Amnpardaz®
Software Corporation

# Advanced
# Cyber Security Solutions

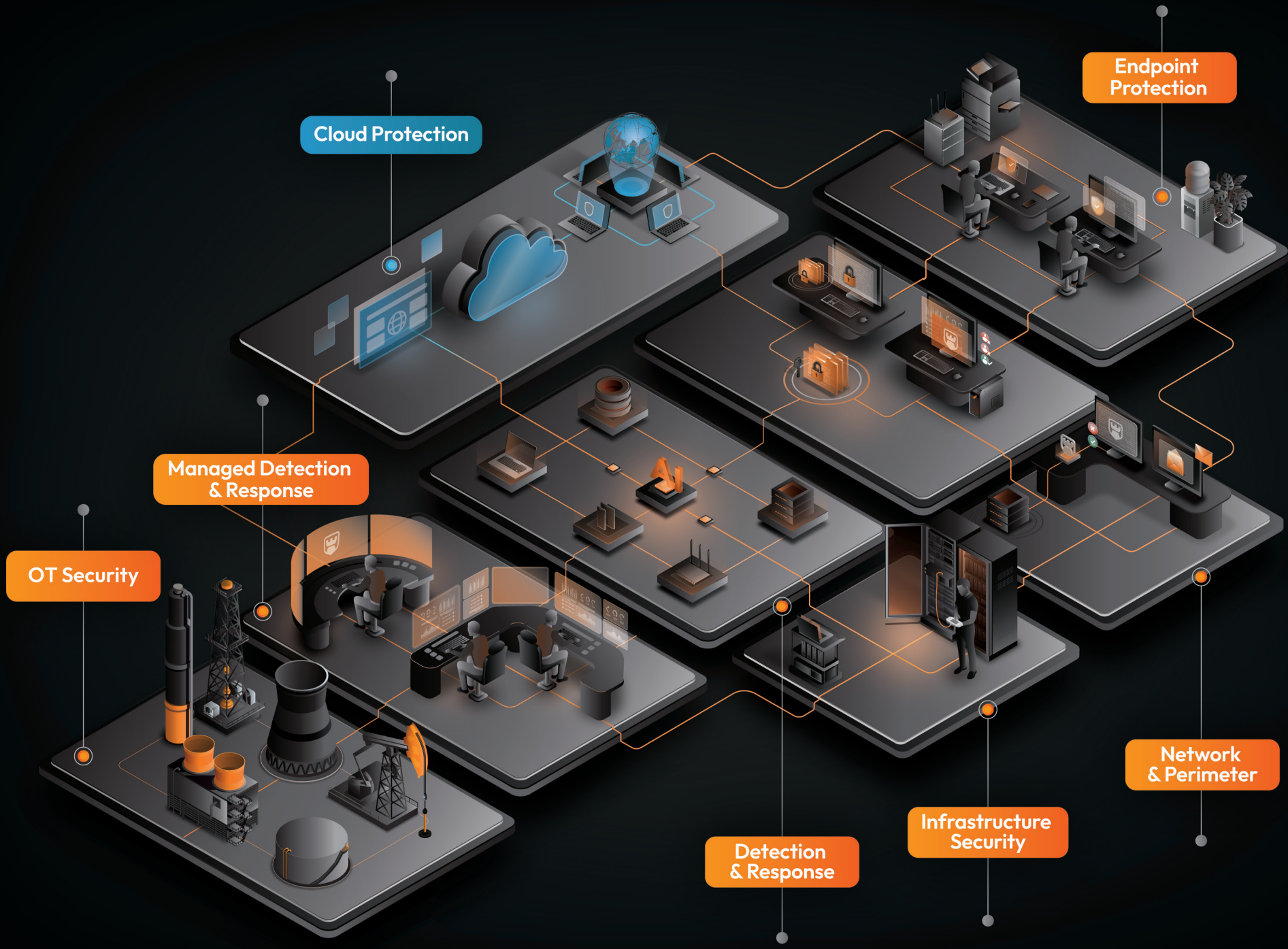
Amnpardaz Cybersecurity Platform

Innovating Cyber Trust

Padvish® | Cloud Guard

# Amnpardaz Integrated Cybersecurity Ecosystem

Innovating Cyber Trust Through Integrated Solutions


Cloud Protection
Endpoint Protection
Managed Detection & Response
OT Security
Detection & Response
Infrastructure Security
Network & Perimeter

# Contents

# About Us

**Amnpardaz was founded in 2004 with a clear and inspiring vision:**

Technology should protect people, not constrain them.

From the outset, our mission has been to engineer solutions that safeguard the privacy, sensitive data, and digital lives of individuals and organizations amid the escalating complexities of the digital landscape

**Padvish, Amnpardaz flagship brand, embodies the culmination of this journey.**

It represents a comprehensive portfolio of globally standardized security solutions, trusted by millions of users and thousands of organizations.

By merging advanced engineering with artificial intelligence and an ethics driven methodology, these solutions deliver robust, integrated security.

Notable achievements, including the global identification of advanced threats like iLOBleed and the domestic detection of WannaCry, alongside Advanced Threat Detection and Endpoint Response (EDR) certification and a 100% ransomware detection certification from Germany's AV-Test Laboratory, as well as Padvish XDR AI's distinguished global standing in the prestigious EDR Telemetry Ranking outperforming many of the world's leading cybersecurity vendors underscore the efficacy of our solutions in consistently defending organizations against the most sophisticated cyber threats.

**Today, Amnpardaz delivers a comprehensive portfolio of consumer and enterprise security solutions, including:**

- Cross-platform endpoint protection for Windows, Linux, and Android
- Data protection
- Network security
- AI-driven intelligent detection and response solutions
- Managed detection and response (MDR) services
- IT service management
- Infrastructure protection
- AI-powered cloud security for networks, digital platforms, and information assets

## Amnpardaz's Seven Core Values

1. **Ethics** at the core of security
2. **Human-centric** approach alongside technology
3. **Simplicity** in design and execution
4. **Transparency** in data and conduct
5. **Responsibility** toward users and society
6. **Integration** of architecture and experience
7. **Continuous** learning and improvement

## Amnpardaz in Numbers

| | | |
|---|---|---|
| **+7** million home and enterprise users | **+20** years of innovation and dedication | **+612** million malware samples analyzed |
| **+200** cybersecurity solutions | **+7000** Protected organizations | **+200** representatives and sales partners |

## Amnpardaz's Security Philosophy

**"For us, security begins with one principle: ethics."**

In a world of increasing technological and cyber complexity, security is not achieved solely through advanced tools. It becomes meaningful when ethics, data, and technology are aligned within a balanced and responsible ecosystem.
From Amnpardaz's perspective, security is not a commodity, but a process, one that must be built on transparency, precision, and accountability.

**We define security around three core pillars:**

- Simplicity at the heart of complexity
- Human at the center of every decision
- Transparency instead of chaos

## Amnpardaz and the Evolution of Cybersecurity Technology

**For years, Amnpardaz has moved beyond traditional cybersecurity models those relying solely on signatures, databases, and known file detection.**

Today's multi-stage threats, fileless attacks, abuse of system behaviors, and complex intrusion chains demand an approach that operates beyond static detection.

**With its Padvish Security Platform, Amnpardaz has taken a step beyond conventional antivirus solutions, entering the era of next generation security combining advanced systems such as EDR, XDR, and artificial intelligence.**

Within this architecture, security is not a "filter," but a continuous system for behavioral analysis, data correlation, and coordinated response. It monitors, tracks, and analyzes threat behavior across all layers from endpoints and networks to cloud and infrastructure environments and delivers coordinated responses.

**Amnpardaz has transformed security from a mere tool into an integrated and intelligent system designed for the current threat landscape, moving beyond the static defenses of the past.**

# Unified Network Security: Single Console & Agent

## Padvish Central Management Console

The Padvish Management Console is an integrated platform designed for centralized management, configuration, and comprehensive monitoring of an organization's digital ecosystem. Leveraging a Primary/Secondary architecture, it enables centralized control of the entire network, streamlined policy distribution, update management, and real-time visibility into the operational status of all clients and servers.

### Key Capabilities of the Unified Management Console:

- Centralized definition and enforcement of security policies at scale
- At a glance visibility into the network's security posture
- Unified management of deployment and installation across the entire network
- Investigation and tracking of security events, alerts, and reports

## Single-Agent Deployment

One of the primary challenges organizations face in security management is the proliferation of multiple agents per product or plugin, incompatibility between tools, and the resulting deployment complexity. This not only increases operational costs but also raises the likelihood of errors and potential security gaps.

At Amnpardaz, the Padvish product ecosystem has been designed so that all products and solutions on the client side are delivered through a single, lightweight, and unified agent, while administrators manage the entire environment through a single management console.

### Operational Advantages of a Single Lightweight Agent:

- Rapid deployment across large scale networks without repeated on site presence
- Reduced operational and administrative burden on security teams
- A unified experience when using multiple security products
- Improved performance with minimal system overhead

## Certifications and Achievements

1. Advanced Endpoint Detection and Response (EDR) Certification by the AV-Test Laboratory, Germany


2. Padvish XDR AI achieved a distinguished global standing in the prestigious EDR Telemetry Ranking, outperforming many of the world's leading cybersecurity vendors.


3. Awarded a 100% Ransomware Detection Certification by the AV-Test Laboratory, Germany


4. The world's first iLOBleed malware detector

5. Detection of Petya, WannaCry, and other advanced malware families

## Comprehensive Support and Continuous Readiness

**Security does not rely solely on technology; it also depends on the presence of professionals who stand beside organizations during critical moments.**

At Amnpardaz, support is not a separate function from our products it is an integral layer of our security architecture.
We believe that cyber trust is built when an organization knows that behind every alert, every decision, and every update, a dedicated team of specialists stands responsibly in support.

