POSITIVE TECHNOLOGIES

## HIGHLIGHTS

- Take Control of Compliance with easy-to-deploy automated checks for PCI DSS, ISO and SOX guidelines; your own corporate IS standards and national/ international regulations
- Prevent Fraud and data breach with solutions and services customized to protect core banking systems, internet banking portals, ATMs and POS
- Focus On Application Security with AppSec solutions to stop zero-day attacks, quickly patch existing security holes and support your SSDL
- Secure Your Future by leveraging our expert knowledge in your security planning and for rapid-response to unfolding incidents

**€132m**

**The total value of reported ATM Fraud in Western Europe in the first half of 2014***

*Source: The European ATM Security Team (EAST)'s European ATM Crime Report H1 2014

# PUTTING YOU IN CONTROL OF BANKING SECURITY AND COMPLIANCE

The financial sector has long been a pioneer of new technology, embracing everything from ATMs to Internet banking in its drive to improve customer service and increase efficiency. But as banking technology becomes more complex and integrated, it is increasingly difficult to maintain information security, prevent fraud and in particular to ensure compliance with the growing list of standards mandated by the industry, governments and your own IT policies.

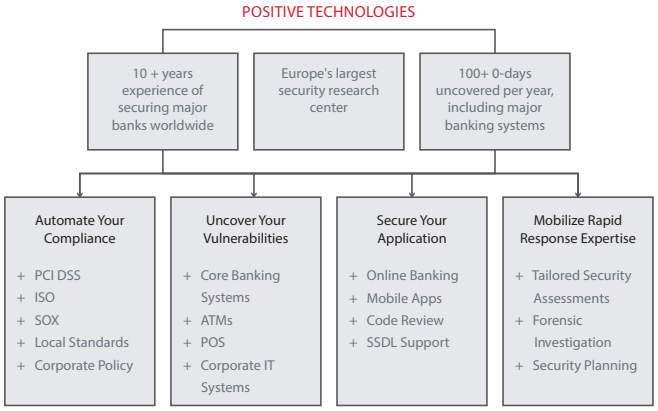
The level of threat is high: Verizon's 2014 Data Breach Investigations Report revealed the biggest issues for the financial industry from 2001 to 2013 were attacks on web applications, distributed denial-of-service attacks and payment card skimming. Together these accounted for 75% of reported industry-related data breach incidents.

And all aspects of the banking ecosystem are at risk, from Core Banking Systems (CBS) and Point of Sale (POS) terminals to ATMs, with the European ATM Security Team (EAST) reporting the first instances of ATM malware in Western Europe in 2014* following a series of so-called "jackpotting" attacks.

It is time for many financial institutions to take a fresh look at their security and compliance strategy.

### A Trusted Partner in Financial Security

Positive Technologies has more than a decade of practical experience securing information systems for many large banks around the world. Using this unique knowledge, we have created a range of solutions and services that solve real-life banking security challenges.




### Take Control of Your Compliance

Financial service providers have more security standards to consider than almost any other sector; from industry regulations like PCI DSS to local regulatory standards and individual corporate guidelines. Implementing regular, automated checks for compliance within this complex framework of banking information systems, appliances, software and business applications can seem like an impossible task. But it is achievable with the right expertise.

The MaxPatrol™ Compliance and Vulnerability Management solution from Positive Technologies comes pre-loaded with hundreds of checks already used and tested by other banks to determine compliance with standards including PCI DSS, ISO and SOX. It can be rapidly configured to check for your own custom standards, allowing your organization to implement an efficient, long-term compliance management process in a matter of days.

A single MaxPatrol scan can determine your level of compliance with many different standards. It works across a wide range of systems: from network equipment and core banking systems to DBMS, ERP and telephony solutions. And because we are actively engaged with the security community, helping to develop international industry standards, MaxPatrol is always up-to-date with the latest guidelines.

### All in One Defense against Fraud and Data Breach

Cyber fraudsters target all aspects of your banking infrastructure; searching for weak spots they can exploit to steal funds or sensitive data. Positive Technologies offers tried-and-tested solutions and services to analyze and protect your CBS, internet banking portals and other Remote Banking Systems (RBS), POS and ATMs as well as the usual range of IT systems used by any major corporation. We work closely with leading developers and vendors of banking software to detect critical vulnerabilities which could allow attackers to bypass One Time Password (OTP) mechanisms and SMS notifications or access users' personal data.

At the same time as it simplifies your compliance procedures, MaxPatrol can automatically find and prioritize vulnerabilities, including zero-day threats, in a wide range of IT systems including network devices, ERP systems and business applications based on SAP™.

### Rapid Response Expertise

To successfully counter cybercriminals, you must think like one. Our specialist banking services team provides swift, tailored solutions for your unique security challenges:

- Reveal weaknesses in your corporate networks, ATMs and e-banking systems with tailored security assessments including penetration testing of network infrastructure, information traffic analysis and zero-day vulnerability detection in ATM hardware.
- Get independent forensic analysis of security incidents. When your existing security mechanisms fail, our specialists will detect and trace attacks that might have been overlooked or misinterpreted by your systems and make recommendations to prevent similar incidents in the future.

