WHITE PAPER

PALO ALTO NETWORKS CORTEX XDR AND PCI COMPLIANCE

A QUALIFIED SECURITY ASSESSOR (QSA) PERSPECTIVE

RYAN MCGOVERN | SENIOR CONSULTANT | PCI-QSA

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Organizations that process, transmit, or store payment card data are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) on an ongoing basis. For organizations to meet these security requirements, they must deploy security measures across all the components of the network and systems that process, store, or transmit payment card information. Merchants as well as Payment Card Service Providers are required to attest to compliance with requirements of the PCI DSS annually.

INTRODUCTION

The intent of this white paper is to provide information to IT professionals implementing Palo Alto Networks Cortex XDR within a Cardholder Data Environment (CDE), as well as a Qualified Security Assessor (QSA) tasked with assessing them. Palo Alto Networks Cortex XDR features and published controls were compared with the PCI DSS 3.2.1 and analyzed for meeting or supporting compliance requirements. The Detailed Notes section reports how these controls meet or support PCI compliance.

Requirements that are not relevant for use of the Palo Alto Networks Cortex XDR product, features, or controls were omitted from the published detailed analysis in the interest of brevity. Furthermore, Palo Alto Networks Cortex XDR controls were not independently tested and validated by Coalfire. The opinions in this whitepaper represent Coalfire's judgment of documented Cortex XDR features and controls, from published information sources supplied by Palo Alto Networks.

PALO ALTO NETWORKS CORTEX XDR OVERVIEW

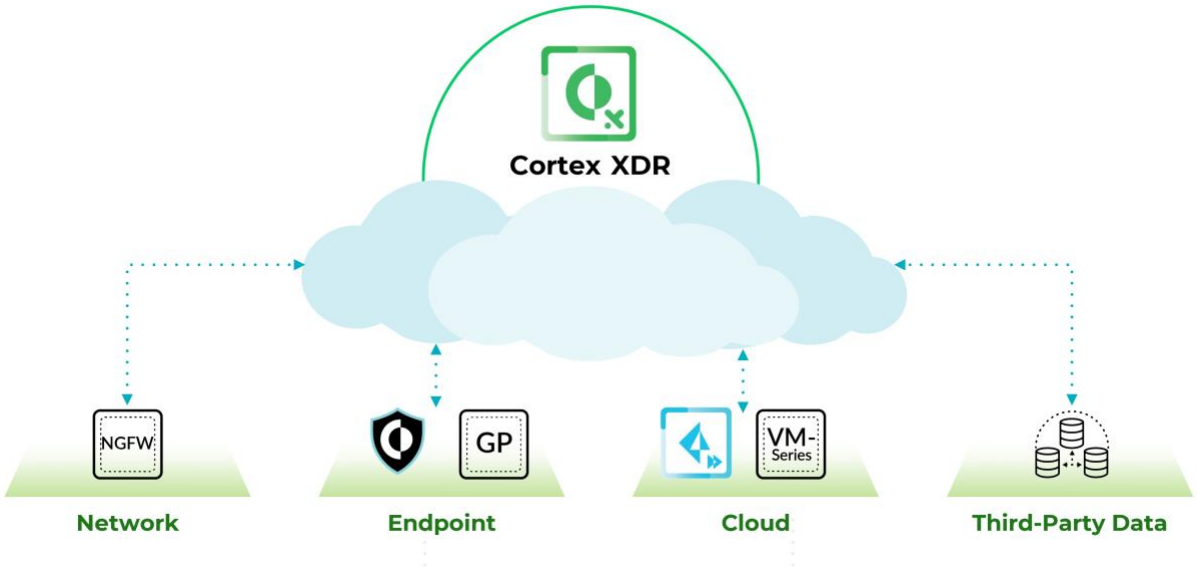

Figure 1: Cortex XDR Diagram

Palo Alto Networks Cortex XDR is a detection and response platform that integrates endpoint, network, and cloud data to protect against attacks. The platform applies machine learning across these data types to offer capabilities that go beyond the traditional Endpoint Detection and Response (EDR) approach of only using endpoint data to identify and respond to threats. At a high level, Palo Alto Networks Cortex XDR delivers detection and investigation features, endpoint protection capabilities, and options to benefit from partner-delivered Managed Detection & Response (MDR) services. Palo Alto Networks Cortex XDR delivers this extensive EDR approach with a single agent and multiple prevention engines.

