VECTRA®

# How Cognito meets PCI DSS 3.2 requirements and security assessment procedures

The Cognito™ automated threat detection and response platform from Vectra® continuously monitors and analyzes all network traffic to detect cyber attacks in progress 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, Cognito reveals the hidden, fundamental attack behaviors that criminals must perform in order to succeed. The intelligence in Cognito learns normal network traffic patterns and host behaviors, which makes malicious attack behaviors stand out – even in encrypted traffic.

Continuously listening and thinking, Cognito detects malicious attack behaviors automatically and in real time over hours, days and weeks, correlates those behaviors with hosts that are under attack, and anticipates the next move of attackers.

Cyber attacks 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

With Cognito monitoring all network traffic 24x7, organizations can protect their in-scope assets, while demonstrating compliance with Payment Card Industry Data Security Standard (PCI DSS) v3.2 and Payment Application Data Security Standard (PA-DSS) across physical and virtual networks and their individual hosts.

Cognito 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.

## PCI compliance through real-time, automated threat detection

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

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

Cognito 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, Cognito will detect cyber thieves 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.

Cognito 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, Cognito tracks the internal Kerberos infrastructure to understand normal usage behaviors and detect when a trusted user's credentials are compromised by an attacker.

Cognito 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. Cognito 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. Cognito does the hard work by recognizing cyber threats amid the normal chatter in your network and anticipating the next move of attackers in real time so they can be stopped.

## HOW COGNITO ADDRESSES PCI DSS V3.2 COMPLIANCE

### Addressing PCI DSS requirements for sections 1 and 2

| | |
|---|---|
| **1.3.4** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | Cognito monitors internal traffic to automatically detect signs of data exfiltration to the Internet and multistage transfers. |
| **1.3.4** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. | Cognito 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. |
| **2.3.b** Review services and parameter files on systems to determine that Telnet and other insecure remote login commands are not available for non-console access. | Cognito 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

| | |
|---|---|
| **3.5.2** Restrict access to cryptographic keys to the fewest number of custodians necessary. | Cognito automatically tracks the behavior of physical hosts and recognizes when a specific host or user account is abnormally accessing resources such as cryptographic keys. |
| **5.1** Deploy anti-virus software on all systems commonly affected by malicious software.<br><br>**5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | Cognito 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. Cognito detects botnet behavior, hidden command-and-control traffic, the internal propagation of worms, and various attacker tools such as remote administration tools. |
| **5.1.2** 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. | Cognito 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. Cognito 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. |

### Addressing PCI DSS requirements for Section 6

| | |
|---|---|
| **6.1.a** Examine policies and procedures to verify that processes are defined:<br><br>• To identify new security vulnerabilities.<br>• To assign a risk ranking to vulnerabilities.<br>• To use reputable outside sources for security vulnerability information. | Cognito 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, Cognito can identify the act of an attacker scanning the network or a specific host for vulnerabilities. |
| **6.4.5** Change control procedures must include:<br><br>• Documentation of impact<br>• Documented change approval by authorized parties<br>• Functionality testing to verify that the change does not adversely impact the security of the system<br>• Back-out procedures<br><br>**6.4.6** 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. | Cognito automatically identifies hygiene issues in the network that can introduce risk, impair performance or provide opportunities for attackers to hide. Cognito alerts IT security teams about unnoticed errors that may have been introduced during a system update. |

## HOW COGNITO ADDRESSES PCI DSS V3.2 COMPLIANCE

### Addressing PCI DSS requirements for Section 6

| | |
|---|---|
| **6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | Cognito 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.<br><br>**7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | Cognito 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. |

### 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 | Cognito 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. |
| **8.1.5** Manage IDs used by third parties to access, support, or maintain system components via remote access | Cognito automatically detects and tracks the presence of external remote access and remote administration tools, regardless of the type of application. |
| **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts | Cognito automatically detects and tracks brute-force attempts against passwords, as well as scanning for commonly used accounts or services. |
| **8.5** Do not use group, shared, or generic IDs, passwords.<br><br>**8.5.a** For a sample of system components, examine user ID lists to verify:<br><br>• Generic user IDs are disabled or removed.<br>• Shared user IDs for system administration activities and other critical functions do not exist.<br>• Shared and generic user IDs are not used to administer any system components. | Cognito 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. |

### Addressing PCI DSS requirements for Section 10

| | |
|---|---|
| **10.1** Implement audit trails to link all access to system components to each individual user. Verify that:<br><br>• Audit trails are enabled and active for system components.<br>• Access to system components is linked to individual users.<br><br>**10.2** Implement automated audit trails for all system components to reconstruct t events<br><br>**10.2.1 and 10.2.2** Verify all individual access to cardholder data is logged. | Cognito 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. |
| **10.2.4** Invalid logical access attempts | Cognito automatically detects brute-force attacks, as well as user and service scans. |
| **10.2.5** Use of and changes to identification and authentication mechanisms.<br><br>**10.2.5.a** Verify use of identification and authentication mechanisms is logged. | Cognito behavioral analysis of the Kerberos infrastructure reveals when an attacker is using or impersonating a valid account. |
| **10.6.1** Review the following at least daily:<br><br>• All security events<br>• Logs of all system components that store, process, or transmit CHD and/or SAD<br>• Logs of all critical system components<br>• Logs of all servers and system<br><br>**10.6.1.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. | Cognito 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. |
| **10.6.3** Follow up on exceptions and anomalies identified during the review process.<br><br>**10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. | Cognito 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. Cognito also allows all hosts in a PCI architecture to be identified and automatically reports all detections on those key assets. |

## HOW COGNITO ADDRESSES PCI DSS V3.2 COMPLIANCE

### Addressing PCI DSS requirements for sections 11 and 12

| | |
|---|---|
| **11.3** Implement a methodology for penetration testing. | Cognito monitors internal and Internet-bound network traffic to identify the techniques performed by a penetration test. Cognito 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." |
| **11.3.1** 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). | Cognito monitors internal and external traffic to identify the techniques performed by a penetration test. Cognito 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." |
| **11.3.2** Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification. | Cognito monitors internal and Internet-bound network traffic to identify the techniques performed by a penetration test. Cognito 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** 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. | Cognito 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, Cognito detects ransomware and other malware variants as well as attacker tools, even if they are unknown to the security industry. |
| **12.3** 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.<br><br>**12.3.4** Develop a method to accurately and readily determine owner, contact information, and purpose. | Cognito 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. Cognito automatically detects if the device is compromised with a backdoor or begins behaving abnormally. |
| **12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | Cognito 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** Implement an incident response plan. Be prepared to respond immediately to a system breach. | Cognito 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. | Cognito 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. |

VECTRA®
Security that thinks®

**Email** info@vectra.ai **Phone** +1 408-326-2020
vectra.ai