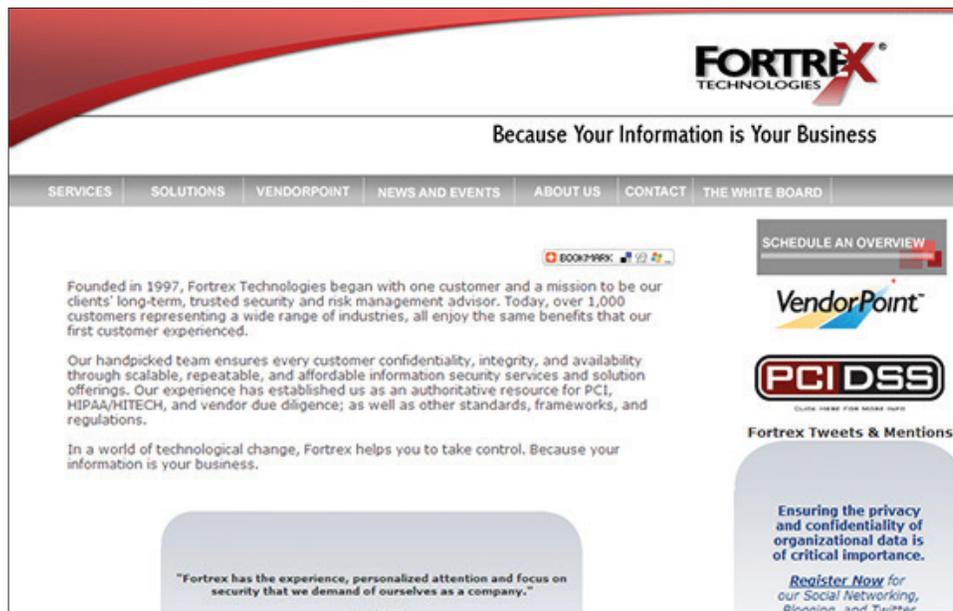# Web Application Security:
Fortrex's Formula for Success

Effective web application security requires three key attributes: the right tools, the right results, and the right skills.

Fortrex Technologies, Inc. partners with customers to serve as their long-term, trusted security and risk management advisor. Fortrex's over 1,000 clients include merchants, banking, financial, and health care providers that face significant IT security and regulatory compliance demands.

To help its clients maintain compliant and resilient applications and IT infrastructure, Fortrex provides risk and vulnerability assessments, penetration tests, and compliance assessments so clients can better defend against modern attack techniques and comply with such regulations as the Payment Card Industry Data Security Standard (PCI DSS), the Health Information Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and many others.

"We have customers of all sizes and industries, including healthcare, financial, e-retailers, and merchant service providers with web-based applications," says Samuel P. Hinson, managing director, information security officer, Fortrex Technologies. "There is certainly steady demand for these risk management and application assessment services."

To succeed at helping its clients better manage their risks associated with web applications, Hinson says three essential elements are needed: an automated web application vulnerability scanner, accurate results, and a knowledgeable security engineer to help provide clients with the best possible customized approach to reducing risk.

QUALYS

Market Demand for Web App Security Continues to Grow

The demand for security and risk management services shouldn't come as a surprise. While concerns around regulatory mandates are growing, so are the pressures to rein in the many types of security weaknesses associated with web applications. And organizations are increasingly seeking solution providers with the skills and expertise necessary to help.

This is largely because as web applications have grown in importance, so has the attention attackers pay to infiltrate them. Many attacks today occur through sophisticated techniques such as injection attacks, Cross-Site Scripting (XSS), and SQL injection. The Open Web Application Security Project, or OWASP, ranks the Top 10 most critical web application vulnerabilities.

"Enterprises know that they have vulnerabilities associated with web-based applications and that more and more attackers are targeting their web applications," says Hinson. "There's also a lot of interest in ensuring that their internal software developers are practicing secure coding techniques and best practices. That requires periodic reviews."

Yet, assessing the security posture of web applications can be complex. "Web applications can be among the biggest challenges to scope during a customer engagement, depending on the types of applications, and the number of applications they have installed. These applications can be very intricate, with integrations that run very deep into their infrastructure," Hinson says.

To succeed, solution providers need to be able to arm their security engineers and analysts with the best available tools to help them more accurately and efficiently identify vulnerabilities than they ever could attempt manually.

However, Fortrex realized over time that web application scanning tools are not equally effective. Previously, Hinson and his team used a commercial web application scanner for their engagements. But the assessment software wasn't as efficient, or as effective, as they needed. First, the application was expensive to buy, required a license for each user, and only one user could use that license at a time. Perhaps more importantly, the software also had to be installed on the notebooks or PCs of the security engineers who were going to perform the assessment – which was highly inconvenient and ineffective. Finally, the assessments too often included false positives that were time-consuming and expensive to verify.

To address its web security needs, Fortrex turned to QualysGuard Web Application Scanning (WAS), from Qualys, Inc. Fortrex had been successfully leveraging QualysGuard Vulnerability Management (VM) for many years, with great success, and decided it would consider QualysGuard WAS in hopes of similar results. "QualysGuard VM, the network vulnerability scanner, is part of our standard penetration test," Hinson says, "so it made sense for us to also choose QualysGuard WAS."

> "It's great to be able to go to one place and manage all of our network vulnerability scans and web application assessments. It [QualysGuard VM and WAS] improves our ability to manage customer assessments."
>
> **Samuel P. Hinson,**
> Managing Director, Information Security Officer, Fortrex Technologies

QUALYS
CONTINUOUS SECURITY

Unifying Vulnerability Management in a Single Cloud Platform

As part of the trusted QualysGuard Cloud Platform, QualysGuard WAS provides accurate web application security assessments for improved application security and resiliency – achieved with all of the advantages, power and scalability of cloud computing – providing a comprehensive and consistent view across environments, including pre-production and production. QualysGuard WAS identifies web application vulnerabilities in the OWASP Top 10 such as SQL injection, Cross-Site Scripting (XSS), URL redirection, and many other vulnerabilities. And, because of its rich dynamic user interface, users experience an intuitive, easy-to-use automated workflow.

"Whenever we have an assessment that includes web applications, we use QualysGuard WAS. It's certainly become an essential tool in our tool bag for whenever we know web applications will be within the scope of the engagement," Hinson says.

Hinson adds that while he hadn't realized it before, having both QualysGuard VM and QualysGuard WAS vulnerability data centrally located turned out to be a substantial benefit. "It's great to be able to go to one place and manage all of our network vulnerability scans and web application assessments," he says. "It improves our ability to manage customer assessments."

Hinson knows that to succeed in delivering trusted security solutions for its clients, his team needs an effective automated web application vulnerability scanner and accurate results – and QualysGuard WAS has proven its ability to meet this need.

"QualysGuard WAS certainly assists us when it comes to performing our assessments in the most efficient way possible. QualysGuard's assessments provide us with excellent results and keeps us on the right path in our analysis," Hinson says.

QUALYS
CONTINUOUS SECURITY