BS2
Penki kontinentai group

Diebold Nixdorf

All-in-one solution for self-service devices security

Vynamic™ Security

25+
years on the market

7
affiliated companies in Azerbaijan, Estonia, Georgia, Kazakhstan, Kyrgyzstan, Latvia and Uzbekistan

80
countries where activities are carried out

1500+
international customers

90+
partners worldwide

25+
years of partnership with Diebold Nixdorf

400+
talented professionals

Competence at the core

The company Penkių Kontinentų Bankinės Technologijos (BS/2) is the part of Penki Kontinentai group of companies, provides services in 80 countries, creating soft ware solutions which help automate and optimize your business.

For more than 25 years, we are developing specialized innovative soft ware and technological solutions for banks, financial institutions and retail companies. We are off ering high-quality IT products that meet your customers' needs.

Our Services

- Soft ware development, sales, installation, support and systems integration services
- IT service outsourcing
- Maintenance and repair of banking, telecommunication, acquiring and retail equipment
- Monitoring of IT infrastructure
- Staff training and consulting
- Spare parts supply
- Sales of specialized equipment for banking and retail companies

Certificates

ISO 27001, ISO 20000, ITIL V3, PCI PA- DSS.

Our Clients

- Banks and fi nancial institutions
- Retail companies
- Gas stations
- Postal services
- Other companies (casinos, hippodromes and others)

International Recognition and Awards

Diebold Nixdorf / Wincor Nixdorf

- Special Achievement Banking 2019.
- Special Achievement Banking 2007, 2013, 2014, 2017.
- Best Banking Solution 2012, 2013, 2016.
- Best Banking Service 2002, 2003, 2012, 2013, 2014.
- Most Innovative Software Solution 2004, 2005.
- Most Innovative Concept 2002, 2003, 2004, 2005.

ATM Industry Association

- Best ATM Security Technology 2002.

Lithuanian Confederation of Industrialists

- Innovation Prize 2016.
- Lithuanian Product of the Year 2001, 2005, 2006, 2007, 2008, 2012, 2017.

Comprehensive security for self-service devices

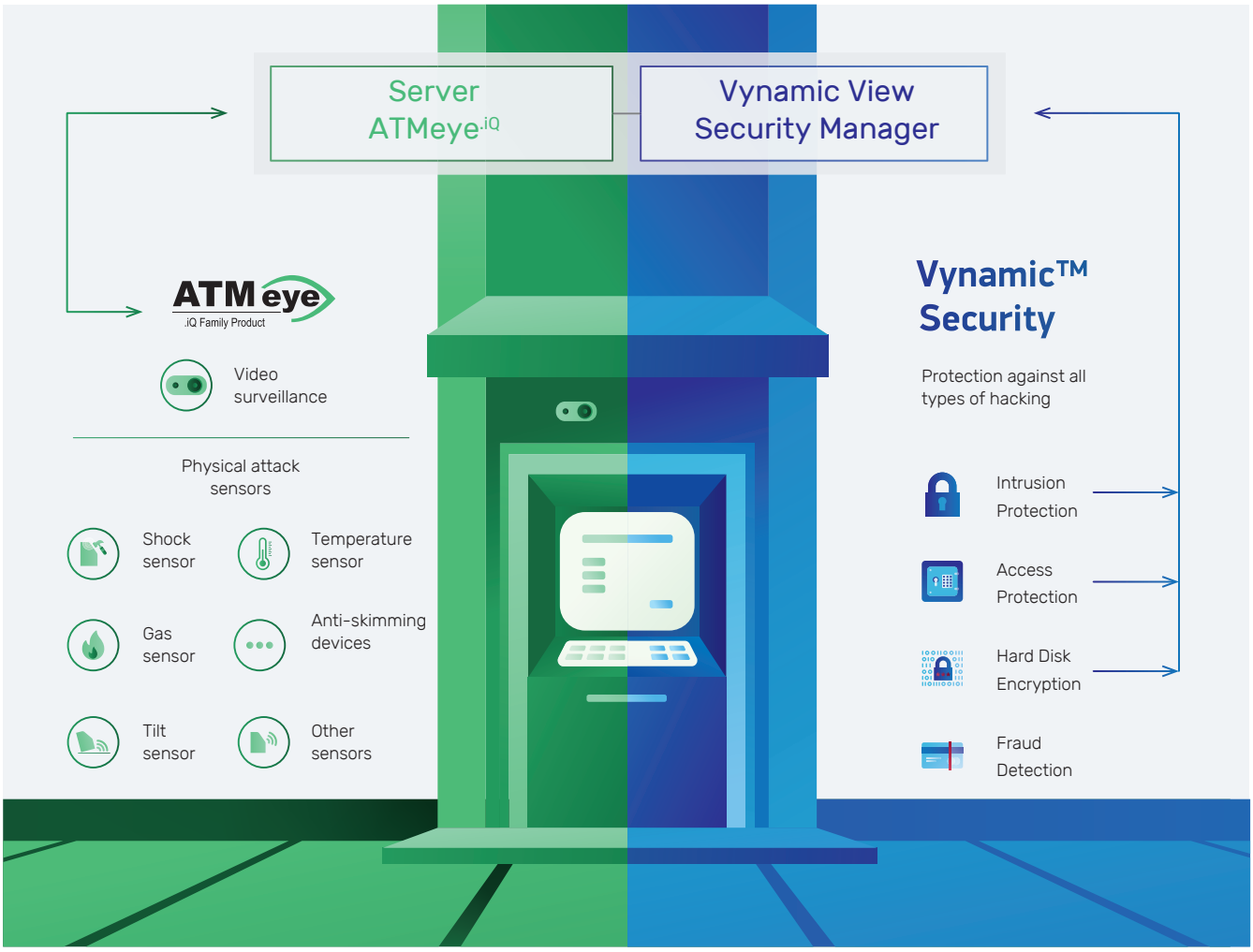
In recent years, the number of attacks on ATMs increases. Criminals come up with new fraud methods and improve the old ones. They create new malware, so logical attacks become more sophisticated. They invent new tools to read data from bank cards. It is worth mentioning that the number of physical attacks on ATMs (explosions, hacking safe, ATMs stealing) also increases from year to year.

