Vynamic™ Security Access Protection

Safeguard Systems and Control User Actions and Access to Information

Investments in data security are essential to protect consumer facing banking and retail devices from external threats such as viruses, worms and spam infected with malicious code. But focusing only on external threats is not sufficient to protect devices from disruption and risk. Banks and retailers must also secure access to their internal systems; fraudulent access can take the form of misused employee identities and privileges as well as insider threats. On one hand, this fraud can be simply a matter of carelessness. On the other hand, extensive access rights and security loopholes in the standard Windows® logon process can mean the potential for a huge risk of data misuse and disruption of operations.

To prevent tampering, data misuse and unauthorized access, and ensure that Windows-based devices run smoothly, it is critical that financial institutions and retail organizations set up extra access mechanisms and other safeguards. The access mechanisms inherent in the Windows operating system need to be extended through tailored user and rights management policies. Vynamic Security Access Protection meets these requirements and offers a higher level of security while ensuring fast access via a convenient user interface.

ALLOWS CONTROLLED ACCESS FOR TECHNICIANS

Remotely grants controlled, onsite access with an innovative password challenge/response mechanism:

- Completely eliminates the need to share any Windows user account or administrator password with a technician or operational user
- Offers secure, controlled access for operational use cases
- Provides instance privileges to technicians with a unique mobile app or with a quick call to the helpdesk

STRENGTHENS OPERATING SYSTEM AND PLATFORM

Extends the standard security services provided by Microsoft® operating systems, strengthening them with automatic, more secure logon procedures:

- Excludes potential security risks from the outset by hardening operating system
- Closes all security loopholes in the standard Windows access mechanism
- Provides unique keyboard shortcuts-blocking and mouse-blocking capabilities
- Offers the ability to harden browsers such as Internet Explorer and Google Chrome

DEFINE DIFFERENT ROLES FOR VARIOUS USERS

Provides a personal security policy for each authorized user so that functions, programs and resources can only be used within the predefined framework:

- Establishes who has accessed what, when and with which authorization
- Configures system logging so that all activities by users and system administrators can be recorded
- Creates a thorough record of user behavior by logging every access attempt and incorrect behavior

Secure Against Internal & External Threats

MULTI-LAYERED APPROACH

Vynamic Security provides a tightly integrated multi-layer approach in order to protect self-service terminals, POS devices, operating systems, and customer data against historical and newly-evolving attack vectors. This model ensures that if one security layer fails, others will take over to shield and secure an organization's critical assets. The Vynamic Security Software Suite consists of Intrusion Protection, Access Protection, and Hard Disk Encryption. Diebold Nixdorf's Vynamic View Security Manager is a special communication package designed to work with the Vynamic Security Suite to provide alerts on possible frauds, based on events correlation, in addition to BIOS password management.

FEATURES

- Access control based on roles and rights
- Uniform configuration for Diebold Nixdorf and multi-vendor self-service systems, including POS devices
- Industry-leading operational tools such as Ticketing using mobile app and Helpdesk tools
- Fast installation and easy administration
- Low maintenance and total cost of ownership (TCO)
- Complies with PCI DSS
- Windows 10 support

BENEFITS

- Effectively protects against unauthorized access to devices running on Microsoft Windows
- Eliminates the need to share administrator or user account passwords with the fleet
- Provides protection of user and group configurations through system configuration masking
- Standardizes the logon mechanism thanks to storage of encrypted passwords
- Securely logs system and user activities for auditing purposes

CONNECTIVITY

- Can be integrated seamlessly into existing IT environments, without affecting other applications or update backups residing on the systems
- Can be installed, configured and managed from a central remote point via a deployment and monitoring system (e.g. Diebold Nixdorf's Vynamic View) or locally (on-site)

WHAT IS DN VYNAMIC?

DN Vynamic is the first end-to-end connected commerce software portfolio in the marketplace. Traversing mobile, ATM, POS, branch, kiosk, and online, DN Vynamic is a system of consumer engagement powered by data and analytics and is cloud/SAAS ready when you are. Built to enable the connectivity businesses of the future require, DN Vynamic extends beyond omnichannel to enable banks and retailers to create seamless, secure, personal connections across the digital and physical channels of today and tomorrow.