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 some known but mainly unknown vulnerabilities to attack hundreds if not thousands of systems across multiple organizations all at the same time.

No financial organization is free from vulnerabilities which allow the perpetrators to launch ransomware attacks, install viruses, malware, or trojans that could infiltrate a self-service environment or worse using the self-service channel to infiltrate the back-office 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 institutions' back-office systems. Such focused attacks cannot be stopped using traditional whitelisting, anti-virus or heuristic security solutions. Vynamic Security Intrusion Protection follows modern security approaches, implementing Least Privilege Confinement procedures that go beyond whitelisting. Together with strict, out-of-the-box modular policies, Intrusion Protection can effectively block these modern and evolving threats such as Direct Memory Access (DMA) attacks, providing recommendations for policy configurations and delivering a stronger security barrier.

ANYTHING THAT IS NOT EXPLICITLY ALLOWED IS FORBIDDEN

Vynamic Security Intrusion Protection 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).
- Delivering Zero-Day protections without a security gap inherent to other security solutions
- Protection against the various forms of direct memory attacks (DMA)
- 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.

ACCELERATED INTEGRATION OF CUSTOMIZED / NON-STANDARD ENVIRONMENTS

- Monitors and Collects all applications, services (OS, Platform, Application, etc.) e.g., file system, internal/external communication, memory access, etc. behaviours information, and sending it to the connected Vynamic Secuirty Server instance.
- Visualization of collected data within Vynamic Security console, improving and accelerating the management (creation – adaptation) of Intrusion Protection policies.

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 automatically issued.
- Control behavior by detecting and preventing specific actions of an application or user.

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 delivering compensating controls for applicable requirements

Be Confident in Your Security Policies and Practices

MULTI-LAYERED APPROACH

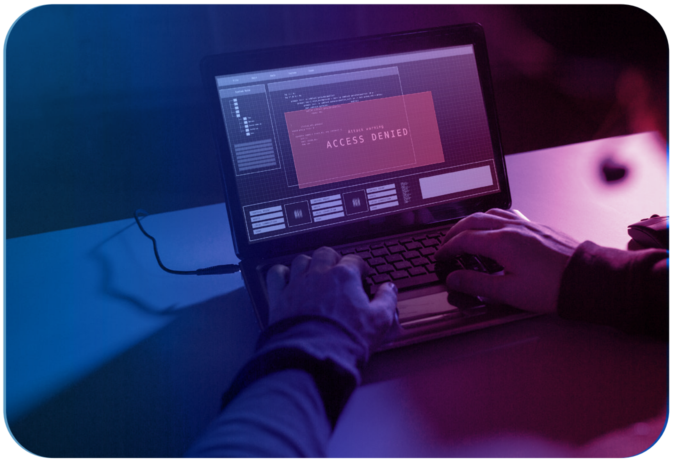
Vynamic Security provides a tightly integrated, multi-layered approach to protect self-service terminals, operating systems, and customer data against historical and newly evolving attack methods. This model ensures that if one security layer fails, others will take over to shield and secure an organization's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

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*, Windows 10 (2016 LTSB, 2019 LTSC and 2021 LTSC) and Windows 11 IOT Enterprise LTSC 2024 (version 24H2)
- Provides instant privileges to technicians with a unique mobile app or with a quick call to the helpdesk
- 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, virus definitions or ACLs 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 or third party solutions such as SOCs and SIEMs

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 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.
- 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.**