Cisco Tetration Analytics and Splunk Drive Performance, Visibility, Security and Compliance across the Entire Data Center IT Environment

Challenges

Applications drive the modern data center infrastructure. But it is becoming increasingly difficult to build a secure infrastructure for these applications, especially when complex applications span hundreds of servers. Two main factors contribute to the challenges.

First, customers are adopting a continuous development model using DevOps. With this approach, applications undergo constant change. This constant change, in combination with virtualization technologies and application mobility, makes it extremely difficult for data center administrators to understand application components and their communication pattern and dependencies. As a result of this dynamic application environment, current static security policies implemented at the perimeter of the network are not sufficient to meet the security requirements of the modern applications.

Second, today's data center is not a single homogenous infrastructure. Components of applications run across different heterogeneous environments, and some run in the public cloud. Gaining full visibility into such heterogeneous environments is important to maintain compliancy. Monitoring endpoints in such a complex infrastructure is increasingly difficult.

How to address these challenges

Organizations require a holistic approach to address these application trends and security challenges. They need a new approach with a solution that:

- Breaks organizational silos: The solution must support different data center operational use cases that span organizational boundaries. It must be able to analyze and correlate data to provide relevant information for network operations, IT operations, Line-Of-Business (LOB), and security teams.
- Enables application segmentation: Customers today must be able to generate policy that can address both application requirements and support business policies. This policy should also enable consistent application segmentation. It should use behavior analysis to identify policy deviations and outliers in near real time with little human intervention. This approach is required to identify issues early and take the necessary remediation steps.
- Supports a dynamic and heterogeneous environment: The solution must implement highly specific enforcement policies to secure applications in a scalable way. In addition, it must enable organizations to roll out this policy consistently regardless of where the workload is; whether it is in a bare-metal, virtualized, or containerized environment; and whether it is running in an on-premises data center, the public cloud, or a private cloud.

Cisco Capital financing to help you achieve your objectives

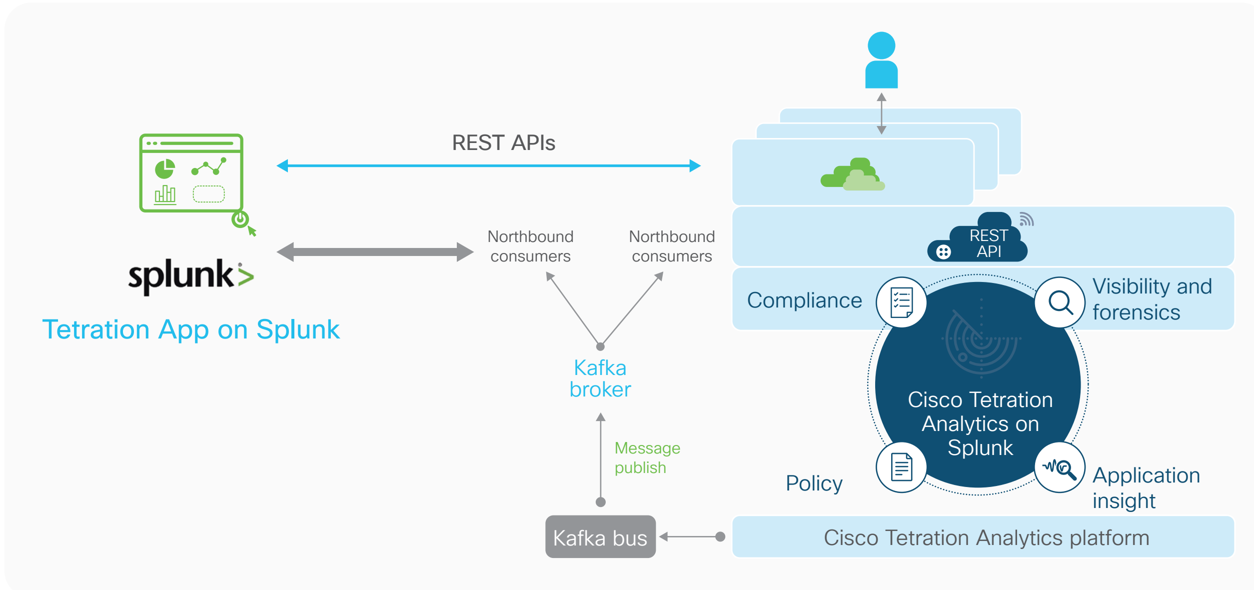
Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce Capital Expenditures (CapEx), accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital financing is available in more than 100 countries.

