SPLUNK

SIEM and SOC as a Service powered by Splunk

MANAGED SIEM AND SOC SERVICES

SageNet leverages Splunk and its premium apps to deliver world-class managed security services. Splunk, the Gartner Magic Quadrant leader in the SIEM space, can be deployed and managed by SageNet either on-premise or in the cloud.

The SageNet Security Operations Center (SOC) operates around the clock with a tiered security analyst/engineer structure paired with automated machine learning for effective security event monitoring, investigation, and response services. SOC services enable identification of anomalous or potentially malicious activity so that action can be taken for containment and remediation, thus helping to mitigate risk to the organization.

SPLUNK ENTERPRISE SECURITY

Splunk Enterprise Security (Splunk ES) is a security information and event management (SIEM) solution that enables security teams to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk, and safeguard your business. Splunk ES enables your security teams to use all data to gain organization-wide visibility and security intelligence. Regardless of deployment model—on-premises, in a public or private cloud, SaaS, or any combination of these—Splunk ES can be used for continuous monitoring, incident response, running a security operations center or for providing executives a window into business risk. Splunk ES can be deployed as software together with Splunk Enterprise, or as a cloud service together with Splunk Cloud.

WHAT IS A SIEM?

An effective defense against cyber attacks 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.

Features

- Gartner Magic Quadrant Leader in SIEM space
- Splunk can be used to operate Security Operations Centers (SOC) of any size
- Support Information Security operations – including posture assessment, monitoring, alert and incident handling, CSIRT, breach analysis and response, and event correlation
- Out-of-the-box support for SIEM and security use cases
- Detect known and unknown threats, determine compliance and use advanced security analytics
- Proven integrated, big data-based security intelligence platform
- Use ad hoc searches for advanced breach analysis
- On-premises, cloud, and hybrid on-premises and cloud deployment options

NEW CRITERIA FOR TODAY'S SIEM

Enterprise security teams must use a SIEM solution that not only solves common security use cases, but advanced use cases as well. To keep up with the dynamic threat landscape, modern SIEMs are expected to:

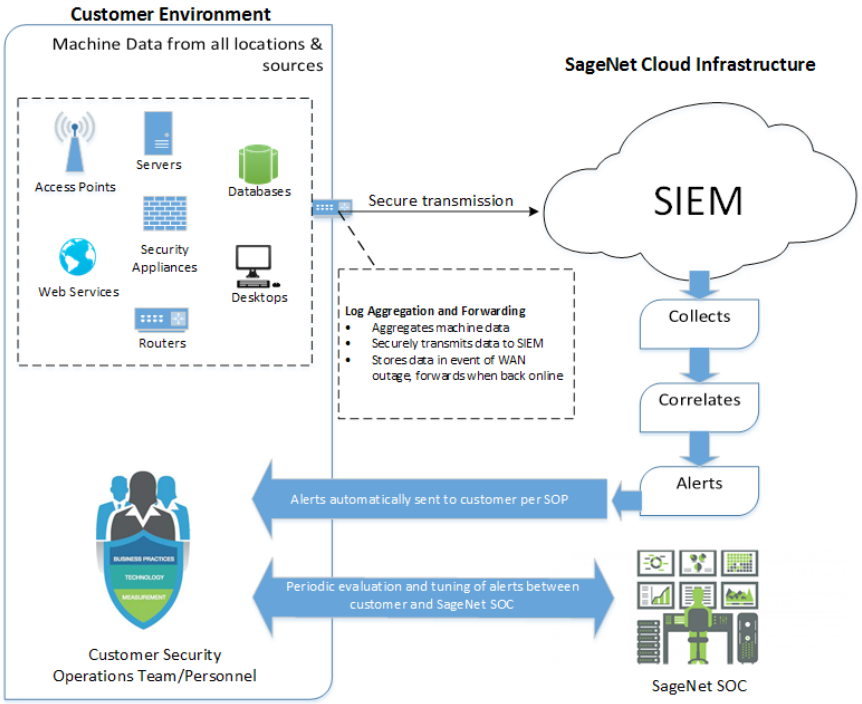
- Centralize and aggregate all security-relevant events as they're generated from their source
- Support a variety of reception and collection mechanisms including syslog, file transmissions, file collections, etc.
- Add context and threat intelligence to security events
- Correlate and alert across a range of data
- Detect advanced and unknown threats
- Profile behavior across the organization
- Ingest all data (users, applications) and make them available for use - monitoring, alerting, investigation, ad hoc searching
- Provide ad hoc searching and reporting from data for advanced breach analysis
- Investigate incidents and conduct forensic investigations for detailed incident analysis
- Assess and report on compliance posture
- Use analytics and report on security posture
- Track attackers' actions with streamlined ad hoc analyses and event sequencing
- Centrally automate retrieval, sharing and responses across the security stack

