splunk>

CASE STUDY

Entrust Datacard Corporation Gains Unified Infrastructure Monitoring With Splunk

Entrust Datacard™
Trusted Identities | Secure Transactions

Executive summary

When consumers, citizens and employees make purchases, cross borders, access e-government services or log on to secure networks, they expect their transactions to be secure and seamless. Entrust Datacard, with its varied portfolio of innovative security solutions, provides the secure foundation to enable frictionless, secure transactions – tied to trusted identities. Recently, the company needed unified infrastructure monitoring and metrics to drive operational success during the development of an innovative new cloud service. Since deploying Splunk Enterprise running on Amazon Web Services (AWS), Splunk App for Infrastructure and VictorOps, Entrust Datacard has seen benefits including:

- Modernizing operations, introducing automation and delivering software faster
- Proactive and collaborative monitoring to ensure a positive customer experience
- Reducing the number of monitoring tools required while increasing coverage

Why Splunk

Entrust Datacard is a privately-held security company serving customers in 150 countries, managing billions of transactions annually. Daryl Robbins, senior enterprise cloud architect for Entrust Datacard, leads the evolution of enterprise solutions into the cloud while addressing critical security and compliance requirements. Robbins and his team are modernizing operations, taking a DevOps approach to monitoring and automation to proactively address issues before they occur — delivering software faster that better responds to customers' needs.

Entrust Datacard is a unique player in the security market, offering integrated solutions consisting of hardware, software and services. In 2015, Robbins' team was charged with delivering Entrust Datacard IntelliTrust™ Authentication Service, a new cloud authentication and identity service running in AWS. This effort was not the company's first SaaS offering, but it was both its first cloud-native architecture and foray into the public cloud.

"When we first started building IntelliTrust, we needed three different infrastructure monitoring tools to cover everything," says Robbins. "Now, with Splunk Enterprise and the Splunk App for Infrastructure, we can do it all. We are in the process of moving all metrics data into Splunk."

Industry

- Technology

Splunk Use Cases

- IT Operations
- Infrastructure Monitoring
- DevOps

Challenges

- Needed unified infrastructure monitoring

Business Impact

- Modernizing operations and introducing automation to respond to issues before they occur
- Delivering software faster and responding to customers' needs better
- Combining metrics and logging for a complete view of infrastructure performance
- Automating incident management

Data Sources

- Amazon CloudWatch
- Amazon CloudFront
- Amazon Inspector
- Amazon ECS
- Amazon Aurora database
- Amazon VPC flow logs
- AWS ALB
- AWS CloudTrail
- AWS Config
- HTTP Access
- Docker

Splunk Products

- Splunk Enterprise
- Splunk Insights for Infrastructure
- Splunk App for Infrastructure
- VictorOps
- Splunk Add-on for Amazon Kinesis Data Firehose
- Splunk Add-on for Amazon Web Services
- Splunk HTTP Event Collector

A significant number of Entrust Datacard's workloads have compliance and regulatory requirements — from PCI-CP for card production to WebTrust for certificates and FedRAMP for federal workloads — and the Splunk platform accommodates the need to configure and deploy workloads in different ways to address those requirements. For example, Entrust Datacard's cloud and heavily regulated on-premises deployments have very different requirements. "Splunk was the only solution that we found that could easily address these variable requirements, both cloud and on-premises," Robbins says.

Endlessly diverse data sources

At Entrust Datacard, the company's diverse data sources span everything from the infrastructure to the application layer. There are many different internal users — from developers to IT operations folks and business partners — who are interested in this data. According to Robbins, the infrastructure and application data sources the company consumes are "just about endless," and may generate different types of monitoring data. "With the addition of metrics and with Splunk App for Infrastructure, metrics have now become a first-class citizen in Splunk, which allows us to have a single tool that can handle all these types of monitoring," Robbins says.

Entrust Datacard is also running Docker containers using Amazon's EC2 Container Service (ECS). "By configuring the Docker containers to directly log to Splunk via journald, it allows us to send all that data in directly," Robbins says.

Complete view of infrastructure performance

Today, Entrust Datacard has Splunk Enterprise, a solution for collecting machine data, and Splunk App for Infrastructure to make sense of the combined data. "Splunk App for Infrastructure cleverly combines metrics and system logging for a more complete view of infrastructure performance," Robbins says. "We can see unusual events such as a CPU spike and correlate it with logs to troubleshoot problems much more quickly."

Fully monitoring the cloud infrastructure is enabling the company to maintain and improve the customer experience. "We haven't had any significant outages in the last year because of our proactive ability to detect problems before they happen," Robbins says.

"When we first started building IntelliTrust, we needed three different infrastructure monitoring tools to cover everything. Now, with Splunk Enterprise and the Splunk App for Infrastructure, we can do it all. We are in the process of moving all metrics data into Splunk."

Daryl Robbins, Senior Enterprise Cloud Architect
Entrust Datacard

Critical incident response

Robbins explains that when the Splunk App for Infrastructure detects a critical incident, it is automatically reported to VictorOps. VictorOps makes it easy for on-call developers and support teams to acknowledge, get context on problems and collaborate with teams to solve critical issues. "We only do this when the issue warrants waking someone up," Robbins says. "VictorOps has a robust mobile app that delivers notifications and context to the right on-call team members. For less critical issues, sending an email directly from Splunk is appropriate."

Designed to scale

For the IntelliTrust solution, scalability was an essential requirement because authentication has a unique usage pattern. Typically, usage spikes on weekday mornings when a large percentage of users are logging in for the first time, with another potentially large spike midday. Throughout the rest of the day, the load is more balanced as users need authentication to new apps as part of their daily work.

According to Robbins, the Splunk platform scales to solve everything from the simplest problems in a single-node deployment to more sophisticated multi-node implementations that address more complex requirements. "At Entrust Datacard, most of our Splunk deployments tend to be more complex due to an assortment of security and compliance requirements," Robbins says. "However, due to the flexibility of Splunk, we can get the same monitoring experience, whether we're dealing with a cloud or an on-premises deployment."