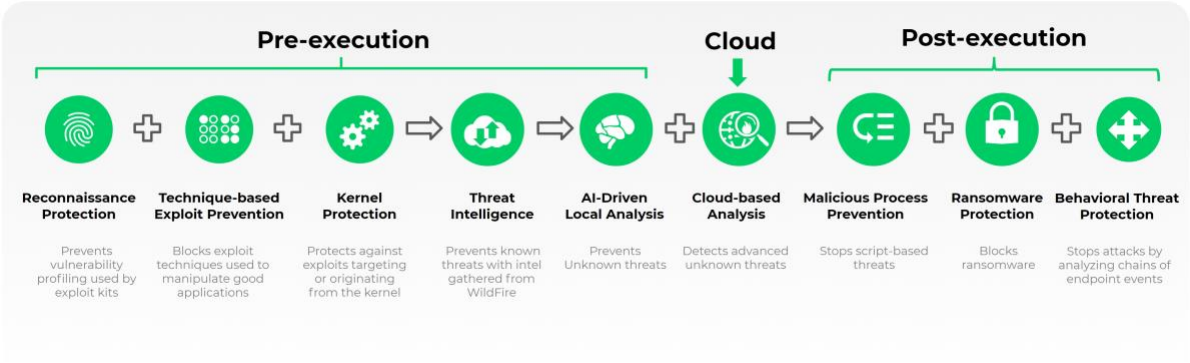

Figure 2: Cortex XDR Engines

Palo Alto Networks Cortex XDR protects endpoints from malware, exploits, and fileless attacks with a single agent by leveraging multiple prevention engines. Prevention engines include:

- AI-driven local analysis to block malware prior to execution.
- WildFire integration for deep inspection of unknown files and intelligence distribution across Cortex XDR endpoint agents, Palo Alto Networks Next-Generation Firewalls (NGFWs), and cloud infrastructure.
- Behavioral threat protection to examine behavior of multiple related processes to protect against malware and fileless attacks.
- Behavior-based ransomware protection to detect processes attempting to modify or encrypt files.
- Credential theft protection to prevent tools from accessing system passwords.

