Solutions for the Financial Services Industry

For businesses in the financial service industry—including banks, credit unions and brokerages—Trustwave® offers the right formula to help these businesses secure data and comply with regulations.

Au Authentication

DLP Data Loss Prevention

IPS Intrusion Prevention System

IDS Intrusion Detection System

NAC Network Access Control

LM Log Management

UTM Unified Threat Management

SSL Digital Certificates

EV Extended Validation SSL Certificate

VS Vulnerability Scanning

PT Penetration Testing

Trustwave, in serving thousands of organizations to help them secure their information, is best positioned to address the information security needs of financial institutions. Our security services provide protection for critical assets, infrastructure and customer data, while our compliance solutions help to ensure the enterprise is meeting and maintaining compliance with the appropriate industry regulations and requirements.

To help businesses in the financial industry defend against malicious attacks and data theft, while also building customer trust, Trustwave offers data and Web site security solutions that address the needs outlined above, among others. These solutions provide risk mitigation, build customer trust and help to ensure policies and procedures are understood and followed.

Meeting Regulations and Requirements

The solutions outlined below can be used to meet a variety of industry regulations and security standards. Our solutions help in addressing the requirements of the following:

- PCI DSS Requirements
- Sarbanes Oxley (SOX)
- Graham Leach Bliley (GLBA)
- Federal Trade Commission (FTC) Red Flag Rules

Risk Mitigation

Protecting Financial Institutions and their Customers

More so than any other industry, institutions in the financial services sector are entrusted to safeguard their customers' sensitive data in the course of doing business. Malicious attacks on computer systems and data theft should be an ongoing concern for these organizations, as these attacks often lead to loss of proprietary or personally identifiable information, or to loss of reputation.

Trustwave has the managed security services to protect businesses around-the-clock, every day of the year.

Unified Threat Management (UTM)—A managed firewall service, UTM provides comprehensive managed security consolidated in a single appliance. Supported and monitored by our dedicated 24x7 Security Operations Center (SOC), the service addresses organizations' major security concerns and controls at the network perimeter, offering cost and space savings over component-specific appliance purchases and the overhead cost of in-house management. The service also helps address compliance requirements for PCI DSS, Sarbanes-Oxley controls, Graham Leach Bliley and other governmental and consortium regulations.

Intrusion Prevention System (IPS)–An asset-centric, easy-to-deploy and adaptive enforcement technology, IPS works to complement the firewall perimeter. Trustwave's IPS auto-tunes in real-time to address vulnerabilities specific to a company's network; this tailored approach strengthens the perimeter defenses while cutting down on false positives that can hinder legitimate traffic.

Intrusion Detection System (IDS)—Trustwave's SOC manages the IDS sensors that monitor network traffic to identify anomalous or potentially malicious activity; the SOC team analyzes events and notifies clients in cases of actual threats. IDS identifies the most severe exploits including worms, viruses, buffer overflows and denial-of-service attacks. With our easy-to-use, Web-based portal, businesses have 24X7 accesses to a range of valuable data and information, which also support audit documentation requirements.

A Analyze

P Protect

V Validate

For more information about Trustwave's Elements of Compliance and Data Security please visit: www.trustwave.com

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Trustwave® Information Security & Compliance

About Trustwave

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure - from the network to the application layer – to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multi-lingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

A Analyze P Protect V Validate

For more information about Trustwave's Elements of Compliance and Data Security please visit: www.trustwave.com

Internal Vulnerability Scanning (IVS)—Trustwave's IVS service places one or more scan engines inside the network firewall to monitor for vulnerabilities on internal systems by deploying IVS appliances pre-configured to the specifications of a company's network environment. Scan setup and configuration is performed through Trustwave's TrustKeeper Web portal, with vulnerability report results also available through the portal. Trustwave scans are designed to detect more than 5,000 known network, operating system and application vulnerabilities--including the SANS Top 20.

Security Event and Log Management (SELM)—The SELM solution collects, analyzes and stores logs from networks, hosts and critical applications. Trustwave's SELM is provided as a managed on-premise event collector, transmitting the raw log data to Trustwave's SOC for analysis, reporting and archiving. The SELM solution helps companies meet requirement 10 of the Payment Card Industry Data Security Standard (PCI DSS), and other regulatory standards.

Network Access Control (NAC)—A network-based solution, NAC requires no agent software and automatically performs risk assessments on all end-points—regardless of IP device type or operating system (OS), or whether the end-point is managed or unmanaged. When an endpoint is determined to be out of policy with respect to network admissions policy, the Trustwave NAC appliance virtually steps in to quarantine and isolate the endpoint from the network.

Data Loss Prevention (DLP)—Trustwave's DLP is the only outbound content control solution that enables businesses of all industries to gain complete visibility into all insider risk, whether inadvertent or malicious, and to control violations before they occur. With predefined compliance packages that specifically address standards such as PCI DSS, HIPAA and GLBA, Trustwave's DLP patented classification technology precisely monitors data to ensure compliance with company policy.

Two-factor Authentication—Trustwave's two-factor authentication solution couples digital certificates with an organization's existing VPN infrastructure. This certificate-based authentication drastically reduces the cost of an authentication solution while eliminating the need to track inventory of physical tokens and maintain associated technology such as servers. This authentication solution meets standards set forth by the PCI DSS.

Building Customer Trust

Online Business Validation and Security

Maintaining a secure Web site by taking the appropriate steps, such as application penetration testing and vulnerability scanning, helps financial institutions meet compliance requirements and other regulations, while also ensuring business continuity. Identity protection services help to secure trust in one's Web presence.

Trustwave has the services to secure and validate any business online.

Application Penetration Testing—Conducted by experienced security investigators, Trustwave's application penetration tests are attack simulations intended to expose the effectiveness of an application's security controls by highlighting risks posed by actual exploitable vulnerabilities within an application. Using a manual testing process, this service goes much further than automated application assessment tools, which are rife with generic responses, false positive findings and lack of depth in testing. Using our proprietary methodology, Trustwave is able to demonstrate actual exploitable vulnerabilities within an application, and then provide both tactical and strategic recommendations to resolve and prevent risks.

Extended Validation SSL—Trustwave offers a variety of SSL certificates, including Extended Validation (EV) SSL certificates, which validate a business' Web identity and ensure visitors are using a trustworthy Web site. EV SSL certification includes a meticulous dual-validation process; Trustwave's expertise allows us to streamline this process.

Web Site Seals—Businesses receiving SSL and other Web identity services from Trustwave are eligible to display the Trusted Commerce security seal—a visible indicator used by countless businesses to assure Web visitors that payment card information and other sensitive data provided to your Web site will not fall into the hands of malicious individuals seeking to profit from stolen consumer data.