SIEMonster

The SIEM Solution for Everyone

SIEMonster is a cybersecurity game-changer. A turnkey, open source, enterprise-grade Security Information and Event Management (SIEM) solution, SIEMonster was developed as a scalable, cost-effective alternative to the existing commercial SIEM solutions. Contrary to traditional SIEM solutions, the base software package is free, and the licensing model has no data or node limitations. SIEMonster is fully documented as well as has optional software, services, and Enterprise Support upgrade packages.

What is a SIEM?

Protecting your company's assets from cyber-attacks is a never-ending complex task. An effective defense requires visibility across your entire environment. Most devices and applications found in a typical IT environment (servers, workstations, security appliances, firewalls, network appliances, anti-virus, endpoint protection, printers, SCADA data, Active Directory, etc.) have the ability to send an event or alert; however, these alerts are not aggregated into a single view, nor correlated across other security events taking place within the environment.

A SIEM solution delivers the critical functionality of 1) collecting data source type event logs 2) correlating this data within a broader security context 3) separating false positives from real threats and 4) alerting security operations that an attack may be underway. Through leveraging SIEM technology, security analysts and engineers are equipped for delivering effective monitoring, response, and remediation services.

SIEMonster: SIEM for Everyone

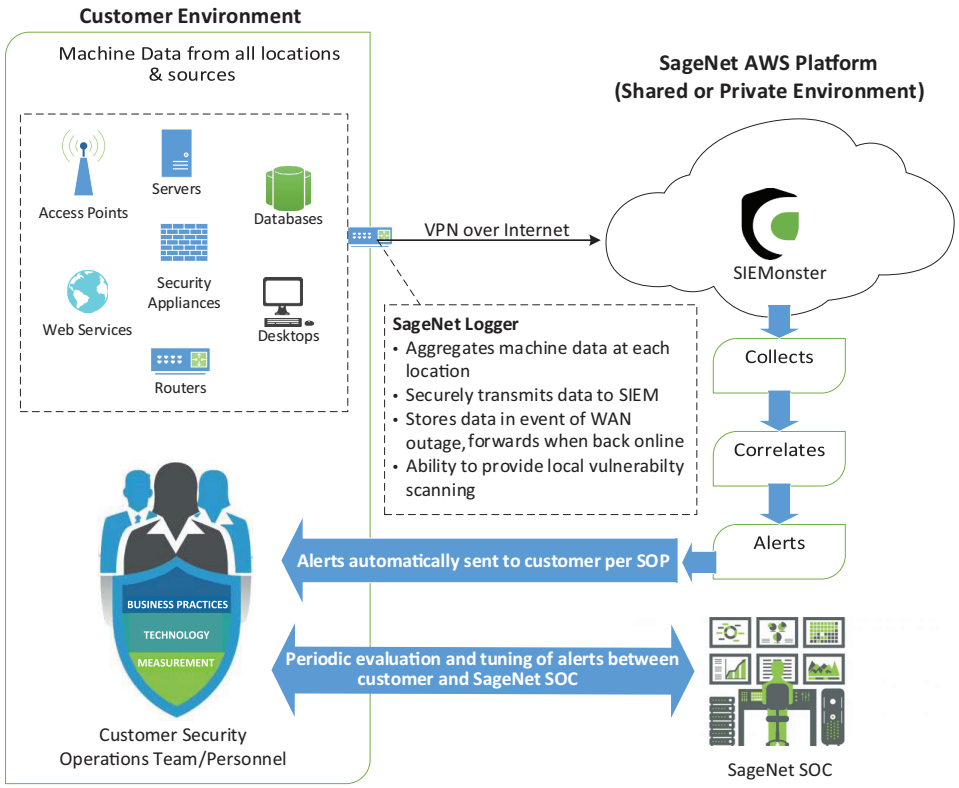
SIEMonster is a turnkey, open-source SIEM solution with security dashboards, plugins and incident response tools that deliver robust enterprise-grade SIEM functionality and empowers Security Operation Centers (SOCs) to operate with great efficiency.

SIEMonster was developed for all companies as a viable alternative to commercial SIEM solutions. As open source components were deliberately selected, the base product will always be free, fully documented, fully scalable, and have no data or node limitations. SIEMonster will continue to be developed by its founding company, as well as support within the community.

