Vynamic® Security Hard Disk Encryption

Secure Sensitive Consumer Data

Military Grade AES 256 Bit Encryption

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 have reported an increase in attacks in which criminals steal the hard disk of the self-service device or try to gain access to the hard disk while the device is offline. 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 as part of an offline attack.

To prevent these types of attacks and others, Diebold Nixdorf offers Hard Disk Encryption (HDE) as part of Vynamic Security. 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 and PCI connected devices or Device Hardware specifics:

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

RECOVERY AND SELF-DESTRUCT TOOL-KIT

Unfortunately, there may be circumstances when human intervention is required. For such circumstances, Vynamic Security Hard Disk Encryption delivers tools to support them:

- Recovery enabling the recovery of the data stored on the encrypted hard disk even when the respective keys have been lost.
- Self-Destruct deletes the respective keys thereby making the data stored on the respective hard disk non-recoverable.

Stop Attacks Before They Happen

MULTI-LAYERED APPROACH

Vynamic Security provides a tightly integrated, multi-layered approach to protect self-service terminals, 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. Vynamic Security consists of Intrusion Protection, Access Protection, Hard Disk Encryption and BIOS Password Management.

FEATURES

- Retrofittable, hardware-agnostic solution supporting a multi-vendor environment
- Self-contained encryption based on environmentally aware system characteristics
- Support both HDDs and SSDs
- Pre-boot integrity checks
- No infrastructure changes are needed in the environment
- Quick to deploy, easy to maintain
- No hindrance to terminal operations
- Supports Windows 7*, Windows 10 (2016 LTSB, 2019 LTSC and 2021 LTSC) and Windows 11 IOT Enterprise LTSC 2024 (version 24H2)

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 into self-service environment
- 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 VYNAMIC SECURITY

- 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.
- Vynamic Security BIOS Password Management enables the secure update of BIOS passwords in alignment with PCI DSS 4.0 recommendations. It also supports password renewal after service interventions, ensuring continued compliance and security.

* Only with Vynamic Security 4.4 & 4.5 client

Learn more at **DieboldNixdorf.com/DNSeries.**