Trustwave®
Smart security on demand

TRUSTWAVE MANAGED SIEM

EMPOWER YOUR SECURITY PROFESSIONALS

Managing security is a 24x7x365 challenge that many organizations struggle with. You may want, or know you need, a security operations center but weren't sure how to make it happen. Trustwave Managed SIEM helps enterprises see through data noise easily, respond to emerging threats quickly, and cost-effectively maximize protection while proving compliance. Whether your challenge is choosing the right SIEM, fully staffing it, containing costs, or keeping up with new threats and compliance requirements, Trustwave can help.

Only Trustwave delivers SIEM technology optimized for Managed Security Service operation, backed by global security operation centers plus SpiderLabs ethical hackers, and easily integrated to many other technologies and Trustwave managed services.

Trustwave makes SIEM ownership easy with managed log monitoring, threat correlation, fully managed and co-managed options. With more than 15 years developing SIEM technology, and as a leading MSS and security research team, Trustwave is uniquely suited to quickly implement and efficiently operate a SIEM for organizations of all sizes.

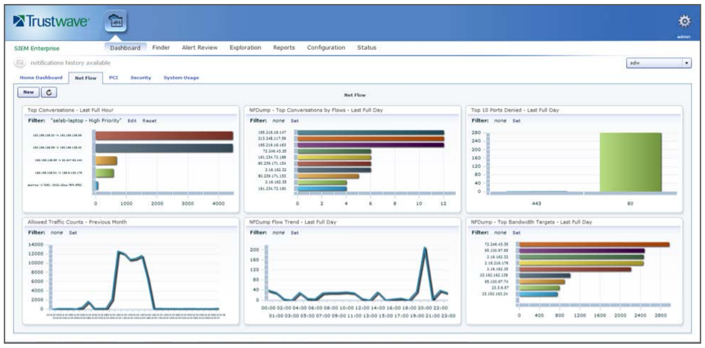
TRUSTWAVE MANAGED SIEM ADVANTAGES:

- **SpiderLabs security intelligence expertise**
- **Industry-leading compliance expertise**
- **Integrated Trustwave security technologies** (SIEM, Big Data, SWG, SEG, UTM, NAC, App/DB/ Network Scanning, DLP, IDS, Endpoint Protection)
- **Transparent, flat-rate pricing**
- **Scales over 1 Billion Events/day**

EASIER SIEM OWNERSHIP

Trustwave empowers your IT security professionals by offloading the tedium of log monitoring and complexity of threat correlation. This frees your team to focus on the escalations they are best situated to investigate and to pursue more strategic concerns. Since Trustwave implements and operates Managed SIEM, deployment is quick and easy. You see everything you want through a "glass-house" portal, and tell us the clear segregation of duties you want with us. Trustwave Managed SIEM helps you reduce the number of incidents and the time it takes to detect and remediate them. We help you achieve "Auditable/Challengeable" metrics for control point monitoring.

If your needs evolve, Trustwave Managed SIEM can evolve with you. Trustwave lets you upgrade appliances from Log Management to SIEM Enterprise inline via license keys. It's simple to add more collectors, managed threat correlation or enhance service level agreements. If you need log collection support for new devices, Trustwave is your best bet. Trustwave is the only SIEM provider that guarantees to add support for new commercially-available devices within 45 days of your request.


Trustwave
admin
SIEM Enterprise
Dashboard
Finder
Alert Review
Exploration
Reports
Configuration
Status
notifications history available
sdw
Home Dashboard
Net Flow
PCI
Security
System Usage
New
Net Flow
Top Conversations - Last Full Hour
Filter: "selab-laptop - High Priority" Edit Reset
0 1000 2000 3000 4000
NFDump - Top Conversations by Flows - Last Full Day
Filter: none Set
0 2 4 6 8 10 12
Top 10 Ports Denied - Last Full Day
Filter: none Set
280 240 200 160 120 80 40 0
443 80
Allowed Traffic Counts - Previous Month
Filter: none Set
NFDump Flow Trend - Last Full Day
Filter: none Set
NFDump - Top Bandwidth Targets - Last Full Day
Filter: none Set

Trustwave Managed SIEM streamlines operations and empowers security professionals.

BEST SIEM VALUE

Trustwave helps you contain many of the costs that make other SIEM offerings break budgets or get thrown out. Trustwave offers the most-fair and transparent pricing model. For a flat monthly fee, your Managed SIEM appliance can hold years' worth of logs on premises. There are no hidden fees for storage or Mb sent to cloud. You know at the start of your subscription exactly how much you will spend for each year of Trustwave Managed SIEM.

Trustwave Managed SIEM reduces upfront budget and headcount requirements.

- We implement SIEM for you as part of a long-term subscription
- No capital expenses
- Our pool of experts eliminates your staffing headaches
- Using our 24x7x365 SOC reduces your SOC costs

"Managed" SIEM more efficient than "Do-It-Yourself."

Managed SIEM prevents paying for an idle or under-utilized in-house threat correlation expert. Our SIEM experts gain skills serving many enterprises, so they recognize threats sooner and more efficiently than in-house staff. Managed SIEM also helps you avoid time consuming, costly recruiting and training of hard-to-find security specialists. Managed SIEM avoids the disruption of security staff being recruited away by other organizations.

