splunk>

CASE STUDY

Discovery Communications Gains Full Operational Visibility Into Security Posture and Critical Services

Executive summary

Founded in 1985, Discovery Communications is the world's No. 1 pay-TV programmer, reaching nearly three billion cumulative subscribers in more than 220 countries and territories. For 30 years, Discovery has been dedicated to satisfying curiosity and entertaining viewers with high-quality content through its global television brands. Discovery needed to ensure compliance, bolster its security posture and to give staff—from administrators to C-level leadership—full operational visibility into the health of its online services. Since deploying Splunk Enterprise and other Splunk solutions, the company has seen benefits including:

- Replacement of legacy SIEM
- Enhanced reliability
- Improved operational and cost efficiencies

Why Splunk

When Discovery Communications went public in 2007, it became subject to the regulatory mandates of the Sarbanes-Oxley Act (SOX) and needed a platform for technical auditing and compliance reporting, as well as tools to monitor its networking environment. Since then, the company has continued to grow through acquisitions and global expansion, adding datacenters worldwide and increasing its networking operations.

Discovery initially deployed Splunk Enterprise to aggregate logs to verify compliance, which the software platform did effectively. Administrators recognized that by indexing and visualizing log data in dashboards, Splunk could provide deep yet flexible visibility into all networked systems and processes. The Splunk platform delivered infrastructure-wide views and eliminated silos.

More recently, Discovery has deployed the Splunk App for VMware for operational visibility into its increasingly virtualized infrastructure. It has also installed Splunk Enterprise Security (ES) to replace a legacy security information and event management (SIEM) solution and to improve forensic investigations. And, finally, the Splunk IT Service Intelligence (ITSI) solution was added to provide service-centric health reporting to various constituencies within the company.

Industry

- Media and entertainment

Splunk Use Cases

- IT operations
- Security

Challenges

- Required to provide a platform for technical auditing and compliance reporting
- Wanted to bolster security posture
- Needed end-to-end operational visibility into health of online services
- Secure the content value chain, from production to the viewer

Business Impact

- Supports regulatory compliance and reporting initiatives
- Eliminated legacy SIEM and improved awareness, detection and investigation of internal and external threats
- Eliminates silos and provides operational insights and infrastructure-wide views across physical and virtual infrastructure for more productive IT service
- Enhances reliability of services and components
- Monitors key business processes for leadership and decision-makers, leading to greater Operational Intelligence
- Improves operational and cost efficiencies with automated remediation

Data Sources

- Unix, Linux and Windows servers
- Firewalls and IPS systems
- Symantec Endpoint Protection Console
- Microsoft Exchange server
- Enterprise applications
- Oracle databases

Splunk Products

- Splunk Enterprise
- Splunk IT Service Intelligence
- Splunk Enterprise Security
- Splunk App for VMware

"We're now collecting data for our Splunk platform from three continents," notes Jeff Lesperance, manager of platform operations for Discovery Communications. "If it's part of our corporate environment, Splunk is involved in some way."

Out with the old (SIEM) and in with analytics-driven security

As a content-driven organization, Discovery needed to secure the value chain around its content—from production to the consumer. Discovery Communications was already using Splunk Enterprise to index Windows security event logs for SOX compliance, as well as security protection data from a variety of security devices and technologies such as intrusion protection systems (IPS). Based on this experience, the firm decided to deploy Splunk Enterprise Security as its new SIEM solution.

"We needed a versatile SIEM platform that could consume the security contextual data from across our environment, out of the box," explains Lesperance. "In addition, we didn't want to manage two different environments and pay licensing fees for another SIEM to ingest the same data we were already feeding into Splunk. Splunk ES has given us real-time visibility into everything—from malicious exploits like advanced persistent threats and phishing attacks to administrative rights, access authentication and anomalies."

Automated infrastructure monitoring

By automatically aggregating data from other monitoring tools into dashboards, the Splunk platform has become Discovery's baseline infrastructure health monitoring tool. Splunk software eliminates the need for administrators to manually collect data from various systems. Additionally, Splunk software triggers alerts based on data automatically consolidated from all other tools, accelerating remediation. "Splunk software lets us track systems and evaluate alerts more quickly and with less effort," says Lesperance. "Having a single repository for all relevant data points makes automating remediation more effective."

"We needed a versatile SIEM platform that could consume the security contextual data from across our environment, out of the box. Splunk Enterprise Security has given us real-time visibility into everything from malicious exploits like advanced persistent threats and phishing attacks to administrative rights, access authentication and anomalies."

Jeff Lesperance, Manager of Platform Operations
Discovery Communications

Service-centric views with KPIs for tier-one applications

Lesperance and his team use Splunk ITSI for insights into the operational health of critical IT services and their underlying infrastructure. The solution presents dashboards that track key performance indicators (KPIs) for tier-one business applications and platforms. The dashboards are tailored for different constituencies within the company and show the performance and availability of components both in real time and as trends. For instance, senior management monitors key business processes; application and platform owners oversee the health of their environments; and administrators track the enterprise network.

Splunk ITSI has enabled Discovery to score underlying infrastructure metrics, correlate them to transactional metrics and display them for all applications on a single dashboard, clearly represented with numbers and colors. Going forward, Discovery can easily define and apply KPI metrics to additional applications as well as create alerts for threshold breaches.

"Splunk ITSI exemplifies the value that our Splunk solution offers. We have data-driven views of our IT resources and services without great costs or complexity. For us, Splunk delivers the leading platform for operational and business intelligence," concludes Lesperance.