splunk>

CASE STUDY

Intermedia Builds an Instant Security Operations Center and Speeds Business Processes

INTERMEDIA

Executive summary

Intermedia delivers cloud-based business applications and IT services like email, voice, file sharing, conferencing and archiving to 70,000 customers. The company's existing SaaS-based security product offered limited alerting and reporting, and searches and investigations were laborious. Moreover, Intermedia lacked comprehensive analytics for IT and business operations spanning its 10 data centers. Since deploying Splunk Cloud, the company has seen benefits including:

- A robust Security Operations Center (SOC)
- Real-time insights and KPIs into its services delivery
- Cost savings through efficiencies and reduced staffing.

Why Splunk

Intermedia's competitive advantage is delivering enterprise-grade security, 99.999 percent uptime and prompt 24/7 phone support. To meet these goals, the company sought security and Operational Intelligence by collecting and analyzing logs from its datacenters, security devices and endpoints.

Intermedia's legacy solution was inflexible and ineffective for real-time alerting into anomalous user behavior or policy violations. Creating risk profiles to prioritize security threats was challenging. Performance issues stifled rapid responses to security events. Searching logs for forensic investigations was arduous and time-consuming. Reporting on security incidents was complex and other tools were needed to provide business trendlines and key performance indicators (KPIs).

Intermedia first considered creating a homegrown solution but rather than install and maintain an on-premises system, it sought a SaaS solution. "We want to be system users, not system administrators," says Ryan Barrett, vice president of security and privacy at Intermedia. Therefore, the enterprise turned to Splunk Cloud, in part because of its 100 percent uptime SLA. Within weeks, Intermedia was collecting data from 4,500 endpoints and security devices scattered across the enterprise.

Industry

- Cloud services (Technology)

Splunk Use Cases

- Security
- IT operations
- Business analytics

Splunk Products

- Splunk Cloud

Challenges

- Limited security alerts
- Identifying anomalous user behavior and policy violations was difficult
- Queries and investigations were time consuming
- No integrated reporting for business trendlines and KPIs

Business Impact

- Stronger security through incisive, enterprise-wide intelligence
- Quicker, more agile responses to threats with real-time alerts for risks and unwanted user behavior
- Cost savings through greater efficiencies and reduced headcounts
- Enhanced visibility into, and oversight of, business and IT operations
- Improved services and greater value for customers

Data Sources

- Windows and Linux operating systems
- Network devices/routers and firewalls
- IPS systems
- VPN Auth logs
- Vulnerability scan data
- Application event logs
- System event logs
- Employee badge logs
- Anti-virus logs
- Netflow logs
- BMC FootPrints ServiceCore

Splunk Cloud delivers "An Instant SOC"

Splunk Cloud anchors Intermedia's first SOC. The security team displays real-time data in dashboards and sets alerts for questionable events. It accelerates investigations by rapidly querying all data to analyze and scope issues and to determine appropriate courses of action.

Splunk Cloud allows administrators to correlate logs from across the enterprise with threat intelligence feeds to contextualize vulnerabilities, build threat profiles and prioritize alerts. Splunk dashboards display broad trendlines of security events such as phishing attacks, and offer granular views into how often an IP address associated with cybercrimes might be seeking network access. Splunk forwarders on desktops help protect against data exfiltration.

Administrators quickly detect policy violations, such as a vulnerability scanner or other unwanted software on the network. They can identify unauthorized or suspicious user behavior like large file transfers out of the corporate environment. They also proactively mitigate threats with such capabilities as geo-locating IP addresses to determine logins from risky locations.

Thanks to Splunk Cloud, Intermedia has a comprehensive, data-driven security posture that was unattainable with its legacy security tool. In just one use case, the cost-saving ease and efficiencies of the Splunk solution substantially reduced TCO by enabling Intermedia to avoid a full-time employee dedicated to vulnerability analysis.

Enhanced customer service delivery

Intermedia relies on Splunk Cloud to improve processes and service delivery. Rather than pore over reports from disparate monitoring tools, administrators consolidate data from multiple tools into Splunk dashboards for centralized views of operations across the infrastructure. They display KPIs and trendlines to measure the performance of systems and applications and to anticipate the impact of additional customers and workloads.

"Splunk Cloud gave us a near-instant SOC that delivers comprehensive yet cost-effective security intelligence. I don't know of another solution providing all-inclusive data-driven analytics that can allow us to do so much, faster and with less staffing. We're prepared for the future because there's nothing we can't do with our Splunk platform."

Ryan Barrett

Vice President of Security and Privacy, Intermedia

With Splunk Cloud, administrators gauge the efficacy of the help desk by visualizing data from a case management system in Splunk dashboards to track the numbers and kinds of tickets and remediation times. Separately, they are evaluating the ability to track the quality of the firm's VoIP offerings, looking for issues like jitter or dropped calls before they impact customers.

Data-driven analytics enhance productivity

Intermedia is expanding its Splunk analytics to improve productivity. Splunk dashboards reveal how and when Intermedia's customers, as well as its own employees, use its services and resources. A bottleneck in data processing, for instance, was impeding billing customers for phone services. Intermedia is now evaluating expediting the process by deploying Splunk Cloud to deliver the necessary billing metrics. As Intermedia's customer base expands, the company intends to track these and other metrics for capacity planning.

With Splunk Cloud, Intermedia enjoys unprecedented visibility into its business and IT operations, helping to ensure security and the availability and quality of its services. Mindful of the value of data-driven intelligence, the company continues to expand its use cases for Splunk analytics into all facets of its business, enhancing its competitiveness by efficiently meeting its customers' needs.