splunk>partner+

PARTNER BRIEF

SPLUNK AND CISCO

Operational Intelligence Across Your Cisco Environment and Beyond

- **Splunk integrations with Cisco products and networking solutions empower IT** organizations to quickly troubleshoot issues and outages, monitor end-to-end service levels and detect anomalies
- **Splunk integrations across Cisco's security portfolio** help provide a comprehensive, continuous view of an organization's entire security posture
- **Splunk and Cisco are collaborating** across a range of emerging use cases to enable business transformation
- **Splunk and Cisco deliver exceptional performance** and scale when Splunk software is deployed on Cisco UCS Integrated Infrastructure

Organizations today operate in an environment that's mobile and connected, with traditional boundaries expanding into the cloud and to the very edge of the network. They're exploring new software-defined datacenters and managing an explosion of data from the Internet of Things—industrial data, sensors, wearable devices and more. Applications are being delivered continuously, with some organizations releasing new code multiple times per day.

Every element of the technology infrastructure running an organization (e.g., the webservers, applications, network devices, mobile devices, sensors, etc.) generates massive streams of data in an array of unpredictable formats that are difficult to process and analyze by traditional methods or in a timely manner. This machine data contains a categorical record of user behavior, cybersecurity risks, application behavior, service levels, fraudulent activity and customer experience. It's also the fastest growing, most complex and valuable segment of big data.

Splunk and Cisco Deliver Operational Intelligence at Scale

The Splunk platform turns machine data into valuable insights. It's what we call Operational Intelligence.

Splunk has closely aligned with Cisco to help organizations gain insights from the vast amounts of data generated by Cisco's industry-leading security, networking, wireless, datacenter and collaboration portfolios. These insights enable our joint customers to minimize operational and security risks, improve efficiency and ultimately transform their organizations.

Turn Silos of Data into Operational Insights

Today's IT infrastructure is a complicated, layered group of siloed and interconnected technologies. Virtualized and cloud infrastructures are challenging to control, manage, secure and scale. Gaining visibility across the infrastructure to identify, diagnose and prevent outages is a time-consuming, manual task. Traditional, siloed tools are ineffective because they can't access or analyze all the relevant events across IT to link the various causes of performance issues.

Splunk software helps organizations gain operational visibility across infrastructure tiers and dramatically reduce mean-time-to-investigate

Splunk apps and add-ons provide ready-to-use functions for many Cisco products and platforms including:

- Cisco Advanced Malware Protection (AMP)
- Cisco AnyConnect Mobility Client
- Cisco Application Centric Infrastructure (ACI)
- Cisco ASR/ISR Routers
- Cisco Call Manager
- Cisco Cloud Web Security (CWS)
- Cisco Email Security Appliance (ESA)
- Cisco ASA/PIX/FWSM Firewalls
- Cisco FireSIGHT (Sourcefire)
- Cisco Identity Services Engine (ISE)
- Cisco IPS
- Cisco Meraki Devices
- Cisco Next-Generation Firewall (NGFW)
- Cisco Next-Generation Intrusion Prevention System (NGIPS)
- Cisco Nexus/MDS/Catalyst Switches
- Cisco pxGrid
- Cisco Secure Access Control Server (ACS)
- Cisco Unified Computing System (UCS)
- Cisco Web Security Appliance (WSA)
- Cisco WLAN Controller

(MTTI) and mean-time-to-resolve (MTTR) to keep critical services running.

Over a dozen free Splunk apps and add-ons for Cisco products and platforms provide ready-to-use functions ranging from optimized data collection to prebuilt visualizations. These integrations help accelerate correlation across infrastructure tiers for comprehensive operational visibility—from the core to the edge and across the cloud. Organizations can better detect problems at their earliest stages, resulting in higher infrastructure availability and performance while improving management efficiencies.

> **"We can do more with our electronic health records system because we've built a solid foundation with Cisco and Splunk."**
>
> Anne Lara, CIO
> Union Hospital of Cecil County

Infrastructure Snapshot

- **Traditional Network Devices.** Search, alert and report on network events and transactions in real time across a variety of Cisco IOS-based routing, switching and wireless devices for visibility across the complete network stack.
- **Software-Defined Networking Controllers.** Provide fine-grained network telemetry, real-time visibility into dynamic traffic flows and the ability to optimize network resources by taking action in response to changing network conditions or security events.
- **Cisco ACI.** Simplify troubleshooting, particularly in multi-tenant environments, leveraging rich network statistics generated by Cisco APIC. Network admins can proactively avoid incidents with real-time monitoring and alerting across the environment and underlying infrastructure.
- **Servers.** Proactively monitor UCS server capacity, look at historical faults over time to identify trends, track power and cooling costs and more.
- **Collaboration Tools.** Easily browse and report on real-time call data with the ability to set proactive alerts and automatically remediate issues to improve operational efficiency.

