شرکت نرم افزاری امن پرداز®
Amnpardaz Software Corporation

راهکارهای امنیتی
شرکت نرم‌افزاری امن‌پرداز

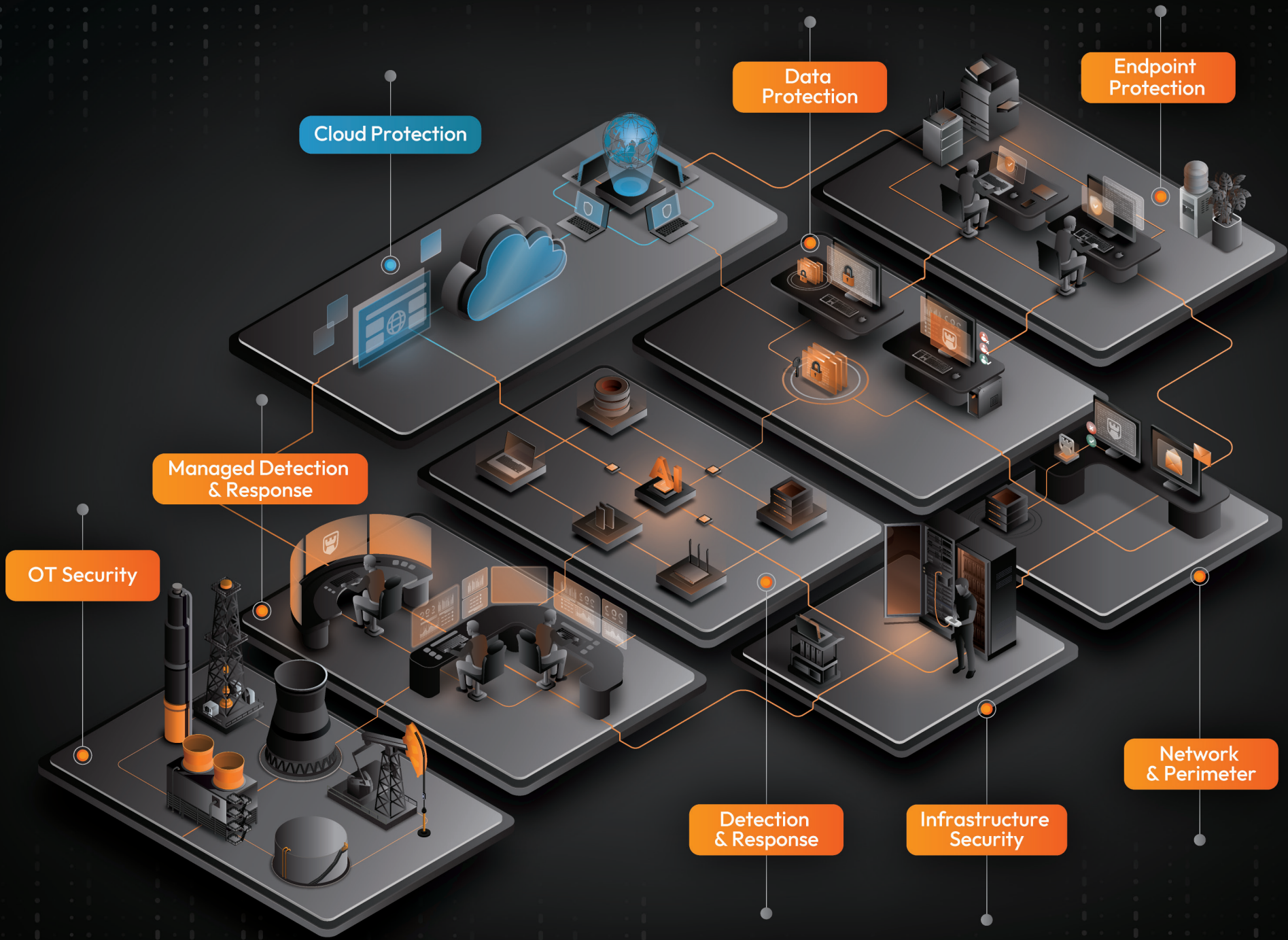
Amnpardaz Security Platform

نوآوری در اعتماد سایبری
Innovating Cyber Trust

Cloud Guard | پادویش® Padvish

منظومه امنیتی یکپارچه امن‌پرداز

توسعه محصولات و راهکارهای امنیت سایبری یکپارچه


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

فهرست

درباره ما

امن‌پرداز از سال ۱۳۸۳ با یک باور ساده و روشن شکل گرفت:

فناوری باید حافظ انسان باشد، نه محدودکننده او.

از همان ابتدا مأموریت ما ساخت راهکارهایی بود که در دل پیچیدگی‌های دنیای دیجیتال، از حریم، داده‌های حساس و زیست دیجیتال افراد و سازمان‌ها محافظت کنند.

پادویش، برند اصلی امن‌پرداز، حاصل همین مسیر است؛

مجموعه راهکارهای امنیتی با استانداردهای جهانی که میلیون‌ها کاربر و هزاران سازمان به آن تکیه کرده‌اند. این راهکارها با ترکیب مهندسی پیشرفته، بهره‌گیری از هوش مصنوعی و رویکرد اخلاق‌محور، امنیتی پایدار و یکپارچه را فراهم می‌سازد.

دستاوردهایی همچون شناسایی تهدیدات پیشرفته‌ای نظیر iLOBleed در جهان و WannaCry در ایران، دریافت گواهی شناسایی و پاسخ پیشرفته به تهدیدات نقاط پایانی (EDR) و همچنین گواهی تشخیص ۱۰۰٪ باج‌افزارها از آزمایشگاه Test-AV آلمان، و قرارگیری محصول Padvish XDR AI در جایگاه نهم جهانی در رتبه‌بندی معتبر EDR-Telemetry، بالاتر از بسیاری از شرکت‌های بزرگ امنیت سایبری دنیا نشان می‌دهد که این راهکارها قادرند از سازمان‌ها در برابر پیچیده‌ترین تهدیدات سایبری محافظت کنند.

امروز امن‌پرداز مجموعه‌ای کامل از راهکارهای خانگی و سازمانی ارائه می‌دهد:

- محافظت نقاط پایانی در سه پلتفرم ویندوز، لینوکس و اندروید
- محافظت داده
- محافظت درونی و شبکه
- راهکارهای کشف و پاسخ هوشمند با بهره‌گیری از هوش مصنوعی
- خدمات مدیریت شده کشف و پاسخ
- مدیریت خدمات فناوری اطلاعات
- محافظت زیرساخت
- محافظت فناوری‌های عملیاتی
- محافظت ابری از وب‌سایت‌ها، شبکه و زیرساخت‌های دیجیتال

ارزش‌های ۷ گانه امن‌پرداز

۱	اخلاق در قلب امنیت
۲	انسان‌محوری در کنار فناوری
۳	سادگی در طراحی و اجرا
۴	شفافیت در داده و رفتار
۵	مسئولیت‌پذیری در برابر کاربران و جامعه
۶	یکپارچگی در معماری و تجربه
۷	یادگیری و بهبود مستمر

امن‌پرداز به روایت اعداد

- **+۲۰** سال نوآوری در امنیت سایبری
- **+۲۰۰** راهکار امنیت سایبری
- **+۷** میلیون کاربر سازمانی و خانگی
- **+۷۰۰۰** سازمان محافظت‌شده
- **+۲۰۰** نماینده و عامل‌فروش
- **+۶۱۲** میلیون آنالیز تهدید

فلسفه امنیت از دیدگاه امن‌پرداز

«امنیت برای ما از یک اصل آغاز می‌شود: اخلاق»

در جهانی که پیچیدگی فناوری و دنیای سایبری هر روز بیشتر می‌شود، امنیت تنها با ابزارهای پیشرفته ساخته نمی‌شود؛ امنیت زمانی معنا پیدا می‌کند که اخلاق، داده و فناوری در یک چرخه درست قرار گیرند.

از دیدگاه امن‌پرداز، امنیت یک کالا نیست، بلکه یک روند است که باید با شفافیت، دقت و مسئولیت ساخته شود.

ما امنیت را بر پایه سه ستون اصلی تعریف می‌کنیم:

- سادگی در قلب پیچیدگی
- انسان در مرکز تصمیم
- شفافیت به‌جای آشوب

امن‌پرداز و مسیر فناوری امنیت سایبری

امنیت سایبری در امن‌پرداز سال‌هاست که از راهکارهای سنتی عبور کرده است؛ مدل‌هایی که تنها بر امضا، پایگاه داده و تشخیص فایل‌های شناخته شده تکیه داشتند. امروز تهدیدات چندمرحله‌ای، حملات بدون فایل، سوءاستفاده از رفتارهای سیستمی و زنجیره‌های پیچیده نفوذ، نیازمند رویکردی هستند که فراتر از شناسایی ایستا عمل کند.

امن‌پرداز با منظومه امنیتی پادویش، گامی فراتر از آنتی‌ویروس گذاشته و وارد نسل جدید حوزه امنیت (Next-Generation Security) شده است؛

ترکیبی از سامانه های مدرن امنیتی مانند XDR، EDR و هوش مصنوعی.

در این رویکرد، امنیت نه یک «فیلتر» بلکه یک سامانه پیوسته تحلیل رفتار، همبستگی داده و پاسخ هماهنگ است؛

سیستمی که رفتار تهدید را در تمام لایه‌ها، از نقطه پایانی و شبکه تا فضای ابری و زیرساخت، رصد، پیگیری و تحلیل نموده و به مقابله با آن می‌پردازد.

امن‌پرداز امنیت را از یک ابزار، به یک «سامانه هوشمند و یکپارچه» تبدیل نموده است؛ سامانه‌ای که برای تهدیدات دنیای امروز طراحی شده؛ نه تهدیدات دهه‌های گذشته.

مدیریت امنیت کل شبکه سازمان تنها با یک کنسول و یک ایجنت

کنسول مدیریتی پادویش

بستر یکپارچه برای مدیریت، پیکربندی و نظارت کامل بر اکوسیستم دیجیتال سازمان است که با بهره‌گیری از معماری Master/Slave، امکان کنترل متمرکز کل شبکه، توزیع سیاست‌ها، مدیریت به‌روزرسانی‌ها و مشاهده وضعیت عملیاتی تمام کلاینت‌ها و سرورها را در لحظه فراهم می‌کند.

مزیت‌های کلیدی کنسول واحد مدیریتی:

- تعریف و اجرای سیاست‌ها و کنترل مرکزی (به وسعت کل کشور)
- مشاهده وضعیت امنیتی شبکه در یک نگاه
- مدیریت نصب و استقرار یکپارچه در کل شبکه
- بررسی و پیگیری رخدادها، هشدارها و گزارش‌ها

نصب با یک ایجنت

یکی از چالش‌های اصلی سازمان‌ها در مدیریت امنیت، تعدد ایجنت‌ها به ازای هر محصول یا افزونه، ناسازگاری بین ابزارهای متعدد و پیچیدگی در استقرار است. این پیچیدگی نه‌تنها هزینه را افزایش می‌دهد، بلکه احتمال خطا و شکاف امنیتی را هم بالا می‌برد.

در امن‌پرداز، منظومه محصولات پادویش به‌شکلی توسعه داده شده است که همه محصولات و راهکارها در سمت کلاینت تنها با یک ایجنت، سبک و یکپارچه ارائه شود و در سمت مدیر شبکه/ ادمین نیز تنها توسط یک کنسول مدیریت شود.