It's important to protect customers personal data, when facing with logical attacks. Sensitive data theft could lead to financial and reputational losses for banks.

Low level of basic terminal protection is the main reason why logical attacks could happen. Operating systems installed on ATMs have many vulnerabilities and require updates.

Internal banking networks can have their own vulnerabilities, through which attackers can get access to terminal networks. Usually, they are associated with configuration or operational errors. So, banks get a challenge to provide complex and comprehensive protection of their terminals.

To protect your self-service devices fleet, BS/2 offers a complete solution, combining modern software products of BS/2 and Diebold Nixdorf.



Implementing this solution helps:

• to reduce the self-service infrastructure potential attack surface by simultaneous operation of several security modules;

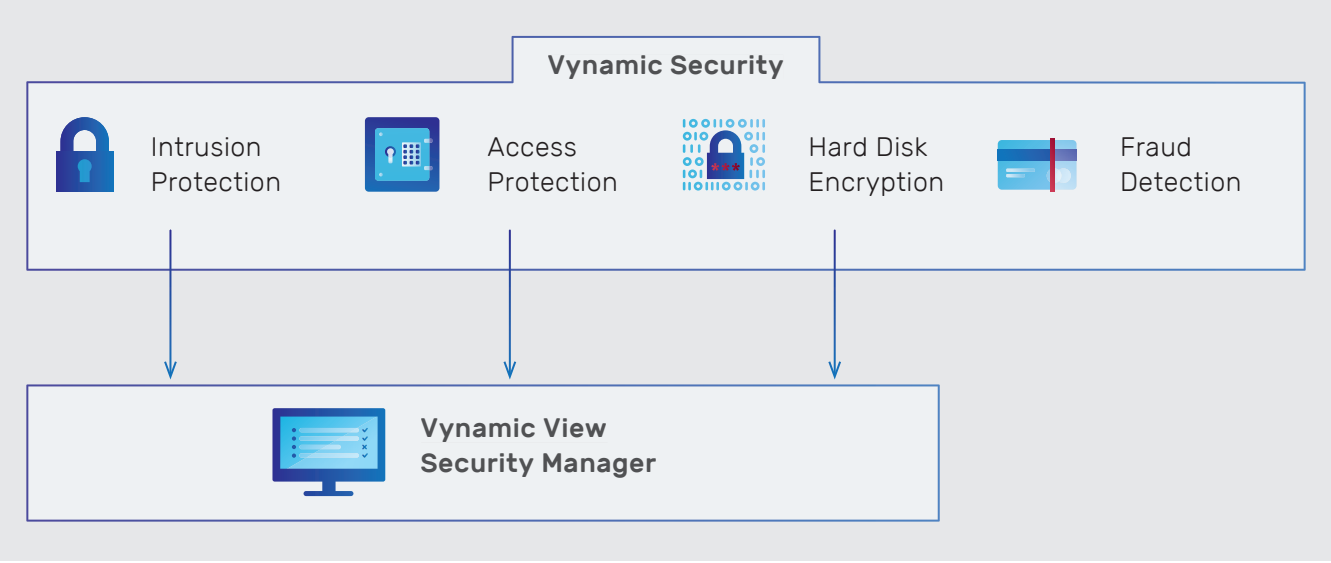
• to reduce the total cost of ATMs ownership by optimizing security related workflows.