### Key Support Commitments at Amnpardaz:

- Dedicated enterprise security team
- Transparent and traceable response
- 24/7 assistance
- Guidance during deployment and operations
- Multi-layered support for large-scale networks
- Training and knowledge transfer

**True security means having real support when it matters most.**


Padvish DLP
Padvish DRM
Padvish™ DataGuard
Padvish vKiosk™
Data Protection
CloudGuard Threat Intelligence
CloudGuard Network Protection
CloudGuard Web Protection
Cloud Protection
Padvish OT
OT Security
Endpoint Protection
Windows
Padvish Corporate
Padvish Base
Android
Padvish Android Enterprise
Linux
Padvish Linux
Managed Detection & Response
Padvish MXDR
Padvish MDR
Detection & Response
Padvish EDR AI
Padvish XDR AI
Infrastructure Security
Padvish iLO Scanner
Network & Perimeter
Padvish NAC
Padvish Mail Gateway

# Padvish Enterprise Cybersecurity Solutions Ecosystem

## Integrated Security Architecture

Enterprise security becomes truly effective when all defensive layers from endpoints to the cloud operate in a coordinated and transparent structure. At Amnpardaz, we do not perceive security as a collection of discrete tools; we view it as a unified and cohesive ecosystem.

### This integrated security ecosystem is built upon eight foundational pillars:

1. **Endpoint Protection:** Advanced defense against endpoint threats, supporting unified security policy enforcement and centralized management across the organization.

2. **Data Protection:** Safeguarding organizational information and data against leakage, internal and external threats, while ensuring access control to sensitive assets.

3. **Network Protection:** Securing the organization's cyber boundaries by managing network access, maintaining communication transparency, and enforcing consistent network policies.

4. **Intelligent Detection and Response Systems:** Delivering the highest level of security through unified visibility across endpoints, networks, and non endpoint devices empowered by integrated analysis and coordinated response augmented by AI.

5. **Managed Detection and Response Solutions (MDR):** Ensuring continuous, 24/7 management of advanced detection and response platforms through the expertise of Amnpardaz's cybersecurity specialists.

6. **Infrastructure Protection:** Ensuring the Integrity and Resilience of the Organization's Hardware Layer.

7. **Operational Technology Protection (OT Security):** Providing comprehensive defense for operational environments against evolving threats.

8. **CloudGuard Protection:** Safeguarding websites, networks, and applications through a depth in defense approach.

# Endpoint Protection

For Windows, Linux, and Android Platforms

## Padvish Base\Corporate

**Padvish Base** | **Padvish Corporate**

## Advanced and comprehensive protection for organizational endpoints, data, and networks.

### Organizational Challenges

In today's complex cyber threat landscape, organizations face rapidly evolving malware, ransomware, fileless attacks, exploitation of operating system vulnerabilities, and intrusions via networks and the Internet.

**This raises a critical question:**

- How can an organization manage all these sophisticated threats in a unified and centralized way?

### Amnpardaz Solution

Padvish Advanced Endpoint Protection integrates next-generation Anti-Malware technology, data loss prevention (DLP), behavioral detection, cloud-based analysis, and network defense layers (Firewall and IDS/IPS) to deliver cohesive, organization-wide protection.

**The solution is available in two editions: Base and Corporate.**

- The Base edition delivers advanced protection against malware, prevents data leakage, and blocks network level attacks.
- The Corporate edition, in addition to all Base features, provides enhanced capabilities such as vulnerability management, Internet access control, and trusted network management.

All these capabilities are centrally monitored and managed through the Padvish Management Console.

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

# Padvish Corporate / Padvish Base

## Product Architecture

Padvish Base and Padvish Corporate are built upon a lightweight, behavior-driven, multi-layered engine that delivers real-time protection, file analysis, network monitoring, and peripheral device control at the endpoint layer.

This architecture is optimized for large-scale networks with high geographic dispersion, numerous devices, and mission-critical operational environments.

### Use Cases

- Protection of organizational and operational systems
- Prevention of malware and emerging threats
- Control of removable media in sensitive environments
- Lightweight policy-based protection for legacy or low-performance systems
- Securing large networks through centralized management

### Key Security Deliverables

- Reduced risk of endpoint infection
- Enhanced resilience against internal and external threats
- Shortened incident response time
- Seamless integration of the endpoint layer within the organizational security architecture
- Lowered support and management costs

**Internet Connection Detection**

Incorporates an intelligent layer for identifying unauthorized client Internet connections and applying adaptive security policies based on network status.

**Trusted Network**

Enables the definition of trusted networks, conditional access based on user location, network connection restrictions, and comprehensive reporting of policy violations within trusted networks.

**Vulnerability Assessment**

Generates detailed reports on operating system vulnerabilities, categorizes them by risk level, and provides patch verification insights.

## Why Choose Padvish Base / Corporate?

Padvish Base is a lightweight, stable, and optimized solution for enterprise networks.

Padvish Corporate, with its three critical capabilities — Internet connection detection, trusted network management, and operating system vulnerability analysis — is designed for large organizations with multi purpose IT environments, providing enterprise-grade protection and manageability.

**Shared Features Across Base and Corporate Editions**

**Threat Protection**

- Anti Ransomware
- Anti-Phishing
- Anti-Rootkit
- AI Detections
- Cloud Protection
- Fileless Malware Detection
- USB Malware Protection (UMP)
- BadUSB Protection
- Mail Protection
- MBR Protection

**Policy Enforcement**

- Device Control
- Application Control
- Web Control
- Transfer Monitoring
- Safe Mode Protection
- Backup Protection
- Event Manager
- Internet Connection Detection

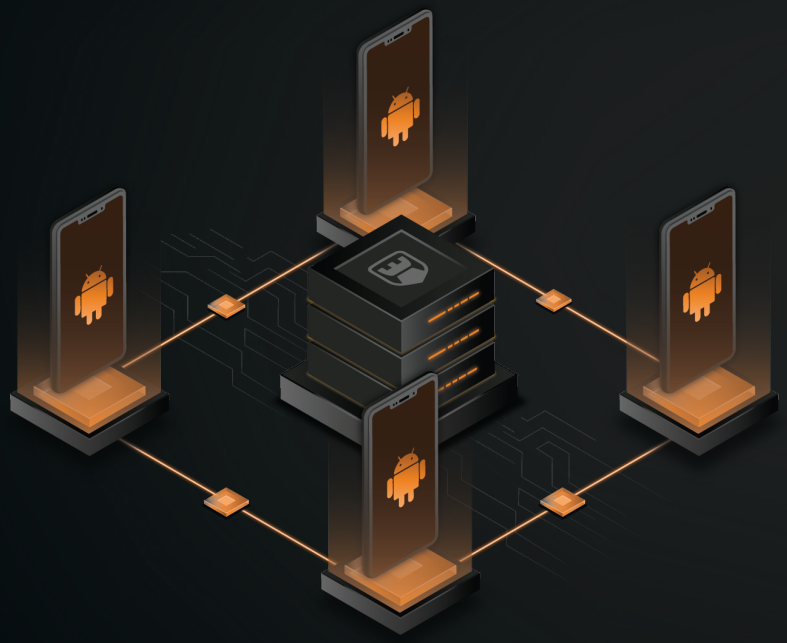
**Management Suite**

- Hierarchical Consoles
- Remote Discovery/Install
- P2P Updates
- Air Gapped Clients
- VDI Support
- Customizable Aggregated Dashboards and Reports
- Unified Management: Windows, Linux, and Android

**Network Protection**

- Network Layer Firewall
- Application Layer Firewall
- Intrusion Prevention System (IPS)
- Automatically blacklist attackers (Shared Folders – RDP session)
- Brute-force Blocker

# Padvish Android Enterprise



Padvish
Android Enterprise

## Enterprise Control, Multi-Layered Security, and Centralized Management for Android Devices

### Organizational Challenges

The widespread distribution of Android devices, unrestricted app installations, and lack of centralized visibility significantly increase the risk of data leak and unauthorized access.

Organizations with geographically dispersed field teams need a solution that enables unified and scalable management of Android device security across the enterprise.

### Amnpardaz Solution

Padvish Android Enterprise delivers multi-layered protection against malware and emerging threats by leveraging artificial intelligence and machine learning technologies.

In addition to unified management, it includes anti-theft features, a built-in firewall, detailed activity reporting, and other advanced controls that collectively form a comprehensive security solution for enterprise Android environments.

This platform unifies security, efficiency, and organizational oversight into a single, centrally managed system.

# Unified Security and Centralized Management

## For Organizational Android Devices

Centralized control and protection of all organizational Android smartphones and tablets

Comprehensive visibility into device security status through the Padvish Management Console

Access to periodic security and usage reports directly from the Padvish Dashboard

Flexible device grouping and independent policy management within the Padvish Console

Centralized and remote enforcement of security configurations through the Padvish Console


## Key Capabilities of Padvish Android Enterprise

Memory optimization and cleanup of unused or temporary files on Android devices

Quick access to activity history within custom time ranges

Cloud-based, full, quick, and custom scanning of files and installed applications

Management and restriction of app internet access across both Wi-Fi and mobile data networks

Extraction and display of detailed information for installed applications

Remote control, monitoring, and location tracking of lost or stolen devices

## Data Protection
Protecting Organizational Data

# Padvish DLP
## (Data Loss Prevention)

Padvish DLP

## Preventing Data Leak and Controlling Data Transfer Channels

### Organizational Challenges

Without centralized oversight of file transfer channels, unauthorized access to and misuse of corporate documents both inside and outside the organization along with insufficient control over networks and peripheral devices, can easily expose sensitive data to exploitation.

Enterprises need a comprehensive solution that protects information in use, in transit, and at rest.

### Amnpardaz Solution

Padvish DLP provides end-to-end control over every potential data leak path across the organization.

