SecureWorks

ADVANCED PROTECTION AGAINST THREAT ACTORS SAFEGUARDS BRAND REPUTATION

Top provider of application security testing makes a great service offering even better using SecureWorks solutions

VERACODE

Industry: Technology | **Country:** United States | **Employees:** 400

Website: www.veracode.com

> “We didn’t call anyone else. Gartner’s Magic Quadrant ranked SecureWorks as the clear industry leader, like we are in our space, so that spoke volumes.”

Bill Brown, CIO and Senior Vice President, IT and SaaS Operations, Veracode

BUSINESS NEED

Veracode’s sophisticated IT security stack required another layer to monitor security events in real time and get alerts about unexpected system and network behaviors.

SOLUTION

The company fortified its security defenses across a mixed-vendor IT landscape with a comprehensive set of SecureWorks solutions, backed 24x7 by world-class Counter Threat Operations Centers.

BENEFITS

- Added 24x7 support of world-class Counter Threat Operations Centers
- Ensured customer trust in company’s brand promise
- Sharpened its competitive edge

PRODUCTS | SecureWorks Managed Services

AMONG ENTERPRISE IT'S BIGGEST SECURITY RISKS ARE APPLICATIONS.

Less than half of enterprises test all of their business-critical apps for basic vulnerabilities. More than 60 percent of vendor-supplied applications fail basic security testing. Worst of all, 90 percent include at least one of the top 10 most critical web application security flaws, as defined by the Open Web Application Security Project.

Enter Veracode. Its cloud-based, application vulnerability testing service delivers a simple, highly scalable solution to reduce global application-layer risk across web, mobile, legacy and third-party enterprise applications. By identifying critical application-layer threats before cybercriminals can find and exploit them, Veracode helps its clients get their innovations to market faster, without sacrificing security.

Recognized as a Gartner Magic Quadrant Leader in application security testing since 2010, Veracode secures hundreds of customers across a wide range of industries, including nearly a third of the Fortune 100, three of the top four U.S. commercial banks, and more than 20 of Forbes magazine's 100 Most Valuable Brands.

LACK OF SKILLS, TIME AND BUDGET

"The biggest reason organizations fail to test their apps sufficiently, if at all, is their lack of skills, time and budget," says Bill Brown, Veracode's CIO and senior vice president of IT and SaaS operations. "Fact is, the traditional on-premises approach to application security doesn't cut it anymore. It's complex, manually intensive and difficult to scale."

Given Veracode's business model of cloud-based application vulnerability testing, the company realized that its sophisticated, defense-in-depth security model needed even more security. "A security breach at our company would devastate our brand, so ensuring our own security is a top priority," Brown explains.

"In looking at our security stack, we had to raise our levels of monitoring security events and correlating any nefarious or unexpected behavior," he says. "Many companies talk a good deal about device monitoring and event correlation around security events, but there's actually very little action. They might log everything but inspect very little."

EXPERTISE AND RESPONSIVENESS

To gain new levels of security, Veracode contacted SecureWorks. "We didn't call anyone else," Brown says. "Gartner's Magic Quadrant ranked SecureWorks as the clear industry leader, like we are in our space, so that spoke volumes. We use a wide range of their services across a mixed-vendor IT environment and are extremely pleased with their threat-intelligence expertise and responsiveness." He emphasized that the threat intelligence that SecureWorks provides was a big differentiator and driver of his choice in security providers.

Brown adds that SecureWorks boosts Veracode's own value proposition by increasing the levels of trust its customers can have in its overall security. At the same time, this helps increase its competitiveness. "In a very real sense," he says, "we can include, as an integral part of our IT security infrastructure, the backstop we have that's provided by the world-class, security-monitoring infrastructure of SecureWorks."

LOOKING FOR DEVIANT NETWORK BEHAVIORS

Fred Owsley, Veracode's manager of information security, manages all of the company's security layers as well as all the managed services SecureWorks provides. He replaced network intrusion detection devices that he built based on open-source Snort software with SecureWorks iSensor Intrusion Prevention Service (IPS). "The Snort boxes were a pain to manage and turned out a ton of false positives," he recalls.

As part of the SecureWorks IPS managed service, Owsley deployed three iSensor devices located adjacent to the company's firewalls: one at its headquarters in Burlington, Massachusetts; the second at its offsite data center, which provides its cloud-based app-testing services; and a third at its London office.

Each iSensor scans incoming and outgoing network traffic, monitored 24x7 by SecureWorks Counter Threat Operations Centers (CTOCs). These facilities correlate all traffic and device behaviors, alerting Owsley to any deviant patterns. "The iSensors were plug-and-play, with virtually no management needed. Now with all the eyes and ears of SecureWorks analyzing our network traffic, I couldn't accomplish the same thing if I hired five people."

> *"Now with all the eyes and ears of SecureWorks analyzing our network traffic, I couldn't accomplish the same thing if I hired five more people."*

Veracode complements its iSensor IPS with Log Monitoring and Retention services from SecureWorks. "We use these services to collect network metrics to determine baseline behaviors and for investigations," Owsley says. "We'll pull logs from all the iSensor devices. And they're all indexed and searchable. We didn't have that with our Snort boxes."

ALERTS IN MINUTES

With about half of Veracode's 400 employees working remotely at any one time, Advanced Endpoint Threat Detection (AETD) is another important tool Veracode uses from its broad suite of SecureWorks managed services. Should a user's desktop or laptop device get infected with malware, Owsley is alerted, so the device can be isolated and the cause identified and remedied. He is also informed why and how the attack occurred, along with guided remediation advice from SecureWorks.

"We get different levels of notifications from the SecureWorks Counter Threat Operations Centers," Owsley says. "For lower-level alerts, I get an email. If it's critical, I get a call in minutes."

As a cloud-based service provider and one of Inc. magazine's fastest-growing U.S. companies, Veracode needs scalability not only in its own operations but also in those of SecureWorks. "It's reassuring for our customers, for us, and for our investors that no matter how fast we grow or big we get, SecureWorks will always be on pace to match our growth."