Hanwha

***Before MaxPatrol, we conducted vulnerability diagnosis only once a year because it took so much time. But with MaxPatrol, we can work much faster. We can also detect and analyze vulnerabilities throughout a wider range of our systems than before and we have reduced costs."***

**Yoon Yong-gu,**
Head of Security Control,
Hanwha Group (Korea)

التجاري وفا بنك
Attijariwafa 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."***

**Mehdi Hamza,**
IT Security Officer,
Attijari Bank (Morocco)

Financial Technologies

***"MaxPatrol gave us a completely new insight on the network, from an angle that we were not looking at, in real time. This single product that does everything for us has saved us a lot of time."***

**Neehar Pathare,**
SVP Corporate IT,
Financial Technologies (India)

HOME CREDIT BANK

***"Remote banking is one of our development priorities. It is especially important to ensure a high level of security. As part of a system upgrade project, we invited the experts from Positive Technologies to test our level of security. With their help we were able to improve our system security. We plan to bring in Positive Technologies to help us on other projects."***

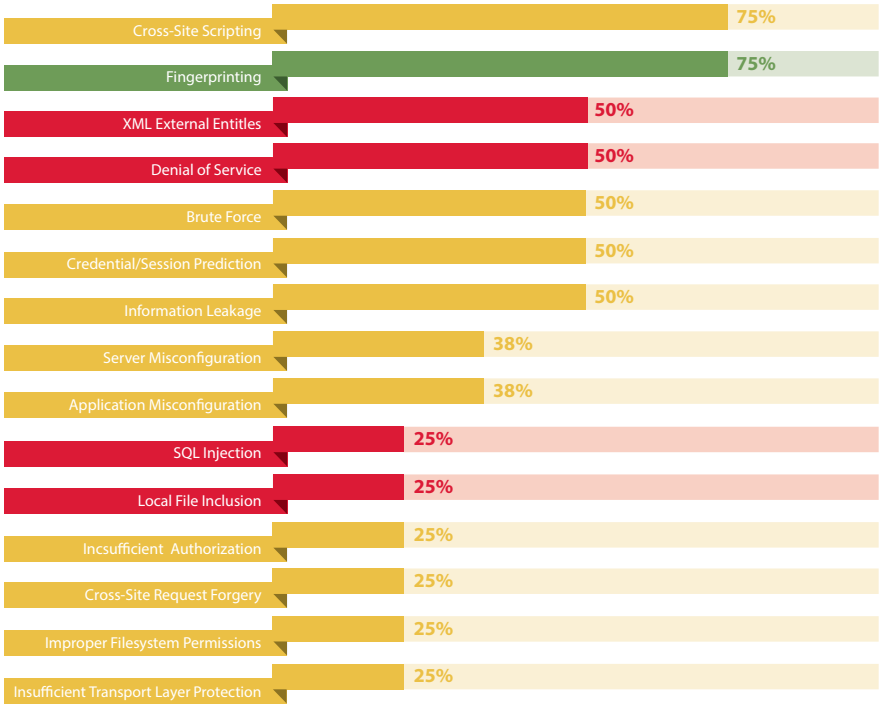
**Yuri Lysenko,**
Head of IS administration,
Home Credit Bank (Russia)

POSITIVE TECHNOLOGIES

**Application Security: Banking's New Frontline**

Most financial organizations know they need to improve application security as the number of apps they use dramatically increases to encompass online and mobile banking apps as well as essential elements of their CBS. But rapid development cycles encourage a focus on functionality over security and most development teams lack security expertise. Information security specialists are often called-in to defend "turnkey" applications once they are ready to deploy, significantly increasing the cost and time involved in eliminating vulnerabilities that could threaten the organization's entire infrastructure.

It's little wonder that Verizon identified web application attacks as the number one security threat for the financial sector. Indeed, in a recent study of e-banking applications, Positive Technologies found high-risk vulnerabilities in half of the systems we tested. In most cases, the flaws were in the source code or in the application's security mechanisms:




Positive Technologies' specialist AppSec products and services help banks to secure all kinds of client-facing and internal applications. Protect your banking and business applications from fraud and data leakage right from the earliest stage of development and throughout their working life:

- Automate source code analysis and QC with PT Application Inspector™ (PT AI), an innovative solution that combines static, dynamic and interactive analysis mechanisms (SAST, DAST, IAST) to find vulnerabilities in web, mobile, ERP and client-server applications
- Prevent 0-day attacks and online fraud with PT Application Firewall™, a self-learning secure gateway for Web 2.0, XML, mobile applications and ERP applications that can rapidly patch security holes, buying you time to fix vulnerable code
- Implement a Secure Software Development Lifecycle (SSDL) based on leading methodologies (SAMM, BSIMM, Microsoft SDL) with PT AI or the services of our specialists
- Benefit from our practical experience of analyzing over 500 enterprise applications per year, with our selection of AppSec services ranging from configuration management to incident investigation

**Prepare For a More Secure Future**

If the scale of your information security challenge seems too great, the experts at Positive Technologies can help you to assess your current security levels and formulate a Security Enhancement Plan to transition from a reactive "hole-fixing" approach to systematic control of security across all of your bank's critical systems.

## 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+.