مزیت‌های کلیدی یک ایجنت در سمت کلاینت:

- استقرار سریع در شبکه‌های بزرگ بدون نیاز به حضور فیزیکی متعدد
- کاهش بار مدیریتی تیم‌های امنیتی
- تجربه یکپارچه در بهره‌گیری از محصولات مختلف
- بازدهی بیشتر، سربار کم‌تر

گواهینامه‌ها و افتخارات بین‌المللی

۱

گواهـی شناسایی و پاسخ پیشرفته
به تهدیدات نقاط پایانی (EDR) از
آزمایشگاه AV-Test آلمان

۲

قرارگیری محصول Padvish XDR AI در
جایگاه نهم جهانی در رتبه‌بندی معتبر
EDR-Telemetry، بالاتـر از بسیاری از
شرکت‌های بزرگ امنیت سایبری دنیـا

۳

گواهـی تشخیص ۱۰۰٪ باج‌افزارها از
آزمایشگاه AV-Test آلمـان

۴

تشخیص نخستین نهان‌افزار
در سرورهای HP (iLOBleed)

۵

شناسایی ابزارهای جاسوسی روز صفر و محافظت
در برابر آن‌ها به گواهی وب‌سایت WikiLeaks
(WannaCry ,Petya و دیگر بدافزارهای پیچیده)

گواهینامه‌ها، مجوزها و پروانه‌های داخلی

- مجـوز افتـا
- پروانـه نمـا
- گواهینامه EAL1

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

پشتیبانی و همراهی کامل

امنیت فقط به فناوری وابسته نیست؛ به همراهی انسان‌هایی نیاز دارد که در لحظات حساس کنار سازمان بایستند.

در امن‌پرداز، پشتیبانی بخشی مستقل از محصول نیست، بلکه لایه‌ای از معماری امنیتی ماست.

ما باور داریم که اعتماد سایبری زمانی ساخته می‌شود که سازمان بداند پشت هر هشدار، هر تصمیم و هر به‌روزرسانی، یک تیم متخصص به‌صورت مسئولانه حضور دارد.

شاخص‌های کلیدی پشتیبانی در امن‌پرداز:

- تیم تخصصی امنیت سازمانی
- پاسخگویی شفاف و قابل‌پیگیری
- همراهی شما به صورت ۷*۲۴
- همراهی در استقرار و عملیات
- پشتیبانی چندلایه برای شبکه‌های بزرگ
- آموزش و انتقال دانش

امنیت واقعی، یعنی حضور پشتیبانی در لحظه‌های مهم


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
Padvish XDR AI
Infrastructure Security
Padvish iLO Scanner
Network & Perimeter
Padvish NAC
Padvish Mail Gateway

منظومه راهکارهای امنیت سایبری سازمانی پادویش

معماری یکپارچه امنیتی

امنیت سازمانی زمانی کارآمد است که همه لایه‌های دفاعی، از نقطه پایانی تا فضای ابری، در یک ساختار هماهنگ و شفاف کنار یکدیگر عمل کنند.
در امن‌پرداز، ما امنیت را مجموعه‌ای از ابزارهای جداگانه نمی‌بینیم؛ بلکه یک منظومه منسجم می‌دانیم.

این منظومه یکپارچه امنیتی بر ۸ ستون اصلی بنا شده است:

- **محافظت نقاط پایانی:** محافظت پیشرفته در برابر تهدیدات نقاط پایانی، با امکان سیاست‌گذاری و مدیریت یکپارچه امنیتی در سازمان
- **محافظت داده:** محافظت از اطلاعات و داده‌های سازمان در برابر نشت اطلاعات، تهدیدات داخل و خارج سازمان و کنترل دسترسی به اطلاعات
- **محافظت شبکه:** امنیت مرزهای سایبری سازمان با کنترل دسترسی به شبکه سازمان، شفافیت ارتباطات شبکه و سیاست‌گذاری یکپارچه ارتباطات سازمان
- **سامانه‌های هوشمند کشف و پاسخ:** بالاترین سطح امنیت با دید واحد بر نقاط پایانی، شبکه و دستگاه‌های غیرپایانی، تحلیل یکپارچه و پاسخ هماهنگ
- **راهکارهای مدیریت‌شده کشف و پاسخ:** برای مدیریت ۲۴*۷ سامانه‌های پیشرفته تشخیص و پاسخ با بهره‌گیری از توان متخصصان امنیت امن‌پرداز
- **محافظت زیرساخت:** اطمینان از سلامت لایه سخت‌افزاری سازمان
- **محافظت فناوری‌های عملیاتی:** برای حفاظت جامع امنیتی از محیط‌های عملیاتی در برابر تهدیدات
- **محافظت ابری کلودگارد:** محافظت از وب‌سایت‌ها، شبکه‌ها، اپلیکیشن‌ها با رویکرد دفاع در عمق

معماری واحد، دید روشن، امنیت قابل اتکا

Padvish Base

Padvish Corporate

محافظت نقاط پایانی
برای پلتفرم‌های ویندوز، لینوکس و اندروید

حفاظت پیشرفته و جامع از نقاط پایانی، داده‌ها و شبکه سازمان

چالش سازمان‌ها

در دنیای تهدیدات پیچیده سایبری امروز با گسترش سریع بدافزارها، باج‌افزارها، حملات بدون فایل، بهره‌برداری از آسیب‌پذیری‌های سیستم‌عامل و نفوذ از طریق شبکه و اینترنت، سازمان‌ها با یک چالش جدی روبه‌رو هستند:
چگونه سازمان باید همه این تهدیدات پیچیده را به‌صورت یکپارچه و متمرکز کنترل کند؟

راهکار امن‌پرداز

محافظت پیشرفته نقاط پایانی پادویش با ترکیب فناوری ضدبدافزار نسل جدید، پیشگیری از نشت اطلاعات، تشخیص رفتاری، فناوری پردازش ابری و لایه‌های دفاع شبکه‌ای (Firewall و IDS/IPS)، حفاظتی یکپارچه را در سطح سازمان فراهم می‌کند.
این راهکار در دو نسخه Base و Corporate ارائه می‌شود:
نسخه Base برای حفاظت پیشرفته در برابر بدافزارها، مقابله با نشت اطلاعات و مسدودسازی حملات سطح شبکه و نسخه Corporate افزون بر قابلیت‌های نسخه Base دارای قابلیت‌های تکمیلی مانند مدیریت آسیب‌پذیری، کنترل اینترنت و مدیریت شبکه‌های مورد اعتماد است.

Padvish Base/ Corporate

AV-TEST The Independent IT-Security Institute Magdeburg Germany

معماری محصول

پادویش Base و Corporate بر پایه یک موتور چندلایه، رفتارمحور و سبک طراحی شده‌اند که حفاظت بلادرنگ، تحلیل فایل، پایش شبکه و کنترل دستگاه‌های جانبی را در لایه نقاط پایانی فراهم می‌کند.

این معماری برای شبکه‌های بزرگ با پراکندگی جغرافیایی بالا، دستگاه‌های متعدد و محیط‌های عملیاتی حساس بهینه شده است.

سناریوهای کاربردی

- حفاظت از سیستم‌های سازمانی و عملیاتی
- جلوگیری از بدافزارها و تهدیدات نوظهور
- کنترل رسانه‌های جانبی در محیط‌های حساس
- محافظت سبک برای سیستم‌های قدیمی یا کم‌قدرت
- امن‌سازی شبکه‌های بزرگ با مدیریت مرکزی

نتایج امنیتی برای سازمان

- کاهش ریسک آلودگی نقاط پایانی
- افزایش تاب‌آوری در برابر تهدیدات داخلی و خارجی
- کاهش زمان پاسخ به حادثه
- یکپارچگی لایه نقطه پایانی با معماری امنیت سازمان
- کاهش هزینه‌های پشتیبانی و مدیریت

امکانات بیشتر و ویژه نسخه Corporate

Internet Connection Detection

دارای لایه هوشمند تشخیص اتصال اینترنت جهت تشخیص اتصال بدون مجوز کلاینت به اینترنت و اعمال سیاست‌های امنیتی متناسب با وضعیت شبکه

Trusted Network

امکان تعریف شبکه‌های مورد اعتماد، بسته به محل اتصال کاربر، محدودسازی اتصال به شبکه، و تهیه گزارش جامع از نقض سیاست‌های تعریف شده در شبکه‌های مورد اعتماد

Vulnerability Assessment

تهیه گزارش جامع از آسیب‌پذیری‌های سیستم‌عامل، دسته‌بندی آسیب‌پذیری‌ها بر اساس میزان خطر، و بررسی جزئیات وصله‌ها

چرا Padvish Base / Corporate؟

پادویش Base انتخابی سبک، پایدار و بهینه برای شبکه‌های سازمانی است؛ درحالی‌که پادویش Corporate با سه قابلیت حیاتی (تشخیص اتصال اینترنت، شبکه‌های مورد اعتماد و تحلیل آسیب‌پذیری سیستم‌عامل) برای محیط‌های سازمانی بزرگ و دارای شبکه‌های فناوری اطلاعات چند منظوره طراحی شده است.

امکانات مشترک نسخه Corporate و Base

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

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

کنترل سازمانی، امنیت چندلایه و مدیریت متمرکز برای دستگاه‌های اندرویدی

چالش سازمان‌ها

پراکندگی دستگاه‌های اندرویدی، نصب آزادانه اپلیکیشن‌ها و نبود دید متمرکز، ریسک نشت داده و نفوذ را افزایش می‌دهد. سازمان‌های دارای نیروی میدانی پراکنده نیازمند راهکاری هستند که امنیت دستگاه‌های اندرویدی خود را به صورت یکپارچه و در مقیاس سازمانی مدیریت کند.

راهکار امن‌پرداز

Padvish Android Enterprise با ارائه محافظت چند لایه در برابر تهدیدات بدافزاری بهره‌گیری از هوش مصنوعی و یادگیری ماشین، مدیریت یکپارچه، ارائه مولفه‌های ضدسرقت، دیوار آتش، تهیه گزارشات فعالیت و سایر امکانات، راهکاری جامع برای تأمین امنیت دستگاه‌های اندرویدی سازمان‌ها است.

این راهکار امنیت، کارایی و نظارت سازمانی را در یک سکوی واحد ترکیب می‌کند.

Padvish
Android Enterprise

تأمین امنیت و مدیریت یکپارچه

با آنتی‌ویروس پادویش، نسخه اندروید سازمانی

- کنترل و حفاظت از تمامی گوشی‌ها و تبلت‌های اندرویدی سازمان
- امکان مشاهده وضعیت دستگاه‌های اندرویدی در کنسول مدیریتی پادویش
- امکان مشاهده گزارشات آماری به‌صورت دوره‌ای در داشبورد کنسول مدیریتی پادویش
- امکان گروه‌بندی و مدیریت گروه‌ها به صورت مجزا در کنسول مدیریتی پادویش
- امکان اعمال تنظیمات امنیتی به‌صورت متمرکز و از راه دور توسط کنسول مدیریتی پادویش

برجسته‌ترین قابلیت‌های آنتی‌ویروس پادویش

نسخه اندروید سازمانی

- امکان آزادسازی حافظه و پاک‌کردن فایل‌های بلااستفاده دستگاه اندرویدی
- نظارت بر معتبر و جعلی بودن درگاه‌های بانکی با ماژول آنتی‌فیشینگ
- پویش فایل‌ها و برنامه‌های نصب شده توسط انواع پویش‌های ابری، کامل، سریع و پویش انتخابی
- مدیریت و جلوگیری از اتصال نرم‌افزارها به اینترنت در دو بستر Mobile Data و WiFi
- استخراج و نمایش مشخصات و اطلاعات برنامه‌های نصب شده در دستگاه
- کنترل، پایش و جستجوی گوشی مفقود شده یا به سرقت‌رفته از راه دور

Padvish
DLP

محافظت داده
برای حفاظت از داده‌های سازمان در برابر تهدیدات

جلوگیری از نشت داده و کنترل مسیر خروج اطلاعات

چالش سازمان‌ها

در نبود کنترل متمرکز بر مسیرهای انتقال فایل، دسترسی و استفاده غیر مجاز از اسناد سازمان در داخل/ خارج از سازمان، عدم کنترل شبکه و ابزارهای جانبی، اطلاعات حساس سازمان به‌راحتی در معرض سوء استفاده قرار می‌گیرد.
سازمان‌ها نیازمند راهکاری هستند که بتوانند از داده‌ها در حال استفاده، انتقال و ذخیره‌سازی محافظت کند.

