Huntington National Bank

www.huntington.com

- **Industry**
  Banking

- **Application**
  Online banking systems and Web-based business applications deployed over Huntington National Bank's intranet.
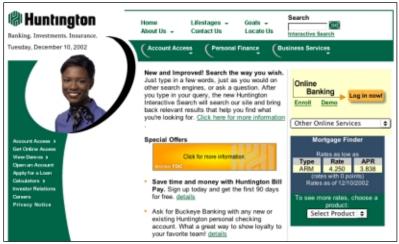
- **Business Problem**
  Huntington National Bank needed to continue to secure the confidential information and financial assets of its customers as well as implement the safeguards mandated by the Gramm-Leach-Bliley Act (GLBA). Additionally, it was committed to putting the same security measures in place for their third-party applications as its homegrown Web-based solutions.

- **Security Solution**
  AppScan™

- **Business Benefits**
  Web application security testing with AppScan enabled Huntington National Bank to redeploy 16 person-hours of work per week to other value-added tasks and helped to ensure GLBA compliance.

- **ROI**
  Immediate payback upon deployment- tens of thousands of dollars saved in IT resources due to automation of security testing; third-party application validation time slashed from two weeks to as little as eight hours; mitigation of risk to customer assets and immense potential losses due to erosion of customer confidence that could result from a security breach.

Huntington National Bank secures the confidential information and financial assets of its customers.

Huntington Cashes In on Web Application Security with AppScan

It was an experience Matt Riddle will never forget: About five years ago, Riddle—assistant vice president, applications development at Huntington National Bank—listened uneasily as a Sanctum Web application security specialist recounted how he had logged onto another organization's supposedly secure e-commerce Web site and changed the price of a $2,000 item to 1 cent using a standard Web browser. "As he explained it, he had never really ordered the merchandise, so no harm was done," Riddle recalls.

"When the Sanctum team ran a proof-of-concept on our Web site, we quickly discovered that AppScan's speed, automation and ease of use provided everything we need from a Web application vulnerability assessment solution."

—Larry Seibel,
Senior Vice President and
Information Security Director,
Huntington National Bank

"GLBA stipulated precisely the sort of requirements we had fulfilled using AppScan, [giving] us further validation that our security strategy was correct."

—Larry Seibel

"But even though our own Web site had substantial security measures in place, the Sanctum security specialist's anecdote was my wake-up call. I could not shake the thought of what would happen to our customers' privacy, to the security of their confidential information—even to the safety of the accounts themselves—if such a vulnerability were ever to creep in."

The Huntington National Bank (Huntington), a $27 billion regional bank, has been serving the financial needs of its customers for nearly a century and a half. Headquartered in Columbus, Ohio, Huntington provides innovative retail and commercial financial products and services through more than 300 regional banking offices and 900 ATMs in Indiana, Kentucky, Michigan, Ohio and West Virginia. Selected financial service activities are also conducted in other states.

Huntington has always considered itself a pioneer in leveraging the power of Internet technology to benefit its customers. Its online banking products were among the first in the world to be introduced. Today, in addition to its Web site huntington.com, the bank's Web presence includes a full-service consumer-facing online bank as well as Huntington View Internet, a 24-hour commercial access system for business customers. Huntington also runs numerous enterprise-wide internal applications across its intranet, including accounts payable, enterprise reporting and human resources systems.

Despite its ever-growing number of Web applications and services, Huntington has succeeded in mitigating the risk of cyber attack, effectively and at low cost. What's more, the bank has also improved the productivity of both its development team and its IT staff—all with AppScan, the automated Web application security testing tool from Sanctum.

Building on a Foundation of Confidence

According to Riddle, ensuring the security of the bank's online systems has always been a crucial priority. "Our customers' confidence in us is the absolute foundation of our business, and our most precious asset," he notes. "We wouldn't have this confidence if we didn't protect our customers' confidential information."

This responsibility became increasingly formidable as Huntington continued to expand its online presence, Riddle recalls. "All across the Internet, hackers had gone from merely breaking into enterprises' firewalls to actually attacking their applications," he notes. "We had always placed vital emphasis on knowing the latest cyber threats and implementing manual safeguards

to avert them. But the more these new vulnerabilities came to light, the more anxious we were that one might slip past us."

