Citadele Bank insures data security by using DeviceLock

About the bank

Citadele Bank is a part of a full-service financial group for both private individuals and companies that offers a complete portfolio of banking, financial and private capital management services in Lithuania. Branch network of Citadele Bank in Lithuania consists of 8 client service units in the country's largest cities and a private banking division.
To maintain its reputation for financial reliability, Citadele Bank is constantly strengthening the IT security infrastructure that protects its information assets. It strives to combat not only external threats to its network and data, but also the threat of data loss or theft due to negligence or malfeasance on the part of corporate insiders.

Data security is an essential success factor in the financial market

The major tasks for Citadele's IT-department was to allocate, identify, and classify sensitive data to reduce data privacy risks, reduce potential data sharing exposure, and improve compliance. To successfully perform these tasks, Citadele's IT-specialists needed a flexible tool to control the network and personal devices across the infrastructure of the Bank: «*Banking organizations have a lot more critical data than others companies, that's why guaranteed security of confidential information is an important competitive advantage in the financial market*», —says Jurij Sirenko, CIO at Citadele Bank.

The integration of the DeviceLock has become one of the stages of bank's infrastructure modernization. This solution gave to IT-department tool for centralized control of user's access to any external devices and allowed to monitor more carefully their actions within the network.

Customer: Citadele Bank

Citadele

Vendor: DeviceLock Inc.

DeviceLock
Proactive Endpoint Security

IT-security provider:
Data Security Solutions (DSS)

Data Security Solutions
Riga, Latvia

«One of the main problems in data protection, for banking organizations,is a content and contextual information protection in various places like network, endpoint and removable devices and in various banking systems. In Citadele Bank project our goal was to cover all main points, from where data can leak out, with a single solution. DeviceLock fitted all client's demands in functionality and price. In addition, it has the best price performance indicators at the DLP market»

Arturs Filatovs, Business Development Executive Baltics

«We have a long partner's relationships with DSS, and they have introduced us the DeviceLock solution»

Jurij Sirenko,
CIO at Citadele Bank.

This project includes implementation of complementary DeviceLock'smodules in order to fully provide effective information security management in the dynamic bank's environment.

The main benefit of using DeviceLock is its ability to cover DLP functionality with minimal IT effort and to achievethe **PCI DSS** and **ISO 2700X** compliance.

Devices Access Control

which users or groups can access USB, FireWire, COM and LPT ports; WiFi and Bluetooth adapters; any type of printer, including local, network and virtual printers; BlackBerry, MTP-enabled devices (such as Android, Windows Phone, etc.), Apple iOS-based PDAs and smartphones; Terminal Services devices; as well as DVD/BD/CD-ROMs, floppy drives, and other removable and Plug-and-Play devices.

Network Communications Control

comprehensive contextual control over endpoint network communications including network protocols, web applications and listed Instant Messenger applications like Skype. Regular and SSL-tunneled email communications (SMTP, Exchange-MAPI and listed webmail services) are controlled with messages and file attachments handled and filtered separately.

Content Filtering

analyze and filter the textual content of data copied to removable media drives, to other Plug-n-Play storage devices, to the clipboard, data sent for printing and even data that might otherwise be hidden in screen prints, graphical files or pictures embedded in documents. DeviceLock also filters data objects and sessions from within network communications.

«Every new security solution implementation in your internal environment requests preparation and planning efforts. Together with technical experts from Data Security Solutions we were able to swiftly create an implementation plan. By following the proposed steps, we have finalized the implementation without any issues. The system is stable and works correctly after fine-tuning and configuration».

Jurij Sirenko, CIO at Citadele Bank

Cover with DLP-solution all users is the next step in the development of information security systems Citadele Bank

In today's business, information is the most valuable and most vulnerable asset. Corporate data leaking is possible not only in case of hackers attacks, but also through deliberate and intentional actions of internal staff. A growing number of devices and channels for transmission of the sensitive data, also complicates the task of providing data security: «*Currently DLP-solution covering most of employer's computers. The next step of development information security of our bank, will be a covering of all users with DeviceLock DLP, to prevent data leaks by enforcing corporate policies with regard to the use of peripheral devices*», says Jurij Sirenko, CIO at Citadele Bank.

BAKOTECH Group is an official distributor of DeviceLock in Baltic countries.