Challenges

Increasing Risk of Cyber-attacks

“JPMorgan was hacked in June but didn’t detect the attack until August, resulting in the exposure of the personal information of 76 million households...” - Wall Street & Technology, 2015.

Banks manage massive amounts of sensitive data, such as payment transactions, PANs and other personal information. Consequently, the finance industry is the primary target for cyber-criminals, who use sophisticated methods to steal client’s identity or hijack privileged employee accounts. The hackers are well organized, well-funded, and highly motivated by the financial gains. According to the Ponemon Institute, the cost of successful cyber-attacks increased to $20.8 million per financial services company in 2014.

Internal Fraud

Nevertheless, the threats are not all external. Fraud caused by internal staff ranges from insider trading to stealing clients’ identities and selling them to outsiders. Research carried out by NICE Actimize showed that full-time IT staff members pose the biggest risk because they have privileged access to more valuable information and are monitored less closely.

Intensifying Regulatory Pressure

“By 2017, more stringent regulations around control of privileged access will lead to a rise of 40% in fines and penalties imposed by regulatory bodies on organizations ...” – Gartner, Market Guide for Privileged Access Management, Felix Gaehrgens, Anmol Singh, 27 May 2015.

Financial institutions need to meet Basel III, MAS, SOX, PCI DSS and local regulations forcing the adoption of IT controls such as ITIL, COBIT or ISO 2700x. Laws and standards require the deployment of IT systems that record all access to sensitive financial information, thus protecting the interests of investors, creditors, and clients. Regulations and failed audits are becoming serious concerns for financial CIOs/CISOs, as auditors are paying closer attention to privileged accounts. They specifically mandate the strict control of privileged users and the creation of tamper-proof evidence of their accesses. FIs must pass these audits as the direct and indirect costs of non-compliance is much higher than the investment in supportive processes and technologies.

Increasing Adoption of IT Outsourcing

“Bank of New York reported that a subcontractor computer technician has stolen over $1 million by using identity theft of employee data...” - New York Times.

In a global financial environment, responsibilities are increasingly outsourced or sub-contracted to third parties. Giving responsibility to an IT provider is always a security risk, especially in a banking environment. You may control the partnership with a contract, but monitoring contracted employees is hardly manageable with a Service Level Agreement (SLA). Usually, financial institutions do not have a reliable and easy-to-use solution for validating SLAs and verifying billable activities. Financial institutions often use custom-developed applications, which are typically supported by external developers. In these cases, third-party developers and administrators might have direct access to sensitive financial databases...
To meet the above security and compliance challenges, it is reassuring for financial institutions to have a comprehensive IT security strategy with privileged access management in focus. **Balabit's Shell Control Box (SCB)** solves exactly these problems by introducing an independent access management layer to supervise the working sessions of privileged users. SCB is a user monitoring appliance that controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions. SCB is a quickly deployable enterprise solution which is completely independent from clients and servers - integrating seamlessly into existing infrastructures.

---

**SCB helps financial institutions to:**

- Protect clients’ data by enforcing granular access control policies (e.g. strong authentication, time & group policies)
- Reduce the risk of fraud by monitoring (and even terminating) privileged sessions in real-time
- Meet compliance requirements by controlling and tamper-proof recording of administrative access
- Support audits by generating compliance reports (e.g. “one-click” PCI DSS and ISO 27001 reports)
- Prevent data leakage by managing sensitive file transfers
- Justify services fulfillments described in the SLA

"If an effective and skilled solution is required for privileged session management, SCB should be chosen." - Mr. Yılmaz Ak, Information Security Manager, Albaraka Turk Bank.

---

**ABOUT BALABIT**

**Balabit** – headquartered in Luxembourg – is a leading provider of contextual security technologies with the mission of preventing data breaches without constraining business. Balabit operates globally through a network of local offices across the United States and Europe together with partners.

Balabit’s Contextual Security Intelligence™ strategy protects organizations in real-time from threats posed by the misuse of high risk and privileged accounts. Solutions include reliable system and application Log Management, Privileged User Monitoring and User Behavior Analytics. Together they can identify unusual user activities and provide deep visibility into potential threats. Working in conjunction with existing control-based strategies Balabit enables a flexible and people-centric approach to improve security without adding additional barriers to business practices.

For more information, visit [www.balabit.com](http://www.balabit.com).

---

FINANCIAL CUSTOMERS USING SCB WORLDWIDE:

[Logos of financial institutions using Balabit's solutions]