** Read more about the ATMeye.iQ solution in BS / 2 material "Video Surveillance and Fraud Prevention".*

Vynamic Security Suit

To protect the terminal network from logical attacks, Diebold Nixdorf offers complex solution Vynamic Security. This solution provides an integrated approach to self-service device protection from any type of hacking and other threats.

Vynamic Security solution consists of four independent modules.



This multi-level protection of self-service device helps to reduce all fraud related risks. If one of the levels dropped, the remaining modules continue to provide all the necessary terminal protection.

Intrusion protection module

Criminals install malicious software on the ATM through the OS vulnerabilities. They connect external drive directly to the terminal via USB ports. It's difficult to track down and prevent such connection, but its consequences bring huge damage to the finances and reputation of the credit organization.

Intrusion Protection module is responsible for protecting the terminal network from the intrusion of all types of malware in the ATM computer.

Intrusion Protection module functions

Malware Protection

Provides effective, state-of-the-art protection against known and unknown threats, including zero-day attacks.

Whitelisting

Terminal launches only approved and validated processes corresponding to the rules set (creating a "sandbox"). The module tracks all unauthorized changes in the ATM equipment and software.

USB ports control

The system locks the ATM computer USB ports to protect the computer from unauthorized access when somebody tries to connect any USB drive.

System integrity monitoring

The module tracks any attempts to replace files or make unauthorized changes in system settings (including BIOS) and neutralizes all potentially dangerous acts of suspicious applications.

Network and data protection

Control of new incoming and outgoing connections based on a list of approved IP-addresses and established rules.

Proactive monitoring

Operators recieve notifications in the case of a potential threat or intrusion, attaching an incident log.

Access Protection module

To protect the ATM computer from the malware, banks focus on external threats, but this is not enough. Financial institutions must also protect their systems from unauthorized access to prevent confidential data leaks.

Access Protection module protects the ATM computer in case of irregular access and controls the user actions in the system. The solution complies with international standards, rules and policies, which reduces the risk of criminal intrusion into the system and misuse of access rights.

Access Protection module functions

Access management

Effective access control through management of rights and roles of various user profiles and user groups, as well as the ability to log all actions.

Operating system hardening

The module disables and removes the optional components of the terminal computer operating system, which can be used as attack vectors.

Authorization procedures optimization

The standard authorization procedure for the terminal network administrator is extended by a special procedure for encrypting the login and password.

Firewall management

Firewall settings management to control incoming and outgoing data, based on established rules.

Hard Disk Encryption module

Many financial institutions encrypt transferring data, but do not pay enough attention to encrypting the information stored on the hard disk of the terminal computer. Stealing an unencrypted hard drive allows criminals to access its data, infect it with malware and install it on another ATM.

The Hard Disk Encryption module prevents unauthorized access to sensitive data stored on your hard disk, even when the ATM is out of operation. Data is stored in an encrypted form and can not be read or copied without unique keys. The module uses supplied parameters of the ATM hardware and software environment, it means that the decryption procedure is possible only on the device using this specified hard disk.

Hard Disk Encryption module functions

Data protection

Encrypting data on the hard disk ensures its security even when the ATM is out of operation (transported or under repair).

Strong encryption

According to PCI requirements, the module encrypts data at rest, data in transit and data in use. The real-time encryption is based on AES (256-bit).