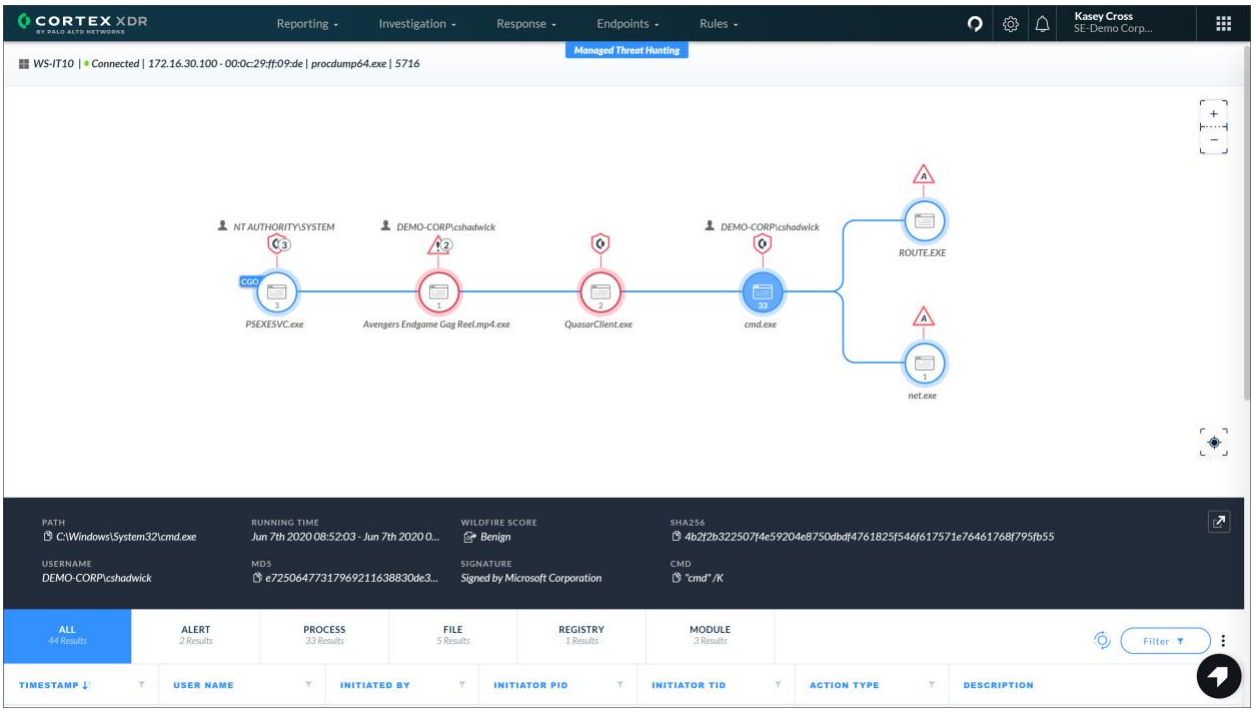

Figure 3: Root Cause Analysis

The design of Cortex XDR makes it capable of immediately blocking an exploit attempt, terminating the process, and generating alerts. For each blocked attack, the Palo Alto Networks Cortex XDR agent collects detailed forensics which are reported and viewable within the Cortex XDR Web-Based Management Interface. As shown in Figure 3, organizations gain detailed insight on attacks which is useful for investigation and triage activities. Within the Palo Alto Networks Cortex XDR Web-Based Management Interface, there are many other modules available that organizations may use for compliance and/or security. For the purposes of this PCI-focused whitepaper, some key features and capabilities to note include:

- Host Firewall
- Endpoint Detection and Response (EDR)
- Disk Encryption with BitLocker
- Malware, Ransomware, and Fileless Attack Prevention
- Agent Upgrades
- Network isolation, quarantine, process termination, file deletion, file blacklist
- Exploit prevention by exploit technique
- Schedule and On-Demand Malware Scanning
- Indicators of Compromise (IOC) and Behavioral Indicators of Compromise (BIOC) rules
- Outbound Integrations (e.g. Slack, ticketing systems)
- Partner-Delivered MDR Services for 24/7 year-round monitoring and alert management
- 30-day to unlimited data storage

PALO ALTO NETWORKS CORTEX XDR AGENTS

Currently, Palo Alto Networks Cortex XDR supports multiple endpoints across various operating systems including Windows, macOS, Linux, Chrome OS, and Android operating systems. Palo Alto Networks Cortex XDR supports these various endpoint operating systems with the following Cortex XDR agents (formerly Traps agents):

- Traps 5.0
- Traps 6.1
- Cortex XDR 7.0
- Cortex XDR 7.1

Cortex XDR agents are installed on endpoints to protect them from known and unknown malware and malicious behavior and techniques through local analysis on the endpoint as well as by consuming WildFire threat intelligence. All endpoint activity reported by the Cortex XDR agents may be viewed in Cortex Data Lake, a cloud-based centralized log collection and storage infrastructure.

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

The PCI DSS is a framework of information security requirements that enforce the minimal set of information security controls necessary to protect an environment of computer systems that process, store, or transmit cardholder data.

Any organization that processes, stores, or transmits cardholder data must comply with the PCI DSS and must attest to their compliance annually. Currently, organizations are required to comply with the PCI DSS version 3.2.1 as of June 2018.

The PCI DSS framework is composed of twelve requirements and each requirement has multiple sub-requirements that provide a detailed description of the control as well as its verification procedures. The PCI DSS requires that organizations define their cardholder data environment (CDE) and that the requirements of the PCI DSS be assessed against the organization's cardholder data environment.

PCI DSS V3.2.1 DETAILED NOTES

KEY DEFINITIONS

Meets PCI: For the PCI DSS requirements listed below, Palo Alto Networks Cortex XDR only meets the intent of the PCI DSS requirement if it is installed and configured properly. See the 'Comment/Explanation' column for additional information about supported features and limitations.