راهکار امن‌پرداز

محصول Padvish DLP با کنترل کامل دسترسی‌ها، جلوگیری از انتقال داده‌ها و فایل، کنترل ابزارهای جانبی، کنترل چاپ، تشخیص شبکه‌های معتبر، تحلیل رفتار، و رمزنگاری اسناد، تمامی مسیرهای خروج اطلاعات از سازمان را مدیریت می‌کند.
این راهکار با کنسول مدیریتی پادویش یکپارچه بوده و امکان اعمال سیاست‌های محافظت از داده را در سطح سازمان فراهم می‌سازد.

Padvish
DLP

آیا نگران نشت داده‌ها و اسناد محرمانه‌تان هستید؟

حفاظت در برابر نشت اطلاعات و اسناد محرمانه سازمان با Padvish DLP

کنترل دسترسی به محتوای اسناد

حفاظت از محتوای اسناد و داده‌ها از طریق رمزنگاری فایل‌ها

جلوگیری از افشا و انتقال داده‌ها و اسناد

حفاظت از اسناد در برابر روش‌های مختلف دسترسی غیرمجاز و انتقال ناخواسته فایل‌ها

قابلیت‌های سازگاری و مدیریتی

- مدیریت کلیه مولفه‌ها و محصولات از طریق ایجنت و کنسول مدیریتی پادویش
- ساختار سلسله مراتبی در کنسول‌های مدیریتی و امکان ساختاربندی Master/Slave
- گروه‌بندی کلاینت‌ها و اعمال تنظیمات مختلف به هر گروه

قابلیت‌های کلیدی DLP در آنتی‌ویروس پادویش نسخه Padvish DLP

۱ حفاظت از داده‌ها و اسناد در حال استفاده

کنترل ابزارهای جانبی

کنترل پرینت با امکان بستن یا مجاز نمودن عملیات پرینت در شبکه و لاگ‌برداری از آن

جمع‌آوری، نظارت و جستجو تمامی اطلاعات سخت‌افزاری و نرم‌افزاری

لاگ برداری از هرگونه انتقال فایل به‌وسیله ابزار جانبی

کنترل برنامه‌ها و تعیین برنامه‌های مجاز/ غیرمجاز

۲ حفاظت از داده و اسناد ذخیره شده

- قابلیت مدیریت دسترسی به اطلاعات، داده‌ها و فایل‌ها
- پشتیبان‌گیری سریع و کم حجم
- محافظت در برابر باجگیرها

۳ حفاظت از نشت داده و اسناد به خارج از شبکه سازمان

- تشخیص شبکه‌های مورد اعتماد و جلوگیری از اتصال به شبکه‌های غیرمجاز
- تشخیص اتصال به اینترنت
- کنترل وب و جلوگیری از اتصال به دامنه‌های غیرمجاز
- دیوار آتش دو لایه
- سیستم مقابله با نفوذ

Padvish
DRM

حفاظت از اسناد؛ حتی خارج از شبکه سازمان

چالش سازمان‌ها

پس از خروج اسناد از شبکه، کنترل سازمان بر فایل تقریبا از بین می‌رود. فایل‌ها می‌توانند بدون محدودیت کپی، چاپ، ارسال شده و در دسترس افراد غیرمجاز قرار گیرند. برای حفاظت واقعی از داده، امنیت باید به‌جای شبکه، همراه با فایل باشد.

راهکار امن‌پرداز

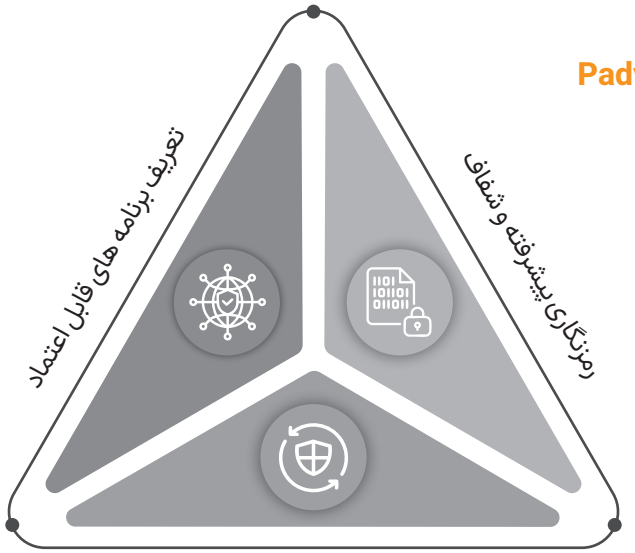
محصول Padvish DRM با رمزنگاری اسناد، اعمال سیاست‌های دقیق دسترسی، مدیریت متمرکز رمزنگاری، تعریف برنامه‌های تحت محافظت، جلوگیری از تهیه تصویر از اسناد، تعیین نقش و مجوز برای کاربران امکان حفاظت مداوم از اسناد را فراهم می‌کند. این راهکار حتی خارج از شبکه، کنترل سازمان بر فایل را حفظ کرده و از طریق کنسول مدیریتی پادویش قابل مدیریت است.

Padvish
DRM

آیا از امنیت داده‌ها و اسناد محرمانه سازمان خود اطمینان دارید؟

تأمین امنیت داده‌ها و اسناد محرمانه سازمان در برابر تهدیدات داخلی و خارجی با آنتی‌ویروس پادویش نسخه Padvish DRM

ویژگی‌های منحصر به فرد Padvish DRM



تکنولوژی‌های محافظت از محتوای داده‌های دیجیتال

- رمزنگاری نامتقارن فایل‌ها به محض ساخته شدن
- امکان ویرایش فایل‌ها در صورت قطع موقت شبکه
- مدیریت متمرکز رمزنگاری
- جلوگیری از نشت اطلاعات از طریق Copy/Paste یا Screenshot
- امکان توزیع کلید رمزنگاری در ساختار درختی سرورهای مدیریتی
- امکان تعریف برنامه‌های تحت حفاظت
- حفاظت و کنترل دسترسی به اطلاعات حساس براساس نقش و مجوز کاربر
- بلااستفاده بودن اسناد در صورت خروج ناخواسته فایل آن‌ها از سیستم و شبکه سازمان

چرا Padvish DRM

۱ بهره‌گیری از جدیدترین فناوری‌های رمزنگاری و کنترل دسترسی به منظور تأمین امنیت داده‌ها و اسناد

۲ محافظت از اسناد و داده‌ها در برابر تهدیدات سایبری، سرقت و نشت اطلاعات

۳ سازگاری با نیازهای سازمان‌ها

۴ بهینه‌سازی فرایندهای امنیتی سازمان

۵ ایجاد شرایط ایمن برای همکاری و اشتراک‌گذاری داده‌ها با خارج از سازمان

مدیریت چرخه رمزنگاری

- رمزگذاری خودکار
- رمزنگاری نامتقارن
- رمزگشایی کنترل‌شده

Padvish DataGuard™

لایه هوشمند محافظت از داده و دفاع پیشگیرانه

چالش سازمان‌ها

یکی از چالش‌های اساسی سازمان‌ها حفاظت از داده‌ها در برابر تهدیدات پیچیده باج‌افزاری، دسترسی غیرمجاز به داده در داخل یا خارج سازمان و تهدیدات مبتنی بر شبکه است.

راهکار امن‌پرداز

این راهکار یک پلتفرم امنیتی نسل جدید است که با اتکا به پنج لایه دفاعی در برابر باج‌افزارها، مجموعه‌ای گسترده از قابلیت‌های حفاظت از داده و اعمال سیاست‌های شبکه، رویکردی رفتارمحور برای تأمین امنیت داده در شبکه‌های سازمانی ارائه می‌دهد.

این پلتفرم برای همزیستی کامل با سایر محصولات امنیتی طراحی شده و تمامی قابلیت‌های اصلی پادویش ـ به‌جز آنتی‌ویروس ـ را در خود جای داده است؛ از این‌رو برای سازمان‌هایی که «یکپارچگی داده» و «تاب‌آوری در برابر باج‌افزار» را در اولویت قرار می‌دهند و به محافظت از داده در کنار راهکارهای امنیتی‌شان نیاز دارند، انتخابی کاملاً مطمئن و قابل اتکا به‌شمار می‌رود.

Padvish DataGuard™

AV-TEST The Independent IT-Security Institute Magdeburg Germany

معماری محصول

این راهکار براساس معماری چندلایه و رفتار محور طراحی شده است که رفتار فرآیندها، تغییرات فایل سیستم، فعالیت‌های غیرعادی دیسک و الگوهای رمزگذاری را پایش می‌کند.

۱ محافظت داده

DataCop Protection	پشتیبان‌گیری از کل داده‌ها به صورت کاملاً خودکار و محافظت شده با سرعت بسیار بالا و حداقل استفاده از فضای دیسک
DRM Encryption	رمزگذاری شفاف و خودکار بلافاصله پس از ایجاد فایل
DLP Rules	تعریف و اعمال سیاست‌های دقیق دسترسی به داده

۲ ضدباج افزار

Tamper Protection	برای محافظت در برابر رمزگذاری فایل‌ها
Backup Protection	برای تهیه نسخه‌های پشتیبان سریع و سبک مبتنی بر VSS
MBR Protection	محافظت از MBR در برابر تغییرات مخرب و باج‌افزارها
Bait Mechanism	برای شناسایی رفتار باج‌افزار با استفاده از فایل‌های طعمه
BitLocker Protection	برای جلوگیری از سوءاستفاده مهاجمان از ابزار رمزگذاری داخلی ویندوز- این مولفه پیشرفته اولین بار در این محصول به دنیای امنیت سایبری معرفی شد.

۳ سیاست‌های شبکه

Firewall	دو لایهٔ محافظتی برای کنترل کامل ترافیک ورودی و خروجی مبتنی بر معماری ویندوز
Web Control	جلوگیری هوشمند از دسترسی به دامنه‌های غیرمجاز
App Control	امکان تعریف قوانین کنترل برنامه بر نقاط پایانی و مسدودسازی اجرای برنامه‌های غیرمجاز
Device Control	مدیریت کامل تجهیزات جانبی و اعمال سیاست برای انواع تجهیزات جانبی

Data Protection

- DataCop Protected Instant Backups
- DRM Encryption
- DLP Rules

Anti-Ransomware

- 5-Layer Protection
- 100% Behavioral
- No update, catching every new threat

Network Policy

- Firewall
- Web Control
- App Control
- Device Control

نتایج امنیتی برای سازمان

- محافظت چندلایه متمرکز بر داده
- جلوگیری از نشت داده‌ها و اطلاعات
- مدیریت کلان و دقیق دسترسی به اطلاعات
- تمرکز بر رفتار تهدیدات بدون به‌روزرسانی مداوم پایگاه امضاء
- ممانعت از خسارت گسترده باج‌افزارها

Padvish
vKiosk™

درگاه مجازی امن و کنترل‌شده برای ورود فایل‌ها به شبکه سازمان بدون نیاز به سخت‌افزار

چالش سازمان‌ها

رسانه‌های قابل‌حمل یکی از رایج‌ترین مسیرهای ورود بدافزار و محتوای غیرمجاز هستند.
بدون یک لایه واسط برای بررسی رفتار، اسکن چندمرحله‌ای و اعمال سیاست‌های امنیتی، فایل‌ها می‌توانند پیش از شناسایی، سیستم را آلوده کنند. برخی سازمان‌ها برای حل این چالش از کیوسک سخت‌افزاری استفاده می‌کنند؛ راهکاری که با توجه به نیاز مکرر به مراجعه به کیوسک، پراکندگی جغرافیایی کیوسک‌ها، ایجاد ترافیک کاری اضافه و هزینه‌های نگهداری مشکلات مضاعفی را برای سازمان ایجاد می‌کند.

راهکار امن‌پرداز

Padvish vKiosk™ با ایجاد یک مسیر امن و ایزوله به‌صورت مجازی و بدون مشکلات استقرار سخت‌افزار، فایل‌ها را قبل از رسیدن به سیستم بررسی می‌کند.
کنترل دسترسی USB، اسکن چند موتوره، بازرسی فایل براساس سیاست‌های سازمان، و تحلیل رفتار کاربران، این محصول را به یک درگاه حیاتی و با استفاده آسان برای امنیت رسانه‌های قابل حمل تبدیل کرده است.