ALL MACHINE DATA IS RELEVANT

The evidence of an attack, as well as its activities, exists in an organization's machine data. For security teams to properly investigate security incidents and identify threats, all data, including more than security data from traditional security products such as firewalls, IDS or anti-malware, should be brought into the SIEM. Organizations are often missing data needed to have real-time status of their full security posture.

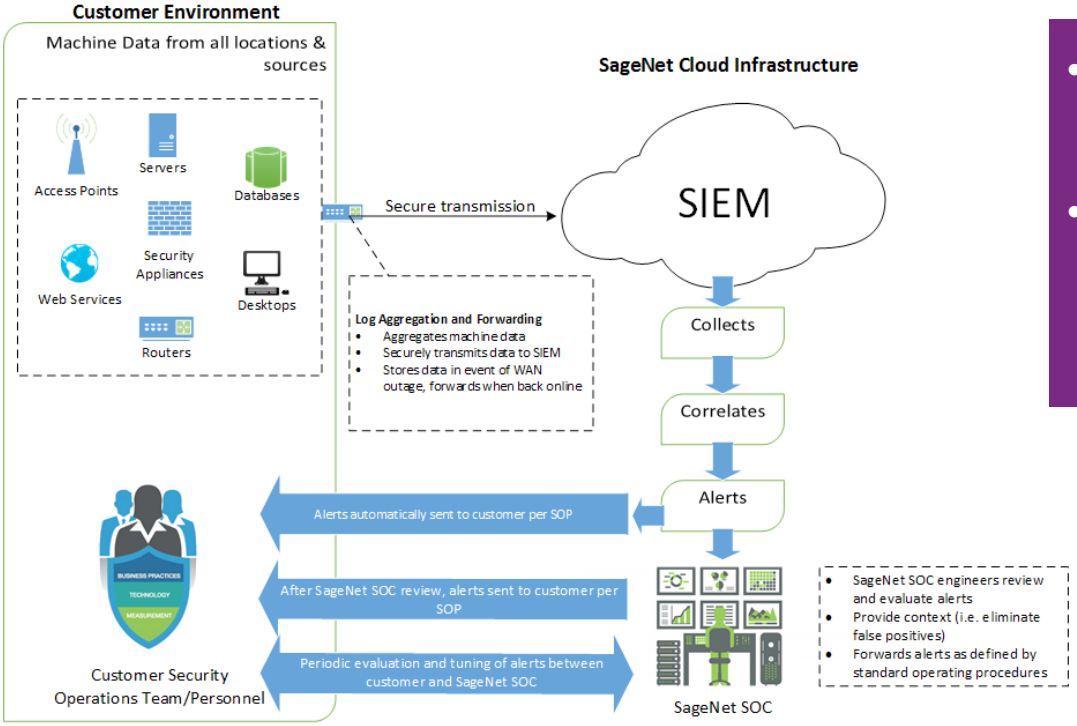
The activities of these advanced threats are often only in the "non-security" data, such as operating system logs, directory systems such as LDAP/AD, badge data, DNS, and email and web servers. Machine data often needs to be supplemented with internal and external threat context such as threat intelligence feeds and other contextual information to aid during incident response and breach detection.

