Cisco Case Study
Sharp HealthCare

Sharp HealthCare modernizes its IT operations with Cisco ACI and Splunk Enterprise

Size: 18,000 employees | Industry: Healthcare | Location: San Diego

Sharp HealthCare is a not-for-profit, integrated regional healthcare delivery system located in San Diego. It is recognized for clinical excellence in cardiac, cancer, multi-organ transplantation, orthopedics, rehabilitation, behavioral health, women's health, home health, and hospice services. The Sharp HealthCare system includes four acute care hospitals, three specialty hospitals, three affiliated medical groups, a health plan, and numerous outpatient facilities and programs. For more information, visit sharp.

Challenges

- Overcome the limitations of an aging data center and legacy applications
- Increase service availability and data protection
- Improve infrastructure visibility and troubleshooting

Solutions

- Application-centric, software-defined networking
- Centralized, policy-driven management and automation
- Machine data aggregation and analysis

Results

- Established a remotely managed, colocation-based data center
- Segmented the network for greater control and security
- Enhanced network monitoring and event analysis via Splunk integration

For More Information

- Cisco® Application Centric Infrastructure (Cisco ACI™)
- Cisco Unified Computing System™ (Cisco UCS®)
- Cisco Firepower® Next-Generation Intrusion Prevention System (NGIPS)
- Splunk Enterprise

Challenge: Modernize IT operations despite legacy application limitations

With an aging data center and desire for more operational efficiency and agility, Sharp HealthCare considered moving its IT resources to the cloud. But the cost involved and the requirements of its applications made a wholesale move to the cloud impractical.

"We have a lot of legacy applications that just aren't suitable for a SaaS model," says Kevin Rothstein, network engineer at Sharp HealthCare. "Instead of rebuilding our data center or attempting to force-fit our applications in the cloud, we decided to put everything in a colocation facility and manage it remotely with a software-defined network."

To anchor its new colocation data center, Sharp HealthCare chose the combination of Cisco ACI, the industry's leading software-defined networking (SDN) solution, and the Intel® Xeon® processor-based Cisco UCS.

"With other SDN solutions, you have to mix and match the underlay and overlay," Rothstein says. "But Cisco ACI is a complete package—a full fabric that brings together physical and virtual systems."

The new infrastructure has dramatically reduced the time and effort of systems maintenance, with all configurations and changes being handled remotely by the Sharp HealthCare IT team.

"Because Cisco ACI is software-defined and policy-based, we don't have to independently manage each and every switch," Rothstein explains. "The environment is heavily virtualized and automated, so it doesn't require much manual intervention. We rarely log on these days except to configure a new port, which is effortless."

"We use Splunk for troubleshooting and diagnostics, and Cisco ACI gives us a much broader and deeper view of our environment. We can look at all of our compute, network, and storage data—both physical and virtual—simultaneously on one screen."

Kevin Rothstein
Network Engineer, Sharp HealthCare

Boosting data security via segmentation

With its new network in place, Sharp HealthCare is using the segmentation capabilities of Cisco ACI to improve operational control and security.

"At first, we were leery of whitelist rules and zone-based firewalls, thinking they would mess up our operations," Rothstein admits. "But segmentation has been seamless with Cisco ACI. We manage everything with policies and endpoint groups, and the firewall handles enforcement."

Sharp HealthCare has created zones based on functional endpoint groups, he explains, including front-end web and desktop groups and back-end database and application groups. Policies that dictate connectivity, access, and data security are centrally defined for each group and pushed to the network fabric through a central console. Cisco Firepower NGIPS provides additional visibility, protection, and control.

"We are significantly more secure with Cisco ACI and Firepower NGIPS," says Rothstein, noting the importance of data protection in the healthcare market. "And we have an opportunity to further strengthen our defenses by tightening our contracts and applying additional segmentation within our zones."

"The combination of Cisco ACI and Splunk has helped us on a number of levels, from infrastructure visibility and troubleshooting to security and audits."

Kevin Rothstein
Network Engineer, Sharp HealthCare

Improving visibility, troubleshooting via Splunk integration

Sharp HealthCare has been particularly pleased with how well Cisco ACI has integrated with its distributed Splunk Enterprise environment, which collects, monitors, and analyzes massive quantities of machine data.

"We use Splunk for troubleshooting and diagnostics, and Cisco ACI gives us a much broader and deeper view of our environment," Rothstein says, noting the two solutions align seamlessly using Python scripts. "We can look at all of our compute, network, and storage data—both physical and virtual—simultaneously on one screen. And ACI only represents a little over one percent of our total Splunk ingestion per day, including production, non-production, and lab network fabrics."

Real-time health scores have enhanced infrastructure monitoring, he adds. And the seamless correlation of historical log data has dramatically improved troubleshooting, while reducing the time and resources required for audits.

"The health scores are very cool, almost like a heads-up display for our networking team," says Rothstein. "And when something goes wrong, we can conduct detailed investigations using authentication and audit logs to see exactly who was on the colocation fabric, when they were there, and what they were doing. We can get to the root cause of any issue quickly, identifying pre-fail indicators and seeing everything that was impacted."

Looking ahead

With better infrastructure management, monitoring, and troubleshooting, Sharp HealthCare IT operations are shifting from reactive to proactive. After moving roughly 350 legacy applications to the new Cisco ACI fabric, Rothstein's team will implement more automation to reduce routine, manual tasks. It will create a self-service portal that allows internal users to configure and deploy their own ports and infrastructure resources. It will continue to refine its segmentation and security policies. And it will share network details and diagnostics, including endpoint group memberships, with the compute team to further improve operational efficiency.

"Cross-tier correlation provides a self-service way for our compute group to investigate and isolate the issues," says Rothstein. "The combination of Cisco ACI and Splunk has helped us on a number of levels, from infrastructure visibility and troubleshooting to security and audits. And we plan to leverage them to do some trend-based logging, access layer endpoint management, and deeper application health monitoring."

Products

- Cisco Application Centric Infrastructure (Cisco ACI)
- Cisco Unified Computing System (Cisco UCS)
- Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS)
- Splunk Enterprise