Padvish
vKiosk™

معماری محصول

Padvish vKiosk™ به‌عنوان «ایستگاه واسط امن» بین رسانه‌های قابل‌حمل و سیستم‌های ویندوزی عمل می‌کند.

به‌جای اتصال مستقیم USB به کلاینت‌های سازمان، همه‌چیز از مسیر Padvish vKiosk™ عبور می‌کند:

۱ انتخاب فایل	۲ تحلیل و تصمیم‌گیری	۳ تحویل امن یا مسدودسازی
کاربر، فایل‌های قابل انتقال را از طریق Padvish vKiosk™ به سرور مدیریتی پادویش ارسال می‌کند.	روی سرور، فایل‌ها با چندین موتور آنتی‌ویروس و براساس سیاست‌های امنیتی سازمان بررسی می‌شوند؛ خروجی این مرحله «اجازه»، «مسدودسازی» یا اعمال محدودیت است.	در صورت تأیید، فایل به‌صورت کنترل‌شده برای سیستم مقصد قابل دسترسی می‌شود؛ در غیر این صورت، مسدود و ثبت رویداد انجام می‌گیرد.

این معماری، یک لایه‌ی جداسازی عملیاتی ایجاد می‌کند تا بدافزار یا فایل‌های غیرمجاز، قبل از رسیدن به کلاینت‌های سازمان متوقف شوند.

قابلیت‌های کلیدی

۱ اسکن چندموتوره پیش از انتقال فایل

هر فایل، پیش از انتشار در شبکه، با چند موتور آنتی‌ویروس بررسی می‌شود تا دقت کشف تهدید به حداکثر برسد.

۲ کنترل نوع فایل و مسدودسازی محتوای غیرمجاز / حساس

امکان تعریف انواع فایل مجاز و جلوگیری از عبور فرمت‌ها و محتوای ناخواسته یا طبقه‌بندی‌شده.

۳ مدیریت و محدودسازی دسترسی USB

کنترل کامل روی اتصال و استفاده از رسانه‌های قابل‌حمل در ایستگاه‌های کیوسکی و سیستم‌های در معرض ریسک.

۴ گزارش‌دهی و تحلیل پیشرفته‌ی رویدادها

ثبت و تحلیل همه‌ی فعالیت‌های مرتبط با رسانه‌های قابل‌حمل برای ساختن سیاست‌های بهتر و انطباق قوی‌تر با الزامات امنیتی و نظارتی.

۵ بازرسی فایل پیش از ورود یا خروج از سازمان

همه‌ی فایل‌ها قبل از انتقال، مطابق قوانین تعریف‌شده‌ی سازمان ارزیابی می‌شوند.

سناریوهای کاربردی

- سازمان‌های با ایستگاه‌های کیوسکی و سیستم‌های مشترک
- محیط‌های با حساسیت بالای داده
- سازمان‌هایی با الزام مستندسازی و بازرسی

نتایج امنیتی برای سازمان

- **حفاظت پیش‌دستانه در برابر بدافزارهای USB**

  تهدیدهای ناشی از رسانه‌های قابل‌حمل قبل از رسیدن به محیط ویندوز شناسایی و مسدود می‌شوند و یک «لایه‌ی امن» میان فایل‌های ورودی و سیستم‌ها ایجاد می‌شود.

- **جلوگیری از نشت داده و انتقال غیرمجاز فایل**

  با سیاست‌های دقیق و کنترل نوع فایل، از خروج اطلاعات حساس و اسناد محرمانه جلوگیری می‌شود.

- **سیاست‌های امنیتی سفارشی برای هر کاربر و هر دستگاه**

  امکان تنظیم قوانین متفاوت براساس نقش، واحد سازمانی یا نوع ایستگاه، برای کنترل ریزدانه و منطبق با واقعیت کسب‌وکار.

- **تشخیص تهدید با دقت بالا به کمک اسکن چندموتوره**

  ترکیب چند موتور تشخیص، احتمال عبور بدافزار و فایل مخرب را به شکل چشم‌گیر کاهش می‌دهد.

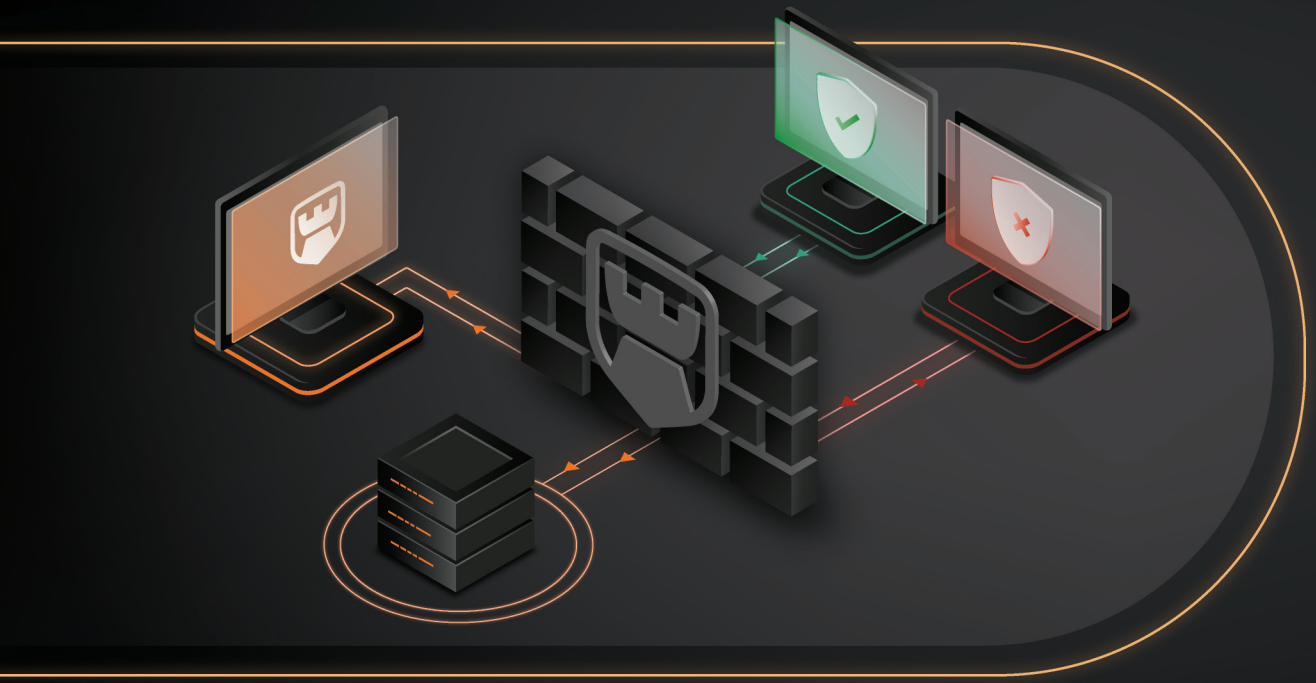
- **گزارش‌دهی و بینش مدیریتی برای بهبود مداوم سیاست‌ها**

  داده‌های رفتاری، لاگ‌ها و الگوهای استفاده از رسانه‌های قابل‌حمل، ورودی عملی برای بازطراحی سیاست‌ها و ارتقای بلوغ امنیتی سازمان فراهم می‌کنند.

Padvish
NAC

محافظت شبکه
برای محافظت از ارتباطات و شبکه سازمان

کنترل هوشمند دسترسی به شبکه بر پایه وضعیت واقعی امنیتی دستگاه



چالش سازمان‌ها

دستگاه‌های ناامن، بدون آنتی‌ویروس، با وصله‌های ناقص یا پورت‌های باز می‌توانند پیش از شناسایی، شبکه را آلوده کنند. سازمان‌ها به لایه‌ای نیاز دارند که پیش از اتصال، صحت حفاظتی دستگاه و هویت کاربر را بررسی کرده و مانع شکل‌گیری مسیرهای دور زدن امنیت شود.

راهکار امن‌پرداز

Padvish NAC با بررسی لحظه‌ای وضعیت امنیتی دستگاه، کنترل پورت‌ها، تأیید وصله‌های حیاتی و اعمال سیاست‌های دسترسی در سراسر شبکه، معماری «دسترسی در صورت محافظت» را عملی می‌کند و سطح وقوع حمله به سازمان را به‌طور چشمگیری کاهش می‌دهد.

Padvish
NAC

معماری محصول

Padvish NAC یک سامانهٔ کنترل دسترسی شبکه است که وضعیت امنیتی کلاینت‌ها را پیش از اجازه دسترسی به شبکه بررسی و تعیین‌تکلیف می‌کند.

معماری NAC در سه لایه اجرا می‌شود:

Client Compliance Check

- بررسی نصب و فعال بودن پادویش
- بررسی آخرین اتصال کلاینت به PMS
- بررسی سالم بودن سرویس‌ها، آپدیت‌ها و ماژول‌های امنیتی
- بررسی داشتن حداقل سطح امنیتی برای ورود به شبکه

Actuator Layer

- اعمال تصمیم اجازه، محدودیت یا مسدودسازی
- امکان استفاده از چند Actuator به‌صورت همزمان
- کنترل ارتباطات لایه شبکه براساس وضعیت امنیتی دستگاه

PMS Integration

- ارتباط امن و دائم با سرور مدیریت پادویش
- دریافت وضعیت لحظه‌ای سلامت کلاینت
- ارسال رویدادها، گزارش‌ها و تغییر وضعیت‌ها

این معماری باعث می‌شود تنها دستگاه‌هایی که استاندارد امنیتی سازمان را رعایت می‌کنند امکان دسترسی به شبکه را داشته باشند.

سناریوهای کاربردی	نتایج امنیتی برای سازمان
شبکه‌های سازمانی با نیاز به کنترل سطح سلامت کلاینت‌ها جلوگیری از اتصال سیستم‌های قدیمی، بدون آنتی‌ویروس، یا فاقد آپدیت.	جلوگیری از گسترش تهدیدات داخل شبکه چون فقط دستگاه‌های سالم اجازهٔ دسترسی دارند.
سازمان‌هایی که چند نقطهٔ حساس اتصال دارند این راهکار تضمین می‌کند فقط کلاینت‌های سالم وارد این نواحی شوند.	ارتقای سطح امنیت سازمان بدون پیچیدگی برای کاربران تصمیم‌گیری امنیتی به صورت خودکار و بی‌نیاز از مداخلهٔ دستی.
جلوگیری از گسترش بدافزار در شبکه داخلی دستگاه‌های ناسالم یا آلوده قبل از آسیب‌زایی شناسایی و ایزوله می‌شوند.	ایزوله‌سازی سریع کلاینت‌های ناسالم دستگاه‌هایی که مدتی به PMS وصل نشده یا ماژول‌هایشان غیرفعال است، فوراً محدود می‌شوند.
شرکت‌هایی با چند Actuator امنیتی جایی که لازم است دسترسی براساس ترکیب چند معیار امنیتی اعمال شود.	کاهش بار تیم امنیت پایش لحظه‌ای سلامت دستگاه‌ها و اعمال قوانین به‌صورت خودکار.

قابلیت‌های کلیدی

۱ کنترل دسترسی هوشمند

- اجرای تصمیمات Allow / Deny براساس وضعیت امنیتی کامپیوتر در لحظه.

۲ ارزیابی سلامت کلاینت

- پایش موارد زیر قبل از اتصال دستگاه به شبکه:
  - فعال بودن پادویش
  - وضعیت محافظت‌های امنیتی (Antivirus, Firewall, EDR)

۳ پشتیبانی از چند Actuator

- امکان استفادهٔ همزمان از چند Actuator برای کنترل سخت‌گیرانه‌تر شبکه

۴ تشخیص وضعیت‌های غیرعادی

- مسدودسازی دستگاه‌هایی که:
  - مدتی طولانی به PMS متصل نشده‌اند
  - ماژول‌های امنیتی لازم را غیرفعال کرده‌اند
  - به‌صورت مشکوک از شبکه جدا و وصل می‌شوند

۵ گزارش‌دهی و تحلیل مدیریتی

- تمام تصمیمات، مسدودسازی‌ها، هشدارها و تغییر وضعیت‌ها در PMS ثبت و قابل تحلیل هستند.

