EventTracker
Actionable Security Intelligence

Security and Compliance at Talbots

The Talbots Inc. is a leading multi-channel retailer and direct marketer of women's apparel, shoes and accessories based in Tampa, Florida. Talbots is well known for its stellar reputation in classic fashion. Everyone knows to look to Talbots when it is time to buy the perfect jacket or a timeless skirt. Talbots customers are women in the 35+ population that shop at their 568 stores in 47 states, catalogs and online at www.talbots.com. Approximate sales for Talbots in 2010 were $991 million.

With its multi-pronged approach to reaching its customers, Talbots must Be constantly vigilant in maintaining its records, having access to reports at any time and making sure it is up-to-date with its Payment Card Industry Data Security Standard (PCI DSS) compliance. PCI DSS is a set of requirements designed to ensure that companies that process, store or transmit credit card information maintain a secure environment for the information throughout the transaction process.

"It was the pursuit of the highest-level of PCI compliance that brought EventTracker to Talbots' attention".

"Talbots' systems move close to one billion separate events per day," said Sean McDermott, security analyst in the IT and security and privacy department, Talbots. "Obviously, that's a great deal of information. When we began looking at EventTracker as well as other solutions, we were at a point where there were so many events handled per day that our old architecture was no longer up to the task. We also needed the ability to more quickly investigate any events or alarms that came up in the network. Scaling up was going to be a challenge as far as we were concerned. But EventTracker has been more than up to the task."

EventTracker is a complete Security Information and Event Management (SIEM) solution that combines real-time log management with configuration and change management in one turnkey software package. EventTracker provides log management features such as real time event log collection, centralized monitoring, event consolidation as well as event analysis and forensics reporting. It provides easy and seamless regulatory compliance with built-in compliance workflows and audit ready reports; items on Talbots compliance wish list.

Talbots had some distinct challenges and requirements that required resolution when EventTracker first assessed the security information and event management needs of the company. The sheer size of the amount of events the company fielded each day, coupled with the compliance needs the company had delineated, made the flexibility and scalability of the solution a prime consideration.

In addition, Talbots IT department had requirements that it needed to achieve including the establishment of benchmarks for normal operation of computer and network systems as well as the ability to investigate incidents. The solution had to be flexible enough to collect information from Windows and UNIX operating systems and provide cross-platform support.

EventTracker's solution was brought on board at Talbots to monitor and collect logs for approximately 3500 systems. These include MS Window servers, workstations and embedded POS registers; Linux systems; AIX systems; a z/OS mainframe; ESX VM appliances; hundreds of WS2000 wireless routers and firewalls and diverse infrastructure devices such as switches, routers, firewalls, and load balancers. These various systems are deployed across 300+ geographic locations, including Talbots' brick and mortar stores, 2 data centers and a call center.

Notably, EventTracker provides a single home for the company's point of sale (POS) logs. The POS system provides easy access to log history as well as the ability to correlate a year's worth of information in a matter of minutes. EventTracker provides security classification for employees who needed access to logs to correlate information. Talbots internal audit department can have access to its information and reports, without gaining access to other departments information in the process. And finally, what might be the most important piece in the EventTracker installation for Talbots was its ability to scale up to handle the number of events a company its size generates each day.

"At one point a few years ago, Talbots had so many individual events coming in, that they were almost unmanageable," said McDermott.

> *"We looked at 5 or 6 different solutions and EventTracker was the best value and simply the best product, straight out of the box..."*

One of its major pluses is its scalability. EventTracker has really matured and evolved with Talbots growing reporting and compliance needs and it functions like a true enterprise product. It lets us know what's going on in the network all of the time."

EventTracker's alerting function is another standard that Talbots was looking for. "We know that when a number of failed logs ins are registered, this is usually a sign of some kind of security breach," said McDermott. "EventTracker's out of the box alerting feature is 'click on and go' and we've found it covers most of the events you'd want to know about, without much tweaking."

EventTracker

Actionable Security Intelligence

Talbots' EventTracker installation also enables analysis of information flow to see if any area is not functioning properly. It provides geographic event collection, which is helpful when you want to know where your customers are, while minimizing the impact of information on various parts of the network. The improved security and reporting capabilities EventTracker has enabled at Talbots have fulfilled federal requirements but have also continue to offer obvious benefit on several other levels.

"In an overall sense, EventTracker has provided a great deal of value; it is saving Talbots money," -McDermott

"Our needs were mostly driven by security and compliance, but we have realized additional operational benefits with EventTracker. It takes less time to resolve issues, it provides our operational support people with access to historical logs and when our registers are closing in on their maximum disc space, EventTracker automatically helps prioritize for hardware upgrades and refreshes."