Features

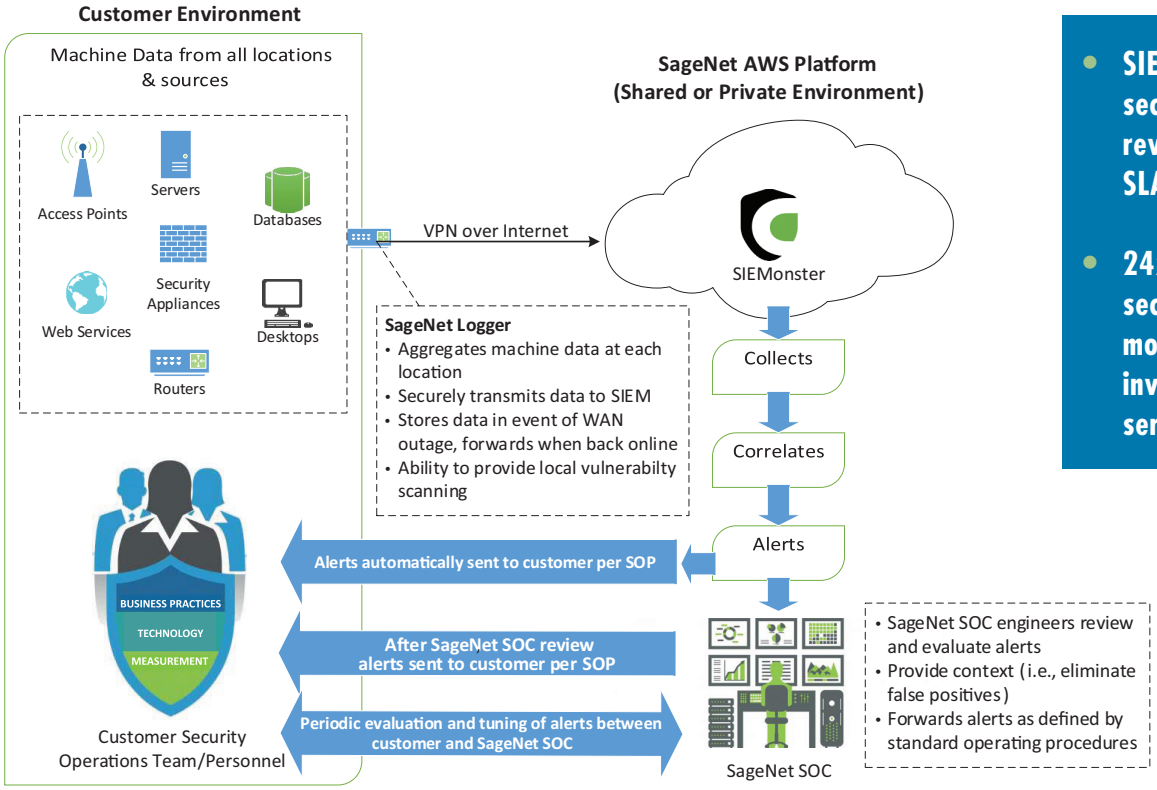
- Open-source, unlimited-use, completely scalable
- User-friendly dashboards provide customized view of security events
- Consolidated vulnerability scanning dashboard
- Incident Ticketing System
- Alerts via dashboard, email, SMS, etc.
- Threat Intelligence
- Available via AWS, Azure, or VM

SIEM as a Service



- SIEM software, infrastructure, automated alerts
- Custom content development & ongoing tuning
- Product support

SOC as a Service



- SIEMaaS plus security engineer review with tiered SLA's
- 24x7x365 security event monitoring & investigation services

Full Lifecycle Services and Support

As the preferred North American reseller of SIEMonster, SageNet offers three ways to take advantage of the SIEMonster platform: Free Community Edition, a Premium Edition, and the Managed Security Service Provider (MSSP) edition. Service and support packages are also available.

	Free	Premium	MSSP
Security Information & Event Management	✓	✓	✓
Live Incident Alerting	✓	✓	✓
VM, Amazon AMI, Azure	✓	✓	✓
Scalable Nodes 2,4,8,16,32,64 Unlimited	✓	✓	✓
Documented	✓	✓	✓
Training Videos	✓	✓	✓
Event Correlation	✓	✓	✓
Interactive Data Visualizations	✓	✓	✓
Incident Ticketing System	✓	✓	✓
Open Source Threat Intelligence	✓	✓	✓
Community Support	✓	✓	✓
Vulnerability Management Integration	✓	✓	✓
Basic Reporting	✓	✓	✓
Elastic Query Conversion Engine	✓	✓	✓
Advanced Scheduled Reporting		✓	✓
Fully containerized for Rapid Deployment		✓	✓
Advanced Event Correlation Engine		✓	✓
Upgrades		✓	✓
Commercial Support and Integration		✓	✓
AD integration Single Sign on		✓	✓
Managed SIEM Infrastructure & Platform			✓
12 Months - 7 Year Data Storage			✓
Disaster Recovery			✓
ISO 27001/27002 Security Framework			✓
Managed 24x7 Real-time Automated Alerting			✓
Optional Add-on Security Operations Center			✓

Support Plans

Feature	Standard Support	Enterprise Support
Access to SIEMonster Documentation	✓	✓
Bug Fixes	✓	✓
Product Roadmap Input	✓	✓
Troubleshooting	✓	✓
Version Upgrade Rights	✓	✓
Support Hours	*8 x 5 M-F*	*24 x 7*
Guaranteed Response Times	*Next Business Day*	*Same Day*
Priority Response		✓
SIEMonster Premium Edition	*Purchased Separately*	✓

The SageNet cybersecurity team consists of experienced professionals with certifications including CISSP, CISA, CISM, CEH, CHFI, AWS Architect as well as many vendor specific certifications. SageNet is vendor-agnostic when delivering security consulting services; however, some leading technology vendors in our partner ecosystem are listed below.

To learn more about SIEMonster visit www.sagenet.com/SIEMonster or call 1-866-480-2263

SIEMonsterBRO062317