

TrustKeeper® Agent



Expand your compliance management solution with TrustKeeper Agent – gain continual insight into the security and compliance status of systems previously out-of-view.

Monitoring Compliance in Distributed Environments

Controlling and monitoring common standards across multiple locations such as retail outlets, subsidiary business units or franchises proves especially difficult for enterprises, merchant banks and other large organizations. Disparate systems make dedicating a centralized resource to monitor and inventory each system costly to implement and maintain. Similarly, for acquiring banks and processors that must ensure their merchants' compliance with the Payment Card Industry Data Security Standard (PCI DSS); monitoring the equipment deployed, security policies enforced and data stored at each merchant's location becomes unmanageable.

Adding to the compliance demands placed on enterprises, acquirers and processors is the fact that many merchants, franchisees and retail outlets lack the IT staff and data security knowledge necessary to address the complexities of compliance. This lack of knowledge can lead to the use of antiquated, vulnerable Point-of-Sale (POS) or back-of-house technology and the improper configuration of work stations and other networked technology. In addition, many smaller merchants or retail stores connect to the Internet via broadband connections that use Dynamic Host Configuration Protocol (DHCP). DHCP connections periodically change a merchant's IP address making the external vulnerability scans required by the payment card brands difficult to execute, if not impossible.

Despite these challenges, various compliance frameworks such as the PCI DSS do not flinch or falter. For example, the PCI DSS prohibits the storage of magnetic stripe or track data and unencrypted payment card data and, like other frameworks, calls for specific security policies on machines that handle sensitive data. The larger an organization's network of subordinate entities, the more difficult it is to monitor policy settings on computers at each location and ensure that sensitive data is not vulnerable to compromise.

TrustKeeper Agent: Real-time Compliance Assurance

TrustKeeper Agent, working in tandem with Trustwave's leading compliance management solution TrustKeeper, eases and accelerates the compliance initiatives of enterprises, merchant banks and other large organizations that must manage compliance among a large group of subordinate units, departments, franchises or retail outlets. By scanning, aggregating and reporting on prohibited data storage, system configurations and security policy settings on any system on which it is installed, TrustKeeper Agent provides current, accurate information about remote systems' compliance and general security status.

About Trustwave

Trustwave is a leading, global provider of information security and compliance management solutions to large and small businesses and the public sector. Trustwave offers and supports SSL certificates, proprietary security appliances, managed security services and compliance management solutions to help organizations simplify, accelerate and validate their compliance with industry standards and regulations such as PCI DSS, HIPAA, SAS-70, GLBA and ISO 27002 (formerly 17799) among others. Trustwave's clients include financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

www.trustwave.com 1-888-878-7817



TrustKeeper Agent facilitates compliance via:

- System scans for forbidden data such as payment card track data and unencrypted account numbers
- Validation of systems' security policies such as passwords, user accounts, configuration and other settings
 - Measures security settings against specific compliance requirements
 - Identifies any gaps between current policy and specific compliance requirements
- Beacon functionality that enables external vulnerability scanning of locations that connect to the Internet via broadband Internet Service Providers (ISPs) and as a result use dynamic IP addresses

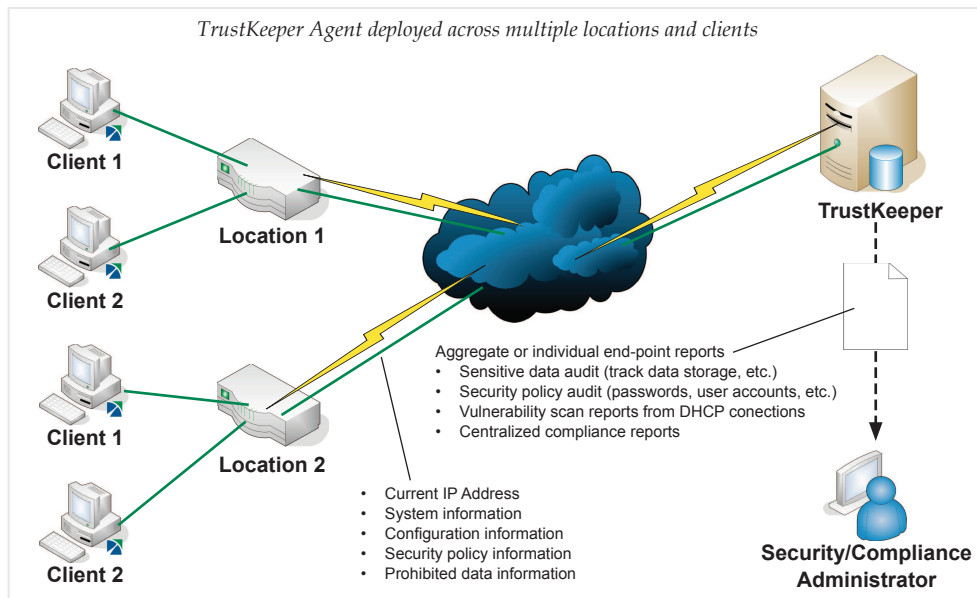
Beyond the Questionnaire: Corroborating Evidence

One major obstacle faced by an organization looking to ensure the compliance of subsidiary units is the lack of IT expertise among staff expected to report on those units' compliance. The payment card brands recommend that merchants complete the PCI SAQ and undergo quarterly vulnerability scans to validate their compliance with the PCI DSS.

For example, among other questions, the PCI SAQ asks merchants the following about their network environment:

- 3.2 Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point-of-sale products?
- 2.5 Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration?
- 8.5 Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?
- 8.10 Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords.

Without an understanding of the intricacies of their Point-of-Sale (POS) system, a merchant may not know where cardholder data would or would not be stored. A franchisee may not know what services and protocols are installed on their back-of-house system. With the turnover common at many retail stores, a store manager may not know how to keep track of active and inactive user accounts or enforce a strong password policy on store machines. Without IT security knowledge, an individual's answers to the PCI SAQ are questionable at best. TrustKeeper Agent solves the problem by automating part of the process and reporting on all clients deployed on a network and the security policies on those devices – to corroborate the PCI SAQ. The agent then reports back to TrustKeeper to give users a concrete inventory of systems and to validate the compliance status of those systems.



Customizable Reports

Once deployed, TrustKeeper Agent scans each system on which it is installed. The information discovered by the agent is sent securely to TrustKeeper that then gathers the information from all deployed agents to provide an aggregate report. Through TrustKeeper's easy-to-use interface, administrators can then drill-down to view detailed reports on each subsidiary, system or device.

Each TrustKeeper Agent report is divided into six sections that include the following information:

- Report Summary
- System Information
- System Configuration Policy
- User and Password Policy
- System Audit Policy
- Prohibited Data Storage

Report Summary	
Policy Compliance	✓
Prohibited Data	●
System Information	
System Configuration Policy	
Status	Name
✓	Default Accounts
✓	Administrator Password
?	Screensaver Password
User and Password Policy	
Status	Name
✓	Password Length
✓	Password History
✓	Account Lockout
✓	Account Lockout Duration
✓	Account Expiry
System Audit Policy	
Status	Name
✓	Audit Administrator Activity
Prohibited Data Storage	
Status	Name
●	Track Data
●	Unencrypted PAN