splunk> listen to your data™

CASE STUDY

Splunk at QTS

Value-added Services Help Gain and Retain Customers

QTS Quality Technology Services

"Splunk's file integrity monitoring and alerting, reporting, and machine data monitoring capabilities help us provide the kind of value-added services that intrigues clients and keeps them happy. In this very competitive market, Splunk helps us attract and retain clients, perhaps more than any other solution we use."

Michael May
Manager of UNIX Systems

OVERVIEW

INDUSTRY
- Managed Service Provider

SPLUNK USE CASES
- Infrastructure and Operations Management
- Compliance Management
- Reporting and Analysis

BUSINESS IMPACT
- Eliminated multiple legacy reporting tools, saving approximately $25,000/year
- Avoided approximately $400,000/year+ in costs versus Splunk alternatives
- Avoided approximately $150,000 per year in costs by using Splunk for file integrity management (FIM) rather than a dedicated FIM solution
- Achieved return on investment (ROI) within three months
- Provided "one view" of machine data and consolidating multiple reporting and analysis tools
- Reduced problem resolution by orders of magnitude

DATA SOURCES
- Command-line logging from Linux, AIX and other UNIX systems
- Cisco firewall and Symantec Endpoint Protection (EP) logs
- Application data from client systems

The Business

Companies of all sizes are increasingly turning to managed service providers (MSPs) to achieve greater cost-efficiency and keep pace with technological change. Quality Technology Services (QTS), the largest private provider of managed services and data center solutions in the US, maintains 12 data center locations in seven states, encompassing nearly 3.5 million square feet of data center infrastructure. Splunk helps QTS consistently and effectively monitor and manage thousands of devices, applications, and systems, meeting the performance, compliance and security needs of more than 600 customers.

Challenges

Some of the firm's key challenges include keeping pace with the rapid influx of new customers, managing changes in technology, implementing custom and off-the-shelf applications and serving customer reporting demands. The ability to consistently deliver high-quality services at any of its data centers nationwide is market differentiator for QTS—but also a continuing challenge due to the distributed nature of the company's operations. Before Splunk, QTS relied on a wide variety of disparate systems and tools that made it difficult or impossible to efficiently and effectively collect and correlate data across multiple sites and geographies.

Enter Splunk

In early 2008, QTS UNIX group manager Michael May and his team set out to find way to troubleshoot IT issues and provide better IT performance along with improved security across the vast QTS infrastructure. The new solution needed to be able to accommodate client data nationwide, be flexible and scalable enough to deploy on a large variety of platforms, accommodate ongoing data center acquisitions and help meet various compliance needs.

The QTS team evaluated Splunk, LogLogic and RSA enVision over a three-month period. QTS liked the flexibility, easy scalability and cost-effectiveness of Splunk's software-only approach. May noted that LogLogic and RSA appliance-based solutions were far more costly and less flexible.

According to May, adopting either RSA or LogLogic would have cost QTS an additional $300,000 to $400,000 per data center to deploy. QTS deployed Splunk Enterprise on its own servers and devices, with no limit on the number of instances of Splunk used. The Splunk model is based daily peak volume of indexed data and can more readily accommodate the growing needs of QTS without expensive upfront costs.

Breakthroughs

Organizational Efficiency

QTS consolidated all of its data logging functions to centralized Splunk indexing systems in New Jersey and Georgia. Splunk forwarders are installed on each event-generating server or device in QTS facilities nationwide. Data is tagged with metadata identifying the host, source and source type before it is sent across the

QTS network to the Splunk indexers where it can be used for multiple purposes and to fulfill search requests. Forwarders also provide redundancy by automatically caching data in event of network interruptions or other outages. The consolidation of monitoring and analysis tools enabled QTS to eliminate numerous legacy servers and associated licenses, saving approximately $25,000 per year.

Splunk also enables QTS to view its operation as a single, geographically distributed entity rather than a collection of acquired data centers. While many clients are deployed in two or more QTS environments, Splunk enables QTS to monitor, analyze and troubleshoot client data as if it were a single system.

Compliance and Visibility

Splunk's ability to capture and retain machine data, file integrity monitoring (FIM) and alerting are critical in meeting many compliance requirements. The extension of Splunk for use in meeting customers' compliance needs is also helping QTS to save on the additional overhead of a separate FIM system such as Tripwire, May notes. He estimates that QTS avoids approximately $150,000 per year in licensing costs by employing Splunk for FIM.

QTS also uses Splunk to efficiently meet the operational intelligence needs of internal functional groups and upper management. With a few clicks, the Splunk team can create custom dashboards and views for specific groups responsible for firewalls, networks, and UNIX and Windows environments. The team also uses Splunk report builder to produce reports on security issues and other factors for C-level management.

Value-added Services

Recently, QTS upgraded its Splunk license from 40GB to 100GB, allowing the firm to test and deploy new services for customers. QTS plans to productize and extend Splunk capabilities for direct customer access and to support new, premium services. May acknowledges that Splunk helps QTS gain and retain customers by enabling the firm to provide the value-added service levels that customers want, but few MSPs can deliver.