Supports PCI: Palo Alto Networks Cortex XDR is equipped with capabilities which allow it to support compliance with the PCI DSS requirement but does not directly meet the PCI DSS requirement.

REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

PCI Requirement	Comment/Explanation	Meets/Supports PCI
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running.	The Cortex XDR Host Firewall feature may be used only on Windows endpoints which are running Cortex XDR agent 7.1 or later release. Host Firewall configuration settings and rules may be managed by selecting Endpoints > Policy Management. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration instructions. For Cortex XDR agents on Windows endpoints, an uninstall password may be created. Cortex XDR Agent Tampering Protection to prevent unauthorized access or tampering with Cortex XDR agent components may only be enabled on Windows endpoints. Refer to the	Meets

• Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	Cortex XDR Pro Administrator's Guide for specific configuration instructions.	

REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI Requirement	Comment/Explanation	Meets/Supports PCI
2.4 Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of the components function/use.	By selecting Endpoints > Endpoint Management, endpoints may be viewed and exported to include information such as endpoint name, endpoint type, endpoint status, operating system, agent version, IP address, endpoint alias, Active Directory.	Supports

REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

PCI Requirement	Comment/Explanation	Meets/Supports PCI
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	BitLocker encryption or decryption can be applied only on Windows endpoints. Refer to the Cortex XDR Pro Administrator's Guide for endpoint pre-requisites and specific configuration instructions.	Supports

REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

The protection of cardholder data during public transmission is the sole responsibility of the customer. This requirement is a typical customer responsibility excluded from an endpoint protection solution like Cortex XDR.

REQUIREMENT 5: PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

There are operating systems considered "to be not commonly affected by malicious software", but may be managed as any other OS and protected by antivirus if deemed necessary by the organization. Organizations must address the malware risk to the management OS using their own formal IT Risk Assessment processes and consultation with their QSA.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	The Cortex XDR agent can be installed on a variety of endpoint operating systems. For a complete list of endpoint operating systems and agent compatibility, refer to the Cortex XDR Compatibility Matrix.	Meets
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Cortex XDR is capable of taking actions to block attempts to run malware, report but not block malware that attempts to run, and disable the module and not examine files for malware when malware is detected. For Windows, malicious executables may be quarantined or the endpoint may be isolated from the network. Refer to the Cortex XDR Pro Administrator's Guide for endpoint requirements and specific configuration options.	Meets
5.2 Ensure that all anti-virus mechanisms are maintained as follows:	Agent Auto Upgrade may be enabled for Cortex XDR agents to ensure that endpoints are always up-to-date with the latest Cortex XDR agent	Meets

Are kept current. Perform periodic scans. Generate audit logs which are retained per PCI DSS Requirement 10.7.	release. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration options. Once configured, agent upgrade status may be monitored for endpoints to indicate in progress, up to date, failure, not configured, pending. Scheduled endpoint scanning can be configured with Cortex XDR to run weekly or monthly. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration instructions. By selecting the Cortex Data Lake instance and Configuration, the retention period for Cortex XDR Logs can be configured. Additionally, Cortex XDR logs may be forwarded to external destinations. Refer to the Cortex XDR Pro Administrator's Guide for configuration options.	
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	For Cortex XDR agents on Windows and Mac endpoints, an uninstall password may be created. Cortex XDR Agent Tampering Protection to prevent unauthorized access or tampering with Cortex XDR agent components may only be enabled on Windows endpoints. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration instructions.	Meets

REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. **Note:** Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk- assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.	For Linux endpoints, the Vulnerability Assessment feature within Cortex XDR identifies security vulnerabilities for applications installed on these endpoints and retrieves the latest data for each Common Vulnerabilities and Exposures (CVE) from the NIST National Vulnerability Database. Refer to the Cortex XDR Pro Administrator’s Guide for pre-requisites and how to use this feature.	Supports
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	For Linux endpoints, the Vulnerability Assessment feature within Cortex XDR identifies security vulnerabilities for applications installed on these endpoints and retrieves the latest data for each Common Vulnerabilities and Exposures (CVE) from the NIST National Vulnerability Database. Refer to the Cortex XDR Pro Administrator’s	Supports

Note: *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	Guide for pre-requisites and how to use this feature.	

REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED-TO-KNOW

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Given that Palo Alto Networks Cortex XDR is a detection and response platform, this whitepaper focuses only on the features and capabilities pertaining to endpoint protection against attacks and malware. Palo Alto Networks leverages Hub (Web-Based Management Interface) to manage Cortex XDR accounts and related access controls. Cortex XDR customers may choose to use Palo Alto Networks' SSO or configure a third-party identify provider (IDP) to access the Hub. Using Palo Alto Networks' SSO, Cortex XDR customers can manage their users, roles, and enable MFA. When configuring a third-party IDP, Cortex XDR customers may enforce all non-Domain Administrators to log in using credentials configured with their identity provider. However, the Domain Administrator will always authenticate using Palo Alto Networks' SSO. Refer to the Cortex XDR Pro Administrator's Guide and Knowledgebase articles for configuration options and additional guidance. Organization's should consult with their QSA to understand how access and authentication controls are configured within their environment and assess implementation against PCI DSS requirements.

REQUIREMENT 8: IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Given that Palo Alto Networks Cortex XDR is a detection and response platform, this whitepaper focuses only on the features and capabilities pertaining to endpoint protection against attacks and malware. Palo Alto Networks leverages Hub (Web-Based Management Interface) to manage Cortex XDR accounts and related access controls. Cortex XDR customers may choose to use Palo Alto Networks' SSO or configure a third-party identify provider (IDP) to access the Hub. Using Palo Alto Networks' SSO, Cortex XDR customers can manage their users, roles, and enable MFA. When configuring a third-party IDP, Cortex XDR customers may enforce all non-Domain Administrators to log in using credentials configured with their identity provider. However, the Domain Administrator will always authenticate using Palo Alto Networks' SSO. Refer to the Cortex XDR Pro Administrator's Guide and Knowledgebase articles for configuration options and additional guidance. Organization's should consult with their QSA to understand how access and authentication controls are configured within their environment and assess implementation against PCI DSS requirements.

REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

Requirement 9 states, "Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data."

While the Palo Alto Networks Cortex XDR must be deployed in a physically secure environment to meet this compliance requirement, there is nothing particular to Cortex XDR that specifically supports or facilitates such compliance.

REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
10.3.1 User identification	Cortex XDR alerts contain a 'User Name' field to identify the user. Refer to the Cortex XDR Pro Administrator's Guide for the complete list of fields.	Meets
10.3.2 Type of event	Cortex XDR alerts contain the 'Alert Source', 'Action Category', 'Alert Name', 'Alert ID', Event Type' and 'Description' fields to provide information about the type of event. Refer to the Cortex XDR Pro Administrator's Guide for the complete list of fields.	Meets
10.3.3 Date and time	Cortex XDR alerts contain the 'Timestamp' field to provide date and time information. Refer to the Cortex XDR Pro Administrator's Guide for the complete list of fields.	Meets
10.3.4 Success or failure indication	Cortex XDR alerts contain the 'Description', 'Alert Name', 'Alert ID' fields to provide information to determine success or failure indication. Refer to the Cortex XDR Pro Administrator's Guide for the complete list of fields.	Supports
10.3.5 Origination of event	Cortex XDR alerts contain the 'Initiated By' field to provide information on origination of the	Meets

	event. Refer to the Cortex XDR Pro Administrator's Guide for the complete list of fields.	
10.3.6 Identity or name of affected data, system component, or resource.	Cortex XDR alerts contain the 'Host Name', 'File Path', 'Description' fields to provide identity or name of affected data, system component, or resource. Refer to the Cortex XDR Pro Administrator's Guide for the complete list of fields.	Meets
10.5.1 Limit viewing of audit trails to those with a job-related need.	From the Hub, Access Management can be selected to manage and assign roles for users. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration options for roles and access privileges.	Supports
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Behavioral Indicators of Compromise (BIOC) rules can be used to monitor and alert on files for 'create', 'read', 'rename', 'delete', 'write'. Outbound integrations such as Slack and ticketing systems can also be configured. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration options and instructions.	Supports
10.6.1 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 components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Query Builder, Native Search, Behavioral indicators of compromise (BIOC) rules, Indicators of compromise (IOC) rules may be used to review Cortex XDR alerts. Additionally, outbound integrations such as Slack and ticketing systems can be configured. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration options and instructions.	Supports
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the		

