## Vynamic® Security Access Protection

# Safeguard Self-Service Systems and Control User Actions

## Making the Windows environment compatible to industry and security standards

Self-service devices have a unique threat model and require continuous protection. Vulnerabilities which have not been recognized, over-permissive services, users, or security loopholes in standard Windows® processes can create a security exposure, disruption of service, and adversely impact an organization's reputation. Vynamic Security Access Protection dramatically reduces the attack surface and contextualize security within Windows operating system for self-service environments.

To prevent tampering, data misuse, unauthorized access, and ensure that Windows-based devices run smoothly, it is critical that financial institutions set up appropriate access mechanisms and 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.

### STRENGTHENS OPERATING SYSTEM AND PLATFORM

Vynamic Security Access Protection extends the standard security services provided by Microsoft Operating systems with purposely built and industry specific hardening, strengthening otherwise security weak configuration and industry incompatible environment:

- Dramatic reduction of inherent attack surface and exposure to potential risk by hardening operating system
- Closes all security loopholes in the standard Windows access mechanism
- Provides unique capabilities to block keyboard shortcuts and mouse
- Offers the ability to harden browsers such as Internet Explorer and Google Chrome

### ALLOWS CONTROLLED ACCESS FOR TECHNICIANS

Controlled, onsite access with an innovative password-less authentication:

- 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 instant privileges to technicians with a unique mobile app or with a quick call to the help desk

### 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, 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.

### FEATURES

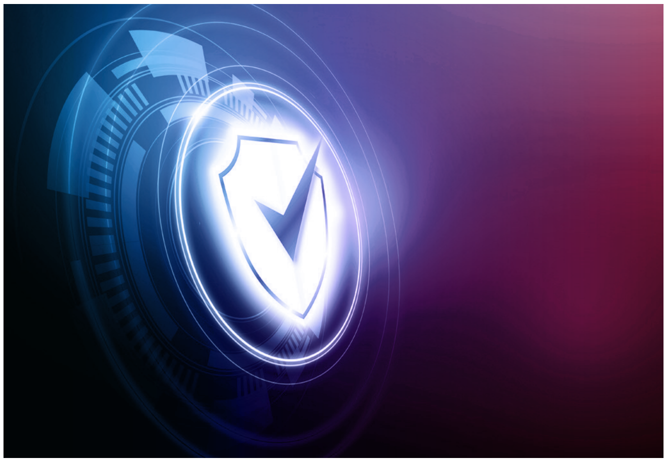
- Central Administration Console for the management of all security settings / parameters / configurations
- Prefabricated configuration incorporating industry OS hardening best practice for DN and multi-vendor systems
- Industry-leading operational tools such as Ticketing using mobile app and Helpdesk tools
- Fast installation and easy administration
- Low maintenance and total cost of ownership (TCO)
- Complies with PCI DSS
- Supports Windows 7, Windows 10 (2019 LTSC and 2021 LTSC) and Windows 11 IoT Enterprise LTSC 2024 (version 24H2)

### BENEFITS

- Effectively protects against unauthorized access to devices running on Microsoft Windows
- Centralized security policy management for the entire self-service fleet with support for multi-vendor software and hardware
- Eliminates the need to share terminal user credentials with branch and/or service personnel
- Provides protection of user and group configurations through system configuration masking
- Securely logs system and user activities for auditing purposes

### CONNECTIVITY

- Can be integrated seamlessly into existing IT environments, without affecting other applications
- Can be configured and managed from the Vynamic Security server
- Provides integration with availability management software like Diebold Nixdorf's Vynamic View or third party SOCs and SIEMs solutions



### DIEBOLD NIXDORF VYNAMIC SOFTWARE

Vynamic is a powerful software portfolio that enables financial institutions to eliminate friction to transform the user experience and the operation. Flexible and adaptable, Vynamic is built to align with how financial institutions operate and is bundled to support the modern banking environment including channels, payments, engagement and operations.

### ADDITIONAL SOLUTIONS UNDER THE VYNAMIC SECURITY SUITE

- Vynamic Security Hard Disk Encryption protects against offline threats and protects data so it cannot be tampered or stolen
- Vynamic Security Intrusion Protection enforces Least Privilege and protects against zero-day threats as well as provides protection from USB-based attacks

Diebold Nixdorf

To learn more, **visit DieboldNixdorf.com.**