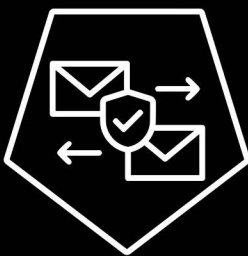


Ampardaz®  
Software Corporation



**Padvish**  
Mail Gateway



## محافظت چندلایه از ایمیل با فناوری هوشمند پادویش

### چالش سازمان‌ها

ایمیل یکی از اصلی‌ترین مسیرهای ورود بدافزار، فیشینگ، اسپیم و حملات هدفمند است. بدون وجود یک لایه که پیش از تحویل ایمیل به کاربر نهایی پیوسته‌ها، لینک‌ها و کدهای مخرب را مسدود کند، سازمان‌ها در معرض باج‌افزار، خروج داده و حملات APT قرار می‌گیرند.

### راهکار امن‌پرداز

Padvish Mail Gateway با اسکن چندلایه، تشخیص هوشمند بدافزار، جلوگیری از فیشینگ و اسپیم، قرنطینه‌سازی فایل‌های مشکوک و استفاده از هوش مصنوعی پادویش، ایمیل‌ها را پیش از رسیدن به صندوق کاربران بررسی و پاک‌سازی می‌کند تا جریان ارتباطی سازمان امن، پایدار و قابل اعتماد باقی بماند.



## معماری محصول

Padvish Mail Gateway یک «دروازه امنیتی چندلایه» است که پیش از ورود ایمیل به سرور سازمان، کل پیام پیوست، لینک‌ها و محتوای داخلی آن را تحلیل می‌کند و در صورت مشاهده رفتار یا الگوی تهدید، ایمیل را در همان مرحله مسدود یا قرنطینه می‌نماید.

### معماری اصلی Padvish Mail Gateway شامل سه لایه کلیدی است:

#### تحلیل دامنه و سرورهای ارسال‌کننده

- بررسی اصالت دامنه فرستنده
- ارزیابی رفتار ارسال‌کننده نسبت به الگوهای اسپم یا فیشینگ
- مسدودسازی ایمیل‌های جعلی

#### تحلیل پیوست‌ها

- اسکن فایل با موتور امنیتی پیشرفته پادویش
- تشخیص بدافزارهای کلاسیک، نوظهور و باج‌افزار
- جلوگیری از عبور انواع فایل‌های پرریسک (طبق سیاست سازمان)

#### تحلیل محتوا

- بررسی بلادرنگ متن ایمیل
- تحلیل محتوای HTML
- شناسایی اسکریپت‌ها، URL‌های جاسازی‌شده و وب‌باگ‌ها
- تحلیل نشانه‌های حمله فیشینگ یا صفحات جعلی

این سه لایه، سنگین‌ترین بخش حملات ایمیلی را پیش از رسیدن به شبکه سازمان حذف می‌کنند.



### نتایج امنیتی برای سازمان

- جلوگیری فعال از حملات فیشینگ، باج‌افزار و اسپم قبل از رسیدن به کاربران.
- کاهش چشمگیر سطح حمله ایمیلی یکی از حیاتی‌ترین بردارهای نفوذ.
- افزایش اعتماد و امنیت ارتباطات سازمانی بدون تغییر در فرآیند کاری کارمندان.
- گزارش‌دهی کامل برای تصمیم‌گیری امنیتی شفافیت کامل در حملات و رفتار ایمیل‌های ورودی.
- بهبود عملکرد تیم امنیت با کاهش هشدارهای کاذب و حذف ایمیل‌های مخرب پیش از تحویل.



### سناریوهای کاربردی

- **بانک‌ها و سازمان‌های مالی**  
برای جلوگیری از فیشینگ بانکی، درگاه‌های جعلی و سرقت اطلاعات.
- **سازمان‌های بزرگ با حجم بالای ایمیل داخلی/خارجی**  
کاهش بار بر تیم امنیت و جلوگیری از ورود ایمیل‌های مخرب.
- **شرکت‌های دولتی و صنعتی با ریسک بالای حملات APT**  
PMG لایه «پیش‌تحویل» را ایجاد می‌کند که اکثر حملات هدفمند از همان جا متوقف می‌شوند.
- **سازمان‌هایی با الزام تطابق امنیتی**  
نیاز به قرنطینه، گزارش‌دهی و ردیابی دقیق ایمیل‌ها.

## قابلیت‌های کلیدی

### ضد فیشینگ

تشخیص صفحات جعلی، درگاه‌های بانکی تقلبی، لینک‌های دستکاری‌شده و الگوهای مهندسی اجتماعی.



