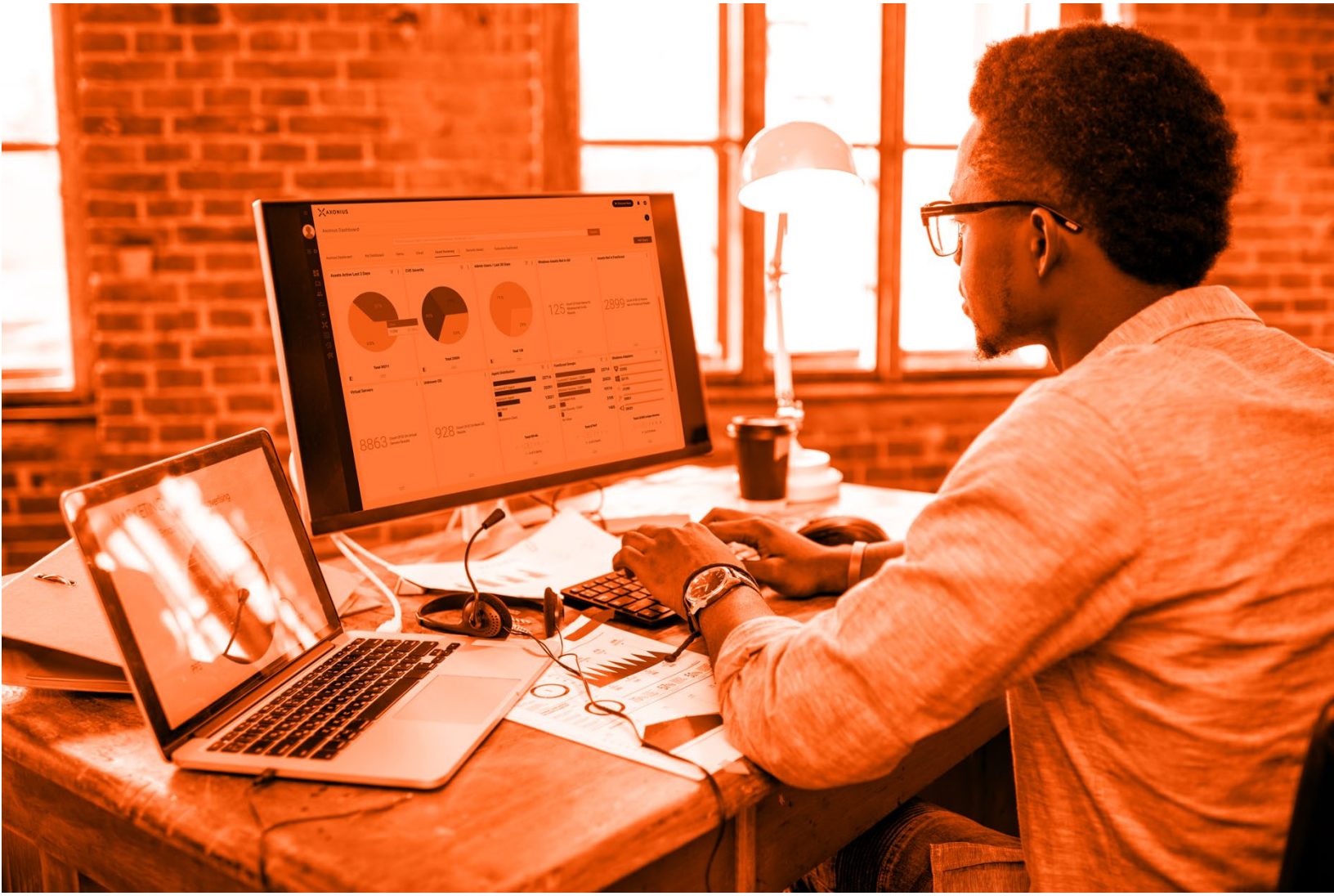
AXONIUS

AXONIUS CYBERSECURITY ASSET MANAGEMENT

PCI DSS Compliance Review



AXONIUS

TABLE OF CONTENTS

DISCLAIMER (TEVORA)

The opinions stated in this guide concerning the applicability of Axonius® products to the PCI DSS framework are the opinions of Tevora. All readers are advised to perform individual product evaluations based on organizational needs.

