splunk>

CASE STUDY

Innovative Cloud-Based SIEM Deployment Delivers Actionable Security Intelligence for Equinix

EQUINIX

Executive summary

Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees and partners in 33 markets across five continents. Security is of paramount importance at Equinix as thousands of companies worldwide rely on Equinix datacenters and interconnection services. To gain a unified view across its security infrastructure, Equinix needed a cloud solution with centralized visibility and SIEM functionality that could be implemented easily, quickly and without significant operational effort. Since deploying Splunk Cloud and Splunk Enterprise Security (ES), Equinix has seen benefits including:

- Full operational visibility
- Enhanced security posture
- Time and cost savings

Why Splunk

To deliver the highest levels of security and data protection to its customers, Equinix implemented a multi-faceted global security infrastructure. However, the company lacked a unified view across this infrastructure and had to rely on alerts and reports from each individual system. To gain insight into security events, Equinix had to extract and correlate the data manually—a very time-intensive process that made sub-optimal use of limited security personnel and resources. It was essential for Equinix to gain centralized visibility and that its SIEM solution be deployed as a cloud service.

Splunk Cloud met all of Equinix' requirements for a cloud service that could aggregate the information from all of its security technologies and easily handle multiple types of data, speeds and feeds. "Splunk Cloud's 100 percent uptime SLA and its SOC2 Type 2 certification gave us the confidence to forward our critical data offsite,“ says George Do, CISO, Equinix. "With Splunk Cloud we had value immediately."

Equinix also utilized Splunk ES with Splunk Cloud as its SIEM solution. According to Do, "For years, we have been very vocal about the benefits of adopting a 'SIEM in the cloud' strategy. With Splunk Enterprise Security, we now have a secure, cost-effective SIEM with

Industry

- Technology

Splunk Use Cases

- Security

Challenges

- Lacked unified view into multi-faceted global security infrastructure
- Manual process for extraction and correlation of data was time and resource intensive
- Wanted centralized visibility and SIEM functionality
- Needed to accelerate time-to-value with cloud SIEM solution

Business Impact

- Gained operational visibility across infrastructure
- Full SIEM functionality to aggregate and correlate data from all security systems
- Innovative cloud SIEM deployment provides cost-and time-savings over traditional SIEM solutions
- 30 billion raw security events reduced down to about 24,000 indicators of compromise, to 20 actionable alerts
- 50 percent TCO savings compared to an on-premises based legacy SIEM deployment
- Achieved 30 percent faster response to security incidents
- Enhanced security posture
- Provide the foundation for planned SOC

Data Sources

- Firewalls, VPNs and other security systems
- Intrusion Prevention and Detection Systems
- F5 load balancers
- Host-based intrusion management platform
- Microsoft Active Directory
- Salesforce.com
- UNIX and Windows servers

Splunk Products

- Splunk Cloud
- Splunk Enterprise Security (ES)

the functionality and scalability to underpin our planned SOC. Having it in the cloud means we have also eliminated the numerous hassles involved with deploying and then maintaining an onsite SIEM implementation."

Overarching visibility into infrastructure with Splunk Cloud and Splunk Enterprise Security

Before Splunk Cloud, Equinix was overwhelmed by more than 30 billion raw security events generated every month. With Splunk Enterprise Security and Splunk Cloud, the security team can now reduce the 30 billion raw security events down to about 24,000 indicators of compromise, and then to 20 actionable alerts, thus providing actionable security intelligence and the foundation for a dedicated SOC.

With all the data aggregated within the Splunk platform, the security team can cross-reference data between systems, enabling them to research, investigate and respond to incidents 30 percent faster than before. "Our ultimate goal is to protect our customers, employees and data. With ES and Splunk Cloud as our SIEM platform, the information we want is always at our fingertips," says Do.

"Whenever we need to investigate an incident, we simply display the relevant data in Splunk dashboards, so the information can be accessed by everyone on our security team as well as our C-level executives. The savings in time and effort are huge, as is the savings of 50 percent in total cost of ownership (TCO) compared to deploying a traditional on-premises based SIEM."

Thanks to Splunk Enterprise Security, Equinix is now armed with comprehensive security analytics. For example, whenever a user account shows signs of suspicious activity, such as a local employee unexpectedly logging in from another continent, high priority alerts are immediately triggered and sent to the security team. Also, using Splunk Cloud with ES enables Equinix to prevent the leakage of sensitive business information. In particular, administrators use correlations to determine whether a departing employee might be seeking to steal confidential data.

"From day one, Splunk Cloud has given us actionable, data-driven intelligence. With Splunk Enterprise Security in the cloud, we're getting comprehensive SIEM functionality, the economics and simplicity of software as a service, and outstanding availability and security. As more employees use the Splunk platform, we're sure to find important new use cases beyond securing our infrastructure."

George Do, CISO
Equinix

Expanding value across the enterprise

The usefulness of Splunk Cloud at Equinix extends far beyond the security team. Upper management, including the CIO, uses Splunk dashboards and analytics to monitor the firm's security posture. Additionally, the company's infrastructure team is looking to deploy the Splunk platform to monitor the health of its applications, and the DevOps team is considering Splunk Cloud to optimize application performance, track key performance indicators (KPIs) and receive critical alerts.

"From day one, Splunk Cloud has given us actionable, data-driven intelligence," concludes Do. "With Splunk Enterprise Security in the cloud, we're getting compelling SIEM functionality, the economics and simplicity of software as a service, and outstanding availability and security. As more employees use the Splunk platform, we're sure to find important new use cases beyond securing our infrastructure."

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

Learn more: www.splunk.com/asksales

www.splunk.com