Vynamic™ Security Hard Disk Encryption

Secure Sensitive Consumer Data

Consumer facing banking and retail devices are subject to many forms of attacks, including a wide range of both physical and logical attacks. The latter mainly involves tampering with the device software, for the purpose of intercepting and stealing sensitive information. Although this data is primarily retrieved from installing malicious software, thefts of hardware are also on the rise.

Banks and retailers have reported an increase in attacks in which criminals steal the hard disk of the self-service device or the POS. 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 re-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 or bootable CD and copy malicious software to an ATM or POS.

To prevent these types of attacks, 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 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 unique keys.

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
- Ensures real-time transparency into the operating system and ATM or POS applications
- Verifies integrity of digitally signed sensitive executables during every pre-boot authentication stage

PROTECTS CRITICAL RUNTIME DATA AS WELL AS DATA AT REST

Supports data encryption and decryption on the basis of various system characteristics such as connected USB devices or Trusted Platform Module (TPM):

- Operates with a modular structure to verify all applications
- Blocks decryption if characteristics cannot be verified
- Protects against modifications in external boot scenarios (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. 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

- Retrofittable, hardware-agnostic solution supporting a multi-vendor environment
- Self-contained encryption based on environmentally aware system characteristics
- No hardware changes required
- No extra costs for external operations
- 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

BENEFITS

- 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

- 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.

Diebold Nixdorf

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