Biggest Potential Savings

Potentially the largest cost-reduction benefit of Managed SIEM is produced by earlier breach detection. Early breach detection helps you contain attacks before they escalate privileges and exfiltrate data. This reduces the number of systems that have to be quarantined, reimaged, and restored. Early breach detection also reduces the chance of legal costs, PR costs, customer retention expenses, and lost revenue from brand damage.

CORRELATION AND ALERTING

Trustwave Managed SIEM offers the intelligence and automation to correlate and analyze high volumes of log and audit events from across disparate systems and applications. Powerful big data enabled intelligence systems cover nine core correlation dimensions including:

- Asset based
- Behavior based
- Heuristic based
- Historical based
- Risk based
- Rule based
- Statistical based
- Threat based
- Vulnerability based

EMBEDDED THREAT INTELLIGENCE

Built into your relationship with Trustwave is a deep and broad amount of embedded threat intelligence. Trustwave solutions pull feeds from our Global Threat Database, which is enriched by many original, best-of-class and unique data sources. Trustwave Managed Vulnerability Scanning, IDS and WAF solutions produce massive amounts of detection information. Many Trustwave customers allow our products to send sanitized detection information to SpiderLabs. Our SpiderLabs group conducts hundreds of forensics and incident responses each year discovering new targeted malware in the wild. SpiderLabs also performs thousands of penetration tests, discovering new vulnerabilities every month. We operate spam traps to find millions of spam, malicious attachments and phishing emails every day. We operate honeypots to monitor evolving hacking techniques. We conduct extensive community monitoring of underground criminal forums, private mailing lists, IRC and even Twitter traffic. From all of this input into our Global Threat Database, we produce many outputs including Known Bad Actor Lists, URL, Domain, IP's, Botnet's, Phishing, malware Hashes and Heuristic feeds.

POPULAR OPTIONS

Service Levels	Log Management Enterprise Appliance	SIEM Enterprise Appliance
Self-Service Compliance (Trustwave installs & administers SIEM platform)	●	●
Compliance Monitoring Service	●	●
Threat Analysis Monitoring (real-time review)	●	●
Local Correlation and Operational Workflow		●
On-premise Integration of Threat Correlation/Spiderlabs KBA		●

*Appliances available as virtual or hardware

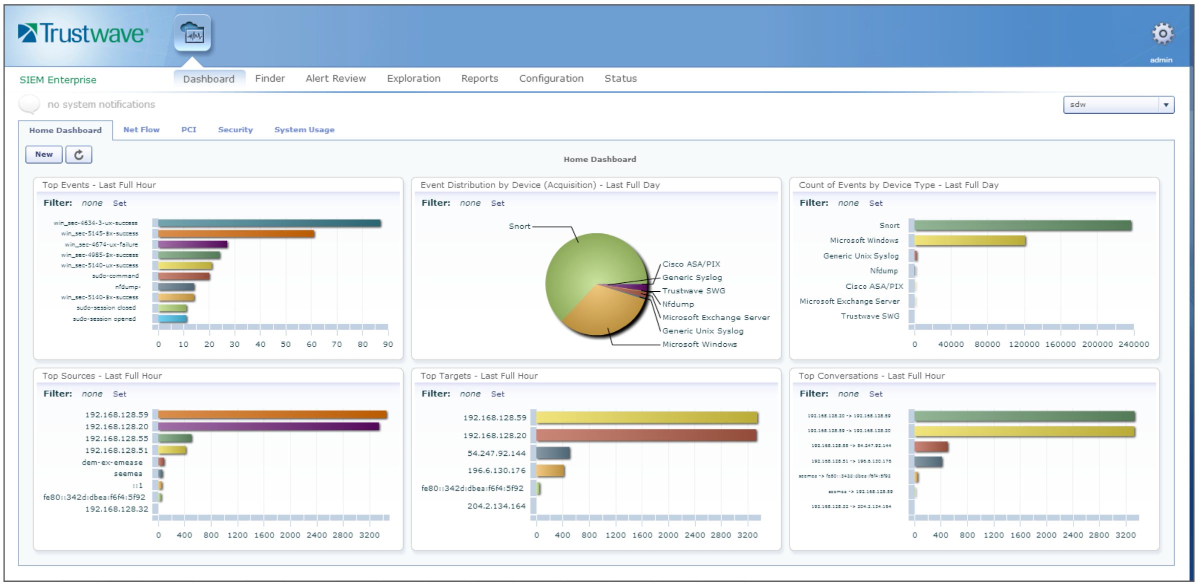
WHAT DO YOU NEED TO ACHIEVE?

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. Our Managed SIEM Appliances can conveniently provide you the insight to comply and the reports to demonstrate compliance. Trustwave offers a central audit point for collection, analysis, and monitoring so you can get automated and sustainable around compliance. Trustwave's model is cost-optimized for compliance, charging only for the elements you need, and providing the expertise to make it as easy and assured as possible. Trustwave provides out of the box tools to help make compliance easier for you, Correlations that support compliance, compliance related dashboard widgets and summarized data ensure you meet the auditors' requirements, on time and in a concise format.

Improve Security Intelligence

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



Trustave Managed SIEM provides convenient and powerful "Glass House" visibility into diverse security processes

Trustwave®

Smart security on demand

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