چرا Padvish NAC؟

زیرا NAC پادویش برخلاف بسیاری از راهکارهای سنتی، از PMS به‌عنوان مرکز تشخیص سلامت امنیتی دستگاه استفاده می‌کند و تصمیماتش مبتنی بر وضعیت واقعی نقاط پایانی‌ست، نه صرفاً MAC یا Policy شبکه.

این یعنی: دسترسی شبکه براساس «**سلامت امنیتی واقعی**» کنترل می‌شود.

Padvish
Mail Gateway

محافظت چندلایه از ایمیل با فناوری هوشمند پادویش

چالش سازمان‌ها

ایمیل یکی از اصلی‌ترین مسیرهای ورود بدافزار، فیشینگ، اسپم و حملات هدفمند است.
بدون یک لایه پیش‌تحویل که پیوست‌ها، لینک‌ها و کدهای مخرب را قبل از رسیدن به کاربر 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 اسپم، 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.

Padvish
Mail Gateway

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 مشاهدهٔ رفتار یا الگوی تهدید، ایمیل را در همان مرحله مسدود یا قرنطینه می‌نماید.

معماری اصلی Padvish Mail Gateway شامل سه لایه کلیدی است:

تحلیل محتوا	تحلیل پیوست‌ها	تحلیل دامنه و سرورهای ارسال‌کننده
• بررسی بلادرنگ متن ایمیل • تحلیل محتوای HTML • شناسایی اسکریپت‌ها، URLهای جاسازی‌شده و وب‌باگ‌ها • تحلیل نشانه‌های حملهٔ فیشینگ یا صفحات جعلی	• اسکن فایل با موتور امنیتی پیشرفته پادویش • تشخیص بدافزارهای کلاسیک، نوظهور و باج‌افزار • جلوگیری از عبور انواع فایل‌های پرریسک (طبق سیاست سازمان)	• بررسی اصالت دامنه فرستنده • ارزیابی رفتار ارسال‌کننده نسبت به الگوهای اسپم یا فیشینگ • مسدودسازی ایمیل‌های جعلی

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

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 لایهٔ «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.

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.

قابلیت‌های کلیدی

۱ • **ضد فیشینگ**
تشخیص صفحات جعلی، درگاه‌های بانکی تقلبی، لینک‌های دستکاری‌شده و الگوهای مهندسی اجتماعی.

۲ • **ضد اسپم و تشخیص ایمیل‌های تبلیغاتی خطرناک**
جلوگیری از ورود اسپم، تبلیغات آلوده و پیام‌های انبوه که ریسک امنیتی ایجاد می‌کنند.

۳ • **ضدبدافزار چندلایه برای پیوست‌ها**
اسکن تمامی فایل‌های ضمیمه قبل از ورود به صندوق ورودی؛ شامل: Ransomware، Worms، Trojans، Miners، فایل‌های دستکاری‌شده یا مخرب

۴ • **قرنطینه و مدیریت پیام‌های مشکوک**
امکان بررسی، آزادسازی یا حذف پیام‌های پرخطر توسط مدیر سیستم.

۵ • **مسدودسازی فایل‌های خطرناک طبق سیاست سازمان**
سازمان می‌تواند انواع فایل‌های حساس یا پرریسک را تعریف کند و PMG از عبور آن‌ها جلوگیری می‌کند.

۶ • **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 لایهٔ 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.

Padvish
EDR AI

سامانه‌های هوشمند کشف و پاسخ
برای شناسایی، تحلیل و پاسخ به تهدیدات سایبری

پلتفرم مستقل و هوشمند تشخیص و پاسخ

چالش سازمان‌ها

تهدیدات بدون فایل، حملات چندمرحله‌ای و رفتارهای مشکوک اغلب از دید ابزارهای سنتی مانند آنتی‌ویروس‌ها پنهان می‌مانند. سازمان‌ها برای مقابله با این تهدیدات به دید رفتاری، ثبت کامل رویدادها و تحلیل هوشمند نیاز دارند.

راهکار امن‌پرداز

Padvish EDR AI با ثبت رفتار سیستم، تحلیل هوشمند، فرآیند هم‌بسته و پاسخ سریع، تهدیدات پیشرفته را شناسایی و مهار می‌کند و دیدی کامل از فعالیت‌ها را در اختیار تیم امنیت قرار می‌دهد. به این صورت، تیم امنیتی سازمان‌ها پیش از وقوع، متوجه تهدیدات می‌شوند.

Padvish
EDR AI

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

هوش مصنوعی در خدمت امنیت سایبری

تنها قسمت اندکی از هشدارها توسط ابزارهایی مانند آنتی‌ویروس‌ها، فایروال‌ها و سایر ابزارهای سنتی گزارش می‌شوند.

تهدیدات تلاش می‌کنند از دید هشدارها پنهان بمانند.

حضور ابزارهای سنتی اگر چه در جای خود مفید و ضروری است، اما برای دفاع در برابر حملات پیشرفته سایبری هک و نفوذ کافی نمی‌باشند.

قابلیت‌های محصول Padvish EDR AI

- شکار تهدیدات با کمک دستیار هوش مصنوعی
- پیشنهاد اقدامات به کارشناسان امنیت، جهت واکنش به حوادث سایبری
- بررسی لاگ رخدادها و شرح آن‌ها به همراه نقاط مشکوک به زبان طبیعی

کاهش هزینه

- تشخیص تهدیدات
- شکار تهدیدات
- گزارش‌دهی

تشخیص دقیق‌تر

- بدافزارهای پیچیده و ناشناخته
- الگوهای رفتاری غیرعادی

افزایش کارایی

- در تیم‌های SOC
- تحلیل خودکار رخدادهای امنیتی

نیروی انسانی

- افزایش راندمان، بدون نیاز به نفرات بیشتر

فناوری‌ها و ماژول‌های Padvish EDR AI

- ضدبدافزار
- پویشگر حافظه
- محافظت رفتاری
- تحلیل‌گر همبستگی رخدادها
- یادگیری ماشین
- سیستم جلوگیری از نفوذ
- تحلیل‌گر تطبیق داده‌ها
- سندباکس
- آنتی‌ویروس مرکب
- تحلیل‌گر ایستای فایل

مولفه های Padvish CyberGPT™

- دستیار تحلیل‌گر سندباکس
- تحلیل‌گر اسکریپت
- دستیار تحلیل‌گر لاگ
- دستیار تحلیل‌گر رخداد
- دستیار جستجوگر

Padvish
XDR AI

پلتفرم یکپارچه تشخیص و پاسخ با بهره‌گیری از هوش مصنوعی

چالش سازمان‌ها

این راهکار پاسخی جامع به چالش‌های ناشی از به‌کارگیری ابزارهای امنیتی جزیره‌ای و داده‌های امنیتی پراکنده در سازمان‌ها است. در راهکارهای جزیره‌ای و مجزا، حجم بالای هشدارها از منابع مختلف باعث می‌شود تیم امنیتی سازمان نتواند تهدیدات پیچیده و چندمرحله‌ای را به موقع شناسایی و مهار کند.

راهکار امن‌پرداز

با یکپارچه‌سازی داده‌ها از نقاط پایانی، شبکه، سرویس‌های اینترنت، فضای ابری و بهره‌گیری از فناوری هوش مصنوعی و یادگیری ماشین، الگوهای رفتاری پیچیده و مشکوک را شناسایی کرده و دید متمرکز و جامعی از تهدیدات سایبری ارائه می‌دهد. این راهکار با همبستگی داده‌ها و فرآیندهای پاسخ پیشرفته، امکان شناسایی تهدیداتی را فراهم می‌کند که از چشم راهکارهای مجزا پنهان می‌مانند و باعث تسریع در کشف، تحلیل و مقابله با تهدیدات می‌شود.

Padvish
XDR AI

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

قابلیت‌های کلیدی Padvish XDR AI

۱ دید کامل و تحلیل متمرکز

- نمایش جامع وضعیت امنیتی در تمام لایه‌ها (نقاط پایانی، زیرساخت، شبکه)
- شناسایی رفتارهای مشکوک با درک ارتباط بین داده‌ها و رخدادها
- تحلیل داده‌های چند منبع مجزا به صورت متمرکز
- قابلیت تعریف قوانین اختصاصی متناسب با محیط سازمان

۲ افزایش بهره‌وری

- کاهش هشدارهای کاذب و تمرکز بر هشدارهای واقعی
- افزایش کارایی مرکز عملیات امنیت سازمان (SOC)
- افزایش سرعت و دقت در کشف، بررسی و پاسخ‌دهی

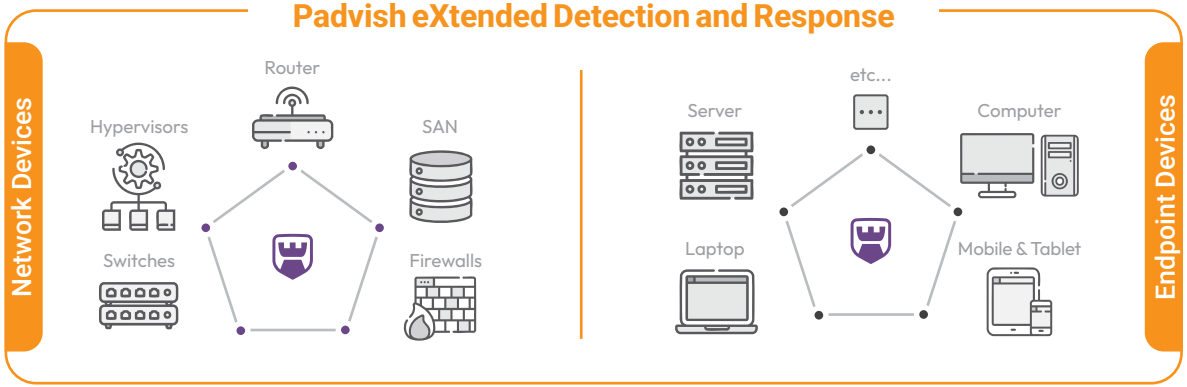
۳ کشف تهدیدات پیشرفته

- تشخیص حملات پیچیده و چندمرحله‌ای
- تحلیل مبتنی بر هوش مصنوعی و یادگیری ماشین
- کشف تهدیدات از میان حجم بالای داده‌ها و رخدادها
- استفاده از هوش تهدیدات پیشرفته

۴ دفاع پیشگیرانه

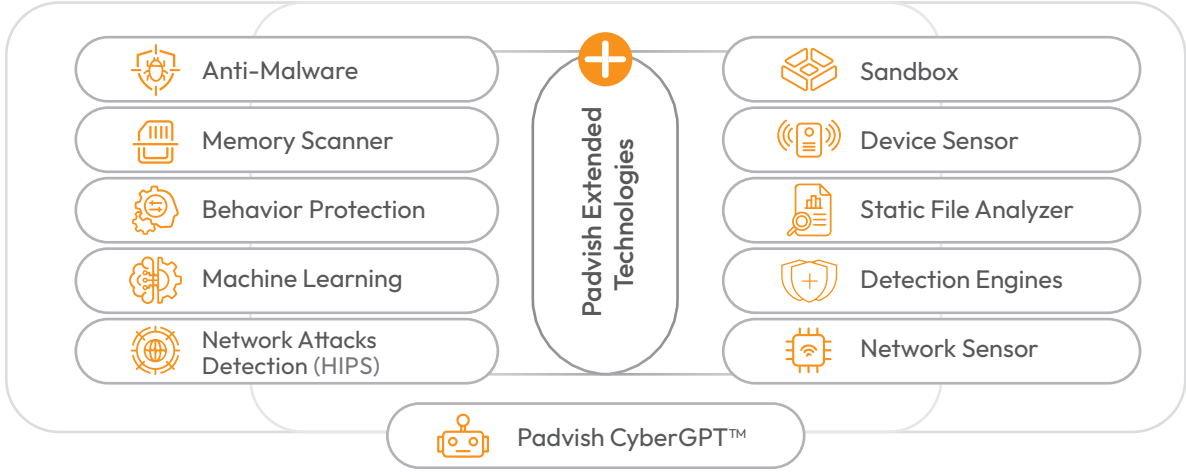
- پیشگیری از نفوذ و نشت اطلاعات
- تشخیص و توقف تهدیداتی که ابزارهای سنتی نادیده می‌گیرند
- تحلیل، کشف و پاسخ به تهدیدات به‌صورت متمرکز
- مدیریت پیشرفته رخدادها
- جایگزینی با امنیت جزیره‌ای و ایجاد هماهنگی بین لایه‌ها

