SecureWorks

ON-THE-GO, 24X7 SECURITY VISIBILITY AND ACCESS

The chief security officer at a multi-billion investment firm gains anytime, anywhere access to his managed security services with the SecureWorks Mobile App

Company: Investment Management | **Industry:** Finance and Insurance | **Country:** U.S. | **Employees:** 180

BUSINESS NEED

Staying on top of security events, escalations and tickets while outside the office or in meetings was a challenge for the CSO of a major private investment company.

SOLUTION

The executive downloaded the SecureWorks mobile application into his smartphone and can now keep the most important current and historical information about his company's security posture at his fingertips, no matter where he is, and now saves hours each week.

BENEFITS

- Saves hours weekly, boosting personal productivity
- Enables more timely views of security posture
- Boosts trust and confidence in cyber security by management
- Accelerates responsiveness to critical events
- Promises improved collaboration as staff grows

PRODUCTS | Advanced Endpoint Threat Protection — Red Cloak™ | Managed Firewall | Managed iSensor Intrusion Protection System | SecureWorks Mobile App | Targeted Threat Intelligence Services

U.S.-based investment management companies need iron-clad security to meet rigorous Securities & Exchange Commission (SEC) regulations and audits. At the same time, investor data and proprietary trading systems must be protected by safeguards that are always up to date and monitored. Even one major security breach can undermine investor confidence and unleash a torrent of share redemptions. That's why having 24x7 anytime, anywhere security visibility is critical.

One such company has more than $80-plus billion in managed assets and its investors number in the tens of thousands. It has 180 employees who work in front-office sales, marketing and portfolio management functions, as well as back-office administration and operations. The company's data centers, both primary and disaster recovery, use colocated facilities. Security is the responsibility of one person, the Chief Security Officer (CSO).

"I KNEW HOW WELL SECUREWORKS STACKS UP AGAINST THE COMPETITION"

This person joined the organization in 2014. He was attracted in large part to the fact that SecureWorks Managed Services had been in place since 2011. "Previously, I was a security consultant, and knew SecureWorks as an industry leader," he says.

"In my consultant role over the years, I had either led or taken part in many competitive shoot-outs for my clients, and I knew how well SecureWorks stacks up against the competition in protecting customers."

Because the CSO is the only person within the organization who has specific cyber security responsibilities, he considers the people providing the company's SecureWorks Managed Services to be his de facto, day-to-day team. Specifically, those services are:

- **Advanced Endpoint Threat Protection (AETD)** — Red Cloak. Lightweight software sensors have been downloaded to all the company's endpoints that continuously search for forensic evidence of malicious activity. At the same time, they monitor device behavior and activities, such as what programs are running, what commands are executed, thread injection, memory inspection and more.

  The collected data is sent off-premises to the Red Cloak Analytics system, where SecureWorks Counter Threat Unit (CTU) researchers analyze it for attacker behavior patterns. If any evidence is found, it is investigated by a security analyst in the SecureWorks Counter Threat Operations Center (CTOC). High-severity events are escalated to Senior Intrusion Analysts, who deconstruct them and then send the CSO actionable guidance to remediate them.

- **Managed Firewall.** This provides the company with 24x7 firewall administration, log monitoring and response to security and device events. Security and health events are correlated across its entire IT environment and analyzed by certified SecureWorks analysts, using global threat intelligence and assessment expertise. Intelligence from our global visibility and CTU research continually feeds the service's safeguards to strengthen policies and improve analysis of firewall logs.

- **Managed iSensor Intrusion Protection System (IPS).** After joining the company, the CSO upgraded its Intrusion Detection System to this managed IPS service. The iSensor appliances provide in-line deep packet inspections, eliminating malicious inbound and outbound traffic in real time. They are monitored 24x7 by SecureWorks CTOC.

  "I wanted to shift this layer of our defense-in-depth strategy from a defensive IDS posture to an offensive IPS one," he says. "With SecureWorks managed iSensor IPS, we reduced our incident escalations from more than 350 a year to less than 30 — an improvement of more than 90 percent."

- **Targeted Threat Intelligence.** Given the high stakes his company faces each day in managing billions for its many customers — life savings, for many — the CSO continued its subscription to this service. It monitors information outlets 24x7 in real time to identify threat actors that may be targeting the firm. If so, SecureWorks provides quick and effective guidance about countermeasures to protect the company's networks, systems, executives, assets and, ultimately, its brand reputation.

SECUREWORKS MOBILE APP: ANYWHERE, ANYTIME ACCESS SAVES HOURS EACH WEEK

Even with all these SecureWorks managed services, the CSO is not a "set-and-forget" executive. After all, he knows that investor trust in the company hinges not only on investment performance but also on how secure they believe their data is. He also knows that executive management and the board of directors count on him to be on top of the company's security 24x7, holidays included.

For that reason, the CSO has become a big fan of the SecureWorks Mobile App on his smartphone. Available for both Apple iOS and Android devices, the app's newest version has a fingerprint login for fast access. Its contents are tied into the SecureWorks Client Portal, so the company's data is always synchronized. This way, too, he can find and review tickets wherever he is without opening his laptop.

"If I'm out to lunch or on the train heading home, I can access, view and act on any and all of our company's tickets with the SecureWorks Mobile App," he says. "In fact, I can do the same in meetings when breaking out my laptop to check the SecureWorks portal would be too distracting. Also, if an issue needs my attention, I can address it immediately without having to call SecureWorks. I can manage all my tickets this way."

PUSH NOTIFICATIONS ACCELERATE RESPONSIVENESS

The SecureWorks Mobile App also delivers security alerts directly to the CSO's smartphone via push-notifications as soon as the SecureWorks CTOC discovers them. These keep him immediately abreast of all threat activities and help accelerate his response to those needing attention. "The faster I can respond, the sooner we can address the issue," he says.

For example, when he gets a mobile alert, he just swipes the notification on his phone to reveal all the details he needs to know. He then can respond or, when he adds team members,

choose to delegate the response to one of them. The SecureWorks Mobile App can scale for any size IT security team and can enhance collaboration across members, even if they're spread around the world.

BOOSTING LEADERSHIP AND BOARD CONFIDENCE IN INFO-SEC MANAGEMENT

According to the CSO, the SecureWorks Mobile App saves him several hours a week versus using the SecureWorks Client Portal, thanks to the app's simple login and upgraded ticket management system. That's time he puts to more strategic projects.

"But even more than the time savings, the SecureWorks Mobile App improves my visibility and responsiveness to all critical incidents," he says. "Not only does this help me do my job better, but it also boosts the confidence of our leadership and board that I've got security covered no matter where I am or what I'm doing."