organization's annual risk assessment.		
10.6.3 Follow up exceptions and anomalies identified during the review process.		
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	By selecting the Cortex Data Lake instance and Configuration, the retention period for Cortex XDR Logs can be configured. Additionally, Cortex XDR logs may be forwarded to external destinations. Refer to the Cortex XDR Pro Administrator's Guide for configuration options.	Supports

REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: WLAN cards inserted into system components Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.) Wireless devices attached to a network port or network device.	For Windows endpoints with Cortex XDR agent 7.0 or later release, the Device Control feature may be used to block USB-connected devices.	Supports
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.	Behavioral indicators of compromise (BIOC) rules enable the ability to alert and respond to behavior of processes, registry, files and network activity. MITRE ATT&CK Tactic and MITRE ATT&CK fields are available for BIOC rules. Indicators of compromise (IOC) rules generate alerts on known artifacts that are considered malicious or suspicious. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration options.	Supports

Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.		
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Behavioral Indicators of Compromise (BIOC) rules can be used to monitor and alert on files for 'create', 'read', 'rename', 'delete', 'write'. Outbound integrations such as Slack and ticketing systems can also be configured. Refer to the Cortex XDR Pro Administrator's Guide for specific configuration options and instructions.	Supports

REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR ALL PERSONNEL

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

PCI Requirement	Comments/Explanation	Meets/Supports PCI
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Cortex XDR can be paired with Palo Alto Networks Managed Detection and Response (MDR) services to provide 24/7 coverage to detect and respond to XDR alerts.	Supports
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	Cortex XDR can ingest Palo Alto Networks Next-Generation Firewall traffic logs and traffic logs from external firewall vendors and use the analytics engine to analyze those logs and raise alerts on anomalous behavior. Cortex XDR may ingest other external alerts using syslog collector and Cortex XDR API but required fields must be mapped to the Cortex XDR format. Refer to the Cortex XDR Pro Administrator's Guide for configuration options.	Supports

CONCLUSION

The primary purpose of whitepaper is to demonstrate how Cortex XDR may be used to meet or support PCI DSS compliance requirements. Palo Alto Networks Cortex XDR offers many features and capabilities to protect against attacks which are not limited to those described in this whitepaper. Organizations should consult with their QSA to understand how to assess the implementation of Cortex XDR within their

environment. When deployed with controls described in this paper, supports or meets PCI DSS compliance requirements.

REFERENCES

1. Palo Alto Networks (2019). Palo Alto Networks Cortex XDR Administrator's Guide.
2. Palo Alto Networks (2020). Palo Alto Networks Cortex XDR Datasheet.
3. Palo Alto Networks (2020). Palo Alto Networks Compatibility Matrix.
4. Palo Alto Networks (2020). How to Create a New Customer Support Portal User Account. Retrieved from: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClNPCA0
5. Palo Alto Networks (2019). How to Enable Two Factor Authentication. Retrieved from: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN9CAK
6. Palo Alto Networks (2020). How to Enable Google Authenticator. Retrieved from: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmSm
7. Palo Alto Networks (2020). How Do I Enable Third-Party IDP For My Account? Retrieved from: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PPXXCA4
8. PCI Security Standards Council, LLC (2018), Payment Card Industry (PCI) Data Security Standard, v3.2.1

ACKNOWLEDGEMENTS

The author would like to acknowledge the following individuals from Palo Alto Networks for their contributions to this paper: Kasey Cross, Peter Havens, Shahar Razon, and Or Cohen. In addition, the author recognizes Divya Jeyachandran of Coalfire for her contributions to this paper.

Published August 2020.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.