Through granular access control, prevention of unauthorized data transfers, peripheral and print device monitoring, trusted network detection, behavioral analysis, and document encryption, the system enforces protection where data moves, is accessed, or stored.

Fully integrated with the Padvish Management Console, it enables centralized policy governance and enterprise-wide data protection enforcement.

## Are you concerned about unauthorized disclosure or leakage of sensitive data and confidential documents?

### Prevent Data Leakage and Protect Confidential Information with Padvish DLP.

Padvish DLP provides multi-layer protection against data exfiltration, ensuring complete control over how your organization's information is accessed, shared, and transmitted.

Protection of Documents Against Unauthorized Access and Inadvertent File Transfer

Protection of Document and Data Content via File Encryption

### Centralized Management and Integration

- Unified Padvish agent and central management console
- Hierarchical console structure with Primary / Secondary configuration
- Client grouping and policy-based configuration for different departments

### Core Capabilities

#### 1 Protecting Data in Use

Logging of all file transfer operations across removable media

Application Control to define authorized / unauthorized software

Real-time collection, monitoring, and searchable visibility of hardware & software assets

Granular control of peripheral devices (USB, external drives, etc.)

Print Control allow, block, or log network printing activities

#### 2 Protecting Data at Rest

- Fine grained access rights management for sensitive files
- Fast, space efficient backup and restore functions
- Protection against ransomware and unauthorized file manipulation

#### 3 Protecting Data in Motion

Intelligent detection of trusted vs. untrusted networks

Prevention of connections to unauthorized Wi-Fi or VPNs

Web access control and blocking of malicious / unauthorized domains

Multi-layer firewall and integrated Intrusion Prevention System (IPS)

# Padvish DRM
## (Digital Rights Management)

Padvish
DRM

## Your Documents Stay Protected Inside and Outside the Network

### Organizational Challenges

Once documents leave the organizational network, governance and visibility over those files diminish drastically.

They can be copied, printed, shared, or accessed by unauthorized individuals without restriction.

To achieve true data security, protection must travel with the file itself, not remain confined within the network perimeter.

### Amnpardaz Solution

Padvish DRM delivers continuous document protection through:

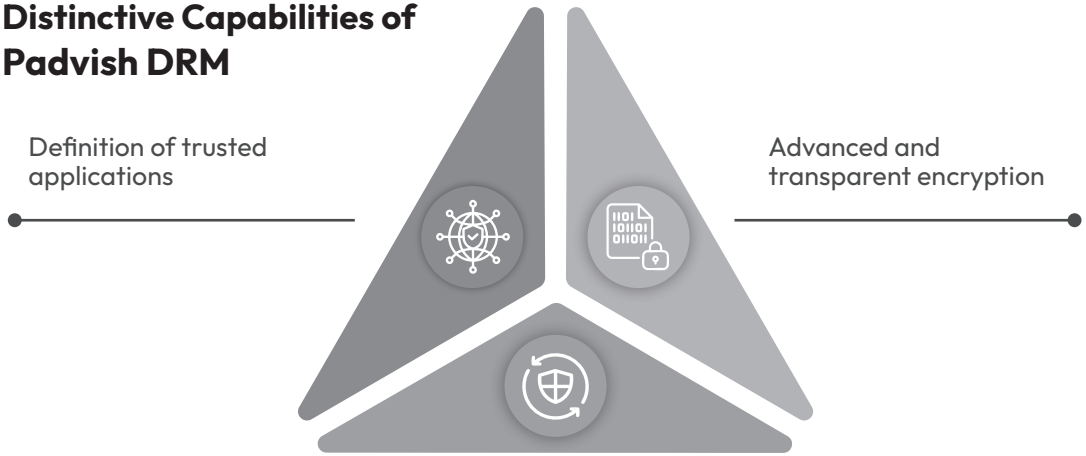
- Content-level encryption ensuring end-to-end confidentiality
- Granular access policy enforcement with centralized key management
- Protected application control and prevention of unauthorized screen capture
- Role-based and permission-based user access control

This enterprise-grade solution maintains organizational ownership and control over every protected file even beyond the corporate network all managed seamlessly through the unified Padvish Management Console.

## Are you confident in the security of your organization's data and confidential documents?

Ensuring the protection of your organization's data and sensitive information against internal and external threats with Padvish Antivirus | Padvish DRM Edition.

### Distinctive Capabilities of Padvish DRM



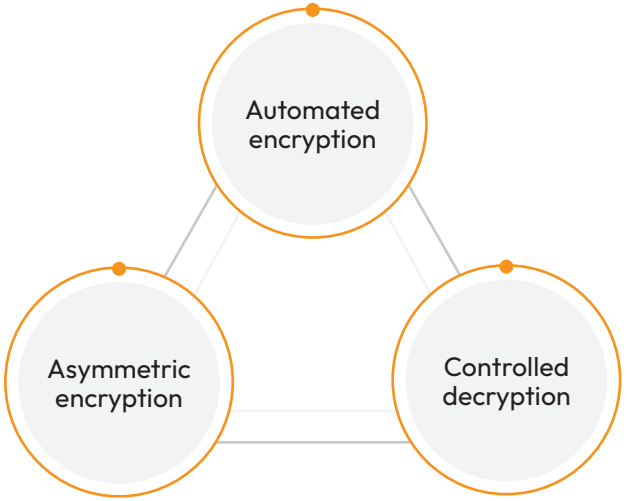

### Digital Content Protection Technologies

- Offline file editing support during temporary network interruptions
- Immediate asymmetric encryption of files upon creation
- Prevention of data leakage through Copy/Paste operations or screenshots
- Centralized encryption management across all endpoints
- Definition of protected applications within controlled environments
- Hierarchical key distribution through multi-level management servers
- Automatic file lockdown if documents are removed or transferred outside the organizational network
- Granular-role and permission-based access control for sensitive data

### Why Padvish DRM?

1. Utilizes cutting-edge encryption and access control technologies to secure organizational data and documents
2. Protects against cyber threats, data theft, and information leakage
3. Fully aligns with organizational security requirements and compliance needs
4. Optimizes internal security processes and data governance workflows
5. Enables secure collaboration and controlled file sharing beyond the network perimeter

### Encryption Lifecycle Management



# Padvish DataGuard™

## Intelligent Data Protection: Proactive Defense & Resilient Security

### Organizational Challenges

Modern organizations face escalating threats from sophisticated ransomware, unauthorized data access (both internal and external), and complex network-based attacks.

The challenge lies in establishing a robust defense that not only reacts but proactively protects.

### Amnpardaz Solution

Amnpardaz presents a next-generation, data-centric security platform engineered to deliver unparalleled protection.

This solution employs five distinct protective layers against ransomware and offers a comprehensive suite of data protection capabilities, underpinned by advanced network policy enforcement.

With a behavioral-driven approach, it ensures superior data security across dynamic organizational networks.
Designed for seamless integration, this platform coexists fully with your existing security infrastructure and incorporates all core Padvish functionalities, excluding the antivirus module.

Consequently, it stands as the definitive choice for organizations that prioritize data integrity and ransomware resilience, seeking to augment their current security posture with a highly reliable and dependable data protection solution.

Padvish DataGuard™

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

# Padvish DataGuard™

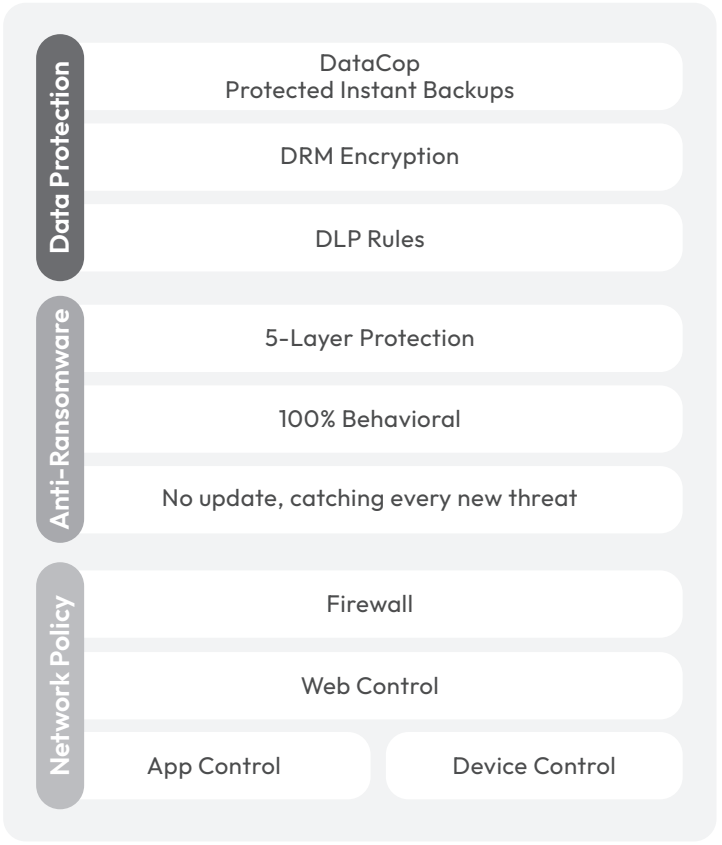
## Product Architecture

The solution is built on a multi-layered, behavior-driven architecture that continuously monitors process behavior, file system changes, abnormal disk activities, and encryption patterns to identify and neutralize threats before they cause damage.

| Data Protection | 1 |
|---|---|
| DataCop Protection | Fully automated, high-speed, secured backups with ultra-low disk footprint. |
| DRM Encryption | Transparent, automatic encryption instantly applied upon file creation. |
| DLP Rules | Precise data access policy definition and enforcement across all endpoints. |

| Anti-Ransomware | 2 |
|---|---|
| Tamper Protection | Blocks unauthorized encryption and file modifications. |
| Backup Protection | Lightweight, high-speed backup utilizing Windows VSS technology. |
| MBR Protection | Guards the Master Boot Record against malicious alterations. |
| Bait Mechanism | Detects ransomware behaviors via intelligently designed decoy files. |
| BitLocker Protection | Prevents abuse of Windows built-in encryption. (This proprietary component was introduced to the cybersecurity domain for the first time through this product.) |

| Network Policies | 3 |
|---|---|
| Firewall | Dual-layer protection controlling inbound and outbound traffic within the Windows architecture. |
| Web Control | Smart prevention of access to unauthorized or malicious domains. |
| App Control | Application Control policies on endpoints to prevent the execution of unauthorized programs. |
| Device Control | Comprehensive management of peripheral and external devices with full policy enforcement. |




## Key Security Deliverables

- Multi-layered, data-centric protection across servers and endpoints
- Prevention of sensitive data leaks via integrated DLP enforcement
- Granular, centralized access management for users and applications
- Behavior-oriented threat detection, no constant signature updates required
- Effective mitigation of ransomware impact and prevention of large-scale data loss

# Padvish vKiosk™

## Secure and Controlled Virtual Gateway for File Entry — No Hardware Required

### Organizational Challenges

Removable media remain among the most frequent attack vectors introducing malware or unauthorized content into enterprise networks.

