Vynamic™ Security Intrusion Protection

Deliver End-to-End Protection Against Network and Local Attacks

No financial or retail organization is safe from the viruses, malware and Trojans that infiltrate or are covertly installed their front-end terminals. In fact, reports on new variants of malware are published every few months.

Recently, security experts discovered that the infamous Ploutus malware is back, joining the hundreds of other malware such as WannaCry affecting terminals worldwide. The new version, Ploutus D, makes use of third-party components that allow it to run on terminals from multiple vendors. While experts work on patches to close security loopholes, the malware may already be wreaking havoc.

The frequency of these types of advanced, persistent attacks is rising. Attackers are not just trying local attack methods, they're now attempting to gain unauthorized access to a terminal remotely by infiltrating financial and retail institutions' back office systems. Such focused attacks cannot be stopped using traditional whitelisting or anti-virus solutions. Vynamic Security Intrusion Protection follows modern security approaches, implementing sandboxing procedures that go beyond whitelisting. Together with strict, out-of-the-box modular policies, Intrusion Protection can effectively block these modern threats and provide a strong security barrier.

ANYTHING THAT IS NOT EXPLICITLY ALLOWED IS FORBIDDEN

Only permits applications, processes and services to access system resources to the extent that is absolutely necessary:

- Operates according to the Least Privilege Confinement principle by using modern sandboxing techniques password with a technician or operational user
- Establishes a ruleset that goes beyond "what is allowed" (whitelisting), and considers "when and where" in terms of specific privileges (behavioral pattern)
- Enables the various software layers to process and communicate within a controlled, sterile environment

ENSURES THE INTEGRITY OF THE RUNTIME ENVIRONMENT IS UPHELD

Detects any change to the defined set of files while running or on system boot, and kills the process:

- Blocks execution of applications if their file integrity check fails
- Protects against unintentional mistakes in security configurations
- Manages and validates so-called checksums (hash values) of individual files and other critical resources such as registry settings
- Unauthorized changes are recognized and the respective security alert automatically issued

OPTIMIZES COMPLIANCE & MINIMIZES RISK

Provides proven support in fulfilling the numerous regulations issued by various regulatory bodies:

- Offers a unique way of protecting a terminal from being exploited via external USB devices
- Provides detailed event logs to understand what is taking place on each protected terminal
- Complies with PCI DSS

Be Confident in Your Security Policies and Practices

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

- Self-contained software
- Ideal for multi-vendor environments and can therefore be used on all terminals, including application platforms from different vendors
- Easy to configure and operate
- Prefabricated and extendable security policy
- Low maintenance and total cost of ownership (TCO)
- Supports Windows 7 and Windows 10

BENEFITS

- Effective, state-of-the-art protection against known and unknown threats
- Locks down with protection against zero-day attacks for which patches are not yet available
- Purpose-built for unattended self-service terminals and their environments
- No frequent updates such as signature files or virus definitions needed for protection
- Device protection is based on out-of-the-box modular software policies, reducing the need for lengthy configurations
- High system availability without any noticeable performance impact

CONNECTIVITY

- Can be integrated seamlessly into existing IT environments, without affecting other applications or update backups residing on the systems
- Security policies can be effectively adapted for specific needs of any terminal fleet to ensure the most effective lockdown of the devices
- 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.**