splunk>

CASE STUDY

Imprivata Manages Containerized Environment Securely With Splunk Cloud

Executive summary

Imprivata, the healthcare IT security company, provides healthcare organizations globally with a security and identity platform that delivers ubiquitous access, positive identity management, and multifactor authentication. Imprivata enables healthcare securely by establishing trust between people, technology, and information to address critical compliance and security challenges while improving productivity and the patient experience. Migrating to Splunk Cloud, Imprivata has seen benefits including:

- DevOps teams freed to focus on high priority business needs
- Streamlined security compliance
- Avoiding the cost of massive on-premises storage infrastructure
- Disaster recovery and business continuity of critical Splunk services

Why Splunk

Imprivata's DevOps and development teams collaborate to maintain the company's tooling and automation infrastructure, employing best practices to ensure maximum performance during peak production. The teams have long relied on Splunk Enterprise for alerting, dashboarding, reporting service level agreements and troubleshooting.

"We're very fortunate that we've always had Splunk; our system logs, Amazon Web Services, firewall logs, and security logs all go into Splunk," says a manager on Imprivata's cloud platform team.

Splunk is essential for visibility and stability in Imprivata's operational environment, which uses both Docker and Kubernetes containerization and Python automation controls to monitor resources deployed in Amazon Web Services. Imprivata developers use Docker on their laptop devices, and instead of keeping logs locally they send them into Splunk Cloud for easier analysis.

"Our highly distributed, cloud-native architecture involves many services and containers, many different moving pieces. You could look at a log file, but you'd never be able to figure out which one to start with. It would be impossible to tell what was going on without Splunk," the manager says.

"At Imprivata, we gather all cloud infrastructure, application, and on-premises appliance logs into a single location so that troubleshooting

Industry

- Healthcare Information Technology

Splunk Use Cases

- IT Operations
- Container Monitoring
- Security Compliance

Challenges

- Needed secure central logging and ad hoc querying capabilities in highly distributed, containerized production and development environments

Business Impact

- Streamline HIPAA, SOC 2 Type II and GDPR compliance auditing
- Free engineering staff to pursue business value, root cause analysis
- Avoid on-premises infrastructure cost and management burden

Data Sources

- Enterprise applications
- Amazon Web Services
- Amazon Elastic Container Service (ECS) Docker container logs
- Amazon CloudWatch
- AWS CloudTrail
- Kubernetes
- System logs
- Firewall logs
- Security logs

Splunk Products

- Splunk Cloud
- Splunk Enterprise

of the application, infrastructure and cloud system is done in a single place: Splunk," he adds. "Splunk dashboards help the product management team and engineering managers determine service level agreements and start to measure them from the very beginning — ingraining a culture of measurement and shared understanding of the product from inception."

Splunk Cloud enables cost-efficient scalability

A corporate initiative to move on-premises solutions to the cloud and scaling needs prompted Imprivata to migrate from Splunk Enterprise to Splunk Cloud. The company's data volume through Splunk is approximately 150GB a day but once spiked to 500GB. Splunk Cloud enables Imprivata to glean answers from machine data without the need to manage infrastructure. "Splunk Cloud lowers our infrastructure cost of ownership while freeing IT time for high-value work," the manager says.

Streamlined compliance and auditing

Splunk Cloud also simplifies compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other regulations, including SOC 2 Type II and the General Data Protection Regulation (GDPR). Imprivata can securely analyze, visualize and monitor machine data from any source — including electronic health record (EHR) systems and connected medical devices — to monitor complex application environments and streamline audit functions. The company's Splunk Cloud contract includes a business associate agreement (BAA) protecting Personal Health Information (PHI) under HIPAA guidelines.

"As a security company in healthcare, we take everything to a higher level of security. So, we work with Splunk. They give us a BAA, which defines if there's a breach and spells out the line of responsibility," the manager says. "We won't do business with a vendor who doesn't provide that."

"Thanks to Splunk Cloud, I can shift my focus from administrative tasks to helping my team and others across the organization analyze the business, conduct root cause analysis, and target tangible outcomes."

Manager, Cloud Platform Team
Imprivata

Faster performance, higher business value

The manager estimates that approximately 100 Imprivata engineers interact with Splunk Cloud in some way, including up to 25 development engineers building cloud applications and perhaps 10 Splunk "ninjas" who run the most sophisticated searches in minutes or seconds. Imprivata recently experienced its first month when Level 1 and Level 2 24/7 network operations center (NOC) staff handled 100 percent of all production incidents with automation and runbooks without escalation to DevOps, greatly improving the mean time to repair and avoiding service impacts by proactively fixing problems.

With these efficiencies — and with infrastructure management and administrative tasks outsourced to Splunk Cloud — Imprivata frees its highly skilled engineers to leverage the system for business value. They spend their valuable time troubleshooting issues, working with performance metrics and conducting root cause analyses.

"When somebody asks me a question, I can I show them how to leverage Splunk Cloud to the maximum value to gain meaningful insights," the manager says. "Instead of just administering Splunk, we use it to dig for gold."

"The HIPAA-compliant version of Splunk that we use gives us a BAA that is very advantageous and critical for any vendor we work with. If some report stops running or the scheduler slows down, we don't have to go figure out why. We let the experts at Splunk do it."

Manager, Cloud Platform Team
Imprivata