Without a dedicated intermediary layer for behavioral inspection, mult-stage scanning, and policy enforcement, these files can compromise systems even before detection.

Many organizations attempt to address this problem with physical security kiosks. However, frequent user interaction, geographical dispersion of kiosk devices, increased operational traffic, and recurring maintenance costs all add complexity and inefficiency to daily operations.

### Amnpardaz Solution

Padvish vKiosk™ creates a secure, isolated, and fully virtual file transfer gateway, eliminating the need for any physical hardware deployment.

Before files reach organizational endpoints, they are thoroughly inspected through USB access control, multi-engine scanning, policy-based file verification, and user behavior analysis.

The result is a seamless and controlled entry point for removable media, delivering enterprise-grade security with simple management, centralized visibility, and zero hardware maintenance overhead.

Padvish
vKiosk™

# Padvish vKiosk™

## Product Architecture

Padvish vKiosk™ acts as a secure intermediary station between removable media and Windows systems.

Instead of connecting USB devices directly to organizational endpoints, all file exchanges are routed through Padvish vKiosk™, ensuring that every transfer is inspected, validated, and controlled.

**1** **File Selection:**
Users submit selected files through Padvish vKiosk ™ to the Padvish Management Server.

**2** **Analysis & Decision Making:**
The server examines files using multiple antivirus engines and evaluates them against established organizational security policies.
**The result:** allow, block, or access with restrictions.

**3** **Secure Delivery or Blocking:**
Approved files are made available to target systems under controlled conditions; blocked items are quarantined, and all events are logged.

This architecture forms a robust operational isolation layer, ensuring that malware or unauthorized files are intercepted well before reaching the organizational clients.

## Key Capabilities

### Advanced Event Reporting & Analytics

Log and analyze all removable media activities to strengthen policy design and meet security or compliance requirements.

### Pre-Transfer File Inspection for Inbound and Outbound Flow

Evaluate all files against organiztioal rules before import or export to ensure no unverified data crosses network boundaries.

### File Type Control & Unauthorized Content Blocking

Define allowed file types and prevent movement of unwanted formats or classified data.

### USB Access Management & Restriction

Enforce full control over removable media connections on kiosk stations and other sensitive systems.

### Multi-Engine Scanning Pre-Transfer

Every file is scanned by multiple antivirus engines prior to network exposure to maximize threat detection accuracy.

## Use Cases

1. Organizations operating shared workstations or kiosk environments
2. Data sensitive sectors requiring strict file intake controls
3. Enterprises with auditing and traceability mandates

## Key Security Deliverables

- **Preemptive USB Malware Protection**

Threats from removable media are identified and blocked before reaching Windows endpoints, forming a secure intermediary layer between incoming files and systems.

- **Data Leak and Unauthorized Transfer Prevention**

Granular file type policies stop sensitive or confidential data from leaving the organization.

- **Custom Security Policies per User and Device**

Define differentiated rules based on role, organizational unit, or workstation type for business aligned control.

- **High Accuracy Threat Detection via Multi-Engine Scanning**

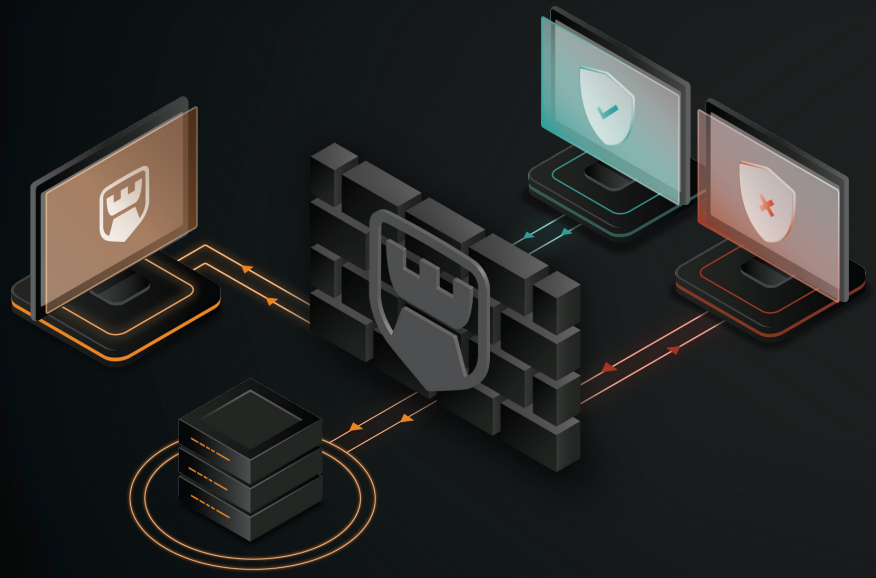
Combining several detection engines dramatically reduces the chance of malware or malicious files bypassing defenses.

- **Comprehensive Reporting & Management Insights**

Behavioral data, event logs, and usage patterns of removable media enable continuous improvement of policies and organizational security maturity.

## Network Protection
Securing Organizational Communications and Networks

# Padvish NAC
## (Network Access Control)



Padvish NAC

## Intelligent Network Access Control Based on Real-Time Device Security Posture

### Organizational Challenges

Unsecured devices lacking antivirus protection, missing critical patches, or exposing open ports can compromise the network before being detected.

Organizations need a layer that verifies both the device's security posture and the user's identity before connection, preventing unauthorized pathways or policy bypasses from being exploited.

### Amnpardaz Solution

Padvish vKiosk™ creates a secure, isolated, and fully virtual file transfer gateway, eliminating the need for any physical hardware deployment.

Before files reach organizational endpoints, they are thoroughly inspected through USB access control, multi-engine scanning, policy-based file verification, and user behavior analysis.

The result is a seamless and controlled entry point for removable media, delivering enterprise-grade security with simple management, centralized visibility, and zero hardware maintenance overhead.

# Padvish NAC

## Product Architecture

Padvish NAC is a next-generation network access control system that continuously assesses the security posture of client devices and integrates with the Padvish Management Server (PMS) before granting network access.

## The NAC architecture is implemented across three layers:

1. **Client Compliance Check**
   Verifies Padvish activation, last PMS synchronization, operational status of security modules, and compliance with minimum protection requirements for network access.

2. **Actuator Layer**
   Implements decisions to allow, restrict, or block access; supports simultaneous use of multiple actuators; and enforces network level communication policies based on the device's verified security posture.

3. **PMS Integration**
   Maintains persistent and secure communication with the Padvish Management Server for real-time client health monitoring, event logging, and policy reporting.

This layered architecture ensures that only devices meeting the organization's security standards can access the network.

## Key Use Cases

- **Enterprise Networks Requiring Client Health Enforcement:** Prevents connection of outdated systems, devices without antivirus, or unpatched endpoints.
- **Organizations with Multiple Sensitive Access Points:** Ensures that only healthy clients can access critical zones.
- **Preventing lateral malware movement across the internal network:** Identifies and isolates infected devices before they cause damage.
- **Companies with Multiple Security Actuators:** Enables access control based on combined security criteria.

## Why Padvish NAC?

Unlike legacy NAC approaches that rely solely on MAC addresses or static network policie, Padvish NAC leverages PMS as a central security health authority.

Access decisions are based on the realtime security posture of each endpoint, not merel its network identity ensuring that network access is controlled by actual security health.

## Key Capabilities

**Intelligent Access Control**
- Executes allow/deny decisions based on the device's real-time security posture.

**Client Health Assessment**
- Verifies Padvish activation and the status of core protections (antivirus, firewall, EDR) before network connection.

**Multi Actuator Support**
- Enables simultaneous use of multiple actuators for stricter network control.

**Anomalous State Detection**
- Blocks devices that have disabled security modules, remain offline from PMS for extended periods, or exhibit suspicious connect/disconnect behavior.

**Reporting and Management Analysis**
- Records every decision, block, alert, and status change in PMS for compliance and security analytics.

## Key Security Deliverables

- Reduced Internal Threat Propagation by restricting access to only compliant devices.
- Automated Decision Making eliminates manual intervention and improves operational efficiency.
- Rapid Isolation of Non-Compliant Endpoints devices with inactive modules or missing PMS check-ins are quickly contained.
- Lower Security Team Workloadthrough real-time monitoring and automatic policy enforcement.

# Padvish Mail Gateway

## Multi-Layer Email Protection Powered by Padvish Intelligent Technology

### Organizational Challenges

Email remains one of the primary vectors for malware, phishing, spam, and targeted attacks.

