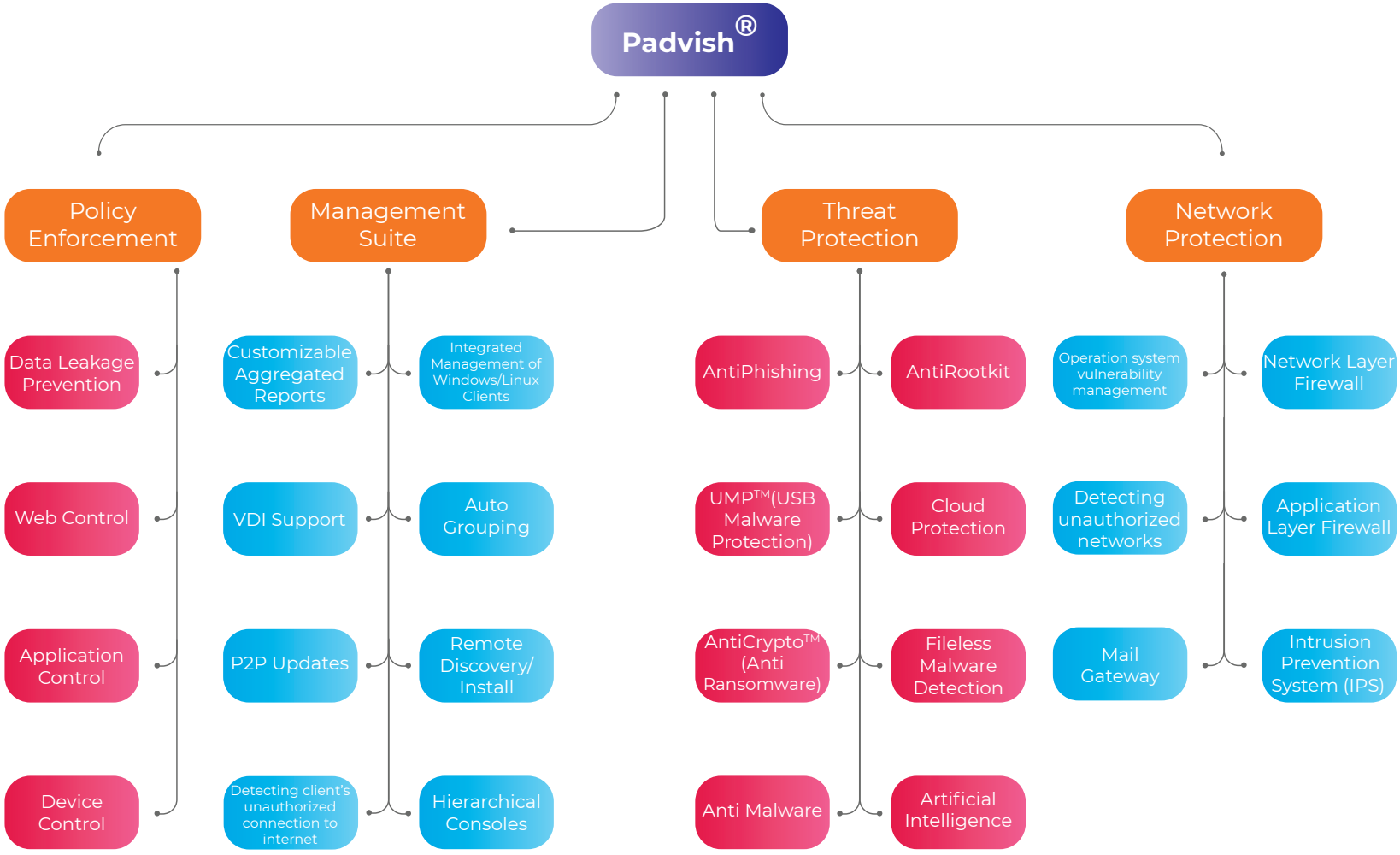
پادویش

راهکارهای امنیت اطلاعات

Padvish Security Solutions

World of Padvish Protection



محافظت همه‌جانبه

محافظت همه‌جانبه

روزانه صدها هزار بدافزار جدید تولید می‌شود که برای محافظت در برابر آنها یک لایه دفاعی یا یک روش به تنهایی کفایت نمی‌کند.
پادویش با بکارگیری لایه‌های متنوع و مکمل امنیتی، حداکثر امنیت را برای شما به ارمغان می‌آورد.