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
- 24x7x365 security event monitoring & investigation services

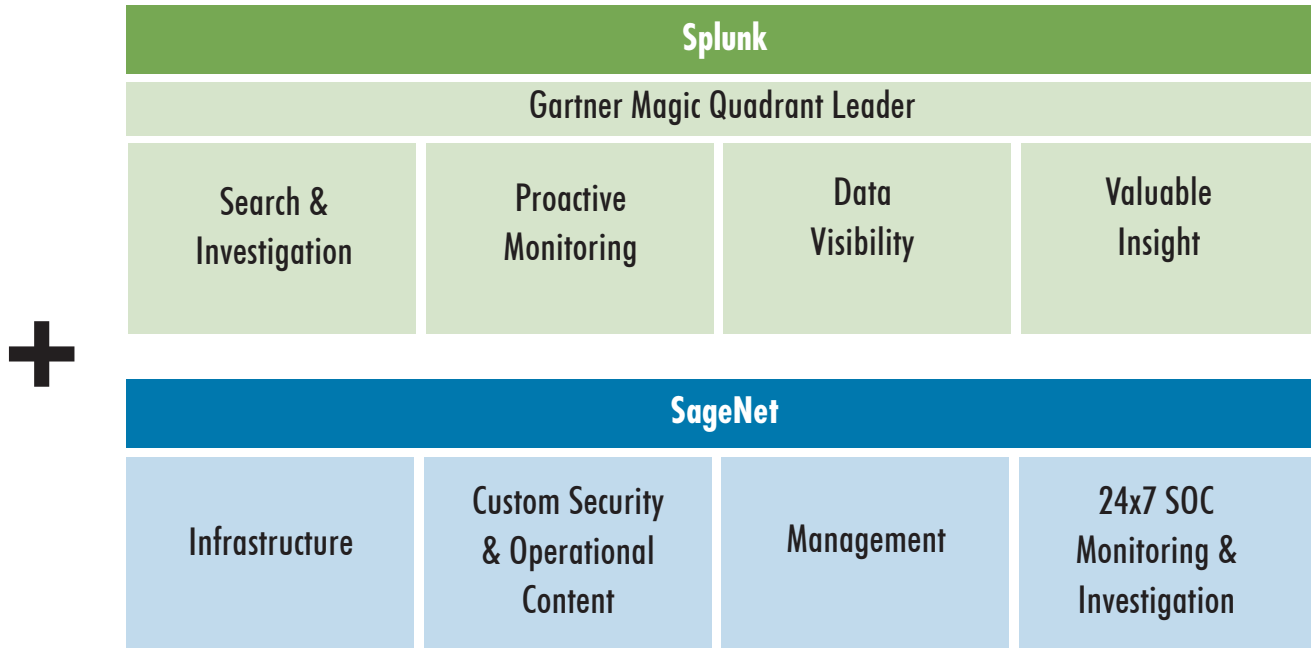
SPLUNK ENTERPRISE SECURITY AT A GLANCE

Analytics-driven security and continuous monitoring for modern threats:

- **Optimize security operations** with faster response times using Adaptive Response and Investigation Workbench
- **Improve security posture** with end-to-end visibility across all machine data, in the cloud and on-premise
- **Increase investigation capabilities** using user behavior analytics, detected anomalies and threats
- **Make better informed decisions** by leveraging threat intelligence

SAGENET AND SPLUNK TOGETHER

Combining the power of Splunk along with our best practices approach and industry leading security knowledge, SageNet can offer our clients fully managed solutions to assist in protecting their environments from the ever changing threat landscape.



= **A Fully Managed SIEM and SOC Solution with the Market Leading SIEM Technology**

To learn more about SageNet and Splunk visit www.sagenet.com/cyber or call 1-866-480-2263.

SplunkBRO_DS090518