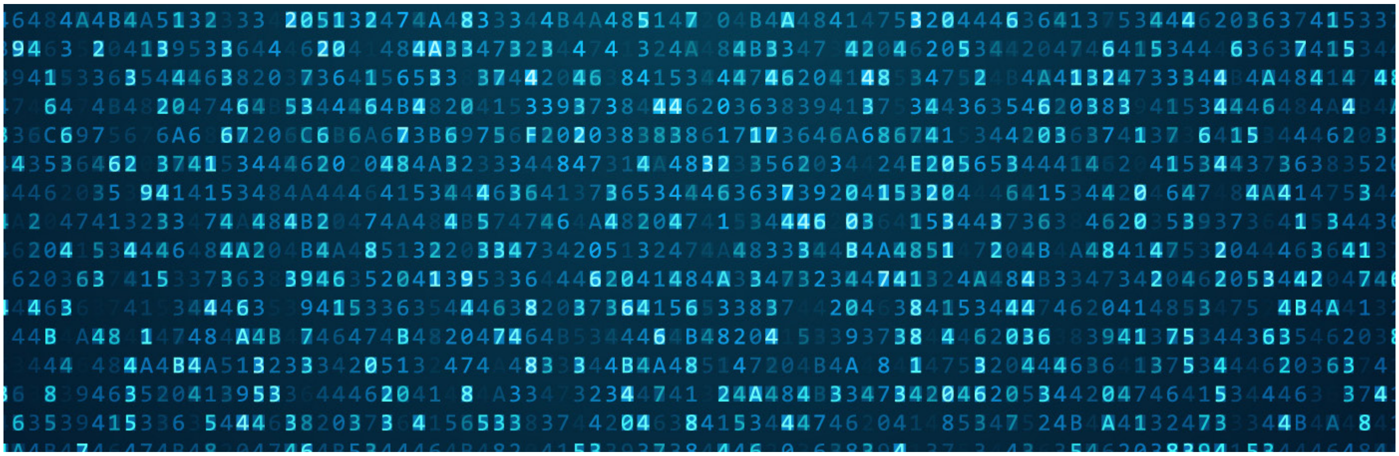
Vynamic® Security Intrusion Protection

Delivers Protection Against Known and Unknown (ZeroDay) Attacks



Zero Trust based, purpose-built product to secure ATMs

Large scale attacks are happening at an unprecedented rate. Sophisticated hackers are using known vulnerabilities to attack hundreds if not thousands of systems across multiple organizations all at the same time.

No financial or retail organization is free from these vulnerabilities which allow the perpetrators to launch ransomware attacks, install viruses, malware, and trojans that could infiltrate a self-service environment. 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
- Establishes a policy of zero trust which goes beyond "what is allowed", and considers "when", "where", "with what", etc. in terms of specific privileges (behavioral pattern)
- Includes zero-day protection for unattended terminals in the financial sector
- Protection against buffer overflow and memory-based attacks
- File and registry protection and monitoring
- Enables the various software layers to process and communicate within a controlled, sterile environment
- Compact size allows for the use of minimal system resources

ENSURES THE INTEGRITY OF THE RUNTIME ENVIRONMENT IS UPHELD

- Identifying when unauthorized changes are made to software stack; not limited to only executable files but also system critical configuration-property files, system registry and BIOS.
- Any unauthorized changes are recognized, and the respective security alert is automatically issued
- Control behavior by detecting and preventing specific actions that an application or user might take

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

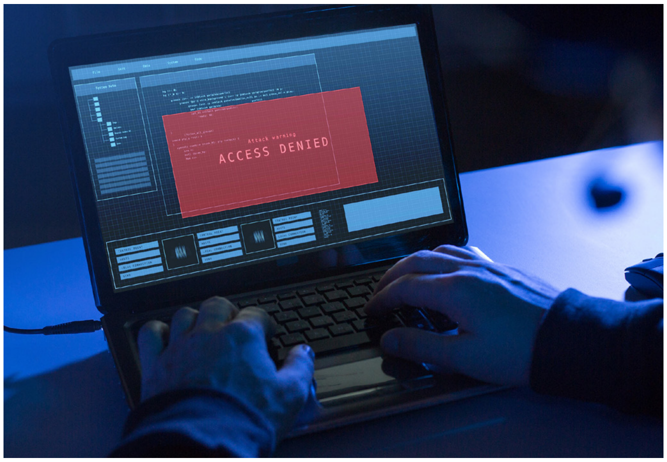
Vynamic Security provides a tightly integrated, multi-layered approach to protect self-service terminals, POS devices, operating systems, and customer data against historical and newly evolving attack methods. This model ensures that if one security layer fails, others will take over to shield and secure an organization's critical assets. The Vynamic Security Software Suite consists of Intrusion Protection, Access Protection, and Hard Disk Encryption.

FEATURES

- Self-contained software providing protection from malware, include zero-day attacks
- Removable Medium usage management (USB devices) based on the When – Where – What principles
- Easy to configure and operate
- Prefabricated and extendable security policy
- Low maintenance and total cost of ownership (TCO)
- No need to rehash files with every software release or update
- Supports Windows 7 and Windows 10 (including Windows 2021 LTSC)
- Provides instant privileges to technicians with a unique mobile app or with a quick call to the helpdesk
- Multi-language support
- Supports multi-vendor environments (for both hardware and software)

BENEFITS

- Single point of management and distribution of security policies for the entire fleet
- Customizable, modular out-the-box security policies covering both DN and non-DN software
- 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
- 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
- Can be configured and managed from the Vynamic Security server
- Provides integration with availability management software 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 Hard Disk Encryption protects against offline threats and protects data so it cannot be tampered or stolen
- Vynamic Security Access Protection facilitates password-less authentication, user management and Operating System and platform hardening

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