splunk> Partnerverse

CDI LLC

Home Security and Smart Home company migrates from Elastic to Splunk to provide better customer service and informed product development.

CUSTOMER SUCCESS STORY

Key Challenges

After experiencing explosive growth and customer adoption, Elastic's inability to scale and stability problems caused customer service staff, SREs and product engineering to consider a move to Splunk but struggled to optimally configure and mange Splunk as well.

Key Results

CDI rearchitected the customer's Splunk Enterprise solutions running on AWS. A critical factor in the implementation has been automation with tools provided by HashiCorp and RedHat's Ansible. CDI manages 3 separate, but integrated, Splunk Enterprise deployments totaling over 300TB of daily ingest, while leveraging more than 1500 vCPUs and 5PB of storage, for the customer through our Splunk Virtual Administration service offering.

Industry: Home Security and Automation

Solutions: Splunk Enterprise

Turning Data Into Outcomes

- 300+TB ingest with sub-second dashboard rendering for mission-critical customer support use cases.
- Zero downtime of Splunk Analytics and tremendous user adoption across multiple departments
- Faster product improvements and new feature releases

Implement scalable, and manageable Splunk deployments.

Customer wanted to ingest over 300TB of data to Splunk, requiring multiple Splunk Enterprise Deployments, with hundreds of indexers and search head nodes. Nodes inevitably will fail and need to be replaced quickly, and upgrades had to be manageable. CDI implemented a highly customized GitOps solution with HashiCorp products and RedHat Ansible Automation platform. Data onboarding was also particularly tricky in many cases, particularly with the potential of cached telemetry being sent to Splunk from IoT devices that have lost network connectivity for some time. There were many issues to overcome regarding event breaking and field extraction as well. CDI developed a custom Splunk modular inputs with Python and digs deep into the Splunk indexing pipeline to optimize the solution. Of course, analytics needed to take these customizations into account, and CDI built the search macros, event types and data models the customer needed to empower end users to both find the needle in the haystack and continuously develop dashboards and alerts..

Provide ongoing operational management services for the Splunk solution.

CDI has been providing our Splunk Virtual Administration managed service to the customer for over 3 years. Our Splunk experts monitor hundreds of hosts Splunk Enterprise on AWS and the associated AWS components that are integrated. We perform regular checks on the operational health of the environment. Further, we continuously review the configuration for changes, closely examine internal logs and metrics, for Issues that are proactively remediated. We regularly patch all operating systems, Splunk software, Splunkbase apps and custom-built TAs without any service disruption.