



# Cardnet's PCI DSS 4.0 Challenges:

The Scanning Process and True Risk Approach

**Isaias Mercado**

Security Manager, Cardnet





## Isaias Mercado

Security Manager, Cardnet

- 14 years with Cardnet; roles included software development & change management
- Professor in malicious algorithms, Intec Univ, Dominican Republic
- B.S., systems engineering Intec Univ; Masters in engineering, O&M University
- ISA & PCIP certification, PCI Council

# A Few PCI DSS 4.0 Changes

- ✓ Req **5.2.3.1.a** malware impact on systems
- ✓ Req **8.6.3.b** password complexities
- ✓ Req **10.4.2.1.a** security events and logs
- ✓ Req **11.3.1.1.a, 11.3.1.1.b** low vulnerabilities management
- ✓ Req **11.6.1.d** security header analysis for public-facing sites
- ✓ Req **12.3.1** risk evaluation, comparings results between evaluations, identifying assets and how critical they are



# PCI DSS 4.0 Challenges



**Solutions on-Premises, in the Cloud or Multi-Cloud causes integration complexities**



**Security Platforms are competing with Cloud providers (e.g.; Amazon AWS vs. security vendors)**



**Many security solutions are “point solutions” that may cause integration problems**



**Internal vulnerability scans must agent based/ authenticated (PCI DSS 4.0 req. 11.3.1.2)**

## What does it mean for you?



Freedom of choice is necessary throughout the transition while ensuring compliance



Impacts security & compliance initiatives due to incompatibilities & vendor friction



Security platforms need to migrate toward Unified View for PCI DSS 4.0 Compliance requirements



Difficult to deploy multiple agents or launch authenticated scans, must comply by 3/31/24

# PCI DSS 4.0 Challenges



**Agent-Based or authenticated scans may generate more vulnerabilities.**



**PCI vulnerabilities should be addressed using a prioritized and risk-based approach.**



**Vulnerability risks should be prioritized based on true risk, CISA KEV, or QDS**



**PCI risk management requires compliance validation beyond provider CVE prioritization**

## What does it mean for you?



Start deployments on time, simplify with scheduled scans based on internal or external sensors.



Ensure processes are documented & consistent; vulnerabilities are analyzed & prioritized based on true risk



Consider Qualys CSAM with VMDR for TruRisk scores or QDL risk dashboards



Ensure consistent organizational true risks are considered and authenticated

# Qualys PCI DSS 4.0 Unified Dashboard



Up and running in  
four days



# Vulnerability Management, Detection & Response



## Capabilities

## PCI DSS 4.0 Requirements



**6.3.1:** Risk based assessment approach for vulnerability management



Need to determine the risk ranking to be associated with each vulnerability



Vulnerabilities for bespoke and custom software are covered.



**11.3.1.2:** New requirement to perform internal vulnerability scans via authenticated scanning



Elevate VM to risk-based VM program with business context



100% coverage of the attack surface - 68% of CISA risky vulns are agent (locally) detected, while 32% require external scanning



Context of threats mapped to vulnerabilities



Automatically tie threats applicable to healthcare industry (with 25+ threat feeds) mapped to detected vulnerabilities



Track risk reduction over time with Qualys TruRisk™

# Policy Compliance



PC

## PCI DSS 4.0 Requirements



**1.2:** Network security controls (NSCs) are configured and maintained



**2.2:** Secure configurations for all system components



Coverage for **wide range of configuration standards** such as CIS, ISO, DISA STIG, NIST, Cloud Security Alliance, and product vendors



## Capabilities



Comprehensive compliance and config risk assessment coverage with 900 pre-configured policies, 20K controls, 350 technologies, and 100 frameworks



Reduce compliance blind spots by discovering middleware applications, web servers, databases from default, non-default locations



Prioritize misconfigurations based on ransomware risks, MITRE tactics & techniques, regulatory compliance objectives, asset business criticality

# CyberSecurity Asset Management

## PCI DSS 4.0 Requirements



**12.5.1:** An inventory of system components that are in scope for PCI DSS.



**2.2.3: Asset classification** - external vs internal. For example, isolating web servers (which need to be directly connected to the Internet) from application and database servers



## Capabilities



Improved risk prioritization with complete asset context and business criticality



Internal Attack Surface Management



Discover blind spots including assets missing from your vuln program



External Attack Surface Management (EASM)

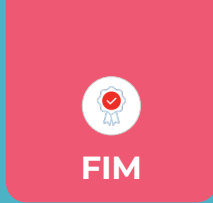


Discover 30%+ unknown internet-facing assets for vuln assessment



EASM is included with CSAM!

# File Integrity Monitoring



## PCI DSS 4.0 Requirements



**10.2.1.1:** Capture user access to card holder data



**10.4.1.1:** New requirement for the use of automated mechanisms to perform audit log reviews



**10.7.2:** New requirement to **address failures of critical security control systems** such as FIM



## Capabilities



File Access Monitoring (FAM) covers all user access even if integrity is not modified



Automated alerts and report for failure of FIM solution



Advanced Noise Cancellation with fine-tuned profiles and inbuilt Threat Intelligence to detect malicious or suspicious hashes



Ready-to-use FIM profiles for PCI DSS 4.0



Real-time FIM capturing of who, when, what, and where details using same agent

## PCI DSS 4.0 Requirements



**Requirement 1:** Install and maintain network security controls, including cloud access controls



**Requirement 6:** Remediate vulnerabilities, including for all **cloud** components; apply patches to less-critical systems in an appropriate timeframe, based on a formal **risk** analysis.