Without a pre-delivery protection layer that blocks malicious attachments, links, and code before reaching users, organizations remain vulnerable to ransomware, data exfiltration, and advanced persistent threats (APTs).

### Amnpardaz Solution

Padvish Mail Gateway applies multi-layer scanning, intelligent malware detection, phishing and spam prevention, and AI-driven quarantine to analyze and sanitize all inbound email content before it reaches user inboxes.

This ensures secure, stable, and trustworthy communication across the organization.

Padvish
Mail Gateway

# Padvish Mail Gateway

## Product Architecture

Padvish Mail Gateway is a multi-layer security gateway that analyzes the entire content, attachments, links, and embedded elements of each email before it reaches the organizational mail server.

When a threat behavior or pattern is detected, the email is blocked or quarantined at the pre-delivery stage.

### The core architecture of Padvish Mail Gateway consists of three key layers:

**Content Analysis**

- Real-time scanning of email text
- HTML content analysis
- Detection of embedded scripts, URLs, and web bugs
- Detection of phishing indicators and fraudulent landing pages

**Attachment Analysis**

- File scanning using Padvish's advanced security engine
- Detection of known, emerging, and ransomware threats
- Prevention of high risk file types according to organizational policy

**Sender Domain and Server Analysis**

- Verification of the sender domain's authenticity
- Assessment of sender behavior against spam and phishing patterns
- Blocking of spoofed or forged emails

① ② ③

These three layers intercept and eliminate the majority of email borne attacks before they reach the organizational network.

## Use Cases

- **Banks and Financial Institutions –** Prevent banking phishing, fake portals, and credential theft.
- **Large Organizations with High Email Volume –** Reduces workload on security teams and blocks malicious messages before delivery.
- **Governmental and Industrial Entities at High Risk of APT –** Creates a pre delivery layer that neutralizes most targeted attacks early.
- **Organizations with Security Compliance Needs –** Supports quarantine, reporting, and precise email tracking.

## Why Padvish Mail Gateway?

PMG is the only solution built on the Padvish security platform that simultaneously combines three layers — content inspection, attachment analysis, and sender domain evaluation.
By focusing on real world threats such as phishing, targeted spam, and ransomware via attachments, it provides a comprehensive defensive shield against modern email borne attacks.

## Security Outcomes for the Organization

- Proactive prevention of phishing, ransomware, and spam before user exposure.
- Significant reduction of the overall email attack surface.
- Increased trust and security in communications without disrupting user workflows.
- Comprehensive reporting for transparent, data driven security decisions.
- Improved efficiency of security teams through fewer false positives and pre delivery blocking of threats.

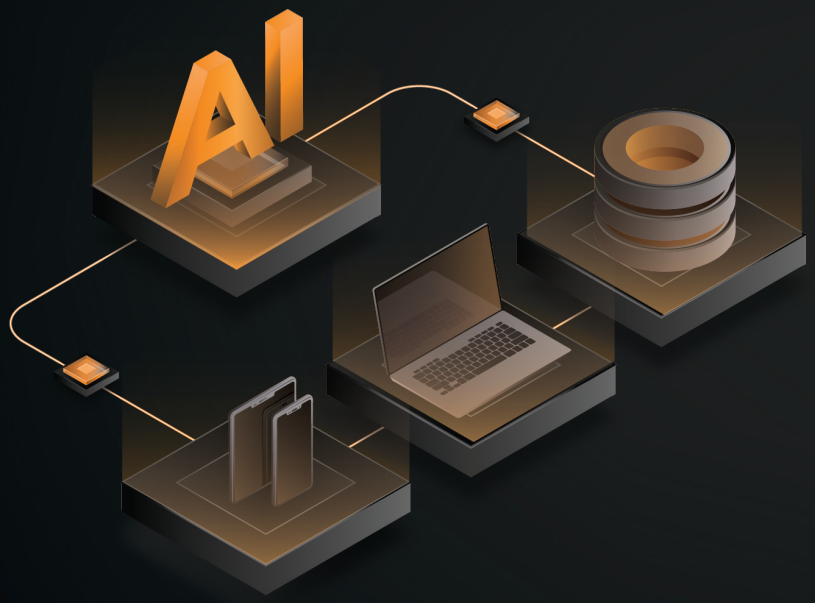
## Key Features

1. **Anti-Phishing**
   Detection of fraudulent pages, fake payment gateways, manipulated links, and social engineering attempts.
2. **Anti-Spam and Malicious Email Filtering**
   Prevents entry of spam, infected advertisements, and risky bulk messages.
3. **Multi-Layer Attachment Anti-Malware**
   Multi-layer scanning of all attachments prior to inbox delivery, including miners, ransomware, worms, Trojans, and tampered files.
4. **Quarantine and Suspicious Message Management**
   Administrators can review, release, or delete high risk emails.
5. **Blocking of High Risk Files per Policy**
   Organizations can define sensitive or risky file types; PMG enforces blocking automatically.
6. **Full Integration with Padvish Infrastructure**
   Security events and telemetry are synchronized with the Padvish management console for centralized analytics and decision making.

# Intelligent Detection and Response Systems

Identifying, analyzing, and responding to cyber threats

## Padvish EDR AI




## Independent and Intelligent Detection & Response Platform

### Organizational Challenges

Fileless attacks, multi-stage intrusion campaigns, and suspicious behaviors often evade traditional endpoint protection tools such as antivirus software.

To combat these evolving threats, organizations require behavioral visibility, comprehensive event telemetry, and AI-driven analytics.

### Amnpardaz Solution

Padvish EDR AI leverages continuous behavioral monitoring, AI-powered analytics, integrated workflows, and rapid automated response to detect, contain, and remediate advanced threats.

It provides security teams with complete operational visibility, empowering proactive threat detection and response before compromise occurs.

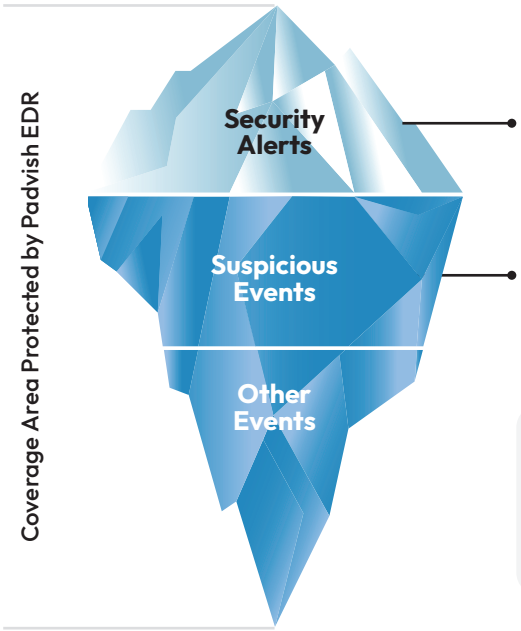
Padvish
EDR AI

EDR TELEMETRY

AV TEST av-test.org APPROVED ADVANCED ENDPOINT DETECTION & RESPONSE WINDOWS

# Intelligent Threat Detection and Response Systems

## Artificial Intelligence Empowering Cybersecurity




Only a small portion of alerts are reported by tools such as antivirus software, firewalls, and other traditional security solutions.

Advanced threats often evade detection by standard alert mechanisms.

While traditional tools remain essential, they alone are insufficient to defend against sophisticated cyberattacks and intrusion attempts.

## Padvish EDR AI Product Capabilities

1. Threat Hunting Assisted by AI.
2. Offers security analysts AI-powered recommendations to respond effectively to cybersecurity incidents.
3. Analyzes event logs and explains suspicious findings in clear, natural, human readable language.

### Cost Reduction

- Threat Detection
- Threat Hunting
- Reporting

### More Accurate Detection

- Complex and previously unknown malware
- Unusual behavioral patterns

### Increased Efficiency

- For SOC teams
- Automated analysis of security events

### Human Resource Optimization

- Improves operational efficiency without requiring additional personnel

## Padvish EDR AI Technologies and Modules

| | | |
|---|---|---|
| Anti-Malware | Memory Scanning Engine | Behavioral Protection |
| Event Correlation Analyzer | Machine Learning | Intrusion Prevention System |
| Static File Analyzer | Hybrid Antivirus Engine | Sandbox |

## Padvish CyberGPT™ Components

| | |
|---|---|
| Search Assistant | Script Analyzer |
| Log Analysis Assistant | Event Analysis Assistant |
| Sandbox Analysis Assistant | |

# Padvish XDR AI

## Integrated AI-Powered Detection and Response Platform

### Organizational Challenges

This solution provides a comprehensive response to the challenges caused by fragmented security tools and dispersed security data across organizations.

In isolated and standalone approaches, the overwhelming volume of alerts from multiple sources often prevents security teams from timely identifying and mitigating complex, multi-stage threats.

### Amnpardaz Solution

By consolidating data from endpoints, networks, internet services, and cloud environments and by leveraging advanced artificial intelligence and machine learning, the platform detects complex and suspicious behavioral patterns and delivers centralized, holistic visibility into cyber threats.

Through deep data correlation and automated response processes, it enables the detection of threats that often evade traditional isolated solutions, accelerating threat discovery, analysis, and remediation.

