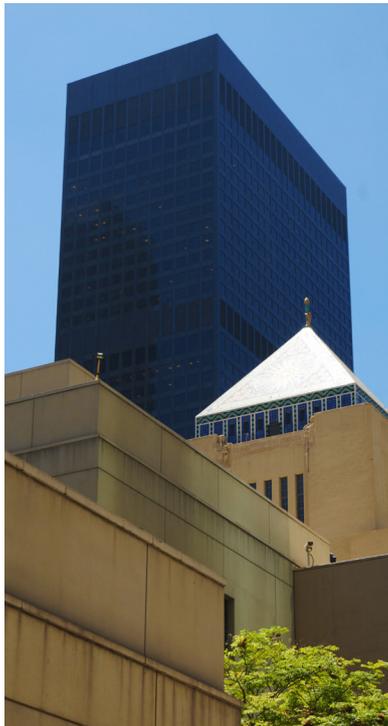




SECURITY THAT KEEPS PACE WITH BANKING'S LATEST INNOVATIONS



The financial services industry has long been a leader in IT development, embracing new technology and the Internet to increase efficiency and improve customer service. But these advances also bring with them new information security risks.

High-profile breaches like the malware attack on US retailer Target show that hackers are probing into all parts of your financial systems: from network and system infrastructure to Core Banking Systems (CBS), Internet banking applications, ATMs and Point-of-Sale (POS) terminals. When Target's POS systems were infected in 2013, personal data on 70 million customers was stolen, with 40 million credit and debit card accounts compromised.

Highlighting the risks, Verizon's 2014 Data Breach Investigations Report shows the biggest threats to the financial industry from 2001 to 2013 were assaults on web applications, distributed denial-of-service attacks and payment card skimming, which altogether accounted for 75% of reported industry related data breach incidents.

With governments turning up the regulatory heat on banks and financial services companies coupled with the demand for mobile banking applications, it's time for many financial organizations to rethink their cybersecurity and compliance strategy.

Stay Ahead of the Bad Guys

For over a decade, Positive Technologies has been conducting security and compliance assessments for dozens of leading banks around the world, giving us unique insights into the practical challenges involved in securing financial systems.

Our dedicated team of banking security researchers are continually in the field learning about the latest threats and newest banking technologies. This practical knowledge is routinely fed back to our product teams, ensuring our solutions remain current and our customers stay ahead of the bad guys. In a 2013 security study of e-banking applications, our experts found that high-risk vulnerabilities were present in half the systems we tested.

Highlights

- + Protect Financial Systems including core banking systems, internet banking portals and ATMs
- + Control Compliance by translating PCI DSS, ISO and SOX guidelines into operational security controls and building compliance checks for internal corporate standards and regionally specific regulations
- + Improve Application Security by stopping zero-day attacks, quickly patching existing security holes and seeing how vulnerabilities can attack your business
- + Get Smarter by leveraging the knowledge of our expert services and research teams that conduct dozens of security assessments and uncover 150+ zero-day vulnerabilities each year

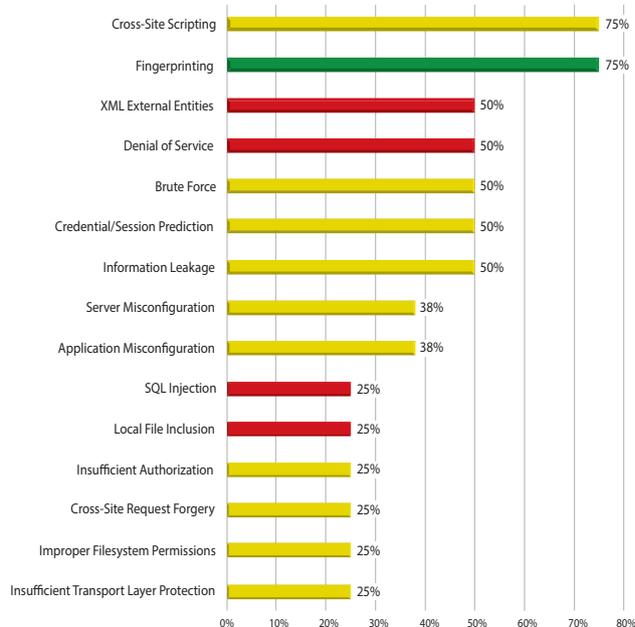


Figure 1: Most common e-banking system vulnerabilities (percentage of vulnerable systems)