Padvish eXtended Detection and Response



Padvish CyberGPT™

دستیار تحلیل‌گر سندباکس | تحلیل‌گر اسکریپت | دستیار جستجوگر | دستیار تحلیل‌گر رخداد | دستیار تحلیل‌گر لاگ



فناوری ها و ماژول های Padvish XDR AI

بهره‌گیری از هوش مصنوعی در تصمیم‌گیری، تحلیل و پاسخ سریع به تهدیدات

- تفسیر وقایع امنیتی و لاگ‌های سامانه XDR به زبان طبیعی
- درک مفاهیم فنی و ساختار داده‌های امنیتی
- تسریع در آنالیز وقایع و پیشگیری از رخدادهای امنیتی
- پیشنهاد اقدامات به کارشناسان جهت واکنش به حوادث سایبری

Padvish
MDR

راهکارهای مدیریت‌شده کشف و پاسخ
برای مدیریت سامانه های کشف و پاسخ

راهکار مدیریت‌شده بر پایه EDR AI؛ با پایش ۲۴x۷ و واکنش سریع

چالش سازمان‌ها

با گسترش حملات سایبری و تهدیدات پیشرفته، لزوم مقابله با این نوع حملات در سطح بالا بیش از پیش احساس می‌شود. طبیعتا مقابله با این حملات که به صورت ترکیبی از فناوری پیشرفته و هدایت انسانی انجام می‌گیرند، برای بسیاری از سازمان‌ها از طریق به‌کارگیری یک محصول یا خدمت به‌تنهایی قابل انجام نمی‌باشد و نیازمند راهکاری است که علاوه‌بر به کارگیری فناوری های پیشرفته، از نیروی انسانی کافی و متخصص جهت مقابله با این نوع تهدیدات برخوردار باشد.

راهکار امن‌پرداز

مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MDR) به صورت یک راهکار امن متمرکز، بر پایه اطلاعات دقیق و عمیق جمع‌آوری شده توسط محصولات پادویش از سیستم‌های، با تگ‌گذاری، تجمیع، تولید هشدار و داده‌نمایی، آن‌ها را مطابق تجربیات و دانش کسب‌شده از حملات قبلی سایبری تحلیل کرده، نفوذ را کشف نموده و از ادامه فعالیت نفوذگر در شبکه جلوگیری می‌کند.

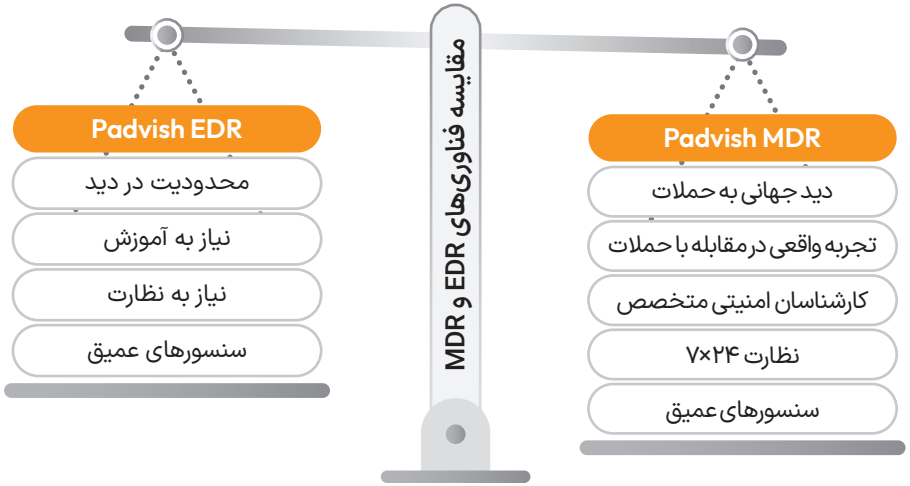
Padvish
MDR

EDR TELEMETRY

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

آیا سازمان شما آمادگی کامل برای شناسایی و مقابله با حملات سایبری را دارد؟

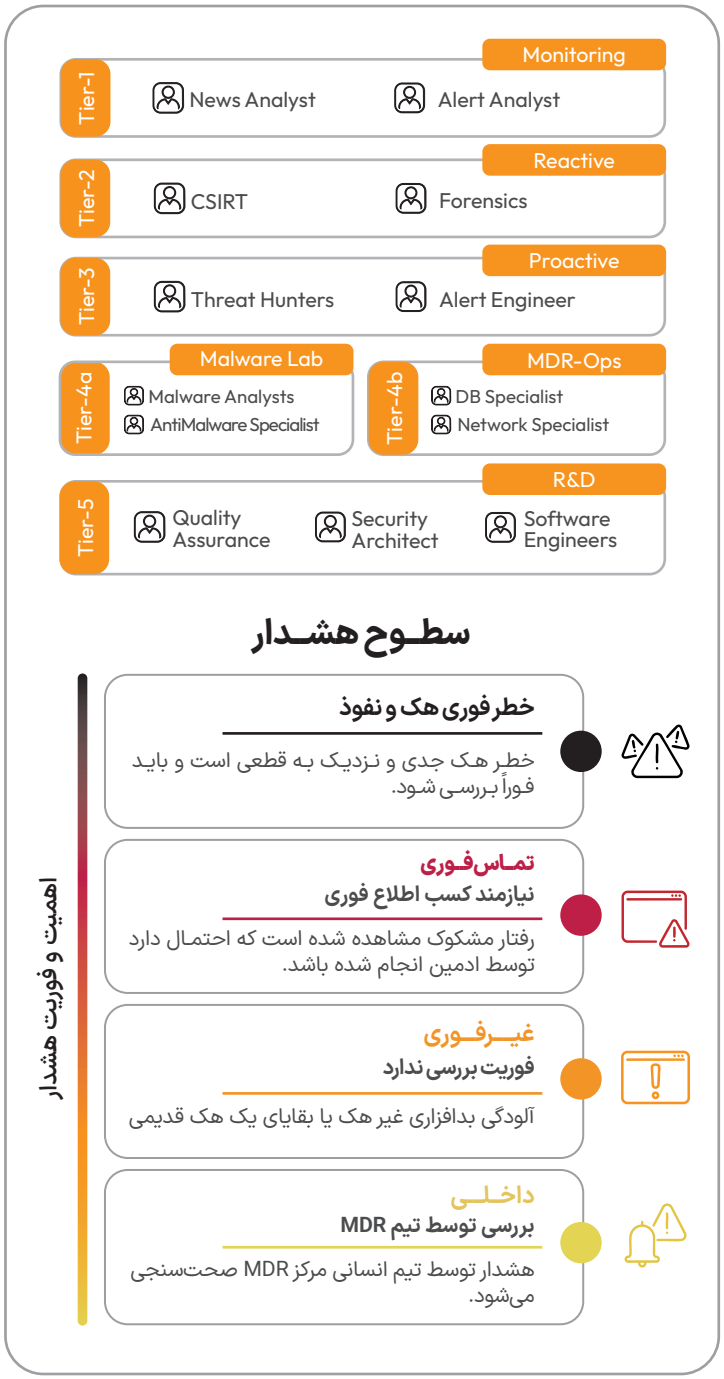
سازمان‌ها می‌توانند با کمک گرفتن از خدمات مرکز کشف و پاسخ به حملات سایبری پادویش، از بهترین متخصصین امنیت سایبری که تجربه مقابله با پیچیده‌ترین حملات سایبری در کشور را دارند بهره بگیرند.



پادویش، نسخه کشف و پاسخ به حملات سایبری با ترکیب آخرین فناوری های هوش مصنوعی در حوزه امنیت و استفاده از متخصصان نخبه داخلی، به صورت ۷×۲۴ از سازمان شما در برابر تهدیدات محافظت می‌کند.

مقابله با حملات سایبری پیچیده نیازمند متخصصان امنیت سایبری با تجربه است.

شما در مواجهه با تهدیدات پنهان سایبری تنها نیستید.
تیم متخصصین امنیتی پادویش جهت مقابله با انواع تهدیدات در کنار شماست.



Padvish
MXDR

راهکار مدیریت‌شده و یکپارچه تشخیص و پاسخ سازمانی

چالش سازمان‌ها

در بسیاری سازمان‌ها، حجم بالای رخدادهای امنیتی، پراکندگی داده‌های تهدید در لایه‌های متخلف، و کمبود نیروهای متخصص باعث می‌شود بخشی از حملات پیچیده یا دیر شناسایی شوند، یا اصلا دیده نشوند. ترکیب ابزارهای ناهمگون، عدم یکپارچگی بین داده‌های شبکه، نقطه پایانی، سرویس‌های اینترنت و ابر، و نبود پایش مداوم، باعث می‌شود SOC سازمان‌ها توان تشخیص تهدیدات چندمرحله‌ای را از دست بدهد و بار عملیاتی تیم‌ها به‌طور مداوم افزایش یابد.

راهکار امن‌پرداز

مرکز جامع و هوشمند تشخیص و پاسخ پادویش با ترکیب توان تحلیلی پلتفرم XDR AI و تیم متخصص عملیات امنیت، یک لایه نظارت ۲۴x۷ ارائه می‌دهد که داده‌های شبکه، نقاط پایانی، سرویس‌های اینترنت و فضای ابری را در یک جریان هم‌بسته تحلیل می‌کند.

Padvish
MXDR

EDR TELEMETRY

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

آیا سازمان شما از منابع داخلی برای مقابله با حملات پیچیده سایبری برخوردار است؟

خدمات مدیریت شده مرکز Padvish MXDR به سازمان‌ها اجازه می‌دهد، بدون نیاز به منابع داخلی گسترده، ابزارهای امنیتی خود را به‌صورت هماهنگ‌تر به‌کار گرفته و از رویکردی جامع‌تر در حفاظت از داده‌ها و زیرساخت‌ها بهره‌مند شوند.

کامل‌ترین راهکار امنیت سایبری پادویش

	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	✓	✓	✓	✓	✓	✓

فناوری ها و خدمات Padvish MXDR

- Anti-Malware
- Memory Scanner
- Behavior Protection
- Machine Learning
- Network Attacks
- Detection
- Network Sensor
- Sandbox
- Detection Engines
- Static File Analyzer
- Appliance Sensor
- CyberGPT

+

- 7*24
- Security Experts
- Exclusive Threat Intelligence
- SLA

سطوح هشدار

غیرقطعی

هشدارهای سیستمی

هشدار توسط تیم انسانی مرکز MXDR صحت‌سنجی می‌شود.

غیرفوری

فوریت بررسی ندارد

آلودگی بدافزاری غیر هک یا بقایای یک هک قدیمی.

تماس فوری

نیازمند کسب اطلاع فوری

رفتار مشکوک مشاهده شده است که احتمال دارد توسط ادمین انجام شده باشد.

بررسی فوری

خطر فوری هک و نفوذ

خطر هک جدی و نزدیک به قطعی است و باید فوراً بررسی شود.