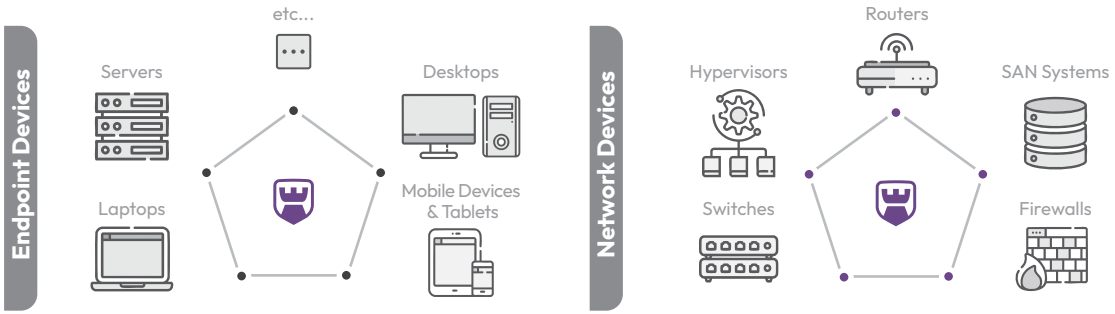
Padvish
XDR AI

EDR TELEMETRY

AV TEST av-test.org APPROVED ADVANCED ENDPOINT DETECTION & RESPONSE WINDOWS

# Smart Detection and Response Systems

## Padvish eXtended Detection and Response (XDR)




## Padvish CyberGPT™

1. Sandbox Analysis Assistant
2. Script Analyzer
3. Search Assistant
4. Event Analysis Assistant
5. Log Analysis Assistant

- Anti-Malware
- Memory Scanner
- Behavior Protection
- Machine Learning
- Network Attacks Detection (HIPS)

**Padvish**
Extended Technologies

- Sandbox
- Device Sensor
- Static File Analyzer
- Detection Engines
- Network Sensor

## Padvish XDR AI Technologies and Modules

**Leveraging Artificial Intelligence for Decision Making, Analysis, and Rapid Threat Response**

- Interprets XDR system security events and logs in natural language
- Understands technical concepts and security data structures
- Accelerates event analysis and helps prevent security incidents
- Suggests actions to security analysts for incident response

## Key Capabilities of Padvish XDR AI

### 1 Comprehensive Visibility and Centralized Analysis

- Provides an integrated view of security status across all layers (endpoints, infrastructure, and network).
- Identifies suspicious behaviors by correlating data and events across systems.
- Analyzes data from multiple independent sources in a centralized manner.
- Allows custom rule definition tailored to organizational requirements.

### 2 Productivity Enhancement

- Reduces false alerts and focuses analyst attention on genuine threats.
- Improves Security Operations Center (SOC) efficiency through automation and AI assistance.
- Increases speed and accuracy in threat detection, investigation, and response.

### 3 Advanced Threat Detection

- Detects complex and multi-stage attacks across heterogeneous environments.
- Employs AI and machine learning-based behavioral analysis.
- Identifies hidden threats within large volumes of data and events.
- Leverages up-to-date advanced threat intelligence feeds for comprehensive coverage.

### 4 Proactive Defense

- Prevents intrusions and data leaks before damage occurs.
- Detects and blocks threats often overlooked by traditional tools.
- Provides centralized analysis, detection, and automated response capabilities.
- Supports advanced incident management and workflow coordination.
- Replaces fragmented, siloed security architectures with coordinated, multi-layer protection.

# Managed Detection and Response Solutions

Managing Detection & Response Systems

## Padvish MDR

## AI-Driven EDR Managed Service
## 24×7 Monitoring & Accelerated Response

### Organizational Challenges

As cyberattacks and advanced threats continue to evolve, the need for high level defense capabilities has become more critical than ever.
Because these attacks often blend sophisticated technologies with human tactics, most organizations find it impossible to counter them through a single product or isolated service.

Effective defense requires a managed solution that combines cutting-edge technology with experienced cyber defense professionals capable of continuous threat monitoring and rapid incident response.

### Amnpardaz Solution

The Padvish MDR (Managed Detection and Response) solution offers a centralized and secure threat detection and mitigation platform, fully managed by Amnpardaz's cybersecurity experts.
Built on rich telemetry and in depth data collected by Padvish security products across organizational endpoints and network systems, it performs data tagging, aggregation, correlation, alert generation, and visualization in a unified environment.

Leveraging threat intelligence and insights from past cyber incidents, Padvish MDR detects intrusions early and halts adversarial activity before it can spread within the network.

Through deep data correlation and automated response processes, it enables the detection of threats that often evade traditional isolated solutions, accelerating threat discovery, analysis, and remediation.

Padvish
MDR

EDR TELEMETRY

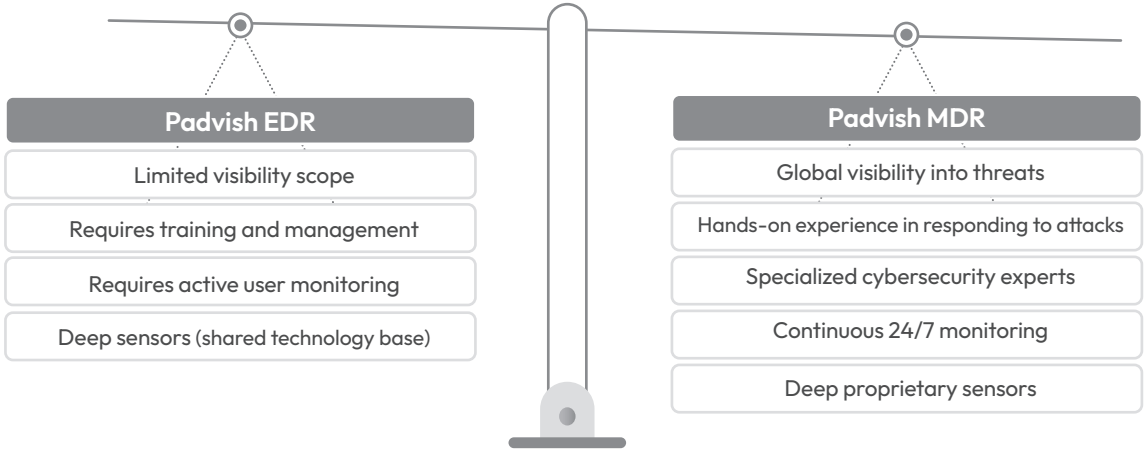
AV TEST av-test.org APPROVED ADVANCED ENDPOINT DETECTION & RESPONSE WINDOWS

# Managed Detection & Response (MDR) Solutions

## Is your organization fully prepared to detect and respond to cyberattacks?

Padvish Managed Detection and Response (MDR) services provide organizations with access to top-tier cybersecurity experts who have demonstrated success in countering the most sophisticated cyberattacks.

## Comparison of EDR and MDR Technologies




Padvish delivers a Managed Detection and Response solution that integrates the latest AI-driven cybersecurity technologies with the expertise of elite in-house cybersecurity experts, ensuring 24/7 continuous protection against advanced threats.

Responding to sophisticated cyberattacks requires seasoned cybersecurity experts.

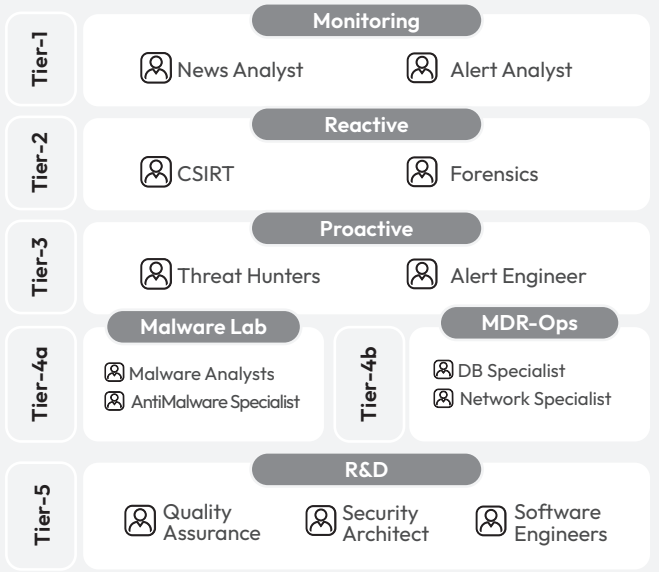
## Why Padvish MDR?

1. Strong Service Level Agreement (SLA) commitment
2. Enhanced organizational security
3. Operational cost reduction
4. Deep visibility via Padvish sensor
5. Continuous monitoring
6. Strengthened overall protection
7. Dedicated security specialists

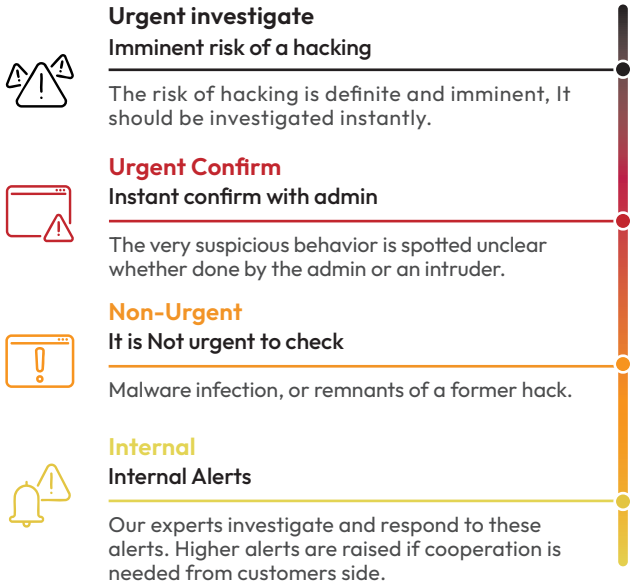
### You Are Not Alone Against Hidden Cyber Threats

The Padvish Security Team stands beside your organization to identify, analyze, and counter a diverse range of hidden cyber threats.

## Padvish MDR Operational Tiers




## Alert Levels



# Padvish MXDR

## Managed and Integrated Enterprise Detection and Response Solution

### Organizational Challenges

In many organizations, the sheer volume of security events, the dispersion of threat intelligence across multiple layers, and the shortage of skilled cybersecurity professionals lead to complex attacks being detected late or remaining completely unseen.
The use of heterogeneous security tools, lack of integration between network, endpoint, internet, and cloud data, and the absence of continuous monitoring prevent Security Operations Centers (SOCs) from effectively detecting multi-stage threats, while operational workloads on security teams continuously rise.

