

Security and Compliance Solutions

TrustKeeper®

Compliance Validation Services (CVS)

- CVS-1 RA Our Compliance Validation Service Level 1 (CVS-1) manages and validates compliance with the Payment Card Industry Data Security Standard (PCI DSS) for Level 1 merchants and Level 1 and 2 service providers. This service includes access to the TrustKeeper Web portal to complete preparations for the required on-site PCI data security assessment performed by Trustwave and to schedule and undergo quarterly network scans. CVS-1 Risk Analysis (RA) also includes a remediation plan developed pending the results of pre-assessment risk and gap analyses.
- CVS-1 Our Compliance Validation Service Level 1 (CVS-1) manages and validates PCI DSS compliance for Level 1 merchants and Level 1 and 2 service providers. This service includes access to the TrustKeeper Web portal to complete preparations for the required on-site PCI data security assessment performed by Trustwave and schedule and undergo quarterly network scans.
- CVS-2&3 Our Compliance Validation Service Level 2 and 3 (CVS-2&3) manages and validates PCI DSS compliance for Level 2 and 3 merchants and Level 3 service providers. This service includes the TrustKeeper Web portal for management and completion of the required annual PCI Self-Assessment Questionnaire and quarterly network scans.
- CVS-4 Our Compliance Validation Service Level 4 (CVS-4) manages and validates PCI DSS compliance for Level 4 merchants. This service includes the TrustKeeper Web portal for management and completion of the recommended annual PCI Self-Assessment Questionnaire and quarterly network scans.

Internal Vulnerability Scanner

- IVS Managed through the TrustKeeper portal, the Trustwave Internal Vulnerability Scanner appliance identifies vulnerabilities on internal servers and up to 5,000 IP addresses from behind an organization's firewall—helping fulfill the internal vulnerability scan requirements of the PCI DSS.

Penetration Testing

- Internal Our experts execute a simulated hack, or “ethical hack,” from inside the client's network in an attempt to obtain classified network assets. Upon completion, the client will receive an easy-to-understand report summarizing the results and prioritizing vulnerabilities.
- External Our experts execute a simulated hack, or “ethical hack,” from outside the client's network in an attempt to access the network and obtain classified network assets. Upon completion, the client will receive an easy-to-understand report summarizing results and prioritizing vulnerabilities.
- Wireless Our experts will identify all wireless access points, attempt to intercept traffic and attempt to introduce an unauthorized wireless device on a network. Upon completion, the client will receive an easy-to-understand report summarizing results and prioritizing vulnerabilities.
- Social Engineering Our experts execute a simulated breach using social and physical testing techniques in an attempt to gain access to a client's restricted physical areas and sensitive networks, systems and data. Upon completion, the client will receive an easy-to-understand report summarizing results and prioritizing vulnerabilities.

Managed Security Services

- MSS-UTM Our data security experts configure, manage, monitor and support our own Unified Threat Management (UTM) solution.
- MSS-IPS Our data security experts configure, manage, monitor and support our own Intrusion Prevention System (IPS) - also available unmanaged.
- MSS-IDS Our data security experts configure, manage, monitor and support our own Intrusion Detection System (IDS).
- MSS-NSM Our data security experts continuously monitor and analyze network events on a 24x7 basis and alert administrators when necessary.
- MSS-SLM Our automated log management solution monitors, analyzes and correlates logs on a 24x7 basis and alerts administrators when necessary.
- MSS-mailMAX Our secure e-mail service scans e-mail for viruses, spam and confidential information and quarantines suspect messages before they enter or leave your network.
- MSS-mailMAX Archiving Our secure e-mail service securely stores and archives inbound, outbound and internal e-mail to support compliance and legal discovery efforts.

Trusted CommerceSM

E-Commerce Security Program

- SSL Certificates As a Certificate Authority (CA), we issue a variety of SSL certificates, including Extended Validation (EV) SSL certificates to validate your Web site identity and enable SSL encryption.
- PCI DSS Certificates The full Trusted Commerce program includes access to quarterly external vulnerability scans and an intelligent compliance questionnaire via the Web-based TrustKeeper solution for management and validation of PCI DSS compliance.
- Trusted Commerce Seal Displaying the Trustwave Trusted Commerce seal on a Web site indicates that information (including cardholder data) transmitted or processed through your Web site is done so in accordance with best security practices.

