



Solution Brief: The ArcSight PCI Protection Suite

Providing Ultimate Protection for Cardholder Data

ArcSight automatically collects information from all system components covered under PCI and provides an intelligent layer of correlation, alerting, analysis and audit documentation.

Highlights

- Facilitates compliance with PCI 1.1
- Real time monitoring and alerting across all 12 PCI requirements
- Proactively mitigates data breaches in an efficient, and audit-friendly manner

Creation of a Common Security Standard

The increasing number of data exposure, digital fraud and identity theft cases has made the protection of consumer information more critical than ever. Over the past several years, the payment card industry has worked to develop and implement security standards to protect consumer data. In December 2004, Visa, American Express, Discover and Diners Club aligned their respective security efforts to create a common set of data security requirements, which is known as the Payment Card Industry Data Security Standard, or PCI.

To protect against the threat of data compromise, PCI established a list of 12 overall requirements that merchants, service providers and other members that store, transmit and process cardholder data must have meet by certain deadlines based on their PCI merchant level. These requirements include the use of network configuration management, data encryption, end-user access controls and user activity monitoring and logging, as well as the need to regularly test security systems and processes. Companies that fail to comply with the PCI standard risk their brand, reputation and customer confidence. Furthermore, they will face significant fines if they are not compliant, or if a data compromise occurs.

The ArcSight PCI Protection Suite Facilitates PCI Compliance

PCI sets forth rigorous standards for the security of all systems and devices that are connected to the overall payment network.

The ArcSight PCI Protection Suite directly assists merchants, service providers and other members that store, process and transmit cardholder data by making their PCI compliance program more efficient, effective and auditable. The ArcSight PCI Protection Suite automatically collects information across widely distributed IT environments, from all systems, devices and components covered under PCI and provide an intelligent layer of analysis, audit and documentation to improve management of PCI compliance requirements.

Protects Cardholder Data

The ArcSight PCI Protection Suite provides a proactive, efficient methodology to protect cardholder data by centrally collecting, monitoring and alerting on all IT related events that impact security and compliance. The ability to collect all data from all in-scope PCI systems provides the greatest level of assurance that PCI compliance is being effectively monitored and managed, which mitigates the affect of non-compliance or data breaches. ArcSight ESM, ArcSight Logger, ArcSight Network Configuration

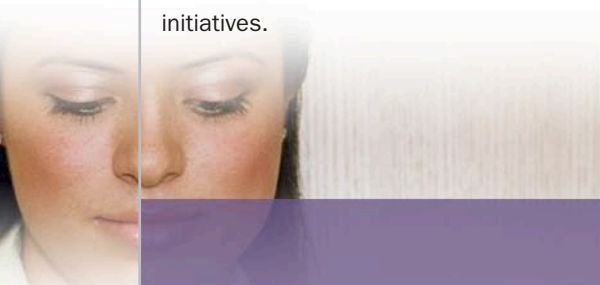
PCI Control Objective	Requirement	ArcSight Capabilities
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data	<ul style="list-style-type: none"> • Reports on firewall rule set usage and configuration standards for routers • Compares traffic from untrusted hosts against required protocols • Alerts if inbound Internet traffic is going to IP addresses beyond the DMZ • Reports on inbound and outbound Internet traffic to ports 80 and 443 • Alerts if databases are not segregated from the DMZ • Controls, tracks, verifies and reports that NAT (or any other technology using RFC 1918) is used • Monitors and enforces to ensure all inbound and outbound traffic is limited to specific protocols
	2. Do not use vendor supplied defaults for system passwords and other security parameters	<ul style="list-style-type: none"> • Automatically compares vulnerability information against policy • Correlates between administrative access and encrypted/unencrypted protocols
Protect Cardholder Data	3. Protect stored data	<ul style="list-style-type: none"> • Monitors and alerts administrators to database and application security issues • Monitors device logs for existence of cardholder data (pattern searching) • Automates enforcement of retention policies for logs by device type (or other logical grouping of devices) • Log data past retention policy automatically rendered inaccessible
	4. Encrypt transmission of cardholder data and sensitive information across public networks	<ul style="list-style-type: none"> • If used in conjunction with Snort, monitors and alerts on policy breaches and violations regarding unencrypted data • Monitors traffic to ensure the necessary traffic that passes through the payment network is encrypted
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software	<ul style="list-style-type: none"> • Provides centralized reporting of anti-virus installation and updates • Correlates updated vulnerability information to PCI assets to prioritize risks and threats
	6. Develop and maintain security systems and applications	<ul style="list-style-type: none"> • Provides centralized repository of vulnerability data • Compares vulnerabilities to corporate standards • Provides centralized documentation of configuration changes to critical systems
Implement Strong Access Control Measures	7. Restrict access to data by business need to know	<ul style="list-style-type: none"> • Alerts application and system owners when new users have been added to ensure these changes are reviewed and approved
	8. Assign a user ID to each person with computer access	<ul style="list-style-type: none"> • Provides centralized repository and reporting of access control changes to systems • Monitors and alerts on terminated employee IDs
	9. Restrict physical access to cardholder data	<ul style="list-style-type: none"> • Serves as central repository for physical security logging and reporting of access and access control changes
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	<ul style="list-style-type: none"> • Monitors and alerts on user or system access to network devices, applications, POS systems, and other IT devices that maintain cardholder data • Performs file integrity monitoring and change detection • Delivers automated audit trail to support forensic requirements
	11. Regularly test security systems and processes	<ul style="list-style-type: none"> • Enhances review of system component logs by performing initial first pass filtering • Continually monitors security systems to validate compliance status
Maintain an Information Security Policy	12. Maintain an Information Security policy	<ul style="list-style-type: none"> • Monitors access to information security policy data • Documents adherence to security incident response and escalation procedures

The ArcSight PCI Protection Suite allows organizations to streamline the execution and documentation of their PCI program.

Manager and ArcSight Compliance Insight Package for PCI provide compliance-specific dashboards, reports and correlation rules that track and monitor any PCI event, allowing organizations to proactively manage compliance to protect cardholder data and protect the organization's brand. Automated monitoring allows organizations to streamline the execution and documentation of their PCI compliance initiatives.

About ArcSight

ArcSight is a leading provider of security and compliance solutions that intelligently identify and mitigate business risk and deliver a centralized view of enterprise-wide events across heterogeneous infrastructures. This real time and historic view into external attacks, insider threats and regulatory compliance provides enterprises, MSSPs and government agencies with the intelligence and response capabilities required to effectively protect and manage their networks and their businesses.



ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com
 email: info@arcsight.com

Corporate Headquarters: 408 864 2600
 EMEA Headquarters: +44 870 351 6510
 Asia Pac Headquarters: 852 2166 8302