



MAXPATROL SOLVES COMPLIANCE CHALLENGES FOR EUROPEAN BANKING FIRM INTESA SANPAOLO

COMPANY PROFILE

- + Industry: Banking – one of the largest banking groups in the Eurozone
- + Locations: 6,000 branch offices in 40 countries
- + Customers: 11.1 million retail and B2B banking customers
- + Assets: €36.8 billion (2014)

INTESA  SANPAOLO

THE CHALLENGE

Automating compliance with both external and internal data security mandates while protecting the privacy of over 11.1 million customers

As a leading bank in Europe, Intesa Sanpaolo manages the personal data of over 11.1 million customers – from private individuals to large corporations. As a prime target for hackers and fraudsters, Intesa Sanpaolo must ensure the security and integrity of sensitive customer data in order to prevent fraud and irreparable damage to its reputation.

European banking rules require Intesa Sanpaolo to comply with data privacy regulations such as PCI DSS, SOX and ISO 27001. In addition, the bank must also satisfy their own strict internal information security policies. Initially, they used a manual process to manage compliance auditing and reporting for the various rules and regulations it had to adhere to. However, after a series of acquisitions led to rapid growth, their IT Security team realized that it was no longer feasible to manage compliance without automation.

Intesa Sanpaolo's team began looking for a solution that could provide continuous, automated monitoring of all their networked information systems, their associated configuration settings and vulnerabilities and could also report on the performance of their IS processes. Anticipating further growth, Intesa Sanpaolo also sought a solution that would be scalable to support expansion into new territories and the burden of additional systems.

HIGHLIGHTS

- + Transformed security compliance from a manual cumbersome process into a convenient set of practices
- + Increased the accuracy and frequency of its security assessments
- + Eliminated the costs associated with a large team of highly-skilled security engineers

THE SOLUTION

MaxPatrol Vulnerability and Compliance Management

MaxPatrol was initially used in Intesa Sanpaolo's Moscow branch offices, to identify and prioritize potential systems' vulnerabilities. In addition, automated monitoring of their hardware and software systems and related configuration settings gave Intesa Sanpaolo a full inventory of their IT assets and provided them a real-time assessment of how each system measured up to regional data security and privacy laws as well as Intesa Sanpaolo's internal corporate security policies.

Since then, and based on the success of the initial rollout, Intesa Sanpaolo has expanded its use of MaxPatrol to over 75 branch offices spanning across more than 25 regions in Russia. In addition to collecting and assessing vulnerability and compliance data, MaxPatrol is also used by IT and IS managers to measure the performance of their teams against security related key performance indicators (KPIs) such as patch management and auditing.

MaxPatrol was implemented at Intesa Sanpaolo by LETA IT, a regional IT security integrator and partner of Positive Technologies.

“Using MaxPatrol ensures our information systems comply with both regulatory requirements and our own internal information security standards...”

IT Security Department
Spokesperson
Intesa SanPaolo

THE BENEFITS

Improved Efficiency, Simplified Compliance and Greater Performance Visibility

MaxPatrol has transformed Intesa Sanpaolo’s security compliance process from a complicated, manual one into an efficiently smooth and predictable set of practices.

“Using MaxPatrol ensures our information systems comply with both regulatory requirements and our own internal information security standards,” explained a spokesman from Intesa Sanpaolo’s IT Security department.

More regularity in assessing compliance also ensures a higher level of security for customers’ personal data. MaxPatrol provides early-warning of any vulnerabilities, prioritizes them according to the level of risk they pose to the bank’s operations and provides clear recommendations for eliminating the associated threats.

But for Intesa Sanpaolo, simply achieving compliance is not enough: it must also be able to show proof of compliance to its own internal standards. MaxPatrol’s flexible reporting capabilities allow its IT Security department to generate KPI-based reports tailored to the different needs of their regional, national and group-level managers – including reporting on the performance of the IT Security department itself. “The English language interface simplifies the process of reporting,” added the company spokesman.

Consolidating the compliance testing for all the bank’s networked systems under a single, all-in-one-solution has translated into significant cost savings at the same time as increasing the accuracy and frequency of security assessments.

MaxPatrol’s automation allows Intesa Sanpaolo to maintain near-continuous monitoring of its IT-infrastructure without the need to employ a large team of highly-skilled security engineers.

MaxPatrol’s modular architecture and support for a wide-range of different IT systems has allowed Intesa Sanpaolo to plan its security to suit its current operational and business needs, while allowing for future expansion to meet the needs of their changing business.



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+.



© 2015 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.