



## AUTOMATED VULNERABILITY MANAGEMENT REAPS DIVIDENDS

*When manual vulnerability scanners proved too costly and ineffective, Fifth Third Bancorp turned to QualysGuard for on-demand, fully automated vulnerability management to improve the accuracy of its network audits and cut the costs associated with third-party consultants.*

***“It’s not about being secure the day the auditors show up. It’s about being secure and compliant every month, week, day, and hour. And QualysGuard helps us to achieve and demonstrate that continuous level of security and compliance”***



Brian L. Klenke, CISSP, Manager of Information Security Vulnerability Management Team  
Fifth Third Bancorp

When the CERT Coordination Center started compiling software vulnerability statistics in 1995, only 171 security related flaws were tallied that year. But little more than a decade later, that number rocketed to 8,064. Also increasing has been the velocity of zero-day attacks and the pace at which attackers develop ways to infiltrate at-risk systems. And attackers no longer are targeting only the network and operating systems—they’re increasingly using sophisticated tools to identify software flaws within Web applications, browsers, and common desktop programs. That’s why a system could be secure one day but highly vulnerable the next.

This means that organizations must work smarter to stay ahead of the rising threats—and this is especially true at financial services firms. “We have a very aggressive vulnerability management program here,” says Brian L. Klenke, CISSP, Manager of Information Security Vulnerability Management Team at Fifth Third Bancorp. “We monitor all new vulnerabilities pertinent to technologies used by Fifth Third, and make sure that mitigation activities are immediately assigned and prioritized,” says Klenke.

### **Manual Vulnerability Scanners Prove Problematic, Ineffective**

Being among the largest money managers in the Midwest, with \$220 billion in assets under care, Fifth Third knows that security is crucial. Based in Cincinnati, Ohio, Fifth Third operates 18 affiliates with 1,167 full-service banking centers. The bank’s Vulnerability Management team, dedicated to keeping its 5,000 servers and 30,000 desktops secure, includes vulnerability analysts as well as representatives from each of the major technology groups across Fifth Third. The vulnerability management test team is dedicated to monitoring new threats and vulnerabilities as they arise and quickly developing and implementing mitigation strategies to reduce the Bank’s risk.

But for a time, Fifth Third’s centralized security team had to rely on various manual open source and commercial vulnerability scanners to try to identify any new vulnerabilities in the network, as well as validate that operation teams had successfully patched vulnerable systems. Unfortunately, these manual-based scanners only allowed the team to run ad-hoc scans, and lacked the ability to centrally manage vulnerability data and trend the bank’s risk management progress over time. “All of our vulnerability data was siloed. And these tools only gave us a look into the state of our security posture for a single point in time,” says Klenke.

## Automated Vulnerability Management Reaps Dividends

---

Compounding the challenges associated with these scanners was the highly inaccurate information they provided, and the fact that data couldn't be organized by business units, system platforms, or any other logical way. "We wasted too much time chasing false positives, and couldn't always get the right vulnerability data to the right support teams," he adds. The result: the bank too often had to turn to costly third-party assessments to ensure adequate levels of security.

"These point solutions did such a poor job of fingerprinting our systems, and they'd declare a system as vulnerable when it really wasn't," Klenke says. "When you're talking about thousands of servers, the time required to sift through all of the false positives to get to the real-world risks really defeated the point of having the tools in the first place," says Klenke.

### **Security-as-a-Service Provides Highly Accurate, Cost-Effective Vulnerability Audits**

In order to attain a more accurate view of its IT security risks, reduce expensive third-party vulnerability assessments, and put into place a centralized database of its security posture, Fifth Third sought a more accurate and cost-effective vulnerability management and auditing solution. Thus, the bank evaluated almost every major vulnerability scanner on the market. The clear and early front-runner proved to be QualysGuard, from Qualys, Inc. QualysGuard shone through all of the bank's tests as the most accurate, easiest to use, and least intrusive way to secure its network through automated vulnerability audits. "We had problems with many other scanners that negatively impacted our servers and services during their scans," says Klenke. "Qualys was the most accurate and the easiest on our systems," he adds.

QualysGuard enables the bank to streamline control of its entire vulnerability management lifecycle: asset discovery, vulnerability assessments, tracking security fixes, and meeting federal, state, industry, and internal security policy regulations. The on-demand solution, entirely managed by Qualys, is delivered as a Web service and requires no software or costly infrastructure to deploy. And QualysGuard's Six Sigma accuracy and comprehensive Knowledgebase of security checks are unmatched. In fact, QualysGuard identifies all networked assets and examines 65,536 system ports for vulnerabilities. The result is a powerful and highly accurate baseline of the network. "What sold us on QualysGuard is its security-as-a-service model," says Klenke. "We don't have teams of people just sitting around, and we're very conservative with our resources and how they're deployed," he says. "QualysGuard provides a service that doesn't add to our current headcount levels to deploy it."

In fact many of the vulnerability assessment tools that Fifth Third evaluated required that the company buy a server and database, and that the database and underlying operating system be manually and constantly hardened and maintained, in addition to other significant backup and storage management costs. "With Qualys, that's all handled as a service. That is very compelling to us," says Klenke.

