Secureworks®

From Patchworks to Secureworks: Global Firm Standardizes Security

Top logistics provider gained a consistent security posture and "single pane of glass" view across all its global operations by outsourcing security to Secureworks.

Company:
Global Logistics Supplier

Key Challenges

As a global enterprise, the client had outsourced security for many years, but saw little value or distinction in this patchwork of services deployed around the world, despite growing threat levels globally.

Solution

The company deployed a comprehensive, single-sourced security model worldwide that provided standardized processes and technology, complemented by a group of dedicated, resident security experts, to harden defenses and improve visibility, all from Secureworks.

Business Benefits

- Gains a standardized security model worldwide
- Deploys a turnkey staff of resident security experts
- Strengthens overall security posture, reducing vulnerabilities
- Provides global "single-pane-of-glass" visibility into specific services
- Improves compliance
- Delivers enhanced security policies and governance

The Challenge

When cybersecurity is at stake, complacency is dangerous—especially for many industries which face rigorous data privacy compliance requirements and a data paradigm in which many different partners need instant access to provider networks and applications. Plus, with an ever-rising tide of security threats increasing in frequency, sophistication and diversity, today's enterprises must continually evaluate their security posture and defenses.

The external landscape is continually evolving and internally, organizations are always changing, to optimize their alignment of people, processes, and technologies to best respond to new opportunities and challenges.

As technologies develop, especially cloud and mobile applications, and user behavior evolves—like BYOD, which expands an organization's attack surface—defending an organization becomes much more complex.

Rapid growth, either organically or via mergers and acquisitions, can compound rates of change within organizations. If the former, the introduction of new or expanded workflows, new processes, new employees, and even new third-party vendors and partners can test the limits of security defenses. If the latter, different enterprises coming together must connect or even fully integrate IT systems, creating new vulnerabilities for threat actors to exploit.

Subject to complacency

These issues are further complicated for organizations outsourcing their security and trusting that their service providers will stay abreast of both external and internal changes. But without periodic reviews of both their defense models and their service providers supporting those models, organizations can be subject to their outsourcers' complacency, leaving their data, intellectual property, compliance and brand reputations exposed.

Security as a strategic priority, not a sideline

This organization had considered security as a tactical matter and addressed local requirements with point solutions, many of which were outdated. The result over time was an emerging patchwork of diverse processes and solutions that used different vendor products, opened gaps in coverage, and lacked organization-wide reporting and visibility.

Vulnerability scanning, for example, was done in one area of their global security ecosystem on an infrequent basis—despite having operations in many other nations—using a technology-only solution with no human intelligence applied to derive insights from the results. The use of a variety of firewalls in various countries also delivered inconsistent levels of protection.

Another problem was that the company could not see any clear value in the security services that were provided. Part of that was the insufficient reporting, but because all the services were bundled into a much larger IT outsourcing agreement, it was difficult to delineate the metrics for any particular service, not to mention how the service was being delivered.

The Solution

Secureworks, a global, end-to-end security solution

Taking a consultative approach to the company's global security requirements, Secureworks suggested to executive management that a strategic, end-to-end security arrangement could be quickly deployed worldwide. The new model would use the latest Secureworks technologies—such as the iSensor™ intrusion prevention system—implemented as managed services. By performing in-line deep packet inspection, iSensor eliminates malicious inbound and outbound traffic in real time.

Then, to amplify the value of this iSensor protection across the U.S. and other nations in which the company operates, it would be coupled with the Secureworks Counter Threat Platform™ (CTP). The CTP would facilitate that active monitoring and correlation of firewall logs with the security logs of Active Directory, DNS, DHCP, content-filtering appliances, and the company's existing anti-virus solutions.

The Secureworks CTP delivers qualitative and quantitative, network-aware intelligence drawn from global visibility across more than 4,400 client environments in more than 55 nations. Should a new threat emerge, the CTP will be the first to report it.

Secureworks Services

- Advanced Remediation Management—12x5
- Counter Threat Platform (CTP)
- Incident Management Retainer
- Managed Firewall
- Server Monitoring
- Managed Security Services
- Security Consulting
- Vulnerability Management Services

Secureworks®

Results

Several factors influenced the company's decision to engage Secureworks for a global, end-to-end security solution. One was the full portfolio of end-to-end Secureworks services that are available globally, plus its experience in interoperating with scores of industry-leading security technology providers.

The executive management team was also impressed to learn that Secureworks was far and away the industry leader in the Gartner Magic Quadrant. Finally, a visit by company leaders to the Secureworks Security Center of Excellence (SCoE) located in Bucharest, Romania, cinched the deal, where he learned that his company's CTP would be monitored 24x7 by more than 150 security experts. Ultimately, the company engaged Secureworks to deliver these additional services:

- **Advanced Remediation Management —12x5:** Provides a seamlessly integrated, managed consulting service via skilled experts, who conduct deep dives and analysis on suspicious and critical events.

- **Incident Management Retainer:** Guarantees fast availability of the Secureworks elite Incident Response and Management team to contain, mitigate and help the company recover from a security breach.

- **Managed Firewall:** Provides 24x7 firewall administration, log monitoring and response to security and firewall health and performance issues.

- **Server Monitoring:** Guards both virtual and physical servers with a common management interface that provides defense-in-depth security by delivering firewall, intrusion detection and prevention, and anti-malware capabilities monitored by experienced managed security experts, 24x7.

- **Managed Security Services:** Provides integration of security services beyond the "Day One" cutover from the previous outsource provider, including customized reporting, escalation procedures and post implementation performance tuning to maximize time to value.

- **Security Residency and Implementation:** Dedicates numerous security experts to the company's security—with many of them onsite at company facilities globally—effectively deploying a highly trained security staff instantly versus taking months to find, hire, train and integrate a security staff of its own.

- **Security Consulting:** Provides expertise and analysis to help enhance the company's security posture, reducing risk, facilitating compliance and improving operational efficiencies.

- **Vulnerability Management Solutions:** Active, continuous scanning, plus expert guidance for remediation with risk and compliance reporting.

Secureworks®

Looking Ahead

In addition to all these Secureworks services that are integrated and optimized for a complete global security model, the company has a critical feature it lacked before: instant, always up-to-date reporting through The Secureworks Client Portal – Powered by the Counter Threat Platform.

The Client Portal provides the intelligence and analytics the company sought to easily understand its risks, make more informed security decisions and easily and quickly demonstrate compliance with such requirements as HIPAA and PCI. It can be accessed via a mobile application on smartphones and tablets, providing the company's security staff with alerts to significant events, even while they're out of the office.

The Portal's reporting also provides the company with crucial visibility into how the various Secureworks services are working—and the value those services provide the company.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist. **secureworks.com**