SSL Certificate Solutions

- | | | |
|--------------------------|---|---|
| <input type="checkbox"/> | Standard SSL Certificates | As a Certificate Authority (CA), we issue premium, enterprise, premium wildcard and enterprise wildcard SSL certificates to validate your Web site identity and enable SSL encryption. |
| <input type="checkbox"/> | Extended Validation (EV) SSL Certificates | As a CA, we issue premium and enterprise Extended Validation (EV) SSL certificates. EV SSL certificates require a stringent validation process and give your Web site visitors the highest assurance of your organization's physical, operational and legal identity. In addition, with most browsers used to view the Internet, the Internet-address bar shades green when an EV SSL certificate is present. |
| <input type="checkbox"/> | PCI DSS + SSL Certificate Bundle | As a CA we issue traditional and EV SSL certificates that include PCI DSS compliance validation services. |

Application Security

Application Certification/Assessment

- | | | |
|--------------------------|---------------------------|---|
| <input type="checkbox"/> | PA-DSS RA | Our certified application-security engineers validate proprietary payment applications according to the Payment Application Data Security Standard (PA-DSS). Our PA-DSS Risk Analysis (RA) service includes a pre-assessment of an application's vulnerability to internal and external exploits. |
| <input type="checkbox"/> | PA-DSS | Our certified application-security engineers validate proprietary payment applications according to the PA-DSS. |
| <input type="checkbox"/> | Penetration Testing | Our application-security engineers execute a simulated hack, or "ethical hack," of an application in an attempt to obtain classified network assets. |
| <input type="checkbox"/> | Secure Developer Training | Our application-security experts provide customized training to an organization's development team based on industry best practices and, ideally, application security reviews performed by Trustwave. |
| <input type="checkbox"/> | Code Review | Our application-security engineers inspect application source code and assess the vulnerability of tools and commercial applications used to create and run the application's front and back-end. |

Incident Response

- | | | |
|--------------------------|----------------------------|--|
| <input type="checkbox"/> | Card Compromise | In the event of a possible payment card compromise due to network intrusion, our forensics experts will investigate and submit documentation to appropriate third parties. |
| <input type="checkbox"/> | Card Compromise (Physical) | In the event of a possible payment card compromise due to physical theft, our forensics experts will investigate and submit documentation to appropriate third parties. |
| <input type="checkbox"/> | Data Compromise | In the event of a possible data compromise, our forensics experts will investigate and submit proper documentation to appropriate third parties. |

Risk ProfilerSM

Web-based Risk Assessment

- | | | |
|--------------------------|-------------|---|
| <input type="checkbox"/> | Banks | Risk Profiler, a Web-based risk assessment and data-gathering tool, prioritizes risk in a bank's merchant population and facilitates targeted communication advising merchants on mitigating that risk. |
| <input type="checkbox"/> | Enterprises | Risk Profiler, a Web-based risk assessment and data-gathering tool, prioritizes risk among an enterprise's subordinate units and facilitates targeted communication advising those units on mitigating that risk. |

TrustMinderSM

- | | | |
|--------------------------|---------------------|--|
| <input type="checkbox"/> | Web Content Scanner | An automated content-monitoring solution that scans, inventories and analyzes Web site content (including linked Web sites). |
|--------------------------|---------------------|--|

VendorTrustSM

- | | | |
|--------------------------|-------------------------------|--|
| <input type="checkbox"/> | Partner Compliance Management | An automated evaluation tool that assesses the security posture of all external entities connected to an organization's network. |
|--------------------------|-------------------------------|--|

Compliance Suite

- | | | |
|--------------------------|--|--|
| <input type="checkbox"/> | Automated Compliance and Risk Management | Compliance Suite automates compliance and risk management processes for standards and regulations such as the Control Objectives for Information and related Technology (COBIT), Federal Information Security Management Act (FISMA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), ISO 27001/27002 (formerly 17799) information security standard developed by the International Organization for Standardization, Critical Infrastructure Protection reliability standards developed by the North American Electric Reliability Corporation (NERC CIP), Special Publication 800-53 developed by the National Institute of Standards and Technology (NIST 800-53), Payment Card Industry Data Security Standard (PCI DSS), Statement of Auditing Standards Number 70 (SAS-70), Sarbanes-Oxley (SOX) Act of 2002 along with internal policies and standards. |
|--------------------------|--|--|

ATM Audit

- | | | |
|--------------------------|------|---|
| <input type="checkbox"/> | TG-3 | Our certified TG-3 auditors validate compliance with the Retail Financial Services Compliance Guideline regarding online PIN security and key management. |
|--------------------------|------|---|

Security Consulting

- | | | |
|--------------------------|-----------------------|---|
| <input type="checkbox"/> | Policies & Procedures | Our data security experts advise in the development and creation of an information security policies and procedures document as required by the PCI DSS. |
| <input type="checkbox"/> | Security Architecture | Our data security experts advise in the development and creation of a centralized, PCI DSS-compliant payment card system. |
| <input type="checkbox"/> | Gap Analysis | Our data security experts present a brief overview of the PCI DSS, perform an on-site facility assessment and create a detailed report based on the findings. |
| <input type="checkbox"/> | Onsite Implementation | Our data security experts will travel to any facility to implement and configure any security device. |