EXECUTIVE SUMMARY

OVERVIEW

Axonius engaged Tevora, a security and risk management consulting firm, an accredited PCI Qualified Security Assessor (QSA), and HITRUST Assessor, to conduct an independent, in-depth evaluation of Axonius against the applicable Payment Card Industry Data Security Standard (PCI DSS) Version 3.2.1 Requirements.

This paper describes the observations and conclusions drawn by Tevora through their partnered review of Axonius. This review included an assessment of key features via an initial demonstration of Axonius, and several testing sessions with Axonius to validate capabilities.

Furthermore, this whitepaper outlines the specific ways the Axonius Cybersecurity Asset Management platform can help organizations fulfill the mandates of the PCI DSS.

CURRENT ASSET MANAGEMENT PRACTICES

Information technology asset management (ITAM) is one of the most critical components of IT organization, but ITAM programs often don't incorporate the data security teams need to secure assets. Cybersecurity asset management (or modern asset management) allows IT and security teams to gather rich data about all assets and understand whether assets meet security policies and frameworks.

From an operational perspective, it is crucial to ensure IT assets are effectively managed, controlled, and protected. In addition, it is important to resolve any risk associated with the deployment and use of these assets. An increase in work from home environments has introduced new challenges to IT security management, where the visibility of assets has declined significantly due to connections with unmanaged and personal networks. It is difficult to enforce the proper use of assets when organizations lack standardized policies and have inadequate visibility to asset environments.

POTENTIAL CHALLENGES

Outdated forms of Asset Management

It is vital for asset management to be strategized in order to benefit businesses. Previous asset management practices have proven to be inefficient and wasteful. One of the most common methods includes manually tracking assets in a spreadsheet or similar document. This poses multiple challenges. For instance, it is very difficult to track all installed software on every device, as well as trace every valid or expired software license. Tracking with a spreadsheet does not allow administrators to record any real time changes or data. Another

challenge of manual tracking is an increased chance for errors. When evaluating the accuracy of a tracking document, human error must be accounted for, bringing the integrity of the data into question. In addition, manually tracking assets is time consuming and interrupts important tasks.

Cloud Asset Management

As cloud-based software gains popularity, it is crucial that all applications, platforms and infrastructure are managed correctly. When relying on a cloud-based application, IT managers and administrators tend to lean on the services of the provider, at times neglecting any responsibility for the asset. Leaving a gap between what IT administrators think they know, versus the actual current state of assets.

Lack of Process Controls and Policies

Many users in an enterprise may view IT asset management as an optional function rather than an organizational discipline. Therefore, it is critical that administrators create process controls and enforce valid policies. Asset policies are typically at the enterprise level and do not reflect the current state of IT assets. Enforcing policies can become a difficult task for administrators with minimal visibility to assets. Additionally, it is common for administrators and regular users to be fully unaware that there are proper controls and policies in place. As a consequence, many of these policies are ignored or bypassed.

Redundant Asset Collection

It is common for department managers, users, and IT management to hold onto assets that are no longer needed or used. This includes software applications, laptops, desktops, and mobile devices. This can lead to continued purchasing of IT

assets, while current unutilized assets go unseen. Assets that are not used also introduce increased security and audit risks.

A lack of proper asset acquisition processes can lead to the purchase of unnecessary assets. Even if processes are in place, being unaware of these asset acquisition processes can promote uninformed purchases and introduce uncontrolled assets to the environment, which also increases security and compliance risks, and amplifies costs.

Lack of Established Scopes

There are times when organizations do not have predefined scopes defining what constitutes an IT asset. Users then purchase assets or install software that has not been approved, presenting more security and compliance risks. This is another instance when more security and compliance risks are presented. The lack of predefined scopes dismisses any type of enforcement or regulations for users to follow.

PCI DSS COMPLIANCE CHALLENGES

When compiling assets, administrators are not only collecting data on physical devices like servers and desktops. PCI DSS requirements require data on all network devices, software, user locations, vendors, business processes and individual users connected to cardholder data.

