Self-service terminals are subject to many forms of attacks, including a wide range of both physical and logical attacks. The latter mainly involves tampering with the self-service terminal software, for the purpose of intercepting and stealing card holders’ sensitive information. Although this data is primarily retrieved from installing malicious software on the terminal, thefts of hardware from automated teller machines are also on the rise. Banks have reported an increase in attacks in which criminals remove the fascia of an ATM and steal the hard disk or even the entire PC. Through this type of attack, criminals gain access not only to so-called “branded” information, but also to the self-service terminal’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’s PC.

To prevent these types of attacks, Diebold Nixdorf offers Hard Disk Encryption (HDE) as part of its Terminal Security suite. This encryption software prevents unauthorized access to sensitive data on an ATM, regardless of whether it’s inside an ATM, or the ATM’s PC 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 self-service system is in transit, temporarily out of operation or has been taken out of service
  - Ensures real-time transparency into the operating system and self-service terminal applications

**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 motherboard details:
  - 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 ATM’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 ATM’s hard disk when connected to the enterprise network
  - Transfer of the key material from the server to the ATM’s PC is performed via a secure TLS channel
STOP ATTACKS BEFORE THEY HAPPEN

MULTI-LAYERED APPROACH
Terminal 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 Terminal Security Software Suite consists of Terminal Security Intrusion Protection, Access Protection and Hard Disk Encryption. Additionally, Diebold Nixdorf’s ProView Security Manager is a special communication package designed to work with our Terminal Security Suite. Fraud detection based on event patterns and event correlation and BIOS password management complement the functions.

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
• Windows 10 Support*

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 ProView) or locally (on-site)

WHY DIEBOLD NIXDORF?
Diebold Nixdorf provides the most comprehensive, time-tested expertise, tools and solutions – but we go one step further. Our 365° Security Concept consists of several security layers that work together to provide a comprehensive protective shield for all channels against all kinds of attacks — physical, logical and fraud. Constantly monitoring for changes to the threat landscape, our approach is proactive and consumer-minded, and it enables FIs to manage risk based on an understanding of both endpoints and consumer behaviors.

DEFEND YOUR SELF-SERVICE ENVIRONMENT AGAINST TAMPERING AND THEFT. CONTACT YOUR DIEBOLD NIXDORF REPRESENTATIVE TODAY.