System-Wide Security with MaxPatrol™

To defend yourself against cybercriminals that target every part of your infrastructure, you need security solutions that let you see into all your systems. MaxPatrol provides automated audit and vulnerability and compliance management across your entire network and system infrastructure including your core banking systems (CBS), internet banking portals and ATMs.

Positive Technologies works closely with vendors such as Diasoft and SAP to develop technical benchmarks and checks for their solutions, letting you use MaxPatrol to protect even highly-customized core banking systems and custom-built applications.



“For us, it is important to provide continuous monitoring of how our workstations comply with the bank’s information security technical standards. The problem is that levels of safety in workplaces differ, and we need to bring them all up to the same level of protection. The introduction of MaxPatrol has allowed us to solve this problem”

Ivan Marshev
Head of Information Security
IT Services
 UniCredit Bank



“By automating the security assessments of our network equipment, servers, workstations, databases, applications and telephony systems, MaxPatrol performs tasks that would otherwise require many hours of work by highly trained security engineers”

Souhail Jribi
CISO
 Banque Zitouna



التجاري بنك
Attijari bank

“MaxPatrol has brought us all the benefits we required from an automated vulnerability and compliance management solution. It has allowed us to take control of security across all of our IT systems”

Amlouk MohamedHédi
IT Security Manager
 Attijari Bank



Take Control of Your Compliance

Since the Global Financial Crisis of 2008, the financial sector has seen a dramatic increase in the number and scope of regulations they must comply with. MaxPatrol translates these high-level guidelines into operational security controls that can be automated to make compliance part of your everyday security process. Its built-in technical checks rapidly establish your level of compliance with standards including PCI DSS, ISO (27001:2005, 27002, 27011:2008) and SOX. MaxPatrol can also be easily customized to check compliance with your own corporate standards or those required in the countries where you do business.

Moreover, MaxPatrol gives you ownership of your PCI DSS compliance, empowering you to carry out quarterly assessments of all perimeter systems and applications involved in payment card transactions, so you can fix vulnerabilities and generate Approved Scanning Vendor (ASV) compliant reports for auditors, before they set foot on your site.

Application Security: Banking’s New Frontline

Most banks have woken up to the fact that they need better application security. Underscoring this need, Verizon’s 2014 Data Breach Investigations Report identified web application attacks as the number one threat to the financial sector. However, with rapid development cycles and on average dozens of applications in use – ranging from online banking apps to essential elements of your core banking system – security concerns often get pushed to the side. This reality is compounded by the fact that most developers lack the expertise required to adequately defend your applications from vulnerabilities and exploits.

With features not found in other solutions, Positive Technologies PT Application Firewall™ and PT Application Inspector™ can plug this gap, providing a comprehensive and modern solution to application security. Together they allow financial institutions to protect both their internal and external-facing applications from attack, stop fraud and sensitive data leakage and prevent the collapse of networks and services.

Security Services Tailored to Your Needs

In addition to its products, Positive Technologies has a strong track record of delivering a wide-range of security services to the financial industry including:

- + Penetration testing
- + Online and Mobile Banking application security assessments
- + Compliance-related security evaluations – PCI DSS, ISO, SOX, etc.
- + Secure Software Development Lifecycle (SSDL) consulting
- + ATM and POS terminal security analysis and zero-day research
- + Core Banking System security assessments
- + Development and enforcement of security guides for Core Banking Systems

With Positive Technologies, you can find all vulnerabilities across all applications and systems. Stop zero-day attacks before they strike. Quickly patch existing security holes. See precisely how vulnerabilities can be used to attack your business and significantly accelerate your incident response and remediation times – all while drastically reducing your costs associated with compliance.

Now that’s a smarter approach to information security.

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit www.ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of \$20M+.

© 2014 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.