This includes systems/servers, workstations, firewalls/routers, and wireless access points (if applicable) as well as populations of network change tickets, system change tickets, custom code/software change tickets, recent hires, and recent terminations.

Inaccurate PCI Scope

One of the most common challenges for organizations when dealing with asset management for PCI compliance is accurately tracking and

accounting for all in-scope PCI assets in an environment. Inventory as a PCI requirement refers to all hardware and software components within each in scope environment and functions for each. Establishing an accurate scope when assessing for PCI compliance is often missed.

Misunderstanding Current Environments

Another common trend is a lack of knowledge about the assets themselves. An organization needs to understand the potential impacts each asset could have. For instance, the value of an asset can only be measured by the data it carries, and the value of that data can demonstrate its importance to the organization as a whole.

Many times, administrators lack business processes to effectively understand assets. Organizations do not consistently conduct risk assessments nor associate potential risks to the asset or how it relates to it, sequentially leaving gaps unresolved. Without a full knowledge of assets and the data flowing through each, it also becomes difficult to apply any type of automated compliance validation.

BEYOND ASSET MANAGEMENT

1. *The Axonius platform was built to go beyond taking inventory of assets. Axonius can discover and evaluate how each of asset is operating, verify settings and configurations, and enforce specific policies. The following are some of the features that demonstrates how Axonius is more than an IT asset management tool. Agentless Tool - Axonius connects via to the management consoles already in use by organizations to collect assets.*
2. *Data Collection – Axonius is designed to discover, aggregate, normalize, and deduplicate all data about devices, users, and cloud instances by connecting to multiple tools that have detected an asset.*
3. *Access Control – Axonius was built to identify both on-prem and cloud-based devices.*
4. *Configuration Management – Axonius integrates over 300 solutions including Configuration Management Database tools to ingest and push changes to configurations.*
5. *Risk Controls - Axonius queries help administrators identify risks and implement risk controls.*
6. *Compliance Frameworks – Axonius can be used to automate compliance checks and compile in-scope environments.*

AXONIUS FOR PCI COMPLIANCE

OVERVIEW

Axonius allows organizations to manage and track assets. This product currently offers integrations with more than 300 of the most powerful business management and security tools to accurately collect data on all assets, users, vulnerabilities, and more. Once this data is aggregated, Axonius provides an asset inventory, uncovers security gaps, and validates security policies. It allows administrators to have a centralized management location for full visibility and control of assets and their data.

Axonius offers a variety of deployments like on-premises and private cloud deployments. In addition, Axonius-as-a-Service (a SaaS deployment) is also available. During an on-premises deployment, Axonius is deployed on a virtual appliance that becomes part of the organization's internal network. If an organization prefers Axonius-as-a-Service, the solution is deployed on an AWS EC2 instance.

KEY FEATURES

Asset Management

The main component of the Axonius Cybersecurity Asset Management tool is to maintain an updated asset inventory, while validating asset security and configurations. This platform actively discovers assets as they appear in other data sources integrated with Axonius. It automatically updates the inventory from connected data sources at customer-defined time intervals.

Axonius offers the capability to identify unmanaged devices that are known only through network connections. This is done by identifying any device that has gone rogue with specific queries.

A rogue device includes any asset with unwanted software, any non-restricted device connected to restricted network segments. Axonius can discover and manage any cloud asset, as it integrates with all major cloud providers. Axonius integrates with other network tools, including firewalls, routers, and switches, enabling administrators to easily find any IoT device – managed or unmanaged - connected to the network.

As cloud computing continues to grow, Axonius wants to ensure full security on all assets hosted by any cloud instance. This is accomplished by mapping the state of currently connected cloud instances against industry standards and benchmarks. The platform reports on how assets adhere to or deviate from common security best practices for Amazon Web Services, Microsoft Azure, Google Cloud Platform and Oracle Cloud.

