About

Plumbing Supplies Distributor Client, based in the southeastern region of the United States, is the largest U.S. distributor of plumbing supplies, PVF, waterworks, and fire and fabrication products. It is also a major distributor of HVAC equipment and industrial products and services.

The Splunk-based solution leveraged much of the client's existing software portfolio to deliver management a fast and efficient way to monitor backend user activity while responding to audit data requests in a timely fashion.

Bob Dore
Senior Splunk Consultant
Sierra-Cedar, Inc.

Location:
Southeast region of the United States

Industry:
Commercial

Technology:
Splunk Enterprise

About Sierra-Cedar

Sierra-Cedar delivers industry-focused client success by providing consulting, technical, and managed services for the deployment, management, and optimization of next-generation applications and technology.
www.Sierra-Cedar.com

Background

This plumbing supplies distributor, a longtime Sierra-Cedar client, wanted to become more proficient in responding to audits, but lacked the ability to effectively log and monitor activity in its PeopleSoft Financials database. The company needed a cost-effective solution that increased visibility into backend system activity to enable timely responses to audit requests. The solution also needed to support compliance with the company's data security policies.

Challenges

Time spent responding to and supporting annual audits was disrupting IT activities as it required significant staff involvement. The client also needed a more effective and consistent process to manage and secure audited data. The solution would need to achieve the following:

- Minimize demand on key staff during yearly audit procedures
- Track changes to backend database resources in a consistent and reliable format
- Be accessible to management and utilize role-based access controls (RBAC) in a way that can change as staff roles change
- Secure audited data and store it in a read-only format

Solution

Sierra-Cedar implemented a solution leveraging the client's existing investment in Splunk Enterprise that was affordable, scalable, and reusable.

Affordable
The solution leveraged a combination of native database functionality, PeopleSoft, and Splunk Enterprise for data collection and analytics. By utilizing technology that was already in place, the client didn't have to invest in additional hardware and software.

Scalable
The Splunk solution enables the client to collect and analyze audit data from additional PeopleSoft database tables as well as other data sources by making use of similar audit rules and passing that output on to Splunk.

Reusable
Sierra-Cedar developed PeopleSoft Query-to-Splunk functionality that allowed for the output of any user-developed PeopleSoft query to be sent to Splunk via the Splunk HRRP Event Collector (HEC). As a result, the client can use Splunk as another way to analyze PeopleSoft data when other solutions may be unavailable or inefficient.