Access Protection

The module blocks access to the hard disk data, when the decryption does not match the specified parameters, or any attempts to make external modification of the operating system detected.

System integrity monitoring

The hard disk runs exclusively within the predetermined hardware and software environment of the self-service device to ensure the integrity of the system.

Fraud Detection Module

Criminals constantly improve their methods, coming up with new types of attacks. It requires more sophisticated security solutions every day. Standard measures based on specified rules and specified models of behavior cannot protect against new threats.

Self-contained Fraud Detection module allows you to use machine learning and big data analytics to detect suspicious operations on self-service devices, and also provides proactive protection for the technical infrastructure of a credit institution or other organization.

Fraud Detection module functions

Proactive fraud detection

The module finds potential vulnerabilities in the self-service infrastructure and terminal fleet management system and makes a list of preventive actions.

ATM Security

The system recognizes ATM and account behavioral changes and targets ATM threats, providing the ability to take actions to prevent jackpotting, skimming, and ATM abuse when earliest signs of anomalous activity determined.

Anti-Money Laundering

The module detects sophisticated money laundering transactions and suspicious activities and to cut overall costs, workload, and time commitment for financial institutions to review and investigate fraud.

Automated risk assessment

Automated processing of incoming information and creating a list of necessary actions for bank security personnel.

Vynamic View Security Manager Module

A complex strategy of protecting the terminal network from various types of attacks (both physical and logical) cannot work without a centralized process of administration and monitoring of the technical equipment and transactions.

For convenient monitoring of all events related to the security of self-service devices, the Vynamic View solution offers a self-contained Security Manager module.

Security Manager module functions

Security Monitoring

Tracking the security status of each connected self-service device and sending proactive threat notifications to responsible personnel for detailed analysis.

Remote terminal management

The ability to remotely turn on, turn off and reboot terminals, their peripheral devices and remote cameras, to activate and deactivate the service mode for each connected terminal.

Terminal network management

The module groups self-service devices and creates the necessary hierarchical links for more convenient security monitoring of the terminals network.

Remote software management

Centralized and remote software installation, updating and configuration to increase a level of self-service devices security.

Solution advantages

Multi-layered protection

Vynamic Security solution contains several modules thus providing multi-level protection of your ATM fleet. If one of the security layers fails, others continue to shield and secure the self-service device.

Work in multi-vendor environment

Vynamic Security is a multi-vendor solution that can be implemented to protect devices of different manufacturers. This allows you to unify the terminal maintenance processes and reduce the total cost of terminal network ownership.

Complex approach

Vynamic Security uses advanced techniques to protect IT infrastructure, such as creating lists of trusted software (whitelisting) and a restricted environment for the safe allowed processes running (sandbox). All this allows to ensure the security of the terminal network in the system.

Easy to use

The software does not require constant updates of anti-virus databases and the system scan. So, the solution simplifies the administration of the terminal network tremendously.

Security standards compliance

The solution is compatible with Windows 7, Windows 10, complies with PCI DSS security standards and can be adapted to the requirements of various regulatory agencies. The solution also allows you to extend running life of the devices where older versions of the OS installed.

Flexible licensing policy and wide integration opportunities

The solution can meet the various needs of the bank. Flexible licensing policy allows you to purchase self-contained modules in the necessary quantity for the business. The Vynamic Security software package is compatible with other security solutions and easily integrates into the of a financial institution infrastructure.

