CHALLENGE

- The Payment Card Industry has established fines of up to $500,000 per incident for security breaches when merchants are not PCI compliant.
- Client payment information continues to sprawl across hybrid IT infrastructures including on premise, private, and public cloud platforms like Amazon Web Services and Azure.
- The PCI DSS standard was just updated, yes, again.
- Companies needing to adhere with The Payment Card Industry Standard (PCI) face enormous challenge to leverage new technologies like Docker, while safeguarding personally identifiable information (PII), across all points in the business transaction supply chain.

Payment Card Industry Data Security Standard (PCI DSS) 3.2

Why comply with PCI DSS 3.2?

With ink barely dry on the latest revision of The Payment Card Industry Data Security Standard (PCI DSS) organizations are on notice that it expires on 31 October 2016. **Cavirin Security and Compliance has already released the latest version of Policy Pack for PCI DSS 3.2, offering secure configuration visibility into most major technology platforms and across all major operating systems.**

Recently revised, PCI DSS 3.2 exists to assess your company's capacity to build and maintaining secure networks, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy. Cavirin's PCI Pack, plus additional modules for ISO/IEC 27002:2013 meets the most challenging aspects of demonstrating compliance to this business critical information security standard.

> *"Compliance with the PCI DSS standard continues to improve, but four out of five companies still fail at interim assessment. This indicates that they've failed to sustain the security controls they put in place."* - Verizon 2015 PCI Compliance Report

Leveraging PCI failure to optimize environments and pass audits faster

Facing PCI audit, organizations often fail due to improper security settings, incorrect configurations, low levels of encryption, or poor policies and procedures. Testing those controls could have prevented costs in business disruption as well as monetary fines, however, finding the evidence of those controls across multiple disparate systems can prove impossible.

Cavirin's ARAP™ solution automatically checks system configuration settings across all target environments, reporting against expected system based PCI policies. Review and response to address recommended fix actions allows timely remediation to found problems, and further rewards the business by rapid completion of unnecessarily disruptive PCI audit events.

Cavirin clients gain further advantage through alignment with the PCI international security standard. The simple act of managing PCI program effectiveness, supports elements in achieving compliance with many other control frameworks including the security aspects of the following laws:

- UK Data Protection Act 1998; The Computer Misuse Act 1990 (UK)
- Federal Information Security Management Act 2001 (US)
- Gramm-Leach-Bliley Act (GLBA) 1999 (US)
- Federal Financial Inst. Examination Council's (FFIEC) security guidelines (US)
- Sarbanes-Oxley Act (SOX) 2002 (US); State security breach notification laws (e.g. California) (US)

Cavirin's ARAP automatically checks company systems against an array of OS and environmental benchmarks sending scheduled and triggered reports informing the compliance team about nodes requiring fix and the exact steps to remediate wrong settings. Producing and retaining a validated summary report used for internal security audits is a primary mechanism proving to third party auditors that systems are configured in a manner that aligns with the PCI DSS 3.2 standard.

Gaining the most from your PCI DSS 3.2 Program implementation

Companies embarking on the path of PCI DSS 3.2 certification need assistance to establish, monitor, maintain and measure improvement in their security program. Leveraging Cavirin ARAP's PCI DSS 3.2 Policy Pack enables:

- Improved company reputation and image, demonstrating proof of senior management's commitment to the security of the organization
- Identify information assets and their associated security requirements
- Assess information security and treat risks according to their relative tolerance
- Monitor, maintain and improve the effectiveness of controls associated with the organization's information assets

THE SOLUTION

Cavirin's Automated Risk Analysis Platform (ARAP™) assists Chief Risk & Security, as well as IT and DevOps leadership in gathering configuration data used to address their top security and compliance challenges:

- Settings that indicate missing patches for operating systems and applications.
- Monitoring and detecting sensitive data loss (data exfiltration)
- Locating policies that enable weak passwords.
- Lack of logs and audit trails necessary to conduct forensics
- Security validation for new systems
- Missing or outdated anti-malware technology
- Settings that enable encryption of sensitive information in transit
- The information necessary to remediate deficiencies that would otherwise be impossible to manage due to the lack of trained staff maintaining security controls.

Compliance in any environment

- Cloud Native platform supporting 12-factor patterns (things like port binding, logs, concurrency…)
- A "hyper plane" of integrated "risk assessment" amongst segmented vulnerability domains
- Works with Private, Hybrid, and Public Clouds and Support **AWS**, **Azure**, **GCP** (Google Cloud Platform)
- Manages thousands of out-of-box policies, well curated and certified (SCAP, XCCDF, OVAL)
- Supports most compliance authorities (PCI, HIPAA, NIST, SOC2, FedRamp, CIS Benchmark, DISA, CIS CSC, CSF)
- Is CIS Certified security content (Multiple OS, Docker, AWS Cloud)
- Complies with DISA standards in all aspects of delivery and reported results

PCI DSS 3.2 Compliance and Cavirin

Cavirin Security and Compliance actively contributes to all major standards and organizations responsible for the mapping of regulatory requirements and the most highly leveraged national and international standards. In addition to organic CIS Benchmarks and DISA STIG NIST based configuration management, Cavirin has implemented all assessments with NIST Cyber Security Framework (CSF) and NIST 800-53 r4 and Appendix J for Privacy. Clients who elect to use multiple policy packs, including ISO/IEC 27002:2013, will benefit by the extended use of multiple frameworks to align Information Security Programs and Policy.