### Amnpardaz Solution

The Padvish Integrated and Intelligent Detection and Response Center leverages the analytical power of the XDR AI platform combined with a team of expert security operations analysts to deliver 24/7 continuous monitoring.

This solution streamlines and correlates data from networks, endpoints, internet services, and cloud environments within a unified analytical workflow, enabling comprehensive, real-time threat detection and response across the organization.

Padvish
MXDR

EDR
TELEMETRY

AV TEST
av-test.org
APPROVED
ADVANCED
ENDPOINT
DETECTION &
RESPONSE
WINDOWS

# Managed Extended Detection & Response (MXDR)

## Does Your Organization Have the Internal Resources to Handle Sophisticated Cyberattacks?

Padvish MXDR centralized managed services empower organizations to operate their security tools in a coordinated and unified manner, utilizing an enterprise-grade protection approach without relying on extensive internal resources.

This enables a comprehensive strategy for safeguarding data and critical infrastructure against modern threats.

## Comprehensive Padvish Cybersecurity Solutions

| Solution Name | EPS without Anti-Malware | Anti-Malware Base Platform | Vulnerability Assessment | EDR Engines | Managed Protection | XDR Engines |
|---|---|---|---|---|---|---|
| Padvish DataGuard | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Padvish Base | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Padvish Corporate | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Padvish EDR Base/Select/Expert | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Padvish MDR Optimum | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| Padvish MDR Base/Select/Expert | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Padvish XDR | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Padvish MXDR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**Alert Priority & Response SLAs**

**Urgent investigate**
**Imminent risk of a hacking**

The risk of hacking is definite and imminent, It should be investigated instantly.

**Urgent Confirm**
**Instant confirm with admin**

The very suspicious behavior is spotted unclear whether done by the admin or an intruder.

**Non-Urgent**
**It is Not urgent to check**

Malware infection, or remnants of a former hack.

**Internal**
**Internal Alerts**

Our experts investigate and respond to these alerts. Higher alerts are raised if cooperation is needed from customers side.

**Padvish MXDR Technologies and Services**

- 24/7 Security Experts
- Exclusive Threat Intelligence
- SLA backed Protection

**Core Technologies:**

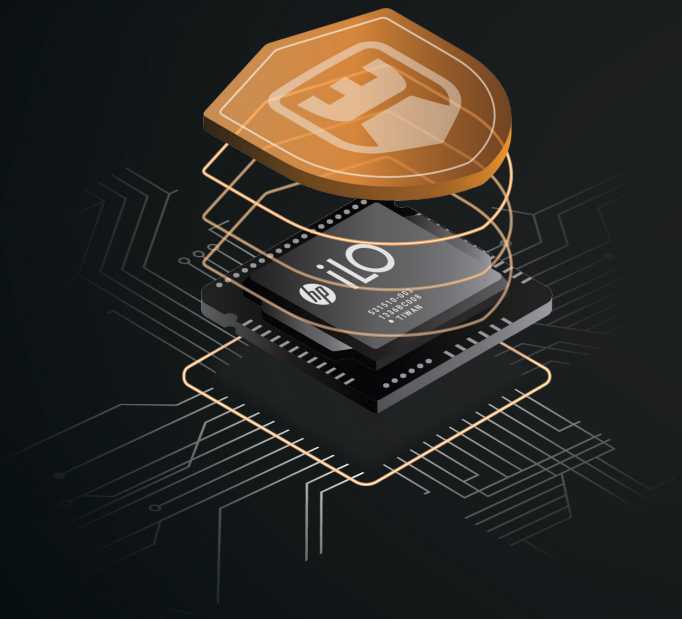
- Anti-Malware Engines
- Memory Scanner
- Behavior based Protection
- Machine Learning
- Network Attack Prevention
- Network Sensor Framework
- Dynamic Sandbox Environment
- Static File Analyzer
- Appliance Sensor Integration
- Detection Engines
- CyberGPT™ AI Model

## Key Capabilities of Padvish MXDR

- Continuous 24/7 network monitoring performed by seasoned security experts for advanced persistent threat (APT) detection.
- Ongoing support from dedicated security teams ensuring rapid incident response and continuous system optimization.
- Accelerated extraction of critical intelligence for informed, high speed decision making during crises.
- Reduced workload for internal security teams through intelligent automation of analysis and response workflows.
- Secure sandbox inspection enabling safe detection of suspicious files without risking production systems.
- Minimized false positives via multi engine antivirus correlation and result validation.
- Unified integration across diverse security tools, eliminating dependency on large internal infra-structures.
- Close collaboration with SOC specialists to strengthen cyber defense effectiveness.
- Cost effective replacement for organizations lacking a fully staffed internal Security Operations Center (SOC).

## Infrastructure Protection
Securing Organizational Servers

# Padvish iLO Scanner




Padvish
iLO Scanner

## Detection of Hardware-Level Compromise; Validation and Cleansing of iLO Firmware in HP Servers

### Organizational Challenges

The Integrated Lights Out (iLO) module in HP ProLiant servers remains active even when the server is powered off, maintaining full access to all system components from firmware and hardware layers to the operating system.

This exceptional level of access, combined with the absence of effective firmware inspection and integrity verification tools, introduces serious cybersecurity risks:

- Hardware-level malware such as iLOBleed can remain deeply hidden.
- Firmware updates may fail to remove or neutralize the infection.
- Data destruction, operational sabotage, or even espionage becomes possible.
- Conventional security solutions are incapable of detecting such threats.
- Infections may stay concealed from network administrators for months or even years.

If compromised, iLO can inflict irreversible damage on critical infrastructure and organizational reputation.

### Amnpardaz Solution

Following the global discovery of iLOBleed by Amnpardaz, the cybersecurity community recognized the pressing need for a precise, hardware-based, independent tool dedicated to direct firmware analysis.

Padvish iLO Scanner is a hardware-level, standalone, portable device designed to connect directly to the NOR Flash chip without powering on the server.
It performs in-depth integrity inspection of the firmware and validates the security health of the system.

This powerful tool represents the culmination of Amnpardaz's multidisciplinary expertise integrating firmware analysis, reverse engineering, hardware design, and software development into a single, reliable solution for infrastructure-level protection.

# Padvish iLO Scanner

## Device Operating Method

Padvish iLO Scanner connects directly to the NOR Flash chip using a dedicated, precision-engineered clip designed for secure and reliable hardware interfacing.

## Operational Steps

1. Direct firmware acquisition from the chip
2. Rapid, real-time analysis using a proprietary Amnpardaz algorithm
3. Delivery of a detailed firmware authenticity and security status report
4. Removal of potential hardware-level infections
5. Update to the latest validated HP firmware version

## Use Cases


1. Ensuring the security and integrity of HP ProLiant servers
2. Continuous monitoring of firmware health and authenticity in data centers
3. Utilized in security audits and periodic compliance inspections
4. Performing rapid firmware analysis without interrupting live services

## Key Capabilities

### Advanced Protection

- Direct monitoring and inspection of iLO firmware
- Verification of firmware authenticity and integrity
- Detection of hardware-level rootkits (e.g., iLOBleed)
- Safe cleansing of potential firmware compromises

### Secure Operation

- Safe connection without the need to power on the server
- Automatic detection of incorrect clip attachment to prevent short circuits
- Direct board level access without removing any components

### Functional Design

- Fully standalone operation — no computer required
- 3.4 inch touch interface for intuitive operation
- Portable design with dual high-capacity battery modules
- SD Card support for secure report storage

### Compatibility

- Supports HP ProLiant Gen8 – Gen11 servers
- Compatible with iLO 4, iLO 5, and iLO 6 firmware versions

# Operational Technology Protection

Comprehensive Security for Operational Environments

## Padvish OT


Padvish
OT

## Protection of Operational Systems

### Challenges in Operational Organizations

Security standards within the Operational Technology (OT) domain, though essential, are not sufficient to counter advanced or persistent cyber attacks. In industrial settings, critical servers and online devices operate continuously as part of tightly interconnected networks.

This constant operation leads to increased exposure to vulnerabilities, inaccurate threat detection due to the lack of behavioral analytics, and a pressing need for rapid access to systems factors that collectively heighten the risk of cyber incidents.

Moreover, the inability to deploy security protections without system reboots, combined with the requirement for uninterrupted operational availability, creates significant challenges for industrial and mission critical organizations.

### Amnpardaz Solution

Padvish OT is a comprehensive cybersecurity platform purpose-built for operational technology (OT) and industrial environments to address the unique challenges outlined above.

The platform delivers a full suite of advanced security capabilities, including:

- Defense of critical operational infrastructure
- Multi-layer, AI-driven threat protection
- Data, network, and isolated environment security
- Unified management and centralized control across all protected assets

Furthermore, Padvish OT is engineered for seamless compatibility with legacy and resource-constrained systems, ensuring sustained security, continuous production, and uninterrupted operations — even in the most demanding industrial contexts.

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

# Padvish OT

## Product Architecture

### Host System Protection Layer

- Advanced real-time protection
- AMSI support and removable media (USB) control
- Intelligent multi-layer anti-ransomware engine certified by AV-TEST Germany for 100% ransomware detection accuracy

### Application and Network Protection Layer

- Application control
- Device control
- Web control
- Trusted networks definition
- Firewall protection

### Centralized Management and Response Layer

- Full support for isolated (Air Gapped) environments
- Predefined configuration profiles
- Compliance assistance tools
- Centralized incident management and policy control

### Monitoring and Behavioral Analysis Layer

- Registry access monitoring
- Continuous operating system vulnerability assessment
- Detection of unauthorized internet connections

### Specialized Industrial Security Layer

- Centralized management
- Detection-only passive monitoring
- Integrates with Amnpardaz MSSP/MDR services

## Why Padvish OT?

Padvish OT combines advanced network protection, fileless threat prevention, and real-time risk management — purpose-built for industrial environments where latency sensitivity and non-reboot constraints are critical requirements.