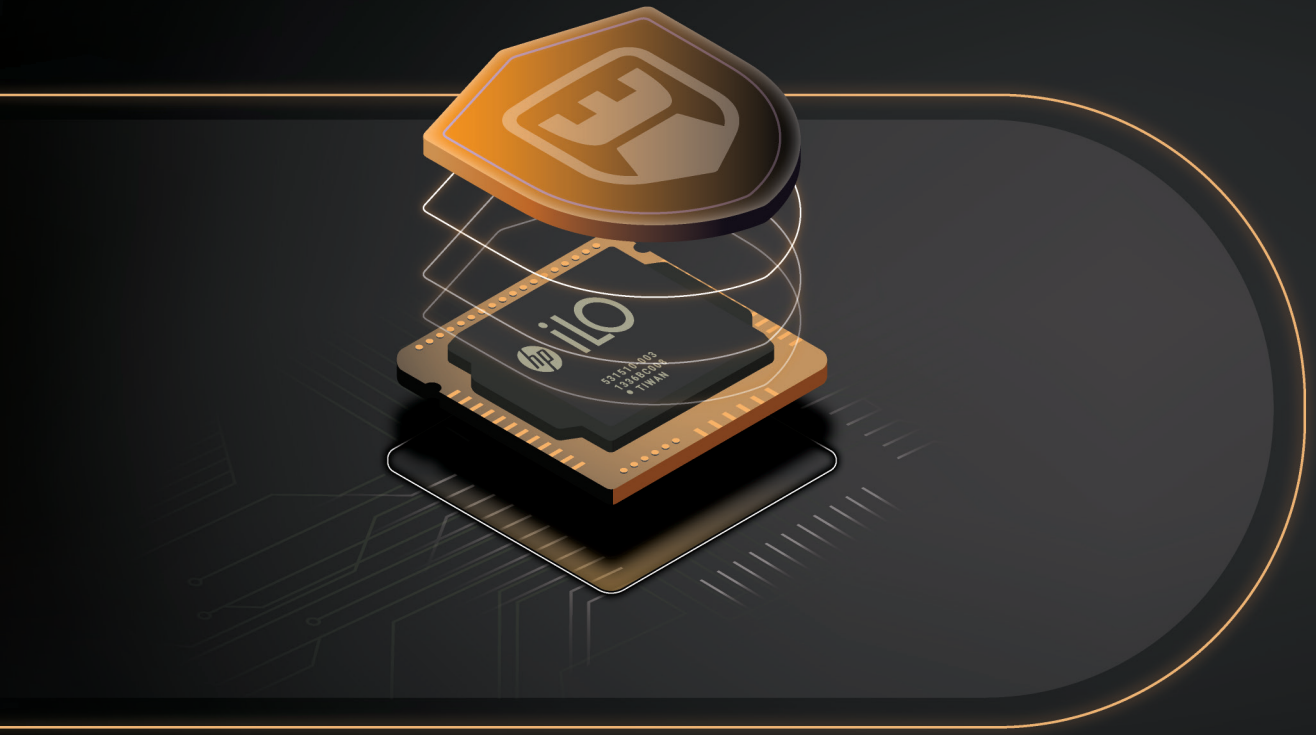
قابلیت‌های کلیدی Padvish MXDR

- پایش ۷×۲۴ شبکه توسط متخصصان زبده برای مقابله با تهدیدات پیشرفته پایدار (APT)
- پشتیبانی مستمر توسط تیم‌های امنیتی مجرب برای واکنش سریع و بهینه‌سازی مداوم
- افزایش سرعت استخراج اطلاعات حیاتی جهت تصمیم‌گیری آگاهانه و سریع در بحران‌ها
- کاهش بار کاری تیم‌های امنیتی از طریق هوشمندسازی فرآیند تحلیل و پاسخ‌دهی
- شناسایی دقیق و ایمن فایل‌های مشکوک، بدون به خطر انداختن سیستم اصلی (سندباکس)
- کاهش خطر تشخیص اشتباه (False Positive) با ترکیب نتایج چند موتور آنتی‌ویروس
- ایجاد انسجام و هماهنگی بین ابزارهای امنیتی مختلف، بدون نیاز به منابع داخلی گسترده
- همکاری نزدیک با تیم‌های مرکز عملیات امنیت برای افزایش اثربخشی دفاع سایبری
- جایگزینی کم‌هزینه برای تیم SOC در سازمان‌های فاقد تیم امنیتی داخلی

Padvish
iLO Scanner

محافظت زیرساخت
برای محافظت از سرورهای سازمان

تشخیص آلودگی‌های سطح سخت‌افزار؛ اعتبارسنجی و پاک‌سازی سفت‌افزار iLO در سرورهای HP



چالش سازمان‌ها

ماژول iLO در سرورهای HP ProLiant حتی زمانی که سرور خاموش است فعال می‌ماند و به تمامی بخش‌های سیستم، از سفت‌افزار و سخت‌افزار تا سیستم‌عامل، دسترسی کامل دارد.

این سطح از دسترسی و نبود ابزارهای بررسی Firmware باعث شده:

- بدافزارهای سطح سخت‌افزار مانند iLOBleed به‌راحتی پنهان شوند؛
- به‌روزرسانی Firmware باعث حذف آلودگی نشود؛
- امکان تخریب داده‌ها، خرابکاری عملیاتی و جاسوسی فراهم باشد؛
- هیچ ابزار امنیتی مرسومی قادر به کشف آن نباشد؛
- آلودگی ماه‌ها و حتی سال‌ها از دید ادمین شبکه پنهان بمانند.

iLO در صورت آلودگی می‌تواند به امنیت ملی، زیرساخت و اعتبار سازمان‌ها آسیب جبران‌ناپذیری وارد کند.

راهکار امن‌پرداز

پس از کشف جهانی iLOBleed توسط امن‌پرداز، نیاز به ابزاری دقیق، سخت‌افزاری و مستقل برای تحلیل مستقیم Firmware کاملا واضح شد.
Padvish iLO Scanner، دستگاهی است سخت‌افزاری، مستقل و قابل‌حمل که بدون نیاز به روشن کردن سرور، مستقیماً به تراشه NOR Flash متصل شده و سلامت سرور را بررسی می‌کند.
این دستگاه نتیجه ترکیب تحلیل سفت‌افزار، مهندسی معکوس، مهندسی سخت‌افزار و توسعه نرم‌افزار در امن‌پرداز است.

Padvish
iLO Scanner

روش عملکرد دستگاه

Padvish iLO Scanner، با یک گیره اختصاصی و مهندسی‌شده مستقیماً به تراشه NOR Flash متصل می‌شود.

مراحل عملکرد

۱. دریافت مستقیم از روی Firmware تراشه
۲. تحلیل سریع و بلادرنگ با الگوریتم اختصاصی
۳. ارائه گزارش اصالت و وضعیت امنیتی Firmware
۴. پاک‌سازی آلودگی‌های احتمالی
۵. به‌روز رسانی به آخرین نسخه معتبر Firmware HP

ویژگی‌ها و قابلیت‌های کلیدی

محافظت پیشرفته

- پایش مستقیم Firmware iLO
- بررسی اصالت Firmware
- تشخیص Rootkitهای سطح سخت‌افزار مانند iLOBleed
- پاک‌سازی آلودگی‌های احتمالی

عملکرد ایمن

- اتصال امن بدون نیاز به روشن‌کردن سرور
- تشخیص اشتباه اتصال گیره و جلوگیری از اتصال کوتاه
- دسترسی مستقیم روی برد بدون جداسازی قطعه

طراحی کاربردی

- دستگاه کاملاً مستقل بدون نیاز به رایانه
- رابط لمسی ۴٫۳ اینچ
- طراحی قابل حمل با دو ماژول باتری قدرتمند
- پشتیبانی از SD Card برای ذخیره گزارش‌ها

سازگاری

- پشتیبانی از سرورهای نسل 8 تا 11 Hp
- تحلیل نسخه‌های iLO4، iLO5 و iLO6

کاربـــردهـا

۱. اطمینـان از امنیت سـرورهـای HP ProLiant
۲. پایش سلامت و اصالت Firmware در مراکز داده
۳. استفـاده در ممیـزی امنیتـی و بازرسـی دوره‌ای
۴. تحلیـل سریع سفت‌افزار بـدون ایجـاد اختـلال در سرویس‌ها

Padvish
OT

محافظت فناوری‌های عملیاتی

برای حفاظت جامع امنیتی از محیط‌های عملیاتی در برابر تهدیدات

محافظت سیستم‌های عملیاتی

چالش سازمان‌های عملیاتی

استانداردهای امنیتی در حوزه فناوری‌های عملیاتی جایگزین کاملی برای حملات پیچیده نیستند. در محیط‌های صنعتی، سرورهای مهم و دستگاه‌های برخط اغلب به‌صورت مستمر و شبکه‌ای در کار هستند؛ در نتیجه، آسیب‌پذیری‌ها، تشخیص نادرست تهدیدات ناشی از عدم تحلیل رفتار و نیاز به دسترسی سریع به سیستم‌ها، موجب افزایش ریسک حوادث سایبری می‌شود. علاوه بر این، نبود قابلیت نصب بدون ریبوت و نیاز به حفظ در دسترس‌بودن سیستم‌های حساس، برای بسیاری سازمان‌های صنعتی-عملیاتی مشکل‌ساز است.

راهکار امن‌پرداز

Padvish OT، راهکار شرکت نرم‌افزاری امن‌پرداز، یک پلتفرم جامع امنیتی برای محیط‌های عملیاتی است که به‌صورت مستقیم به این چالش پاسخ می‌دهد.

این راهکار با توانمندی‌های ویژه خود مانند محافظت پیشرفته از زیرساخت‌های حیاتی عملیاتی، دفاع چندلایه و تقویت‌شده با هوش مصنوعی، محافظت از داده، شبکه و محیط‌های ایزوله و همچنین قابلیت‌های مدیریت و کنترل یکپارچه و سازگاری با سیستم‌های Legacy و کم‌توان، با تأمین امنیت پایدار، تداوم تولید و عملیات را فراهم می‌کند.

Padvish
OT

AVTEST
The Independent IT-Security Institute
Magdeburg Germany

معماری محصول

لایه محافظت سیستم میزبان

- محافظت بلادرنگ پیشرفته
- پشتیبانی از AMSI
- کنترل حافظه‌های جانبی (USB)
- موتور هوشمند ضدباج‌افزار چندلایه با گواهی تشخیص ۱۰۰٪ باج‌افزارها از آزمایشگاه AV-Test آلمان

لایه محافظت برنامه و شبکه

- کنترل برنامه
- کنترل ابزار
- کنترل وب
- شبکه‌های مورد اعتماد
- فایروال

لایه پایش و تحلیل رفتار

- پایش دسترسی به رجیستری
- ارزیابی مستمر آسیب‌پذیری‌های سیستم‌عامل
- تشخیص اتصال‌های غیرمجاز به اینترنت

لایه مدیریت متمرکز و پاسخ

- پشتیبانی کامل از محیط‌های ایزوله (Air-Gapped Mode)
- پیکربندی‌های آماده (Out-of-the-Box-Profiles)
- ابزارهای کمک به انطباق (Compliance Assitance)

لایه امنیت تخصصی صنعتی

- کنسول مدیریت متمرکز
- حالت صرفاً شناسایی
- قابلیت یکپارچه‌سازی با خدمات مدیریت‌شده (MSSP/MDR) امن‌پرداز

چرا Padvish OT ؟

Padvish OT ترکیبی است از بهترین ابزارهای حفاظت شبکه، پیش‌گیری از تهدیدات بدون فایل، و مدیریت ریسک در زمان واقعی، طراحی‌شده برای نیازهای خاص صنعتی که از جمله آن‌ها حساسیت نرخ تأخیر و عدم امکان ریبوت در زمان‌های بحرانی است. این محصول در همان لحظه برطرف‌سازی آسیب‌پذیری‌های شناسایی‌شده، عملیات را به‌صورت خودکار ایمن کرده و در عین حال به مدیران کنترل کاملی بر جمع‌آوری اطلاعات و تجزیه و تحلیل حوادث می‌دهد؛ این محصول کلیه زنجیره عملیاتی سازمان‌های صنعتی را برای تداوم عملکرد و تولید ایمن می‌سازد.

