties to access, support, or maintain system components via remote access	**Vectra AI automatically detects and tracks the presence of external remote access and remote administration tools, regardless of the type of application.**
8.3.4	Limit repeated access attempts by locking out the user ID after not more than ten attempts	**Vectra AI automatically detects and tracks brute-force attempts against passwords, as well as scanning for commonly used accounts or services.**

Addressing PCI DSS requirements for Section 10

10.2.1	Implement audit trails to link all access to system components to each individual user. Verify that: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users.	**Vectra AI continuously tracks the internal Kerberos infrastructure to understand normal usage in terms of the physical host, user account, and services requested. Kerberos client anomalies can identify when a user's credentials are compromised and when multiple user devices begin sharing access information.**
10.2.1	Implement automated audit trails for all system components to reconstruct events	
10.2.1.1	Verify all individual access to cardholder data is logged.	

HOW VECTRA ADDRESSES PCI DSS 4.0 COMPLIANCE

Addressing PCI DSS requirements for Section 10

10.2.1.4	Invalid logical access attempts	**Vectra AI automatically detects brute-force attacks, as well as user and service scans.**
10.2.1.5	Use of and changes to identification and authentication mechanisms.	**Vectra AI behavioral analysis of the Kerberos infrastructure reveals when an attacker is using or impersonating a valid account.**
10.2.1.5	Verify use of identification and authentication mechanisms is logged.	
10.4.1	Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system	**Vectra AI automatically logs and reports all signs of an attack, including ransomware activity, command-and-control communication, internal reconnaissance, lateral movement, and data exfiltration. This detection can be based on the direct detection of attacker behaviors and tools, the identification of malicious behavior or locally learned baselines.**
10.4.1.a	Examine security policies and procedures to verify that procedures are defined for reviewing all security events at least daily, either manually or via log tools.	
10.4.3	Follow up on exceptions and anomalies identified during the review process.	**Vectra AI automatically identifies anomalies and threats, correlates them to physical host devices, prioritizes the physical host devices with threats that pose the greatest risk, and provides IT security teams with supporting data and recommended next steps. Vectra AI also allows all hosts in a PCI architecture to be identified and automatically reports all detections on those key assets.**
10.4.3.a	Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process.	

HOW VECTRA ADDRESSES PCI DSS 4.0 COMPLIANCE

Addressing PCI DSS requirements for Section 11

11.4	Implement a methodology for penetration testing.	**Vectra AI monitors internal and Internet-bound network traffic to identify the techniques performed by a penetration test. Vectra AI provides a real-time dashboard for security "blue team" staff who are charged with detecting and validating the work of the penetration testers or "red team."**
11.4.3	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**Vectra AI monitors internal and external traffic to identify the techniques performed by a penetration test. Vectra AI provides a real-time dashboard for security "blue team" staff who are charged with detecting and validating the work of the penetration testers or "red team."**
11.4.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification.	**Vectra AI monitors internal and Internet-bound network traffic to identify the techniques performed by a penetration test. Vectra AI provides a real-time dashboard for security "blue team" staff who are charged with detecting and validating the work of the penetration testers or "red team."**
11.5	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	**Vectra AI provides highly advanced network-based threat detection that identifies all phases of attack without the need for signatures or reputation lists. By detecting the fundamental behaviors of attackers, Vectra AI detects ransomware and other malware variants as well as attacker tools, even if they are unknown to the security industry.**
11.5.1.1	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	**Vectra AI monitors internal and Internet-bound traffic to identify Command & Control (C2) infrastructure within the customers' network environments. This includes C2 that may originate from Vectra AI infrastructure. In the event that any such C2 is detected, the customer is alerted to investigate and take corrective action.**

Addressing PCI DSS requirements for Section 12

12.1	Develop and examine usage policies for critical technologies and define proper use of these technologies, including remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.	**Vectra AI maintains consistent tracking and behavior history associated with physical host devices on the network. This physical identity remains intact even if the IP address of the device changes or multiple users use the device. Vectra AI automatically detects if the device is compromised with a backdoor or begins behaving abnormally.**
12.5.1	Develop a method to accurately and readily determine owner, contact information, and purpose.	

HOW VECTRA ADDRESSES PCI DSS 4.0 COMPLIANCE

Addressing PCI DSS requirements for Section 12

12.8.1	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	**Vectra AI automatically tracks and logs external remote access of all types. Custom rules allow staff to identify proper usage of external remote access, while continuing to log and monitor the behavior.**
12.10.1	Implement an incident response plan. Be prepared to respond immediately to a system breach.	**Vectra AI provides real-time automated analysis and investigation to enable rapid incident response. This ensures that incident response activities occur in real-time and are not dependent on a security analyst or third-party incident response firm.**
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	**Vectra AI provides highly advanced network-based threat detection that identifies all phases of attack without signatures or reputation lists. Alerts are delivered via syslog to virtually any syslog-capable system. Email alerts and reports can also be delivered to staff based on policy.**

For more information please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai

© 2023 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, and Security that thinks are registered trademarks and Vectra Detect, Vectra Recall, Vectra Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

Version: **092623**