Visibility

Axonius Cybersecurity Asset Management connect with key security and management solutions used by the organization to discover any asset on the network. It then collects and correlates information about devices, cloud instances and users. This allows administrators to have full visibility of all assets as they report back to Axonius through multiple connections. In addition, administrators can discover any security gap and enforce security policies. Axonius Dashboard is a customizable page for organizations to track any relevant metrics and show any insights based on saved queries. It offers full visibility to critical events in the current environment.

Access Management

Access management focuses on validating that secure exchange of credential operations are conducted, as well as ensuring authorization and provisioning functions are secure. Policies

based around access are also contained within access management functions.

Axonius has the ability to automate queries that benefit access management. This platform enables administrator and privileged access to be validated by creating queries with specific tool connections. There is also a big focus on finding unauthorized wireless access, queries to search for unknown, unmanaged, and rogue devices on network interfaces across connected network infrastructure.

Compliance Management

Axonius is designed to integrate into the dynamic, agile, and scaling cloud architectures deployed by organizations at the forefront of modern technology. Primarily focused on cloud asset compliance, Axonius is set to comply with specific industry benchmarks and frameworks. Some of those compliances include CIS Amazon Web Services Foundations, CIS Microsoft Azure Foundations, CIS Oracle Cloud Infrastructure Foundations and CIS Google Cloud Platform Foundations benchmark.

Incident Management

Axonius can help accelerate incident response investigations by providing clear asset inventories. This is accomplished by connecting adapters to critical sources that will provide detailed information on devices, users, and clous assets. Administrators can then correlate any incident alert to data Axonius has provided.

By providing a full asset inventory Axonius will indicate which devices and users were associated with the alerts, where the devices were located, all software running on those devices and which users are associated with the device. In addition, Axonius

data can be sent to different security information and event management (SIEM) and security orchestration, automation and response (SOAR) systems to provide rich asset data that can contextualize log data.

Policy Management

Security policies can be validated by Axonius on a continuous basis using queries that look for specific conditions. Using any query or select assets, actions can be designed to alert or create incident response tickets during an event. Axonius can be integrated with Slack, ServiceNow, Zendesk and other ticketing systems to notify users and create tickets. Other actions include enriching device and user data with third party sources, updating vulnerability assessments, creating, and updating CMDB records, or isolating devices from the network. Third Party Integrations

In addition, Axonius can integrate with more than 300 pre-built solutions. For a list of available solutions, please visit Adapters List. These tools include IT, Security, and business solutions that can securely send Axonius asset data. This is accomplished by configuring supported adapters with the necessary credentials to fetch asset data. For more information on how to configure an adapter, please visit the Adapters Page.

Reporting and Analytics

Axonius can also generate reports based on the information being displayed on the Dashboard. Dashboard spaces can be customized to show specific spaces, saved queries, users or a combination of all. Additionally, administrators may configure email notifications when reports are generated. The Report PDF

file contains a cover page, contents, discovery summary, dashboard charts, and saved queries for both devices and users.

COMPLIANCE REQUIREMENTS

Here is how Axonius addresses each applicable PCI DSS v 3.2.1 Requirements:

PCI DSS 3.2.1	AXONIUS FEATURES	SUPPORTS COMPLIANCE
Requirement 1: Protect your system with firewalls		
1.1 – Establish and implement firewall and router configuration standards that include the following:	Axonius allows administrators to create queries based on the configurations that need to be validated. This includes any configuration on a network device like a router or firewall. The following is an example on a query that can be used to validate firewall rules: *Show ALL Axonius assets with INGRESS traffic in Firewall Rules AND targets all possible IPs (0.0.0.0) OR ALL Axonius assets with EGRESS traffic in Firewall Rules AND targets all possible IPs (0.0.0.0)* The query will depend on the client's environment	Yes

	and how networks are segmented.	
1.2 – Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	Through the use of a saved query, firewall rules can be validated. Verify any connection or firewall rule with a query by specifying which networks or IP addresses should be blocked.	Yes
1.3 – Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Axonius queries can consistently check whether specific traffic is being prevented by a saved query. The following is an example of a query that can be used to verify outbound internet access: *Show ALL Axonius assets with OUTBOUND traffic in Firewall Rules AND targets all possible IPs (0.0.0.0)*	Yes
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:	Axonius queries help verify which software is in currently installed on each device. This includes any type of firewall software. When searching for the specific firewall software, administrators can filter by software, or by user ID. The main Dashboard page will display all assets with designated software.	Yes

