Vynamic® Security Hard Disk Encryption

Secure Sensitive Consumer Data

Zero Trust based, purpose-built product to secure ATMs

The global rise in the attacks against personal and financial data poses a unique challenge for self-service devices. Vynamic Security Hard Disk Encryption address these threats to self-service devices by protecting the integrity of the executables and confidentiality of the data on the disk.

Banks and retailers have reported an increase in attacks in which criminals steal the hard disk of the self-service device. Through this type of attack, criminals gain access not only to so-called "branded" information, but also to the device's software stack, making it possible for reverse engineering to take place. Another common attack method for criminals, even when the hard disk is not stolen, is to boot from an external USB drive and copy malicious software to an ATM or POS as part of an offline attack.

To prevent these types of attacks and others, Diebold Nixdorf offers Hard Disk Encryption (HDE) as part of its Vynamic Security suite. This encryption software prevents unauthorized access to sensitive data, regardless of whether it's inside a system or the hard disk has been stolen. Unauthorized data cannot be written to the hard disk, and the encrypted data from a stolen hard disk cannot be used without the cryptographic keys unique to the system.

ENSURES THE HARD DISK CAN ONLY BE ACCESSED AND USED IN ITS ORIGINAL SECURE ENVIRONMENT

Operates with machine-specific encryption so data cannot be accessed if removed or stolen:

- Protects hard disk data when the respective system is in transit, temporarily out of operation or has been taken out of service
- Support for Trusted Platform Module (TPM)
- Verifies integrity of digitally signed sensitive executables during every pre-boot authentication stage

UTILIZATION OF DEVICES ECOSYSTEM TO ENCRYPT/DECRYPT AND PROTECT DATA WHILE AUTHENTICATING THE BOOT PROCESS

Supports data encryption and decryption on the basis of system characteristics such as connected USB devices or Device Hardware specifics:

- Authorization of boot process based on terminals' (USB) devices and not user and/or system credentials
- Blocks decryption if characteristics cannot be verified
- Protects against modifications in external boot sequence (CD-ROM, etc.)

CENTRAL KEY MANAGEMENT

Provides a server component (optional) that moves key computation and storage to a central server for infrastructure that are suitable for it:

- Never stores keys on the system's PC; rather the server always provides upon each PC boot
- Ensures that it is only possible to boot up the operating system on the encrypted hard disk when connected to the enterprise network
- Transfer of the key material from the server to the frontend device is performed via a secure TLS channel

Stop Attacks Before They Happen

MULTI-LAYERED APPROACH

Vynamic Security provides a tightly integrated, multi-layered approach to protect self-service terminals, POS devices, operating systems, and customer data against historical and newly evolving attack methods. 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

- Retrofittable, hardware-agnostic solution supporting a multi-vendor environment
- Self-contained encryption based on environmentally aware system characteristics
- No hardware upgrade required
- Pre-boot integrity checks with TPM support
- No infrastructure changes are needed in the environment
- Quick to deploy, easy to maintain
- No hindrance to terminal operations
- Supports Windows 7 and Windows 10 (including Windows 2021 LTSC)
- Multi-language support

BENEFITS

- Stops malicious activity to the hard disk when the terminal is offline
- Encrypts all the data on a self-service terminal's hard disk
- Safeguards confidentiality and integrity when a system is out of operation
- Option to operate in conjunction with central key management server
- Real-time encryption (based on military grade AES – 256-bit encryption standard)
- Can be remotely deployed

CONNECTIVITY

- Seamless deployment and integration in to self-service environment
- Can be configured and managed from the Vynamic Security server
- Provides integration with availability management softwares like Diebold Nixdorf's Vynamic View

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 Access Protection facilitates password-less authentication, user management and Operating System and platform hardening
- 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.**