قابلیت‌های کلیدی

۱ ادامه‌پذیری

- حفظ در دسترس بودن ادامه خدمات با تأثیر بسیار کم بر زمان پاسخ‌یابی سیستم‌های بلادرنگ صنعتی

۲ نصب بدون راه‌اندازی مجدد

- امکان نصب و پیکربندی بدون نیاز به ریبوت‌کردن تجهیزات مهم، که در محیط‌های حساس زمان توقف را به‌حداقل می‌رساند.

۳ تاب‌آوری عملیاتی

- افزایش تاب‌آوری عملیاتی و امکان ادامه خدمات در مواجهه با حوادث سایبری و بازیابی سریع.

۴ محافظت یکپارچه

- ترکیب راهکارهای امنیتی‌های سنتی (آنتی‌ویروس، فایروال، کنترل برنامه و دستگاه) با قابلیت‌های خاص OT در یک پلتفرم یکپارچه.

۵ مدیریت متمرکز ریسک

- محیط مدیریتی متمرکز برای دید و کنترل همزمان بر دارایی‌های صنعتی پراکنده، با امکان تعیین سیاست‌ها و واکنش سریع به تهدیدها.

۶ سازگاری با سیستم‌عامل‌های قدیمی (Legacy)

- سازگار و بهینه‌شده برای سیستم‌های مبتنی بر Windows XP SP3+، Windows 7 SP1+ و نسخه‌های بعدی، با درنظرگیری محدودیت منابع.

۷ سازگاری با زیرساخت‌های حیاتی

- مناسب برای زیرساخت های حیاتی (Critical Infrastructure)، شبکه‌های کاملاً ایزوله (Air-Gapped) و سیستم‌های کنترل بلادرنگی که تحمل هیچ‌گونه توقف عملیاتی را ندارند.

محافظت ابری کلودگارد
برای محافظت هوشمند از شبکه، وب‌سایت‌ها و اطلاعات

محافظت ابری و هوش تهدید برای سازمان‌ها

چالش سازمان‌ها

در معماری‌های امروزی، حملات دیگر محدود به شبکه داخلی نیستند و طیف وسیعی از تهدیدات سرویس‌های آنلاین و کاربردی سازمان‌ها را هدف قرار می‌دهند.

راهکار امن‌پرداز

امن‌پرداز با ارائه راهکار جامع و یکپارچه کلودگارد، از وب‌سایت‌ها و شبکه‌ها در برابر تهدیدات پیشرفته محافظت می‌کند. کلودگارد با بهره گیری از فناوری‌های پیشرفته مانند دیواره آتش WAF + CDN، سیستم‌های ضد DDoS و هوش تهدیدات امنیت و پایداری زیرساخت‌های دیجیتال مشتریان را تأمین کند.

Cloud Guard

Managed Security Services

خدمات MSSP

این خدمت به سازمان‌ها امکان می‌دهد تا امنیت فناوری اطلاعات خود را با نظارت ۷/۲۴، مدیریت رخدادها، شناسایی آسیب پذیری‌ها، استفاده از HoneyPot برای جذب و شناسایی مهاجمان، هوشمندی سایبری برای پیش‌بینی تهدیدات و همچنین فناوری‌های پیشرفته مانند NDR (تشخیص و پاسخ در شبکه)، EDR (تشخیص و پاسخ در نقاط انتهایی) و MXDR (تشخیص و پاسخ مدیریت‌شده جامع) به بالاترین سطح برسانند. با بهره‌گیری از این راهکارها، سازمان‌ها می‌توانند از پیشرفته‌ترین ابزارهای نظارت و تحلیل برای شناسایی و مقابله با تهدیدات سایبری بهره‌مند شوند.

Honey Net

هانی نت

سرویس HoneyNet، یک فناوری امنیتی فوق پیشرفته است که به‌طور عمدی برای جذب مهاجمان و هکرها توسط کلودگارد طراحی شده است که شامل مجموعه‌ای از سیستم‌ها و شبکه‌های طعمه‌ای است که به‌صورت هماهنگ عمل می‌کنند و به عنوان یک طعمه پیچیده برای شناسایی تهدیدات و جمع‌آوری اطلاعات درباره تکنیک‌های نفوذ مورد استفاده قرار می‌گیرد.

Web Application Firewall

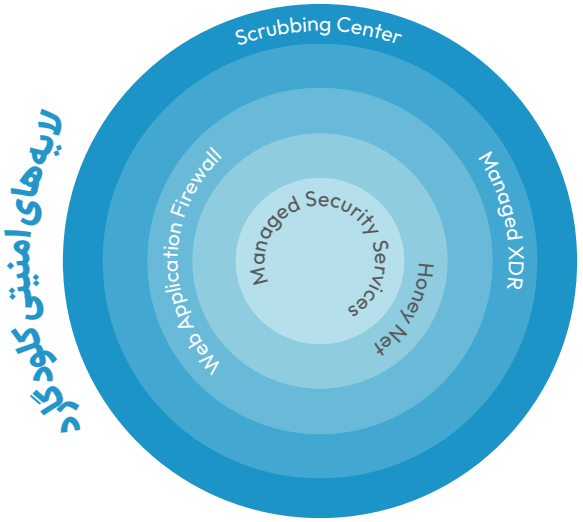
دیوار آتش وب

سرویس WAF کلودگارد با فناوری پیشرفته بی‌نظیر، سپری نفوذناپذیر برای برنامه های وب در برابر حملات پیچیده‌ای مانند (Cross site ،SQL Injection Scripting XSS) و Flood است. این لایه امنیتی بین کاربران و برنامه‌های وب قرار گرفته و ترافیک HTTP و HTTPS را هوشمندانه تحلیل و فیلتر می‌کند تا از هرگونه تهدید جلوگیری کند.

Managed XDR

تشخیص و پاسخ مدیریت شده جامع

سرویس MXDR کلودگارد نظارت ۷/۲۴ و واکنش بلادرنگ به تهدیدات سایبری را با ترکیب هوش مصنوعی و تحلیل‌های پیشرفته ارائه می‌دهد. این راهکار با ادغام NDR، EDR و هوشمندی سایبری، حملات پیچیده را در مراحل اولیه شناسایی و خنثی کرده و امنیتی جامع و هوشمند برای شما فراهم می‌سازد.



Scrubbing Center

مرکز پاک‌سازی ترافیک

کلودگارد با پاک‌سازی بی نقص ترافیک‌های ورودی در لایه‌های ۳ و ۴ و با استفاده از قواعد هوشمند و فوق دقیق، سد راه هرگونه تهدید است که در دیتاسنترهای کلودگارد با منابع عظیم پهنای باند و پردازش قدرتمند، مقابله‌ای بی‌وقفه و پایدار را در برابر حملات حجیم و گسترده فراهم می‌کند.

کلودگارد در یک سال گذشته بیش از

۵۶۰.۰۰۰ حمله

سایبری را شناسایی و دفع کرده است !

فناوری هوشمند

NetSpine

فناوری بی‌نظیر **NetSpine** یک سیستم پیشرفته و خودکار است که در پاسخ به تمامی تهدیدات سایبری و شبکه‌ای عمل می‌کند. با جمع‌آوری و تحلیل گسترده داده‌ها و رخدادها، نظارت بر رخدادهای امنیتی و برقراری ارتباطات پیچیده بین رخدادها، اقدام به تصمیم‌گیری‌های هوشمندانه و واکنش‌های سریع و مؤثر می‌نماید.

- شناسایی کاربران غیرقانونی به‌صورت هوشمند
- بررسی سیستم از پایین‌ترین سطح تا بالاترین سطح
- کشف نفوذهای انجام شده قبلی درصورت وجود **Zero-Day Exploit**

چرا سازمان‌ها **امن‌پرداز** را انتخاب می‌کنند؟

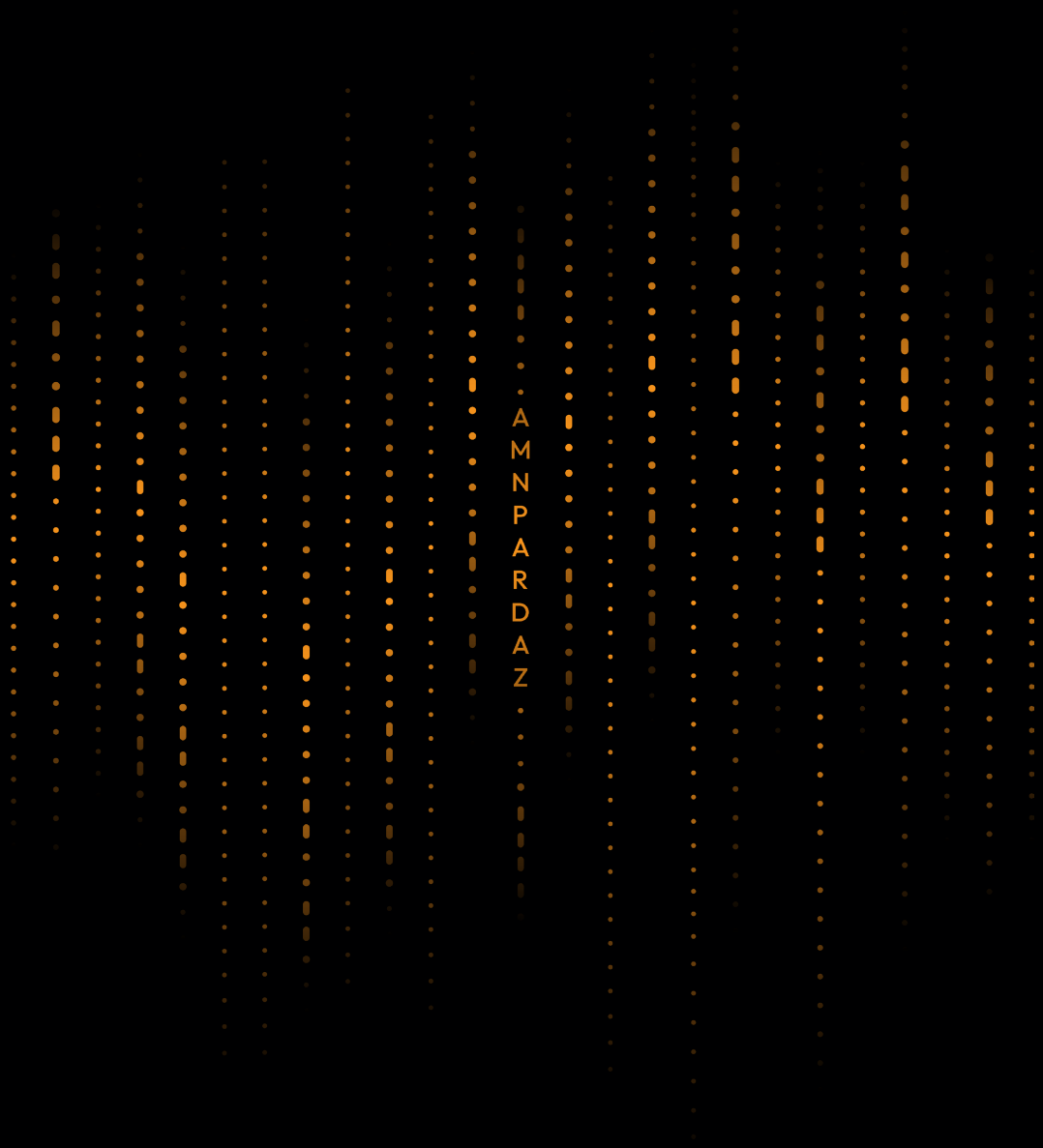
- ارائه راهکارهای امنیتی متناسب با نیاز سازمان‌ها
- ارائه محصولات در لبه فناوری جهان
- خدمات ۷/۲۴
- پشتیبانی همراه و متخصص
- شفافیت، پایداری و رفتار حرفه‌ای

نـوآوری در اعتمـاد سایبـری

Innovating Cyber Trust

راه‌هـای ارتبـاطـی

۰۲۱ - ۴۳۹۱ ۲۰۰۰ info@amnpardaz.com amnpardaz.com


AMNPARDAZ