Today Fifth Third has twenty QualysGuard appliances that audit more than 30,000 specific IP addresses throughout Fifth Third's internal and external infrastructure. Through the automated capabilities provided by QualysGuard, the bank has been able to establish continuous internal and external network audits.

***“What sold us on QualysGuard is its security-as-a-service model. We don't have teams of people just sitting around, and we're very conservative with our resources and how they're deployed. QualysGuard provides a service that doesn't add to our current headcount levels to deploy it.”***

Brian L. Klenke, CISSP, Manager of  
Information Security Vulnerability  
Management Team  
**Fifth Third Bancorp**

## Automated Vulnerability Management Reaps Dividends

What's more, incomplete reporting capabilities no longer are a problem. Through QualysGuard's ability to assign highly-specific asset tags, the bank now can parse its vulnerability information in any way it wants. "We can break down reporting by machine types, business units, or any other way we need," Klenke says. "At the end of the day, it comes down to getting the right information to the right people, and that's exactly what QualysGuard provides for us."

### Continuous Regulatory Compliance and Tight Risk Management Integration

Whether it's federal regulations that govern the security and privacy of the networks of financial services organizations, Sarbanes-Oxley, or the PCI Data Security Standard (PCI DSS) that mandates strict controls to protect credit cardholder account information, QualysGuard's accuracy and flexible reporting capabilities means Fifth Third always is maintaining its systems so that they're compliant. "There are plenty of regulations out there that mandate patch frequencies and security controls, and QualysGuard helps us to stay on top of compliance with a very aggressive vulnerability management program," he says.

PCI DSS is of particular importance to Fifth Third, which is both a credit card acquiring and issuing bank. "And as a payment processor, we have significant security responsibilities to our merchants, and we must report our compliance directly to the major credit card companies. Because QualysGuard is a certified PCI scanning vendor, any reports we get from Qualys' PCI templates can be provided to our auditors as evidence that our systems are in compliance," Klenke says.

Building on this success, Fifth Third Bank currently is working on additional ways to utilize QualysGuard to streamline operating efficiencies and security. While the bank's vulnerability audit reports now are dispatched by the security team, Klenke is using the QualysGuard API to automate report distribution to all IT managers, systems administrators, and others. "We're always looking for areas where we can cut unnecessary steps, and Qualys' API is very useful in these efforts," he says. QualysGuard also will be put to use through the upcoming integration of QualysGuard's vulnerability audit data with the bank's security event management software. In this way, vulnerability information will be correlated instantly with intrusion detection alerts. "This will significantly tone down the number of events our IDS triggers. When we're not vulnerable to an exploit or certain probe, we don't want to be alerted about it. The accuracy of QualysGuard's information will enable us to focus our efforts on real-world risks," Klenke says.

Fifth Third sought a way to reduce the onerous amount of false positives that wasted internal resources and administrators' valuable time, slash costly third-party audits, and attain a better, more proactive approach to its vulnerability management and regulatory compliance initiatives. QualysGuard certainly has helped the bank to get there. "It's not about being secure the day the auditors show up. It's about being secure and compliant every month, week, day, and hour. And QualysGuard helps us to achieve and demonstrate that continuous level of security and compliance," says Klenke.

### FIFTH THIRD BANK SCOPE & SIZE

Fifth Third Bancorp operates 18 affiliates with 1,167 full-service banking centers in Ohio, Kentucky, Indiana, Michigan, Illinois, Florida, Tennessee, West Virginia, Pennsylvania, and Missouri.

### BUSINESS

Diversified financial services company with five main businesses: Commercial Banking, Branch Banking, Consumer Lending, Investment Advisors, and Fifth Third Processing Solutions.

### BUSINESS PROBLEM

Provide effective IT security and regulatory compliance risk mitigation for global network.

### OPERATIONAL HURDLE

Manual vulnerability scans lacked visibility into Fifth Third's infrastructure, failed to provide accurate results, and offered no way to trend vulnerability management progress over time.

### SOLUTION

Fifth Third turned to QualysGuard's on-demand Web service appliance to automatically identify and more easily mitigate system vulnerabilities and misconfigurations inside the corporate network.

### WHY FIFTH THIRD BANK CHOSE QUALYS

- Automated on-demand security and vulnerability audits.
- Highly accurate vulnerability and configuration scans.
- Easy to deploy, manage and operate
- Scalable enough to secure Fifth Third's sizable network.
- Comprehensive reporting capability for technical teams, business managers and auditors.
- Integrates with other areas of Fifth Third's risk management program, including its intrusion detection system.



**USA – Qualys, Inc.**  
1600 Bridge Parkway  
Redwood Shores  
CA 94065  
T: 1 (650) 801 6100  
sales@qualys.com

**UK – Qualys, Ltd.**  
224 Berwick Avenue  
Slough, Berkshire  
SL1 4QT  
T: +44 (0) 1753 872101

**Germany – Qualys GmbH**  
München Airport  
Terminalstrasse Mitte 18  
85356 München  
T: +49 (0) 89 97007 146

**France – Qualys Technologies**  
Maison de la Défense  
7 Place de la Défense  
92400 Courbevoie  
T: +33 (0) 1 41 97 35 70