Accelerate Threat Detection and Response

In today's advanced threat environment, simple monitoring of traditional security events is insufficient. Security teams must be able to leverage all machine data for advanced analytics capabilities and contextual incident response; and they must be able to rapidly implement new threat detection techniques to reduce time-to-threat-response and make business-centric decisions. Your enterprise requires big data security solutions that can adapt to advanced threats, evolving adversary tactics and changing business demands, providing your security staff with broader insights from new data sources generated at massive scale across IT, the business and the cloud.

Splunk security solutions allow your security teams to quickly detect and respond to internal and external attacks, simplify threat management, and minimize risk. Splunk's analytics-driven security solutions are an ideal complement to Cisco, which has more than 25 years of network security experience and one of the broadest security portfolios in the industry.

Splunk integrations across Cisco's security portfolio facilitate a holistic approach that spans heterogeneous environments, a range of security platforms and all security-relevant data to deliver a complete, continuous view of your organization's security posture.

Better Insights to Drive Innovation and Business Transformation

The Internet of Things is generating enormous quantities of data from billions of new connections that are often located beyond traditional boundaries. With the explosion of web-based and cloud applications, the number of data sources has skyrocketed. Every new data source your company creates or accesses has the potential to provide your business in invaluable insights, if it can be analyzed effectively.

Together, Splunk and Cisco can help organizations transform their businesses across a broad variety of industries and use cases, including:

- **Helping rail operators improve service** by analyzing massive quantities of data from heterogeneous sources and geographically dispersed networks of assets. This helps them track defect forensics, identify the top sources of track defects and improve service reliability.
- **Optimizing customer interactions** for theme parks seeking to provide better experiences for their customers. Splunk's ability to analyze data captured by Cisco Meraki wireless devices can provide insights on line queues via cell phone pings that ultimately enable park customers to spend more time enjoying attractions and less time in line.

Accelerate Time to Insight With Splunk on Cisco UCS

Splunk software scales to collect and index hundreds of terabytes of data per day, across multi-geography, multi-datacenter and cloud-based infrastructures. Cisco's Unified Computing System (UCS) Integrated Infrastructure for Big Data offers linear scalability along with operation simplification for single-rack and multiple-rack deployments.

Technical Reports and Reference Architectures

- Cisco UCS Single Instance and Distributed Architectures for Splunk Enterprise
- Cisco Validated Design: Cisco UCS Integrated Infrastructure for Big Data with Splunk
- Cisco Validated Design: Cisco Cloud Security Virtualized Multiservice Data Center
- Cisco "How to" Guide: Integrating and Monitoring Cisco ISE User-Device Context in Splunk
- Cisco "How to" Guide: Splunk and pxGrid Adaptive Network Control Mitigation Workflow Actions

Cisco UCS has a proven ability to deliver predictable, outstanding performance capable of supporting Operational Intelligence at scale. In addition to being validated in more than 100 worldwide industry performance benchmarks, Cisco UCS delivers exceptional performance and scale in Splunk Enterprise performance benchmark assessments. For example, the latest release of Splunk software was shown to complete searches up to six times faster then the previous release when tested on a 32-core Cisco UCS system.

To facilitate faster and more predictable deployments, Cisco has published multiple reference architectures for Splunk software plus a comprehensive Cisco Validated Design that provides prescriptive, step-by-step guidance for deploying Splunk Enterprise on Cisco UCS.

Together, Splunk and Cisco enable organizations to realize the potential of Operational Intelligence across the organization and gain real-time business insights that create a strategic advantage.

Security Snapshot

- **Threat Intelligence and Analytics.** Sourcefire eStreamer integration with Splunk delivers intrusion, impact, connection, change, application and malware event data as well packet data to Splunk, enabling more comprehensive and up-to-date integration than any legacy SIEM can offer. Cisco IPS data that conforms to the Security Device Event Exchange (SDEE) standard can also be easily consumed and analyzed.
- **Network Activity/Security.** Integration with Cisco firewalls enables advanced monitoring for network-based attacks and helps detect security anomalies. Connections accepted and denied by port is an example of information made easily available by a popular Splunk add-on that supports data from Cisco ASA, PIX and FWSM firewalls.
- **Web Security.** Track and report on web surfing, conduct forensics evaluations to gather evidence, and correlate web logs with other communication and authentication data, such as HR requirements.
- **Email Security.** Simplify email transaction tracing with a form-search dashboard that enables organizations to enter information about the transaction, the sender, recipient and attachments and mine for any email transaction.
- **Access Identity and Context.** Contextual device and user data can be correlated with other security event data to make it easier and faster to investigate a suspicious event to determine if it is malicious or against policy. Compromised users or devices can be instantly quarantined and removed from quarantine when appropriate.
- **Endpoints.** Streamline the collection and reporting of IPFIX flows from laptops and other endpoints both on- and off-premise generated by Cisco AnyConnect NVM endpoint sensor technology. Get granular usage information with drilldowns of destination domains, applications and endpoint processes.

Download Splunk for free at www.splunk.com/download and check out the full library of Splunk Apps and Add-ons at https://splunkbase.splunk.com/. For more information about Cisco products, platforms and solutions please visit www.Cisco.com.

splunk>   ✉ sales@splunk.com   www.splunk.com