• *Specific configuration settings are defined.* • *Personal firewall (or equivalent functionality) is actively running.* • *Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.*		
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
2.2 – Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • *Center for Internet Security (CIS)* • *International Organization for Standardization (ISO)* • *SysAdmin Audit Network Security (SANS) Institute* • *National Institute of Standards Technology (NIST).*	Compare cloud configuration and asset data against industry frameworks through the Cloud Asset Compliance page. The following are currently available to assess against: 1. *CIS Amazon Web Services Foundations Benchmark v1.2* 2. *CIS Microsoft Azure Foundations Benchmark v1.1* 3. *CIS Oracle Cloud Infrastructure Foundations Benchmark v1.0* 4. *CIS Google Cloud Platform Foundations Benchmark 1.1*	Partial
2.4 – Maintain an inventory of system components that are in scope for PCI DSS.	Axonius can maintain an inventory of all in scope PCI assets as long as the	Yes

	customer tags them PCI. Tags can be used to label a single asset or group of assets that have shared characteristics or configurations.	
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs		
5.1 – Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Axonius can check for any asset missing specific software, including anti-virus. The following is an example of a query that can be used to verify which assets are missing anti-virus software: *Show ALL Axonius assets that do NOT contain Adapter Properties that equal Endpoint_Protection* This query will show any asset missing the specified Adapter Property, which is endpoint protection software in this case.	Yes
5.2 – Ensure that all anti-virus mechanisms are maintained as follows: • *Are kept current,* • *Perform periodic scans* • *Generate audit logs which are retained per PCI DSS Requirement 10.7.*	Automated queries can be updated at any time and set to run as often as administrators prefer and configure. By specifying a specific version of anti-virus, queries can verify that the most recent version is currently installed on all assets.	Partial

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.	The following is an example of a query that can be used to ensure that anti-virus is actively running: *Show ALL assets that have a McAfee ID AND have reported back to Axonius in the last three days AND have NOT been seen in the last three days by McAfee* A similar query may be run continuously to ensure that data is being returned to the anti-virus software and to Axonius.	Yes
Requirement 6: Develop and maintain secure systems and applications		
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.	Axonius allows administrators to check for recent patches. Because patches tend to change often, these queries are usually manually run. The following is a generic example of a query checking for assets with no pushed patches: *Show ALL Axonius assets that have existing Vulnerable Software AND with NO OS Installed Security Patches in the last 30 days* With certain data sources connected, Axonius	Yes

	constantly adds new patches to verify against when running these queries.	
Requirement 8: Identify and authenticate access to system components		
8.1 – Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	Axonius offers a full view of all users under the Users page. This page displays users under a specific query and when no query is chosen, it displays all users. In addition, administrators can define queries to look up specific users by Axonius ID or by employee ID. The following is an example of a query that can be ran to show a specific user: *Show ALL Axonius assets that have an existing ID OR ALL Axonius assets that have an Employee ID*	Yes
8.2 – In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • *Something you know, such as a password or passphrase*	Axonius can integrate with Microsoft Active Directory (AD) to ensure that users are signing in through an identity solution. Additionally, Axonius can enforce specific password policies through Microsoft Active Directory (AD).	Partial

• *Something you have, such as a token device or smart card* • *Something you are, such as a biometric.*		
8.3 – Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	An Axonius query can validate specific actions, such as whether users authenticate with certain multi-factor authentication. Under Action Library, administrators have full visbility of the main actions available to push. Although there are actions to be enforced, Axonius is still limited when it comes to completing certain controls.	Partial

Requirement 9: Restrict physical access to cardholder data

9.9.1 - Maintain an up-to-date list of devices. The list should include the following: • *Make, model of device* • *Location of device (for example, the address of the site or facility where the device is located)* • *Device serial number or other method of unique identification.*	Axonius is an asset management solution designed to keep track of all devices and users. In the main Dashboard page, administrators have full visibility of each asset with device details and installed software. Additionally, it can push configuration settings to designated groups of assets.	Yes