Upon detection of vulnerabilities, the solution enables immediate mitigation and automated security enforcement, while providing administrators with comprehensive control over data collection and incident analysis.
It safeguards the entire industrial operational chain, ensuring business continuity and secure production processes.

## Key Capabilities

1. **Continuity**
   Maintains high service availability with minimal impact on response time in real-time industrial systems.

2. **Installation Without Restart**
   Allows installation and configuration without rebooting critical equipment, minimizing downtime in time-sensitive environments.

3. **Operational Resilience**
   Improves resilience and service continuity during cyber incidents, supporting rapid recovery and operations restoration.

4. **Integrated Protection**
   Unifies traditional security layers — antivirus, firewall, application control, and device control — with OT-specific capabilities in a single, integrated platform.

5. **Centralized Risk Management**
   Provides a centralized management environment for visibility and control of distributed industrial assets, enabling policy orchestration and rapid threat response.

6. **Legacy Operating System Compatibility**
   Optimized for Windows XP SP3+, Windows 7 SP1+, and later versions, ensuring reliable protection for resource limited legacy systems.

7. **Critical Infrastructure Compatibility**
   Designed for critical infrastructure, fully isolated (Air Gapped) networks, and real-time control systems that cannot tolerate operational interruption.

# Cloud Protection – CloudGuard

Intelligent protection for networks, platforms, and data

## CloudGuard

Cloud Guard

## Cloud Protection and Threat Intelligence for Organizations

### Organizational Challenges

Cyberattacks are no longer confined to internal networks.

An expanding range of sophisticated threats targets online services and applications across every industry sector.

### Amnpardaz Solution

Amnpardaz CloudGuard delivers an integrated and comprehensive cloud security solution that safeguards websites and networks against advanced and evolving threats.

CloudGuard leverages cutting-edge technologies — firewall capabilities, CDN and WAF services, anti-DDoS systems, and threat intelligence integration — to ensure security, availability, and resilience across customers' digital infrastructures.

# CloudGuard Cloud Protection

## Intelligent protection for networks, platforms, and data

### Managed Security Services (MSSP)

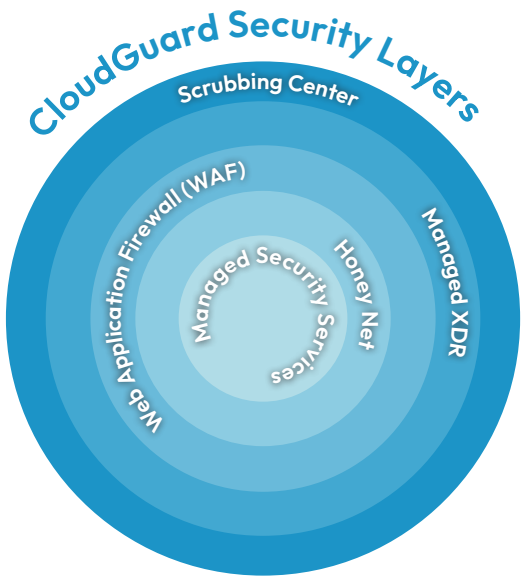
This service enables organizations to elevate their IT security through 24/7 monitoring, incident management, vulnerability assessment, the use of honeypots for attacker engagement and identification, cyber intelligence for threat anticipation, and advanced technologies such as NDR (Network Detection and Response), EDR (Endpoint Detection and Response), and MXDR (Managed Extended Detection and Response).

By leveraging these solutions, organizations can utilize advanced monitoring and analytical tools to detect and respond to cyber threats effectively.

### Honey Net

The HoneyNet service is an advanced security technology intentionally designed by CloudGuard to attract threat actors.

It consists of a coordinated set of decoy systems and networks that function collectively as a sophisticated bait, enabling precise threat identification and intelligence gathering on exploitation techniques.




### Web Application Firewall (WAF)

CloudGuard's WAF provides an advanced, resilient security layer for web applications against complex attacks such as SQL Injection, Cross-Site Scripting (XSS), and HTTP Flood.

Positioned between users and web applications, this layer intelligently analyzes and filters HTTP and HTTPS traffic to prevent potential threats.

### Managed XDR

The CloudGuard MXDR service offers 24/7 monitoring and real-time response to cyber threats by combining artificial intelligence with advanced analytics.

Integrating NDR, EDR, and cyber intelligence, this solution identifies and mitigates complex attacks in their early stages, delivering comprehensive and intelligent security coverage.

### Scrubbing Center

CloudGuard's Scrubbing Center cleans incoming traffic at layers 3 and 4 using highly precise and intelligent rules, providing a robust barrier against all types of threats.

Leveraging substantial bandwidth and processing capacity within CloudGuard data centers, it ensures uninterrupted and resilient protection against large-scale distributed denial-of-service (DDoS) attacks.

Over the past year,

**— CloudGuard has identified —**

and repelled over

**560,000 cyberattacks**

## NetSpine

## Intelligent Technology

The unique NetSpine technology is an advanced and automated system designed to respond to all cyber and network threats.

By collecting and extensively analyzing data and events, monitoring security incidents, and correlating complex event relationships, it enables intelligent decision making and timely, effective responses.

### Capabilities

- Intelligent identification of unauthorized users
- Comprehensive system inspection from the lowest to the highest operational layers
- Detection of previous compromises, including zero-day exploits

## Why Do Organizations Choose Amnpardaz?

Cutting-edge products built on global technology

Tailored security solutions for every organization


24/7 availability and responsive service

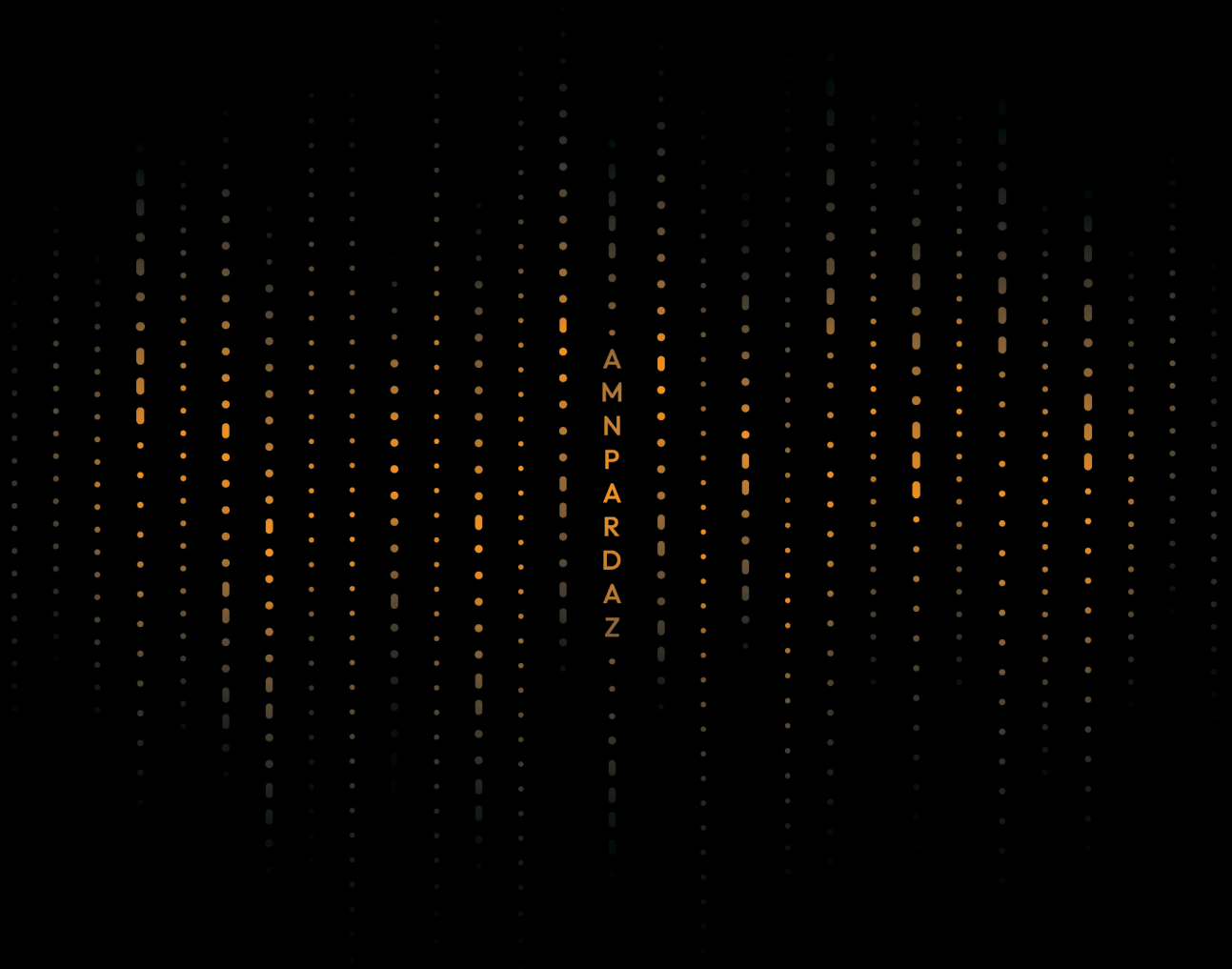
Dedicated and expert support at all times

Transparency, stability, and professional ethics

Innovating Cyber Trust

## Contact Information

info@amnpardaz.com
amnpardaz.com
padvish.com
cloudguard.ir


AMNPARDAZ