Cisco Tetration Analytics and Splunk solution

The Cisco Tetration Analytics™ and Splunk joint solution covers three main key use cases to address these challenges. Cisco Tetration Analytics and Splunk together offer exceptional data center analytics capabilities, with application insight, visibility, compliance, and policy enforcement. You get complete visibility into your IT operations, enabling you to build agile, secure, and compliant data centers.

The use cases discussed in this document focus on the general areas of visibility, performance monitoring, operational analytics, and security and policy enforcement. To address the use cases, the combined solution enhances the capabilities of both Cisco Tetration Analytics and Splunk using an open communication system between the two platforms. It uses the Cisco Tetration Analytics open API (using Representational State Transfer [REST]) and integrates Apache Kafka publish and subscribe messaging interfaces. Figure 1 illustrates the integrated architecture.

Figure 1 Cisco Tetration Analytics and Splunk technical architecture



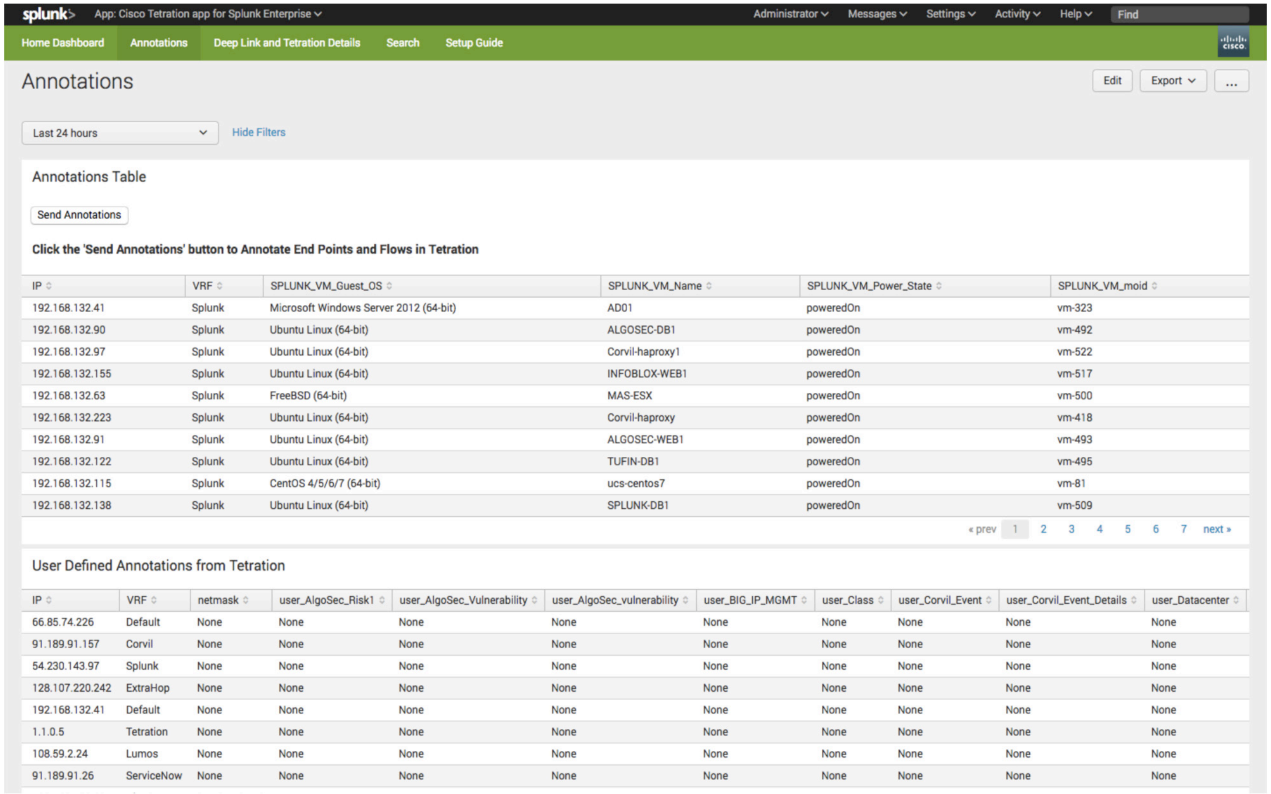
Conclusion

Cisco Tetration Analytics application insights and policy enforcement capabilities can augment the data in Splunk's Security Information and Event Management (SIEM) system (called Splunk Enterprise Security) and enforce policies to address any compliance issues flagged in Splunk. In addition, Splunk brings value to Cisco Tetration Analytics with application-layer information and machine data analytics across the entire IT and security environment. Together, Splunk and Cisco Tetration Analytics provide complete visibility into customers' IT operations and enables them to build agile, secure, and compliant data centers.

