

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



Highlight of Business benefits

- Allows JCHCI to provide 24/7 security monitoring of internal and external activity and threat elimination
- Enables JCHCI to provide vertical-specific regulatory expertise and a customizable set of capabilities with support for PCI, Sarbanes-Oxley, GLBA, HIPAA, FISMA and more
- Reduces time spent by security analysts on time-consuming, labor-intensive tasks
- Allows JCHCI to grow with a growing customer base with comprehensive, extendable device support and scalable architecture and pricing

About JCHCI

Ensuring regulatory compliance, while building a robust cyber defense program, is a challenge for many organizations. For smaller businesses with limited skilled security resources and smaller budgets this task often takes on daunting proportions and many turn to Managed Security Service Providers (MSSPs) to improve security and lower costs. JC Hanlon Consulting, Inc. (JCHCI) is a MSSP that specializes in helping businesses identify and manage risk to their business information through its Business Impact Analysis, Risk Assessment and real-time monitoring, reporting and remediation services for a comprehensive approach to security management. JCHCI also offers Penetration Testing, Access Control solutions including Enterprise Single Sign-on (SSO) and integrated Facility Access.

JCHCI Challenges

For MSSPs, Log Management is a critical enabling technology to ensure that customers are compliant and secure and JCHCI monitors millions of logs from its customers everyday. The challenge lies in the nature of JCHCI's business – its customers have very different IT environments and devices, many of which generate an enormous amount of event log data. JCHCI needed a solution that could securely and automatically collect and consolidate log data from thousands of disparate devices in real-time in order to quickly pinpoint and respond to security threats and breaches. A second challenge was scalability. As a fast-growing MSSP, JCHCI depends on solutions that can quickly support new devices and custom applications. *"We needed a solution like EventTracker that could not only support a large number of devices and multiple requirements spanning a variety of verticals, but also scale as we added new customers,"* said Jim Hanlon, CEO of JCHCI.

The EventTracker solution

Prior to selecting EventTracker, Jim put together a short list of vendors who fit his requirements and tested them in the company's in-house lab under real-world scenarios. *"EventTracker really proved that it was the superior solution"* he says. Key areas where EventTracker surpassed the competition was its support of the most comprehensive list of devices from the network to the application layer and an extensible collection engine, which spoke directly to the scalability and flexibility of the software. EventTracker's collection engine – based on regular expression processing - can be quickly extended to support new devices or custom applications. *"It allows us to support almost any device or application in any customer environment,"* adds Hanlon

Another incentive for JCHCI was EventTracker's simple pricing structure. Since pricing is based on number of devices managed and not on event volume, the MSSP does not have to worry about expensive bulk upgrades, as is the case with appliance vendors, when event volume goes up. It can add devices one at a time, as needed, for a highly-scalable alternative to appliance based solutions.

JCHCI was also impressed with the comprehensive nature of EventTracker's features, all included in one license fee with no extra-cost modules to worry about. EventTracker comes integrated with real-time log collection, storage, correlation, reporting, change management, USB device monitoring and all compliance packs (PCI, Sarbanes-Oxley, GLBA, FISMA, HIPAA and more) allowing the MSSP to tailor its services to each specific customer environment, and meet a large number of requirements. *"Of all the solutions evaluated, EventTracker really stood out in terms of the comprehensiveness of its features at a price that was extremely competitive – it was an easy decision to make"* says Hanlon.

Business Benefits

EventTracker has delivered significant value to JCHCI and its customers. Its advanced correlation and alerting features allow JCHCI's IT Security staff to focus on real security threats in real-time rather than wasting time chasing false alarms or monitoring routine log data. EventTracker provides more than 500 out-of-the-box correlation rules to monitor internal and external threat activity such as changes in user rights, login failures across multiple systems, unauthorized access, suspicious network activity, insertion of recording devices such as CDs or USBs, files added to/deleted from external storage devices, irregular user activity and more, giving JCHCI staff complete security insight into customer environments for quick remediation.

EventTracker's consistent high performance and ability to process and correlate an ever-increasing volume of log data from a number of devices, allows JCHCI to ensure that its customers' data and systems are always secure from both inside abuse and external attacks. Customers benefit from 24/7 coverage, security monitoring and threat elimination before serious damage is caused. What's more, JCHCI is able to bring more customers aboard

without increasing headcount. *"Even though the number of events generated keeps increasing, EventTracker is able to keep pace, and more importantly make sense of all that data with ease,"* says Hanlon

On the compliance front, JCHCI leverages EventTracker's support of a number of regulatory standards with over 800 pre-configured reports mapped to PCI, Sarbanes-Oxley, HIPAA, FISMA, GLBA and more, to provide vertical-specific expertise to customers. *"This really removes the headache of having to invest in additional technology to meet different regulatory agendas. Plus in the event that a client forgets to sign-off on an internal change, which happens quite often, we can quickly pull up user activity and change reports to prove to onsite-auditors that due process was followed in accordance with internal policy"*

"Of all the solutions evaluated, EventTracker really stood out in terms of the comprehensiveness of its features at a price that was extremely competitive – it was an easy decision to make"

"It allows us to support almost any device or application in any customer environment."

-JC Hanlon, CEO, JCHCI

Equally important, EventTracker has driven significant efficiency improvements for JCHCI. In particular, EventTracker's technology has freed JCHCI security analysts from time-consuming labor intensive tasks. For instance, agents, necessary for real-time collection, can be centrally installed, configured and managed from the EventTracker Console without having to spend a number of hours visiting each system to manually install an agent. Furthermore, because EventTracker can interoperate with a large number of devices out of the box, the time-consuming barriers to transferring data to a central location are removed.

For more Information

To find out how EventTracker can help you with your security, compliance or operational needs, call us at (877)-333-1433 or visit us at www.prismmicrosys.com

For information on JC Hanlon Consulting Inc. call (586) 435-6231 or visit www.jchci.com