Trustwave SIEM Solutions

SIEM

Security Information and Event Managment

Trustwave Security Information and Event Management (SIEM) solutions provide a wide range of effective, efficient logging, logging and event management, threat management, and incident response information.

For organizations that need a log and event management solution to identify security threats, or comply with regulations

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 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

Effective Analysis, Multiple Solutions

Trustwave features a low total cost of ownership across our SIEM solutions. As organizations add more data sources or evolve risk management policies, our SIEM solutions can be configured to meet those demands. Trustwave's industry-recognized security expertise features in the extensive compliance reporting, metrics and correlations of our SIEM solutions, to the insight offered by our Technical Assistance Center (TAC), Security Operations Center (SOC), and professional services staff.

We offer three flexible product options: SIEM, SIEM Operations Edition (OE) and Managed SIEM.

Trustwave SIEM: Turnkey Appliances

For the fastest path to securing the network, Trustwave offers plug-and-play SIEM appliances.

- Audit-ready reporting on compliance objectives
- Real-time access to security events and logs
- Powerful correlation and analysis
- Rapid search using visual analysis
- Granular permissions support organizational roles
- Turnkey appliance requires no other infrastructure
- High-speed secure log collection

Trustwave SIEM Operations Edition: Customizable Software

With SIEM OE, Trustwave provides daily automated value for organizations concerned with regulatory compliance or monitoring the effectiveness of internal controls:

Advanced Correlation

- Advanced configuration such as time-of-day logic, out-board filters, etc.
- Custom rule logic including lookup and updated dynamic lists for stateful correlation
- Prioritization and false positive reduction via advanced alert scoring algorithms

Alert Contextualization

- Add context from state, history, and external lookups for asset and other details
- Custom rules logic for alert routing, assignment, resolution and escalation

Alert Management Console

- Alert view with auto-assessment, customizable detail, and contextual forensic tools
- Complete reporting for audit trail of comments and actions, including both automated and manual

Trustwave Managed SIEM: Cloud Services

Perfect for PCI DSS compliance and organizations with limited staffing, Managed SIEM offers several benefits:

- Zero capital expenditure
- No staffing required
- Interactive reporting portal
- Scales effortlessly as the network grows
- Expert analysis from Trustwave's 24x7 Security Operations Center (SOC)

Advanced, Customizable Solutions

SIEM is a critical element of a comprehensive information security strategy. With Trustwave's SIEM solutions, customers can protect vital information assets from cybercriminals, malicious insiders and involuntary mistakes that threaten data security.

Security Monitoring Your Way

Regardless of how SIEM is delivered, security monitoring can be managed in one of four ways:

- Product Purchase: Trustwave SIEM provides the right tools for you to manage security events better, faster.
- Self-Service: Businesses conduct their own review and analysis of logs while Trustwave builds and maintains the infrastructure.
- Daily Analysis: Need assistance analyzing logs? With this option Trustwave experts review logs once daily, sharing any relevant information and analysis. Our Daily Analysis option is ideal for helping businesses achieve compliance with requirement 10.6 of the Payment Card Industry Data Security Standard(PCI DSS).
- Real-Time: For the highest level of security and full service, Trustwave experts will provide real-time monitoring and alert escalation.

Trustwave offers the flexibility of matching the right technology and service level to the business needs. As a business grows and changes, Trustwave can easily change the technology or service level without switching vendors or technology platforms.

Demonstrate Compliance and Mitigate Risk

Trustwave SIEM helps customers demonstrate compliance for:

- Payment Card Industry Data Security Standard(PCI DSS)
- Sarbanes-Oxley (SOX)
- Health Insurance Probability and Accountability Act (HIPAA)
- Graham-Leach-Bliley Act (GLBA)
- North American Electric Reliability Corporation (NERC)
- Federal Information Security Management Act (FISMA)
- And state and other data security regulations

Automated, on-demand reports and dashboards improve visibility into security events to help accelerate investigation and demonstrate that compliance threats have been remediated.

Our SIEM technology can also assist in the implementation of a strategic, framework-based approach to risk mitigation. Robust features and reporting can be tailored for ISO, CoBit, ITIL and NIST standards as well as numerous government regulations. Trustwave SIEM solutions provide a simple way to monitor the effectiveness of controls and provide audit-worthy reports to demonstrate the standard of due care.

Defend Against Security Threats

Continuous monitoring from Trustwave SIEM identifies security threats to help protect valuable information assets. Efficient monitoring, analysis and reporting give meaningful insight into the events that threaten the network and can also improve the effectiveness of insider surveillance.

Lower the Cost of Data Security

Insight provided by Trustwave SIEM can lower the cost of managing and remediating data security threats. By helping businesses focus on the most important threats, our solution reduces the time required to investigate and respond.