Related Products

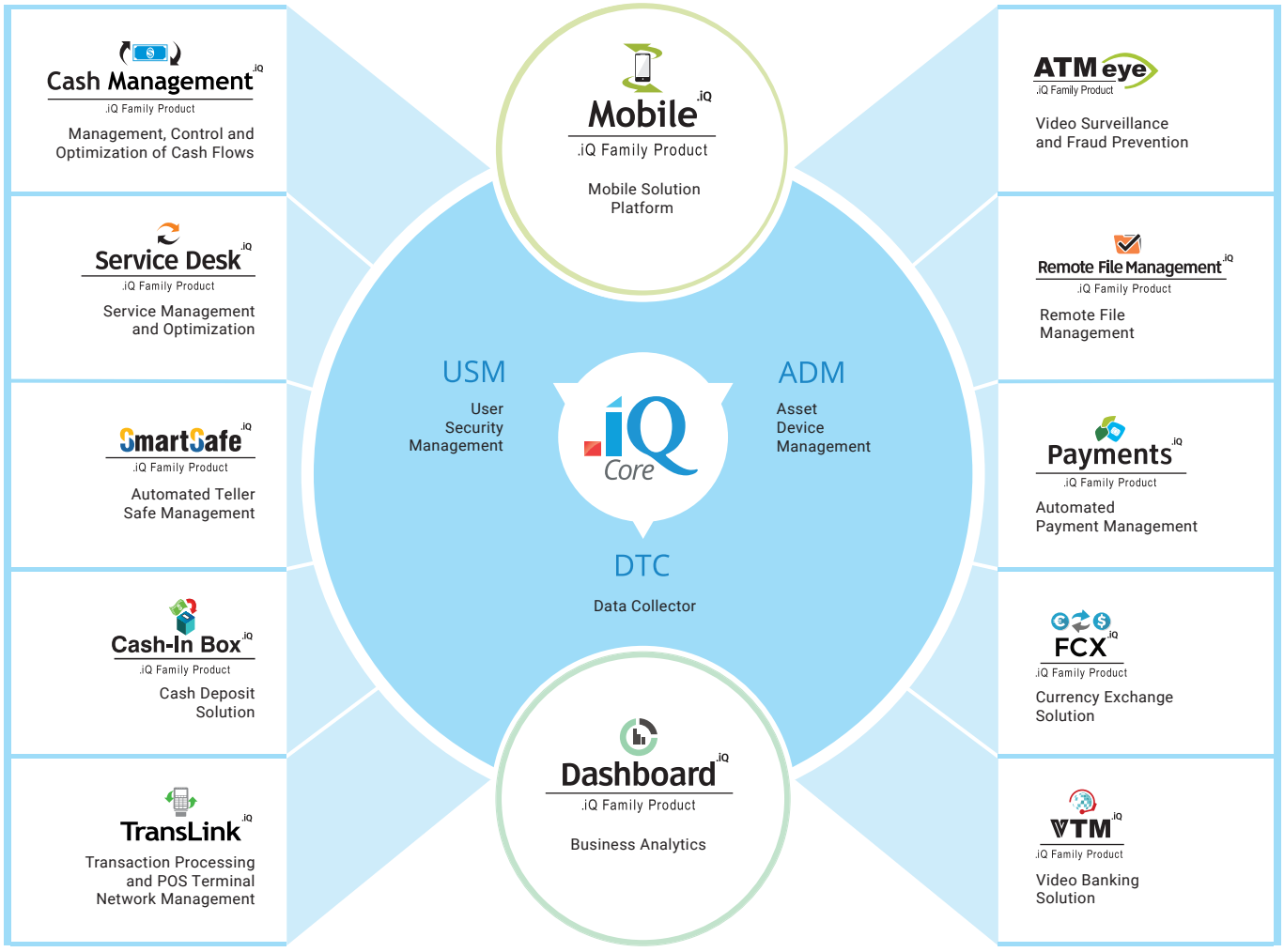
ATMeye.iQ — a comprehensive solution to improve the security level of self-service devices. It includes a video surveillance system with facial recognition functionality, as well as the sensors that react to any unlawful actions against terminals.

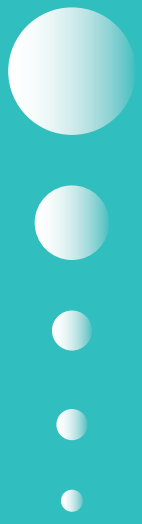
FRN.iQ — face recognition system to ensure the security of user authorization during payments and other operations.

Remote File Management.iQ is .iQ family product that provides secure file transfer between self-service devices and the administrator's workstation or data collection server.

Vynamic™ View — a software package designed to monitor and manage networks of banking self-service devices. The solution provides functions for retrieving information from devices, remote administration, diagnostics, and report generation.

Product family of .iQ





JSC “PENKIŲ KONTINENTŲ BANKINĖS TECHNOLOGIJOS”
Kareiviu st. 2, Vilnius, LT-08248, Lithuania
E-mail: info@bs2.lt | Tel.: +370 5 266 45 95 | www.bs2.lt