Requirement 10: Track and monitor all access to network resources and cardholder data

10.2.5 – Use of and changes to identification and authentication mechanisms – including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges	Axonius enables administrators to create and modify different types of notifications. Notifications can be altered for different queries and are uniquely available to individual administrators that create them. Administrators can be notified when any automated or manual query is run, as well as when users gain permissions.	Yes
Requirement 11: Regularly test security systems and processes		
11.1 - Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	*Needs review from client* The following is an example of a query to automatically check for wireless access points: *Show ALL Axonius assets that do NOT have ENDPOINT PROTECTION PLATFORM, MANAGER, AND VULNERABILITY ASSESSMENT adapter properties.*	Yes
11.2 – Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network	An Axonius query can help identify how often scans are run. This includes any type of vulnerability scan run with a vulnerability management tool. The following is an example of	Yes

topology, firewall rule modifications, product upgrades).

a query that checks if a vulnerability scanner has been used in the past 90 days:

Show ALL Axonius assets that have shown Adapter Properties as Vulnerability_Assessment AND have NOT been seen in the last 90 days

TECHNICAL ANALYSIS METHODOLOGY

Tevora reviewed the Axonius solution to observe effectiveness for the following PCI DSS compliance requirements:

- *1: Install and maintain a firewall configuration to protect cardholder data*
- *2: Do not use vendor-supplied defaults for system passwords and other security parameters*
- *5: Protect all systems against malware and regularly update anti-virus software or programs*
- *6: Develop and maintain secure systems and applications*
- *8: Do not use vendor-supplied defaults for system passwords and other security parameters*
- *9: Do not use vendor-supplied defaults for system passwords and other security parameters*
- *10: Do not use vendor-supplied defaults for system passwords and other security parameters*
- *11: Regularly test security systems and processes*

CONCLUSION

The Axonius Cybersecurity Asset Management Platform supports many features that facilitate PCI DSS compliance for multiple requirements. This tool provides a wide variety of queries to discover security gaps and subsequently enforce security policies by pushing action configurations into selected assets. Axonius works as more than an asset management tool – it displays customized views of the most critical characteristics of each asset, facilitating decision-making for managers.

With over 300 available integrations, Axonius should ideally be integrated with any data source that knows about assets, if possible. This will provide the most accurate data results for all assets. Axonius provides a full view into assets and helps control asset, compliance, incident, policy, and access management.

This solution will enable the means for administrators to effectively fulfill multiple PCI DSS v 3.2.1 compliance requirements.

APPENDIX

Definitions – compliance standards

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is intended to protect cardholder data wherever it resides to ensure that members, merchants and service providers maintain the highest information security standard. PCI DSS is a set of comprehensive requirements for enhancing payment account data security. The standard was developed by the founding payment brands of the PCI Security Standard Council to help facilitate the broad adoption of consistent data security measures on a global basis.

ABOUT AXONIUS

Axonius was founded in June 2017 to answer a simple question. Despite all of the high-tech, sci-fi tools we have in cybersecurity, why is it so difficult to answer simple questions about the devices, users, and cloud instances we're tasked with securing? Asset management is so foundational, yet it's a nagging problem that is only getting worse. Co-Founders Dean Sysman, Ofri Shur, and Avidor Bartov, veterans of an elite intelligence unit of the Israeli Defense Force built Axonius to solve the asset management challenge for cybersecurity. Axonius is headquartered in New York, NY and our R&D team is based in Tel Aviv, Israel.

It's 2021, and security teams are still spending time and manual effort trying to understand the assets they have, whether those assets are secure, and whether they adhere to or deviate from their security policies. Our mission is to give customers a comprehensive and always up-to-date asset inventory, uncover security gaps, and automate as much of the manual remediation work as our customers want. When organizations stop spending time on manual asset management tasks, they're able to take on the high-value cybersecurity initiatives that highly trained and skilled cybersecurity professionals love doing.

ABOUT TEVORA

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that has the ability to fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication has established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information please visit www.tevora.com.