Empower your security professionals yes

Whether your challenge is choosing the right SIEM, fully staffing it, containing costs, or keeping up with new threats and compliance requirements, Optus Managed SIEM combined with Security and Compliance Monitoring powered by Trustwave® can help.

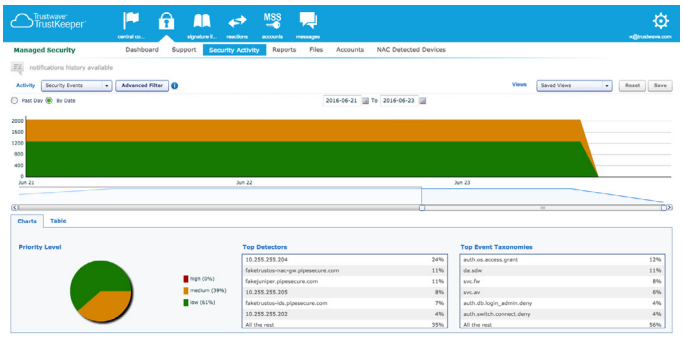
Advantages

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

Managing security is a 24x7x365 challenge that many organisations struggle with. You may want, or know you need, a security operations centre but weren't sure how to make it happen. Optus Managed SIEM powered by Trustwave combined with Optus Security and Compliance Monitoring services powered by Trustwave helps enterprises see through data noise easily, respond to emerging threats quickly, and cost-effectively maximise protection while proving compliance.

Optus Managed SIEM powered by Trustwave delivers SIEM technology optimised for managed security service operations, backed by global security operation centres plus Trustwave SpiderLabs ethical hackers, and easily integrates many other security technologies and Optus managed security services powered by Trustwave.

Optus makes SIEM ownership easy. A managed SIEM scales and adapts to your needs and capabilities – from acting as a smart collector performing log analysis and working in conjunction with Optus' Manage Security Services powered by Trustwave or providing SIEM capabilities on premise to your security team. 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 organisations of all sizes.



Example of the TrustKeeper® portal that help you to see the current security state of your network.

Easier SIEM ownership

Optus Powered by 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 Optus powered by 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 from us. Optus Managed SIEM powered by Trustwave helps you reduce the number of incidents and the time it takes to detect and remediate them.

If your needs evolve, Optus Managed SIEM powered by Trustwave can evolve with you. You upgrade appliances from Log Management to SIEM Enterprise inline via license keys. It's simple to add more collectors, or managed threat correlation services. If you need log collection support for new devices, you can also add support for new commercially-available devices within 45 days of your request adding to the already diverse set of 500 supported sources.

Best SIEM value

Optus Managed SIEM powered by Trustwave helps you contain many of the costs that make other SIEM offerings break budgets or get thrown out. 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.

Optus Managed SIEM powered by Trustwave 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

OPTUS | Trustwave®

staffing headaches

- Use our 24x7x365 SOC by subscribing to Compliance Monitoring or Threat Analysis services and reduce your SOC costs

"Managed" SIEM more efficient than "Do-it-yourself"
Optus Managed SIEM powered by Trustwave prevents paying for an idle or under-utilised in-house threat correlation expert. Because Trustwave SIEM experts gain skills serving many enterprises, they recognise threats sooner and more efficiently than in-house staff. Optus Managed SIEM powered by Trustwave also helps you avoid time consuming, costly recruiting and training of hard-to-find security specialists. Optus Managed SIEM powered by Trustwave avoids the disruption of security staff being recruited away by other organisations.

Biggest potential savings
Potentially the largest cost-reduction benefit of Optus Managed SIEM powered by Trustwave 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

Optus Managed SIEM powered by Trustwave offers the intelligence and automation to correlate and analyse 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
- Behaviour
- Heuristic
- Historical
- Risk
- Use case
- Statistical
- Threat
- Vulnerability

Embedded threat intelligence

A deep and broad amount of embedded threat intelligence is available with the Optus Security and Compliance Monitoring Service powered by Trustwave. This service pull feeds from our Global Threat Database, which is enriched by many original, best-of-class and unique data sources. Optus Vulnerability Scanning, IDS and WAF solutions powered by Trustwave produce massive amounts of detection information. Many customers allow our products to send sanitised detection information to Trustwave SpiderLabs. Trustwave SpiderLabs group conducts hundreds of forensics and incident responses each year discovering new targeted malware in the wild. Trustwave 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.

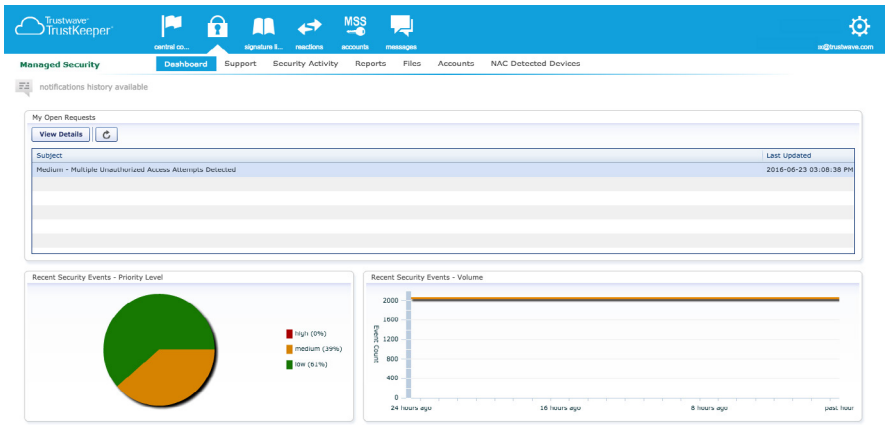
Popular Options

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

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, Optus' Security and Compliance Monitoring powered by Trustwave can help you meet evolving compliance requirements and centrally manage the compliance process seamlessly across multiple mandates. The Managed SIEM Appliances can conveniently provide you the insight to comply and the reports to demonstrate compliance. The Optus Managed SIEM powered by Trustwave offers a central audit point for collection, analysis, and monitoring so you can get automated and sustainable around compliance. The Optus Managed SIEM powered by Trustwave model is cost-optimised for compliance, charging only for the elements you need, and providing the expertise to make it as easy and assured as possible. The Optus Managed SIEM powered by Trustwave provides out of the box tools to help make compliance easier for you, Correlations that support compliance, compliance related dashboard widgets and summarised 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. Optus Managed SIEM powered by Trustwave, with patented analytics engines combined with threat intelligence 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.



Example of the TrustKeeper® portal that helps you to see the current security state of your network.

GMO_N 0454 1116MZ