

Logging In Depth

EventTracker is a Security Information and Event Management (SIEM) solution designed to enhance the security of critical systems, ensure confident compliance and improve overall performance and availability



Credit Union Central of Ontario

Business Needs:

- **Pro-active Security Management**
- **Compliance Automation**
- **System Health Monitoring**

Credit Union Central of Ontario (Central) is the only organization in the Canadian province of Ontario that provides a full range of operational and financial services to almost 160 member credit unions, who serve 1.2 million customers. In partnership with its members, Central develops and delivers innovative products and services to ensure credit union strength, stability and growth. Its primary financial role is to maintain a large pool of funds to ensure that member credit unions have the required cash flow to meet the needs of their respective customers.

Operating in a highly regulated environment that's designed to protect credit union member deposits, Central must ensure that customer and other sensitive information is completely secure and that system downtime is avoided. Alex Maynard, Central's Technical Security Specialist, is responsible for monitoring critical systems for potential security threats and for ensuring that the technology that supports Central is up and running 24/7.

Prior to implementing EventTracker, Alex would spend 3-4 hours per day manually reviewing thousands of log files on dozens of file, print and email servers for potential security and system issues. This was a time-consuming and cumbersome process that caused significant losses in productivity. Realizing that he needed a more efficient solution in place, Alex researched 4-5 log management vendors and after much due diligence chose EventTracker to automate his processes. A unique selling point for him was its scalable collection engine, which had the ability to manage events generated by multiple operating systems and network devices.

With EventTracker's ability to automatically collect, analyze and archive logs in real-time, Alex now no longer needs to manually weed through data on every server. A central and secure management console and customizable event classification rules accelerate his daily review process by providing him immediate access to analysis and reporting capabilities, thereby saving him up to 4 hours per day in log management activity.

Deployment

Deploying EventTracker across Central's architecture was a quick process and Alex confirms that he was "able to install and configure it right out of the box." He was also impressed with the quality of support provided to him by the technical support team. Immediately after installation, EventTracker's automatic, unattended consolidation of events began to pay dividends. "EventTracker provided us with advance notice about an issue that we were having with our Exchange e-mail server. This prevented unnecessary downtime and really showed us the value of the software right away."

Business Benefits

In addition to providing Alex with the necessary network insight to make intelligent decisions about capacity, performance, availability and resource utilizations, the software was also configured by Alex to monitor their PIX firewalls. He points out that "we had limited visibility into our firewalls before EventTracker, but now we can closely monitor any changes and pull reports quite easily."

System transparency is a critical requirement for any financial institution dealing with highly sensitive data.

With 'defense-in-depth' capabilities, EventTracker is able to protect the servers where data resides, and not just the perimeter, by monitoring unauthorized network-port usage, host-based intrusions and network connections. EventTracker's powerful rules-based correlation engine tracks user and network activity patterns and system access-related behavior including failed log-in attempts across Central's systems to capture any intrusions or suspicious activities. Real-time email alerts instantly notify Alex and allow him to take a proactive approach to potential security breaches.

EventTracker has been instrumental in demonstrating due diligence as part of

Central's regulatory response to regulations, including Sarbanes-Oxley. The company uses the software's reporting features to quickly respond to auditor requests to see how log data is managed and reviewed, how Central monitors and controls data access and the steps it takes in response to security breaches and other suspicious activity. Alex confides that "EventTracker really helps us when working with Audit and Compliance personnel, plus its forensic capabilities are great."

"EventTracker really helps us when working with Audit and Compliance personnel, plus its forensic capabilities are great."

- Alex Maynard,
Technical Security Specialist,
Credit Union Central of Ontario

Bottom Line

EventTracker has helped Central reduce system downtime and the business risk associated with security breaches by proactively detecting potential issues and alerting personnel in real-time for immediate response. The company is now able to securely collect and report on a variety of system activity and data-access information integral to maintaining a secure and compliant infrastructure. In addition, the software provides Alex and his department with an efficient and reliable way to review automatically-captured log information resulting in significant productivity gains and labor savings.

Alex concludes that "besides saving me up to 4 hours per day in log maintenance, EventTracker has been a great proactive management tool. I give it a big thumbs up!"