Create a remediation schedule based on **risk** and priority."

-PCI Security Council Quick Reference Guide page 27



## Capabilities



Continuous discovery provides 100% visibility into workloads and misconfiguration risk across multi-cloud environments.



Automate patching for vulnerabilities and customize risk remediation via Qualys QFlow



True risk insights from 180K+ vulnerabilities sourced from over 25+ threat and exploit intelligence sources

# Endpoint Detection & Response + EPP

## PCI DSS 4.0 Requirements



**5.2.2:** New requirement, anti-malware solution should not just detect but remove, block, or contain all known types of malware



**5.3.2:** New requirement, performs continuous behavioral analysis of systems or processes

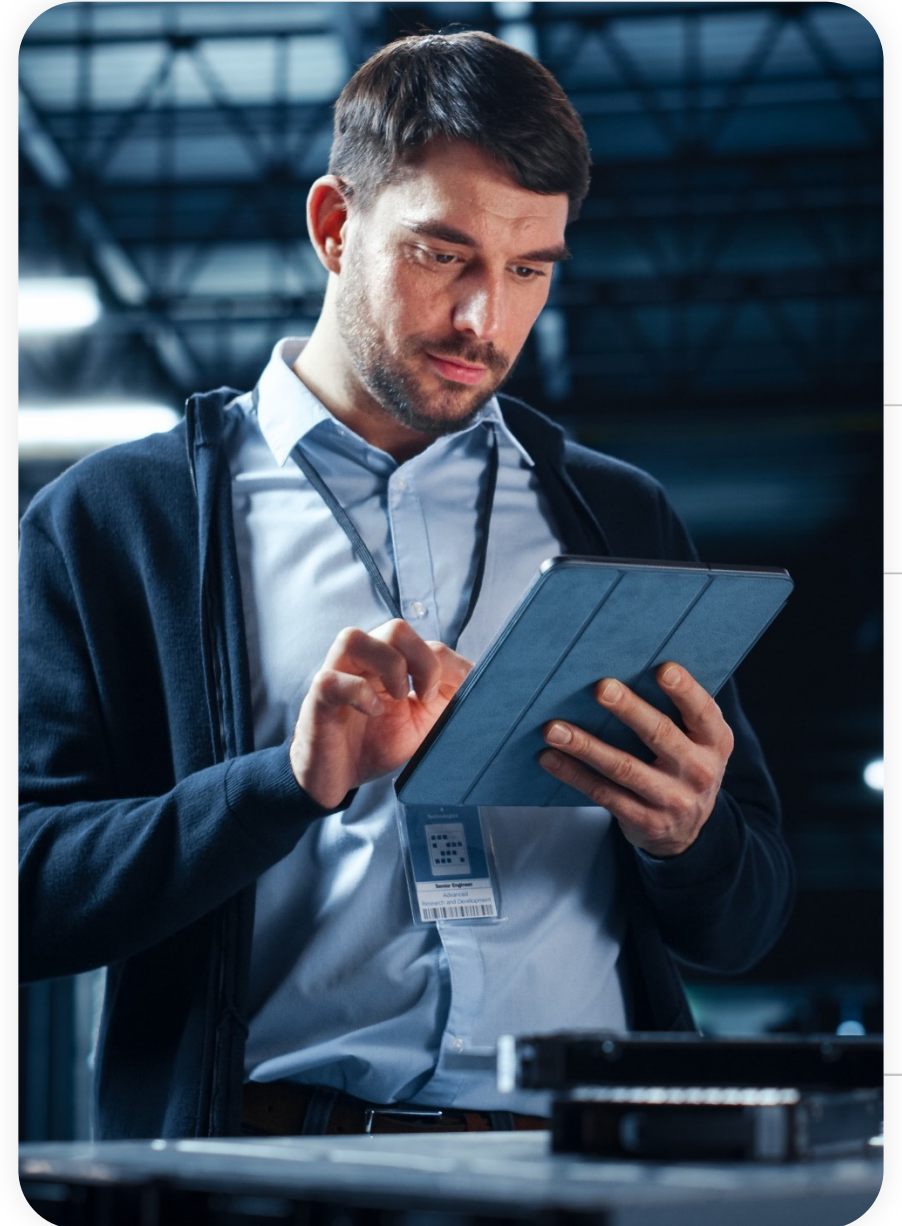


## Capabilities

-  Known & unknown malware detection
-  Blocks zero-days including ransomware, fileless attacks and credential theft
-  Continuous behavioral analysis
-  Complete endpoint protection

# Recommendations

- ✓ Explore solutions that address compliance with minimal fatigue
- ✓ Focus on compliance-native integrated solutions
- ✓ Expand to other solutions, integrations, and innovations to cover more PCI DSS 4.0 requirements
- ✓ Build your own risk template and choose available resources to do so
- ✓ Build your own dashboards
- ✓ Monitor your compliance progress and establish one or more Pass/Failed criteria based on true risk.
- ✓ Continue planning and work together with teams, including GRC, within your organization
- ✓ Implement as many automated tools and strategies as you can for internal and external scans



# Questions?



**CARDNET**  
NOS UNE



**CARDNET**

**NOS UNE**