Use case 1: Visibility, performance monitoring, and operational analytics

Cisco Tetration Analytics ingests flow telemetry from hosts and network switches and provides unsupervised machine learning to map the ingested data to create application insights, also known as Application Dependency Maps (ADMs). Cisco Tetration Analytics shares useful endpoint and sensor information as well as the ADM data with Splunk, and this data is correlated with network, health, and performance metrics stored in Splunk log files. This correlation creates annotations and context for the Splunk performance metrics, which enhances Cisco Tetration Analytics application insights (Figure 2).

Figure 2 Splunk and Cisco Tetration Analytics correlated annotations



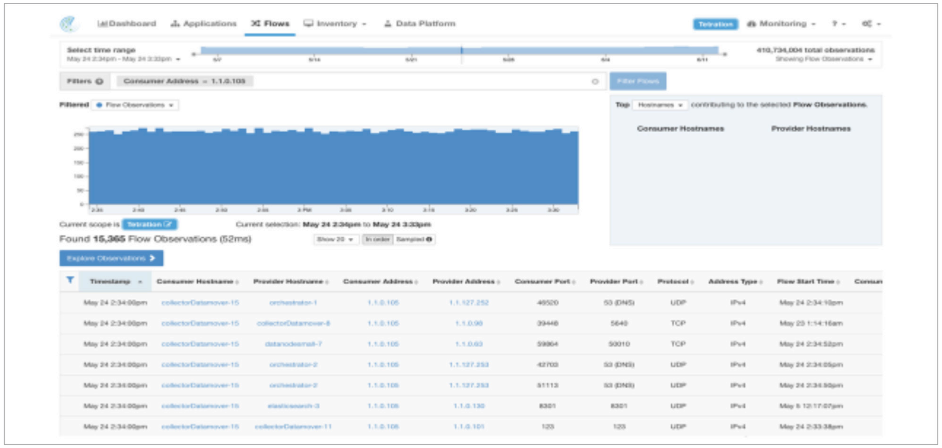
Cisco Tetration Analytics users can use the Splunk application to send correlated endpoint information in the form of annotations for endpoints that Cisco Tetration Analytics discovers. Users can analyze flows and give further meaning to these flows by uploading annotations collected by the Splunk application. Cisco Tetration Analytics also provides existing annotations to Splunk to help Splunk users correlate endpoint information with information from other Splunk applications in the environment. The application correlates meaningful endpoint information from other existing Splunk applications in the environment. Cisco Tetration Analytics consumes these annotations to annotate the massive flow and inventory information.

Another requirement in many day-2 operations is operational analytics to troubleshoot and remediate incidents and faults faster. The Splunk and Cisco Tetration Analytics joint solution correlates ADM and inventory data from Cisco Tetration Analytics with Splunk log files containing configuration data, faults, etc. to enable faster root-cause analysis.

Use case 2: Security, compliance, and root-cause analysis

The Cisco Tetration Analytics and Splunk solution provides a deep-linkage feature, which enables Splunk users to easily view flows for any endpoint (virtual machine) inspected in Cisco Tetration Analytics by using the Deep Link IP feature in Splunk. The application renders a URL that takes you to Cisco Tetration Analytics, applies the necessary filters, and displays the flows. Alarms or incidents recorded in Splunk can be used as indicators in Cisco Tetration Analytics to look more deeply into the flows and drill down to the root cause of the incident. The Cisco Tetration Analytics application for Splunk also provides endpoint and sensor details that assist the user with deep-link information. This information helps achieve compliance across the enterprise (Figure 3).

Figure 3 Deep-Link VM/End-Point information from Splunk with Tetration flow data



Use case 3: Policy enforcement

Cisco Tetration Analytics shares information about security policy outliers and anomalies with Splunk. Using this shared data, Splunk recommends policy actions, which are sent to Cisco Tetration Analytics for enforcement.

Next steps

- For more information about successful real-world examples of this solution, visit www.splunk.com.
- For additional information, see https://www.cisco.com/c/en/us/solutions/data-center/data-center-partners/ecosystem-partner-collateral.html.
- www.cisco.com/go/dcecosystem