EventTracker supplements IT department of financial organization

Analyst: Javvad Malik

27 Jun, 2013

Company name:
Anonymous financial services firm

Activities:
Community banking services (consumer and commercial)

Head office:
New Jersey

Number of employees:
450

Organizational Model:
Centralized IT head office and 25 branches

Key suppliers:
EventTracker

A long-standing community bank that provides consumer and commercial financial services was in need of a log management offering that would monitor its IT infrastructure. As such, the company (which prefers to remain anonymous here) reached out to EventTracker, which was able to provide the technology and act as an extension to its IT department.

The community bank, with assets of around $2.3bn, has a centralized IT function that manages all of the IT for the head office and 25 branches. Like many financial services organizations, the company falls under regulations, such as Office of the Comptroller of the Currency, that dictate monitoring and auditing requirements. A team of eight manages the entire IT estate for the bank, including security.

Early Adopter Snapshot

The company's first logging system was ManageEngine's EventLogger. It was very affordable and, according to the company, had a very nice user interface, which served as an entry-level logging product. It produced useful daily reports and met audit requirements; however, it wasn't very proficient at complex searches, which resulted in it not being very useful for incident response or investigations. Managing the storage requirements for the product also created additional work for the small team.

After a couple of years, the company decided to retire the product, and outsourced log management to its WAN management provider. A cloud-based logging product appealed to the company since it meant it could deploy an on-site collector and leave the rest of the management to the provider. However, the user interface and experience were very cumbersome, and the product never got any traction, so it was never fully deployed.

The head of IT reached out to industry peers to seek recommendations for an SIEM product to deploy. Tripwire came highly recommended by several peers who were very satisfied with the product. However, the company found Tripwire's quote to be too expensive, stating that even at half-price, it would have been too much. Finally, the company decided to trial a pilot with EventTracker's Simplified SIEM, since it offered the required features within budget, in a managed service offering.

Deployment summary

The company says that after a pilot across a portion of its IT estate, it was extremely pleased with EventTracker's capabilities, and quickly expanded to monitor around 700 endpoints, which include in the region of 100 servers, with about 60% of them being virtualized. Over time, the company has expanded its EventTracker deployment to cover as much of the IT scope as possible, including servers, switches, UPS system, etc. These generate between five and six million events a day, which previously resulted in the IT department having to pore over 50-page reports on a daily basis. However, now EventTracker collates all these events, which are analyzed by its professional services group to summarize the important information into a handful of events that need attention on a daily basis.

Because of this summary, the company says it very rarely has the need to go into the product console directly itself – although on occasions where it has needed to, it has found the functionality and search capabilities to be very good.

In addition to the daily reporting, if any notable events are picked up during the day, EventTracker will contact the company to bring attention to the potential incident. The company says the support and timely reporting from EventTracker have been superb, and greatly reduced the overhead associated with log management, allowing the IT team to focus on more pressing issues.

Challenges and obstacles

The head of IT states that the company has a pretty flat structure, so the decision to procure and deploy EventTracker was an easy one. Furthermore, the installation was pretty much a 'nonevent,' with EventTracker coming on-site prior to deployment and then getting the monitoring up and running.

Historically, the company has found that an organization of its size will find it challenging to integrate an SIEM or DLP type of product. However, with EventTracker, it didn't encounter any of the usual challenges associated with integration, cost, features or service.

Innovation and roadmap

For now, the company is very satisfied with its EventTracker deployment, and has no plans to move away from it. It is interested in seeing what new features EventTracker will develop, but aside from that, is pretty well set with the existing deployment.