### ضد اسپم و تشخیص ایمیل‌های تبلیغاتی خطرناک

جلوگیری از ورود اسپم، تبلیغات آلوده و پیام‌های انبوه که ریسک امنیتی ایجاد می‌کنند.



### ضد بدافزار چندلایه برای پیوست‌ها

اسکن تمامی فایل‌های ضمیمه قبل از ورود به صندوق ورودی؛ شامل: Trojans, Worms, Ransomware, Miners فایل‌های دستکاری‌شده یا مخرب



### قرنطینه و مدیریت پیام‌های مشکوک

امکان بررسی، آزادسازی یا حذف پیام‌های پرخطر توسط مدیر سیستم.



### مسدودسازی فایل‌های خطرناک طبق سیاست سازمان

سازمان می‌تواند انواع فایل‌های حساس یا پرریسک را تعریف کند و PMG از عبور آن‌ها جلوگیری می‌کند.



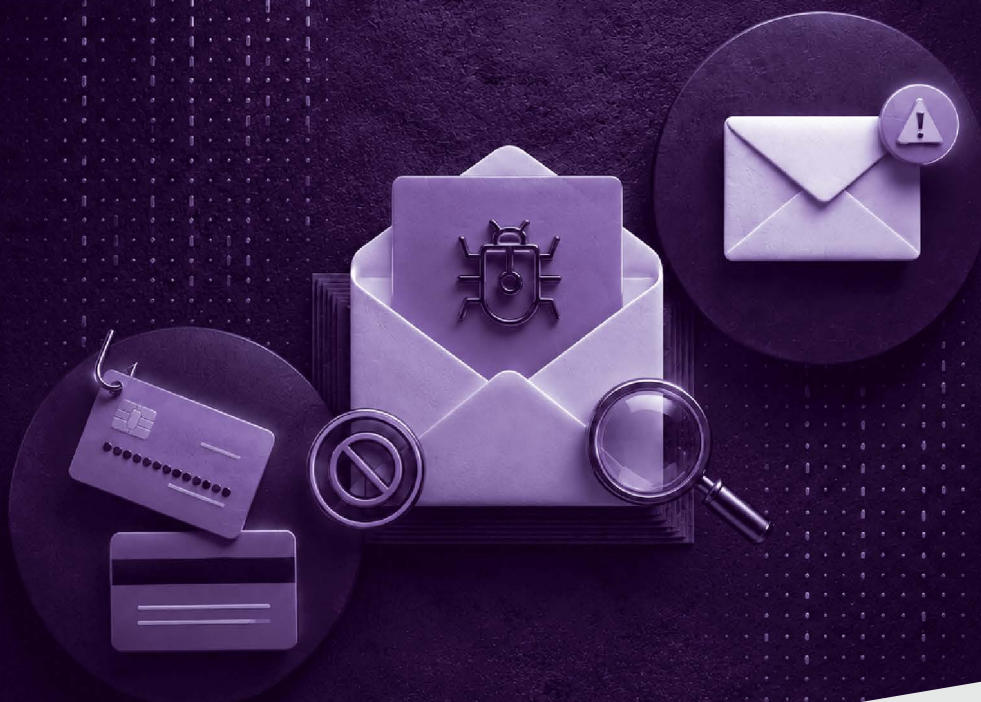
### یکپارچگی کامل با زیرساخت پادویش

رویدادهای امنیتی و گزارش‌ها به کنسول مدیریتی منتقل می‌شوند تا تیم امنیت بتواند تحلیل روند و تصمیم‌گیری انجام دهد.



## چرا Padvish Mail Gateway؟


زیرا PMG تنها راهکاری است که در بستر پلتفرم پادویش، سه لایه تشخیص محتوایی، تحلیل پیوست و ارزیابی دامنه را هم‌زمان ترکیب می‌کند و با تمرکز بر تهدیدات واقعی در ایران (فیشینگ، اسپم‌های هدفمند، باج‌افزار از طریق فایل‌های ضمیمه)، یک سپر کامل در برابر حملات ایمیلی ایجاد می‌کند.



"شرکت نرم افزاری امن پرداز محصولات و خدمات متنوعی را با نام تجاری پادویش جهت مقابله با طیف گسترده تهدیدات و حملات سایبری در بخش خانگی و سازمانی ارائه می نماید."



 [www.padvish.com](http://www.padvish.com)

 [info@amnpardaz.com](mailto:info@amnpardaz.com)

درباره ما