Retail bank improves IT security and compliance

Platinum Bank enhances security, ensures regulatory compliance and minimizes downtime with AD and Exchange auditing from Quest®

Platinum Bank is a leading and fast-growing retail bank in Ukraine with 1.5 million clients. The bank turned to Quest when it needed help to implement Windows auditing and event log management for security and compliance.

One of the primary responsibilities of Platinum Bank’s security department is to track potentially malicious users, not only to prevent security breaches, but also to protect the bank’s reputation. With this goal in mind, the bank decided to implement a security information and event management (SIEM) system. This was partly driven by the need to comply with the global Payment Card Industry Data Security Standard (PCI DSS) and the ISO 27001 standard.

**AD AUDITING AND EVENT LOG MANAGEMENT**

To protect its Windows environment and to audit its critical systems, the bank needed to understand what was happening in its Active Directory-based infrastructure better than native tools permitted. It needed detailed visibility to Active Directory (AD) changes such as which users had made the changes, and the impact of the changes on the environment. In addition, the bank needed to audit the log files from its critical systems — including Microsoft Exchange, AD and file servers — to be directed to one central access point, and for the information to be organized and stored logically.

**SOLUTIONS THAT DELIVER THE GREATEST FUNCTIONALITY**

Platinum Bank’s IT security team attended an event organized by its trusted IT supplier, Bakotech, a local Quest partner. The team saw demonstrations of AD auditing and heterogeneous security auditing tools from Quest. These solutions, along with products from Symantec and ArcSight, were also considered by the bank. Platinum Bank ran pilot projects and considered Gartner’s views, and ultimately selected three solutions from Quest — Change Auditor for Active Directory, Change Auditor for Exchange and InTrust — because they offered the greatest levels of functionality while also being the most cost-effective.

**BUSINESS NEED**

Driven partly by the need for compliance with global and industry regulations and standards, Platinum Bank needed to improve security by implementing Windows (AD and Exchange) auditing and event log management.

**SOLUTION**

With Change Auditor for Active Directory, Change Auditor for Exchange and InTrust, Platinum Bank can now keep abreast of changes to Active Directory and Exchange in real time, so issues can be quickly identified and resolved.

**BENEFITS**

- Enhanced security, protecting the bank’s reputation
- Dramatically reduced time to resolve Exchange and AD change-related issues — from multiple days to a few hours
- Minimized system downtime, maintaining employee productivity
- Ensured compliance with industry standards and government regulations

**SOLUTIONS AT A GLANCE**

- Microsoft platform management
- Security and compliance

“Together, Change Auditor and InTrust satisfy the needs of our auditors and management in full.”

Sergey Popov
CIO and board member, Platinum Bank
Change Auditor for Active Directory is a powerful AD auditing tool that proactively tracks, reports on and alerts on vital configuration changes — in real time and without the overhead of native auditing. It enhances security by telling you instantly who made each change, when, where and from which workstation, eliminating the risks associated with daily modifications. Moreover, it compares original and current values for fast troubleshooting and remediation.

InTrust provides event log management for security and compliance; it securely collects, stores, reports and alerts on event log data from Windows, UNIX and Linux systems, helping organizations comply with external regulations, internal policies and security best practices. InTrust audits user access to critical systems from the time they log on until the time they log off, detecting inappropriate or suspicious access-related events and sending alerts in seconds. With this tool, you can easily collect, analyze and report on all relevant access-related events across heterogeneous networks.

Extensive logging facilities delivered by Change Auditor and InTrust provide a valuable view of Platinum Bank’s business-critical AD infrastructure and core systems, which has dramatically improved system security. “Our solutions from Quest ensure that IT security threats do not impact our 4,528 users and the bank’s productivity,” says Sergey Popov, CIO and board member at Platinum Bank. “For instance, we use Change Auditor for Exchange to audit mailbox access rights and to protect and restrict access to critical objects, to comply with our corporate policy.”

Platinum Bank was impressed by Change Auditor’s wide selection of pre-built templates, especially for PCI DSS compliance, and its web-based interface.

The bank’s security department now uses the solutions from Quest in an integrated way on a daily basis. In addition, the system administrators have access to security logs in order to track changes to the AD environment.

The extended logging facilities delivered by Change Auditor and InTrust provide a valuable view of Platinum Bank’s business-critical AD infrastructure and core systems, which has dramatically improved system security. “Our solutions from Quest ensure that IT security threats do not impact our 4,528 users and the bank’s productivity,” says Sergey Popov, CIO and board member at Platinum Bank. “For instance, we use Change Auditor for Exchange to audit mailbox access rights and to protect and restrict access to critical objects, to comply with our corporate policy.”