

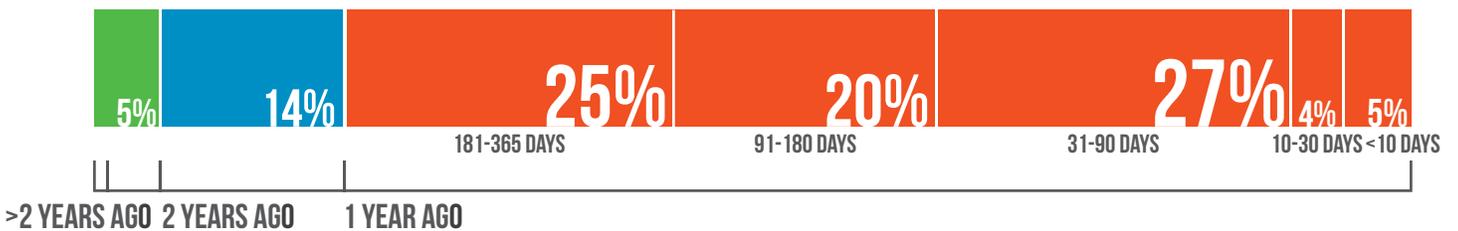
# SIEM PORTFOLIO OVERVIEW

## CONTINUOUS WEB PROTECTION

SIEM technologies are helping businesses improve compliance management, and helping safeguard them from data breaches and fraud. Proactively “seeing” and preparing for evolving threats, and minimizing the impact of those threats by enabling you to collect, analyze, and assess security and non-security events for rapid identification, prioritization, and response are core benefits of our SIEM solutions.

Organizations require the ability to meet today’s compliance and security challenges with the flexibility to address tomorrow’s evolving needs. Trustwave SIEM solutions help organizations meet their mandates with powerful features to monitor and detect threats and manage risk and compliance controls. Our solutions provide the critical insight and information needed for organizations to proactively respond and manage risk in easy to understand ways.

### TIMELINE: INTRUSION TO CONTAINMENT



According to the 2013 Trustwave Global Security Report, businesses took – on average – 210 days to detect an intrusion, while mostly relying on third parties, such as customers, law enforcement or a regulatory body, to detect the breaches. Source: 2013 Trustwave Global Security Report

“Today’s security professionals are demanding more value and manageability out of SIEM. They are looking for ways to advance from traditional log management to more sophisticated threat correlation,

### SIEM YOUR WAY

Trustwave SIEM solutions help businesses of all sizes protect their environment as part of both organizational compliance and defense-in-depth security strategies. We offer a variety of SIEM deployment options including software, virtual, managed security services and appliances that:

- Are engineered and designed to address the full breadth of needs - from log management to sophisticated enterprise security demands.
- Can scale from a single business site to multiple global 24x7x365 Security Operations Centers.
- Function as the nerve center of your unified security approach, enabling other products to share intelligence and events that uncover threats that single, point products miss.
- Include big data intelligent security capabilities as well as interoperability that enable flexible architectures and meets the toughest business, compliance, and technical requirements.

improved security intelligence and sustainable risk management, without the deployment and management complexity that often turns traditional SIEM tools into shelfware.”

## TRUSTWAVE'S SIEM PORTFOLIO

### Log Management Appliances

Simplified log management, compliance, and security coverage for organizations in an easy to manage and use appliance. Can be combined with SIEM Enterprise, SIEM OE, and MSS services for broad SIEM and SIM requirements.

#### Log Management Enterprise

Reporting, Correlation, Dashboards, and ad-hoc analysis and forensics investigation capabilities including powerful searching, and filtering, enabling Security and Compliance deliverables from an easy to use appliance platform.

#### Log Management Operations

Designed for IT Operations with a focus on ad-hoc analysis, powerful search and filter capabilities, with a small number of operationally focused dashboards and correlations.

#### Log Collector

Collects, compresses, encrypts, and forwards logs from one location to an upstream SIEM Product Portfolio component for further processing, analysis, and correlation.

### SIEM Enterprise

Rich appliance or virtual based solution with ease of use, maintenance, exceptional correlation, alerting, and reporting flexibility. Natural fit for customers with more mature requirements than appliances offer by themselves to meet evolving use cases easily.

### SIEM Operations Edition

Advanced, fully customizable software solution for organizations with mature security and compliance programs and skilled staff. Most often leveraged by organizations with a 24x7x365 Security Operations Center and where custom bi-directional integration with enterprise applications is desired.

### Managed SIEM

Focus on your core business and what you do best. Trustwave's global 24x7x365 Security Operations Centers monitor your auditing devices and notify you of threats and compliance risks. Various service levels are available to meet differing requirements. Service may include Managed Log Management Appliances, monitoring, and staff augmentation for management of other SIEM solutions too.



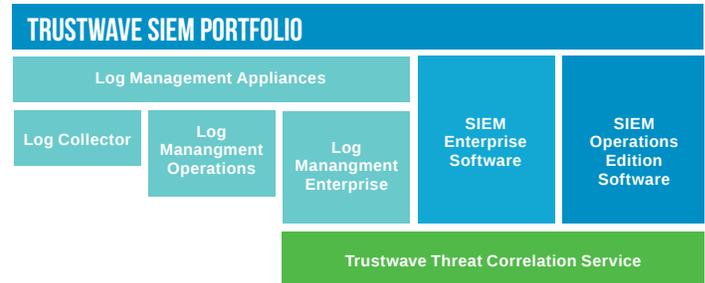
Smart security on demand

For more information: <https://www.trustwave.com>.

Copyright © 2014 Trustwave Holdings, Inc.

### Trustwave Threat Correlation Services

Enhance SIEM Enterprise and SIEM Operations Edition by leveraging valuable intelligence about evolving threats enabling organizations to take proactive measures to protect organizational assets, data, and stakeholders.



Trustwave SIEM Portfolio—fitting your diverse needs—from log management and threat detection to alerting and remediation

## WHAT DO YOU NEED TO ACHIEVE?

### Drive Efficient Compliance

Need to turn compliance into a repeatable, sustainable process and get broader oversight into mandates? Across PCI, GLBA, Sarbanes Oxley, GPG 13, HIPAA, FISMA, NERC/CIP and more, Trustwave's SIEM portfolio can help you meet evolving compliance requirements and centrally manage the compliance process seamlessly across multiple mandates. From our Log Management Appliances that are easy to deploy and use, to robust and highly configurable software, Trustwave delivers a central audit point for collection, analysis, and monitoring so you can get automated and sustainable around compliance, no matter where you need to begin.

### Improve Security Intelligence

The threat landscape is hostile and attackers are more sophisticated than ever. To combat today's advanced and persistent threats proactively, you need holistic intelligence. Trustwave SIEM Enterprise and SIEM OE, with their patented analytics engines combined with the threat intelligence of Trustwave's Threat Correlation Services can cross-correlate data from almost any source, delivering anomaly and trend detection, automated learning, and the ability to easily incorporate critical metadata context intelligence and flexible rule-based and role-based frameworks. That means you can monitor, detect and respond quickly and intelligently to known and unknown threats.

### Turn Information into Action

Information technology can enable new revenue opportunities for business. Through deeper analysis of heterogeneous data across your business, you can gain insights into customer behavior, transaction patterns, and external events. Trustwave's SIEM solutions can deliver advanced and fully customizable platforms and bi-directional integration with a broad range of data sources and applications so you can turn even more information into action.