augustschell

CASE STUDY

Department of Defense Organization Overcomes Stressful Business Catastrophes Using Enterprise Monitoring and Management

Executive Summary

A Department of Defense (DoD) organization was struggling to achieve ongoing compliance with a number of DoD-specific regulations related to network security. Their team struggled to keep tabs on a multitude of devices connected to the network, plus, they weren't sure how to manage authorization to view security-relevant data appropriately.

Challenges

- The customer's large data center and lack of a central repository caused difficulties with consolidating audit-related content in a meaningful way
- Issues of authorization for viewing security-relevant data created the need for better segregation and control of data
- A lack of a centralized platform for understanding their compliance state made extracting meaning from data challenging

Business Impacts

- ✓ The customer optimized and increased utilization of Splunk Enterprise.
- ✓ By adding and properly configuring Splunk Enterprise Monitoring and Management, as well as Nagios, the customer was able to access a better picture of their organization-wide IT and network activities.
- ✓ Achieving compliance with the necessary regulations was no longer a struggle.
- ✓ Service delivery and the customer experience were greatly improved.

Solutions

Primary

- Increased utilization of Splunk Enterprise
- Leveraged Splunk Enterprise for additional insight into monitoring and management

Supporting

- Integrated Nagios infrastructure to provide additional visibility into environment

Department of Defense Organization Struggles to Understand Their Network Environment Comprehensively, Has the Need to Achieve Compliance

A Department of Defense organization was juggling multiple DoD-specific compliance requirements related to network security. In particular, they needed to gain total visibility into all of the devices on their network and ensure proper reporting into monitoring tools; this included capturing all machine data and audit-related content.

The agency was experiencing various challenges with service interruptions leading to customer complaints, but couldn't seem to determine what was going on within the environment. Given their state of operations, resolving problems quickly and effectively wasn't within reach. After continued struggles with service delivery, the customer decided it was time to take on an enterprise-ready role in order to reach mean time to recovery rapidly, keep customers happy, and foster better business growth.

"We really wanted to give them the ability to capture information and generate reports covering all network-connected devices," Michael Albert, Director of Enterprise Management Solutions & Services at August Schell said. "This type of capability is designed to show customers which devices are communicating with monitoring tools and provide a compliance score capturing any gaps. It was an important objective both in helping them achieve compliance, as well as fulfilling a critical security use case."

Properly Measuring Compliance Benchmarks and Consolidating Data Across the Enterprise

Additionally, the customer needed a way to measure and record compliance benchmarks, including failed authentication. This meant developing an understanding of their desired benchmarks and the data needed to measure appropriately.

"Within DoD and NIST guidelines, there are certain generally accepted practices for measuring these requirements, so we needed to show them the way," Albert continued. "Essentially, we wanted to enable the ability for them to scan machine data, syslogs, and audit content, look for patterns, and create an analytic that matched their compliance requirements so they could get the answers they were looking for. So, for instance, if they had 100 systems and only 80 percent reported in with health and status-related messages, plus there were 100 failed authentication attempts against those that did report in, then they'd be able to answer more questions about specifics on the devices themselves."

When it comes to regulations, complexity is an obstacle to contend with for most federal agencies, and it doesn't get any easier where entire enterprises are concerned due to sheer volume of devices. It was critical that the customer accurately map out all of their security requirements. Virtual machines, Linux machines, Windows machines, database servers, hypervisors, switchers, routers, networks, and storage—all of these technologies coincide with different compliance measures and map to other areas of dependency.

Finally, the customer required the ability to visualize the enterprise in a consolidated fashion, capture all data, and create security centric visualizations and dashboard, easily accessible to both security personnel and executives.

Uncovering Network Visibility, Laying Out Interdependencies, and Enhancing Human Communications

With requirements laid out, Albert and the ASE engineering team began the process of bringing the customer into compliance and creating total visibility into network activity with enterprise monitoring and management.

"When the implementation began, it was definitely a phased approach. We started by helping the customer really understand their environment," Albert explained. "Prior to bringing on August Schell, they had some tools that provided some visibility, but it wasn't holistic like it needed to be. What they had in place was geared toward disparate pieces of the environment, but the systems all operated independently without knowledge of one another."

Being able to meet SLA's was ASE's objective. Albert and his counterparts applied enterprise monitoring and management best practices to identify stakeholders (including customers) and paint points to provide a cost-efficient solution that would deliver results immediately. "We wanted to find an approach that would work for their immediate pains. Their situation called for enterprise mechanisms that would fold into a sustainable architecture moving forward," Albert said.

After extensive fact gathering, meeting with customers, identifying stakeholders and business uses cases, and reviewing inventory, policies, and procedures, the ASE team found that many of the problems stemmed from common hiccups. It turned out that lack of communication overall and mismatched interdependencies were the primary culprits.

"For example, if a certain app depended on hardware that depended on the network that depended on storage, if just one of those pieces was impacted, nobody thought it'd impact anyone else because all their IT components operated in a silo. That was what we needed to fix," Albert remembered.

With pain points identified and management stakeholders who could help enforce enterprise monitoring and management, ASE engineering executed on the installation. Next, it was time to configure Splunk Enterprise Monitoring and Management and Nagios in order to generate the necessary information to gain further insights into their environment.

The team also spoke with relevant subject matter experts to uncover the necessary background on applications and dependencies.

"It was an iterative process, and it is continuous as the environment and business needs change, but we quickly put in place an enterprise monitoring and management system that brought them into compliance and provided the visibility they really needed," Albert recalled.

Owning Compliance Regulations and Accomplishing Environmental Transparency with Enterprise Monitoring and Management

In the end, the customer successfully achieved compliance with their regulations, which allowed them to continue functioning and sidestep the risk of dealing with their environment going down.

"The primary win for our customer was meeting compliance measures, because this was an agency directive that had to be done. Otherwise, they'd have to turn off their environment and discontinue the mission, but we were able to bring them into compliance so that they could continue functioning," Albert concluded.

Thanks to the consolidation of data sources, plus the integration of health and status, the customer gained a significantly better understanding of events happening in their environment. Mean time to recovery and troubleshooting were reduced, ultimately increasing service availability to their customers.

> "I wouldn't be able to do my job without August Schell. Thanks to the work their team delivered on, we're more secure, and we're able to understand what types of activities are happening in our environment quickly."
>
> - Information Systems Security Engineer, DoD Agency