مولفه‌ی تشخیص و جلوگیری از نفوذ پادویش، با بررسی ترافیک شبکه، جلوی انواع حملات از این طریق را گرفته و بدافزار را قبل از رسیدن به سیستم شما متوقف می‌کند.

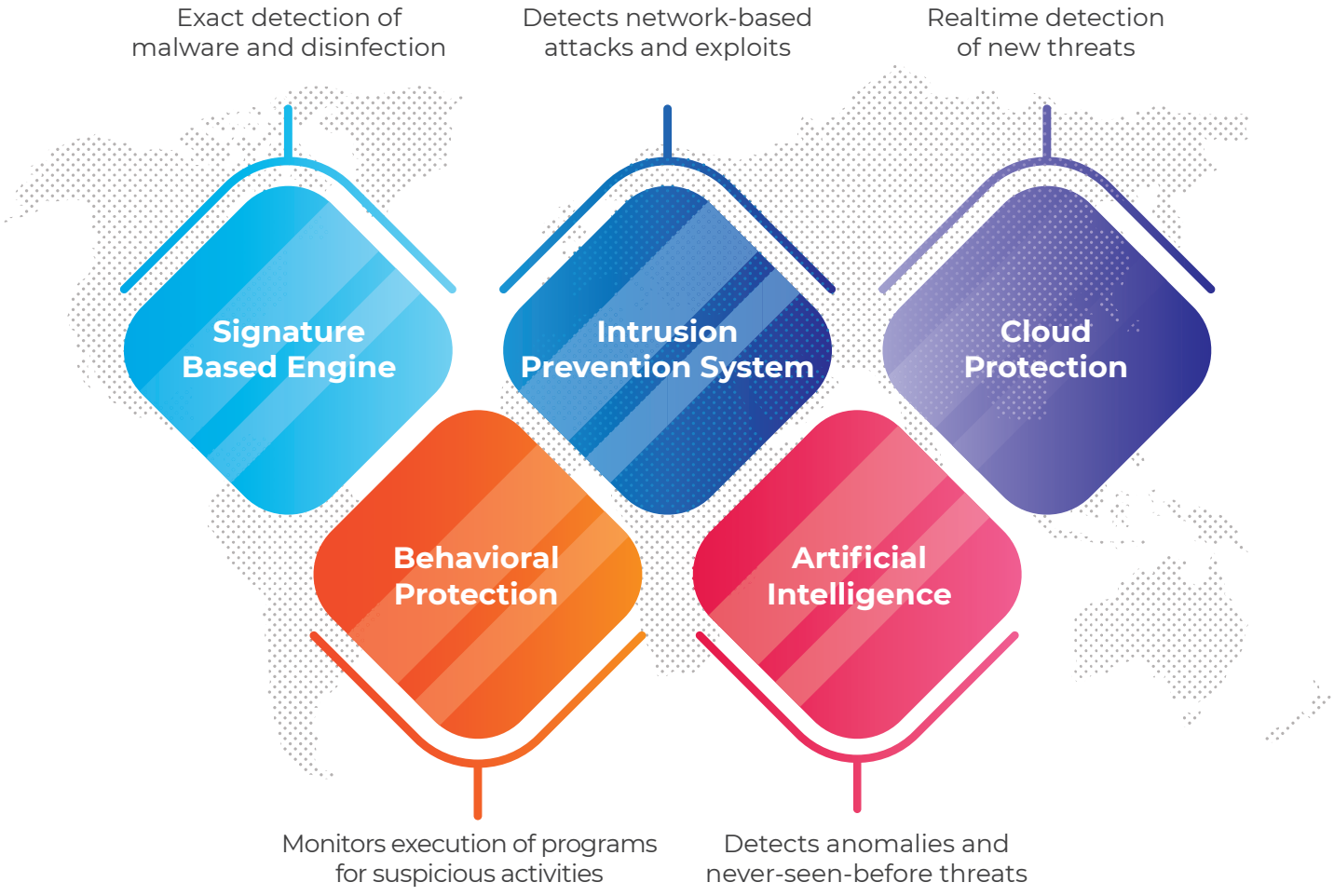
موتور تشخیص بدافزار پادویش، مجهز به انواع تکنولوژی‌های رمزگشایی Packer، شبیه‌سازی اجرا، پویش حافظه، پویش روت‌کیت، رجیستری و ... و با تکیه بر پایگاه امضای چند میلیونی خود، انواع خانواده‌های بدافزاری شناخته شده را قبل از اجرا تشخیص داده و پاکسازی می‌کند.