That risk was not Huntington's only concern. While the bank's development team employed the most rigorous quality assurance and testing procedures to keep its homegrown Web applications impervious to attack, the demand for sophisticated functionality—such as online mortgage and trust-fund services—meant implementing third-party applications as well. Riddle and his colleagues wanted to be sure they could impose the same level of control on purchased software as they did with their own solutions.

Slashing Costs, Boosting Productivity

Huntington concluded that it needed a user-friendly tool that could automate and streamline security risk assessment throughout the development and deployment of all Web applications. It would have to identify vulnerabilities clearly and accurately, with a minimum of false positives. It would have to provide maximum detection of security holes without impacting application availability—and to cope with new types of hacks as they were identified.

But, as Huntington Senior Vice President and Information Security Director Larry Seibel recalls, these were the early days of Internet security, and there were very few solutions from which to choose. "When the Sanctum team ran a proof-of-concept on our Web site, we quickly discovered that AppScan's speed, automation and ease of use provided everything we need from a Web application vulnerability assessment solution," Seibel says.

Riddle agrees: "AppScan goes through our system, identifies potential vulnerabilities and categorizes them far more quickly and efficiently than I could ever do myself—or train my developers to do. Using AppScan, I can scan one of our internally developed Web applications or a third-party solution and have a full report in just 8 to 16 hours. It would take one of my employees about two weeks to provide that manually."

According to Riddle, AppScan is actually paying for itself by saving Huntington tens of thousands of dollars per year on the cost of IT resources alone—not to mention the potential cost of the security breaches it is preventing. Moreover, AppScan has made the bank's development team much more productive by eliminating the con-

siderable effort needed to confirm that secure development processes were correctly followed. "By running an AppScan audit at the end of the development process, each of our developers can save about four hours per week," he notes. "That time can be invested in critical development tasks, saving the cost of additional IT staff."

According to Seibel, AppScan has also helped Huntington comply with the Data Protection Rule of the Gramm-Leach-Bliley Act (GLBA), the 1999 legislation that regulates data security in the financial services industry. "We were using AppScan long before GLBA came out," he says. "The fact that the new law stipulated precisely the sort of requirements we had fulfilled using AppScan, gave us further validation that our security strategy was correct."

"AppScan identifies potential hacks and categorizes them far more quickly and efficiently than I could ever do myself—or train my developers to do. Using AppScan, I can scan one of our internally developed Web applications or a third-party solution and have a full report in just 8 to 16 hours. It would take one of my employees about two weeks to provide that manually."

—Matt Riddle
Assistant Vice President
Applications Development,
Huntington National Bank

Actionable Results

Huntington's application team initially used AppScan primarily for quality assurance, to identify security defects in the course of development, but the team is now using the solution as an auditing tool for applications it purchased from third parties as well. Riddle's team scans the bank's third-party Web-based banking solutions to detect any security holes before it begins to customize or integrate them into the production environment. Riddle says AppScan's intuitive, easy-to-use interface makes it simple for developers to test and re-test applications as often as they need to. "We repeat the security testing process throughout the application lifecycle. This enables us to provide the vendors with summary and detailed reports of all vulnerabilities identified and tested during the assessment, so they can take action to resolve them." In fact, Huntington is so confident of AppScan's results that the bank will only sign off on purchased Web applications when AppScan has found them to be vulnerability-free. "We're hoping to see some of our application vendors start using AppScan in their own development environment," he adds.

Seibel concludes, "Huntington National Bank has brought its tradition of service excellence into the 21st century with a rich variety of Web-based banking solutions. Thanks to AppScan, we now have the capability to mitigate risk in our applications without compromising their functionality or convenience."

Huntington National Bank Success Story

SANCTUM

2901 Tasman Drive, Ste. 205
Santa Clara, CA 95054
Phone: 877-888-3970 (US/Canada)
+972-9-958-6077 (Israel)
+44 7710 939512 (European HQ)
408-352-2000 (International)
Fax: 408-352-2001
www.SanctumInc.com