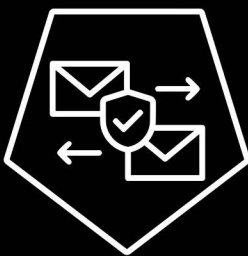


Ampardaz®
Software Corporation



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.

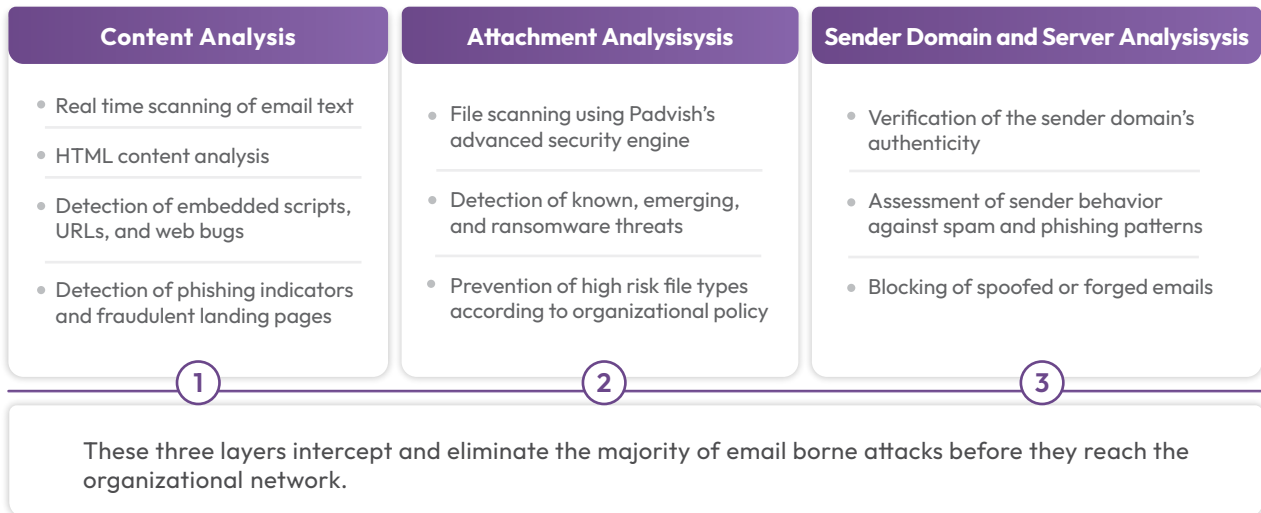


Product Architecture

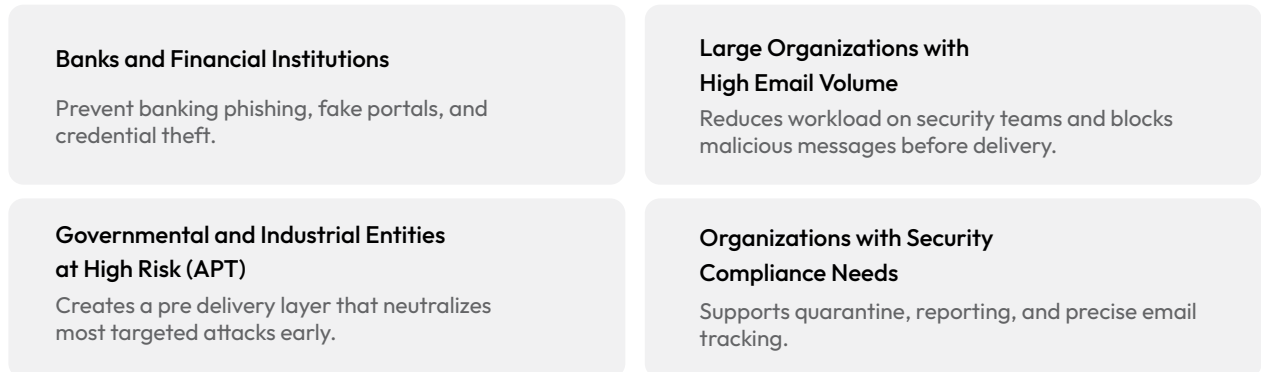
Padvish Mail Gateway is a multi layer security gateway that analyzes the entire content, attachments, links, and embedded elements of each email before it reaches the organizational mail server.

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:



Use Cases



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



Anti Phishing

Detection of fraudulent pages, fake payment gateways, manipulated links, and social engineering attempts.



Anti Spam and Malicious Email Filtering

Prevents entry of spam, infected advertisements, and risky bulk messages.



Multi Layer Attachment Anti Malware

Multi layer scanning of all attachments prior to inbox delivery, including miners, ransomware, worms, Trojans, and tampered files.



Quarantine and Suspicious Message Management

Administrators can review, release, or delete high risk emails.



Blocking of High Risk Files per Policy

Organizations can define sensitive or risky file types; PMG enforces blocking automatically.



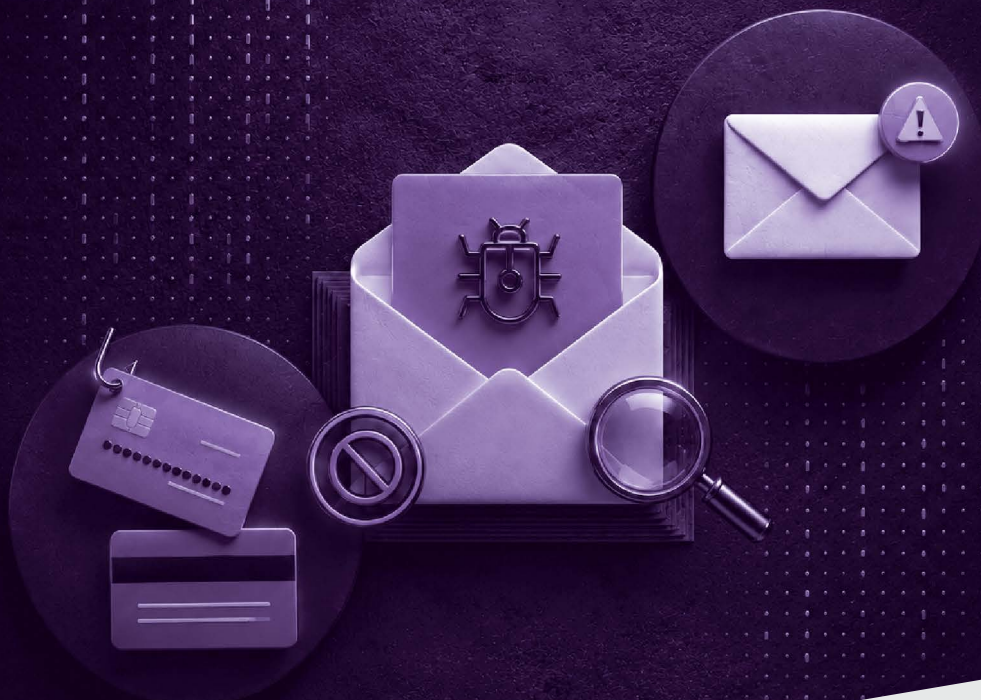
Full Integration with Padvish Infrastructure

Security events and telemetry are synchronized with the Padvish management console for centralized analytics and decision making.

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.



“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](#)