At-a-Glance

Highlights

- Defend against multidimensional cyber attacks and known and unknown threats.
- Improve detection and more quickly investigate, contain, and remediate security issues to reduce the impact of security breaches.
- Analyze unlimited types of real-time and historical security and business data for comprehensive, continuous visibility.
- Enable massive scalability, outstanding performance, and low total cost of ownership (TCO) to efficiently keep pace with growth in security analytics data and in the number of simultaneous users.
- Accelerate time to value with a prevalidated solution and applications that facilitate fast integration with your existing security solutions.

Security Analytics on Cisco UCS with Splunk

Maintaining infrastructure and data security has never been more challenging. Today's networks extend beyond traditional walls and include data centers, endpoints, virtual environments, branch offices, and the cloud. They constantly evolve and spawn new attack vectors, including mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, home computers, and an increasing number of smart devices. By 2020, 50 billion connected, data-producing devices will dramatically increase an enterprise's potential attack surface.

Mitigating security risk in today's advanced threat environment is a race against time. Security analysts work in an environment of constant triage—often encountering millions of potential security events each week. Their investigations, however, may reveal only one or two real threats hiding within those events. Their effectiveness hinges on their ability to:

- Filter massive quantities of data
- Make the right decisions about which issues to investigate more deeply to detect real threats
- Conduct forensic searches to identify root causes
- Contain and remediate threats—all while the clock is ticking

Because speed is so important, a security analytics solution must consist of software and hardware infrastructure designed for exceptional big data and analytics performance at scale.

The Cisco Unified Computing System™ (Cisco UCS®) and Splunk deliver a big data security analytics solution that:

- Provides the outstanding performance and scalability needed to process massive quantities of data
- Enables the comprehensive visibility and forensic searches needed to detect threats sooner and respond faster
- Reduces the financial impact of security breaches

Cisco and Splunk: Combining powerful analytics, comprehensive infrastructure visibility with outstanding scalability and performance at a low TCO.

Designed for Today's Advanced Threat Environments

Multidimensional cyber attacks traverse a multitude of systems, networks, protocols, files, and behaviors. The security team must be able to trace the various stages of an advanced threat and link the sequence of events together by finding relationships using any field, across any data, over any time frame. Splunk integrates with your existing security solutions, creates a single data repository to eliminate silos, and provides security analysts with comprehensive, continuous visibility and the capability to analyze unlimited types of real-time and historical data.

Enterprises can choose between two types of solutions to use Splunk for security analytics:

- **Splunk Enterprise** is at the foundation of the Splunk next-generation security intelligence platform. It offers a fundamentally different approach to security and compliance that excels at identifying known and unknown threats. Customers can use Splunk Enterprise to build a customized security analytics solution, using nearly 250 security-relevant applications, most of which are offered free of charge.
- **Splunk App for Enterprise Security** is a ready-to-deploy solution. It uses Splunk Enterprise to extend beyond legacy security information and event management (SIEM) use cases to include comprehensive and continuous monitoring and alerting for fraud detection, incident response, computer security incident response team (CSIRT) support, and compliance functions. It provides support for the most common security data sources and includes more than 45 prebuilt searches, 37 prepackaged dashboards, and 160 reports, as well as incident response workflows, analytics, and correlations that support the most common security use cases.

Both Splunk solutions provide the full lifecycle of security monitoring and management capabilities to deliver end-to-end protection and threat mitigation.

Software can perform only as quickly as the infrastructure on which it is running. Cisco UCS is a powerful and efficient foundation for Splunk security analytics to help security analysts win their race against time.

- **Industry-leading scalability** is essential to keep pace with the large volumes of real-time and historical security and nonsecurity data critical to threat detection. The Cisco UCS portfolio can scale to more than 6,000 servers, so enterprises can be confident that they can scale to support the massive quantities of data required for effective security analytics. And with UCS Manager's service profiles, enterprises can add new UCS servers in minutes.

- **Proven performance at scale:** Your security analytics infrastructure must support large numbers of complex, forensic searches and simultaneous users. Cisco UCS delivers industry-leading performance that has been proven in more than 100 world-record benchmarks, including the TPCx-HS benchmark for big data performance. In real-world Splunk environments, Cisco UCS has delivered outstanding and predictable performance for demanding, large-scale environments with thousands of simultaneous searches.

Next Steps

To accelerate deployment and reduce risk, Cisco and Splunk have created an in-depth Cisco® Validated Design to accelerate deployment of Security Analytics on Cisco UCS with Splunk. Visit Splunk's security website to learn more about Splunk security solutions and gain access to Splunk's range of security applications. Visit www.cisco.com/go/bigdata to learn more about the value of Cisco UCS for your big data and analytics deployments.

C45-735636-00 08/15