Padvish®

Padvish DataGuard™

Padvish DataGuard

Padvish DataGuard™ is a next-generation, data-centric platform that functions as a host-based intrusion prevention system (HIPS). It provides robust, policy-driven protection with five layers of ransomware defense, along with capabilities for data protection, network policy, etc. Designed for seamless coexistence with other solutions, it includes all the features of Padvish except for antivirus protection, making it ideal for organizations that prioritize data integrity and ransomware resilience.

HIPS

Tamper Protection:

Activates against file encryption attempts. This layer requires no signature updates and has successfully blocked zero-day ransomware, including WannaCry.

DataCop Protection:

Creates lightweight, fast Volume Shadow Copy Service (VSS) backups twice daily and actively prevents the deletion of these backup files.

MBR Protection:

Defends the Master Boot Record from modification by ransomware and other threats that target the boot sector to take control of a system.

Bait Mechanism:

Deploys decoy files to attract and identify ransomware activity, triggering an immediate interception upon any encryption attempt.

BitLocker Protection:

Defends against the malicious misuse of Microsoft's native encryption tool, which has been used in attacks to irreversibly lock data. For the first time in the market, Padvish delivers unique protection against this weaponization of this trusted utility.

Data Protection

DataCop Protection

Padvish's DataCop is designed to prevent user data loss. It operates by creating fully automatic backups in the fastest and most storage-efficient manner possible and protects these backups from malware threats.
The capabilities of these backups are as follows:

- Fully automatic backup, requiring no user configuration.
- Extremely fast (completed within seconds).
- Protected against malware, ransomware, and tampering.
- Highly storage-efficient (using only 5% of disk space).

DRM Encryption

- Files are automatically encrypted immediately upon creation.
- Encryption and decryption happen transparently without user action.
- Leaked files remain protected, exposing no usable data.
- Each file is secured with a unique encryption key for granular control.
- Encryption keys are managed through a centralized server hierarchy.
- All protection features remain available even when disconnected from the network.

DLP Rules

Our Software Device Control (SDC) defines and enforces device and data access policies across endpoints. It lets you specify exact access rules that determine permitted and denied behavior based on six dimensions. It provides precise control and policy-level auditing.

- **Who (User):** Define policies by identity or group membership.
- **Where (System / Endpoint):** Scope rules to endpoint, network segments, or locations.
- **What (File / Object):** Target rules to file extention.
- **When (Time / Workhours):** Apply time-based controls.
- **Which (Device / Peripheral):** Control by specific device.
- **How (Application / Process):** Bind rules to the executing application or process.

Network Policy

Firewall

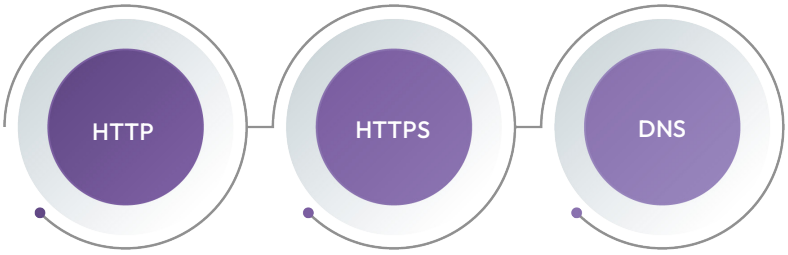
Padvish is equipped with a dual-layer firewall based on the Windows architecture:

Layer 3:
A stateless, packet-based firewall operating at the lowest level of the Windows kernel, just above the network card driver. It controls incoming and outgoing packets.

Layer 7:
A stateful, connection-based firewall operating at the highest level of the Windows kernel, just below user applications. It controls incoming and outgoing connections based on the application.

Web Control

The web control component prevents connections to unauthorized domains. It inspects the content of the following protocols to detect attempts to connect to unauthorized domains:



This capability can be activated in the following modes:

- **Blacklist:** Unauthorized domains are blocked, while all other domains are allowed.
- **Whitelist:** Only pre-defined domains are allowed, and all others are blocked.
- **Logging:** This can be used in combination with the modes above to log activity without blocking.
- **The feature also supports partial domain matching (*example.org)**

App Control

Application Control prevents the use of unauthorized programs.

Rules can be defined based on the following criteria:

Application Inventory Discovery:

The Application Inventory feature creates a centralized database of all software installed on clients across the network, enabling rule creation based on this inventory.

Device Control

This component provides comprehensive monitoring and policy enforcement for peripheral device connections across 14 categories, including USB storage, network adapters, Bluetooth devices, and mobile connections. The system supports advanced rule creation based on device attributes (name, ID, vendor/product IDs) and offers multiple enforcement actions from simple logging to read-only access, complete blocking, or even system lockdown/restart.

Device Management Features

The integrated Device Bank centralizes visibility of all network peripherals, enabling easy authorization, tagging, and renaming. The Trusted Devices feature simplifies mass device management through one-click authorization and provides reporting on lost or inactive devices, offering a streamlined alternative to complex rule configurations.

Core Values

1 **Data-Centric Protection Across Layers:**
- System, network, and data protections work together to guard data regardless of compromise vectors.

2 **Non-Conflicting with Existing AV:**
- Designed to complement existing antivirus solutions without duplicating AV engines.

3 **Behavioral Security Focus:**
- Emphasis on ransomware behavior detection and adaptive protection without needing constant signature updates.

4 **Policy-Driven Access Control:**
- Fine-grained control over applications, devices, and network interactions.

5 **Visibility and Control:**
- Real-time monitoring, reporting, and detailed analytics for informed decision-making.

6 **Automated and Lightweight Backups:**
- Fast, space-efficient backups with integrity protections.

Managing your security is hard, Amnpardaz makes it easy

"Amnpardaz Software Corporation, operating under the Padvish brand, offers a comprehensive range of cybersecurity solutions tailored to safeguard both home and enterprise environments against evolving cyber threats"

Amnpardaz®
Software Corporation

Padvish®

www.padvish.com
info@amnpardaz.com

Learn More