موتور هوش مصنوعی پادویش، با استفاده از روش‌های یادگیری ماشین و تمرکز بر ویژگی‌های متمایز کننده بدافزار از فایل سالم، امکان تشخیص گونه‌های ناشناخته و جدید بدافزار را فراهم می‌کند.

مولفه‌های محافظت رفتاری پادویش، حین اجرای برنامه‌ها فعال شده و در صورت مشاهده رفتارهای خطرناک مانند باج‌افزارها، آنها را در حین اجرا تشخیص داده و قبل از انجام هرگونه فعالیت مخرب متوقف می‌کند.

همچنین **شبکه‌ی ابری پادویش** با پردازش لحظه‌ای اتفاقات بدافزاری در سطح جامعه‌ی آماری کاربران پادویش، رفتارهای مشکوک و بدافزارهای نوظهور را شناسایی و از فعالیت مخرب آنها جلوگیری به عمل می‌آورد.

Padvish® Anti-Malware Technologies



باج ندهید!!!

باج‌افزار نوعی بدافزار است که اطلاعات سیستم شما را با آخرین الگوریتم‌های روز، رمز کرده و برای بازگشایی و استفاده از اطلاعات از شما طلب باج می‌کند.

برای جلوگیری از باج‌افزار، داشتن یک آنتی‌ویروس خوب کافی نیست، چرا که باج‌افزارها مجهز به روش‌های دور زدن آنتی‌ویروس‌ها هستند و حتی بهترین‌ها هم ۱۰۰٪، شما را محافظت نمی‌کنند.

مولفه‌ی ضدباج‌گیر پادویش با مکانیزم‌های چندلایه و تودرتوی خود، از اطلاعات شما محافظت می‌کند. تمامی این مولفه‌ها به صورت رفتاری عمل می‌کنند، یعنی زمانی که موتورهای تشخیص آنتی‌ویروس نتوانسته‌اند باج‌افزار را تشخیص دهند، این مولفه با بررسی رفتار باج‌افزار، آن را تشخیص داده و متوقف می‌کند.

۱. لایه‌ی محافظت اطلاعات: اولین لایه‌ی محافظتی تکنولوژی ضدباج‌گیر است و به محض تلاش برای رمزگذاری فایل‌های شما وارد عمل می‌شود. این مولفه مانند سایر مولفه‌های ضدباج‌گیر، نیازی به به‌روزرسانی ندارد و در همان اولین سال فعالیت خود موفق به تشخیص و جلوگیری از ده‌ها باج‌افزار کاملا نوظهور، حتی باج‌افزار خطرناک WannaCry گردید، کاری که کمتر نرم‌افزار امنیتی در آن زمان موفق به انجامش شده بود.

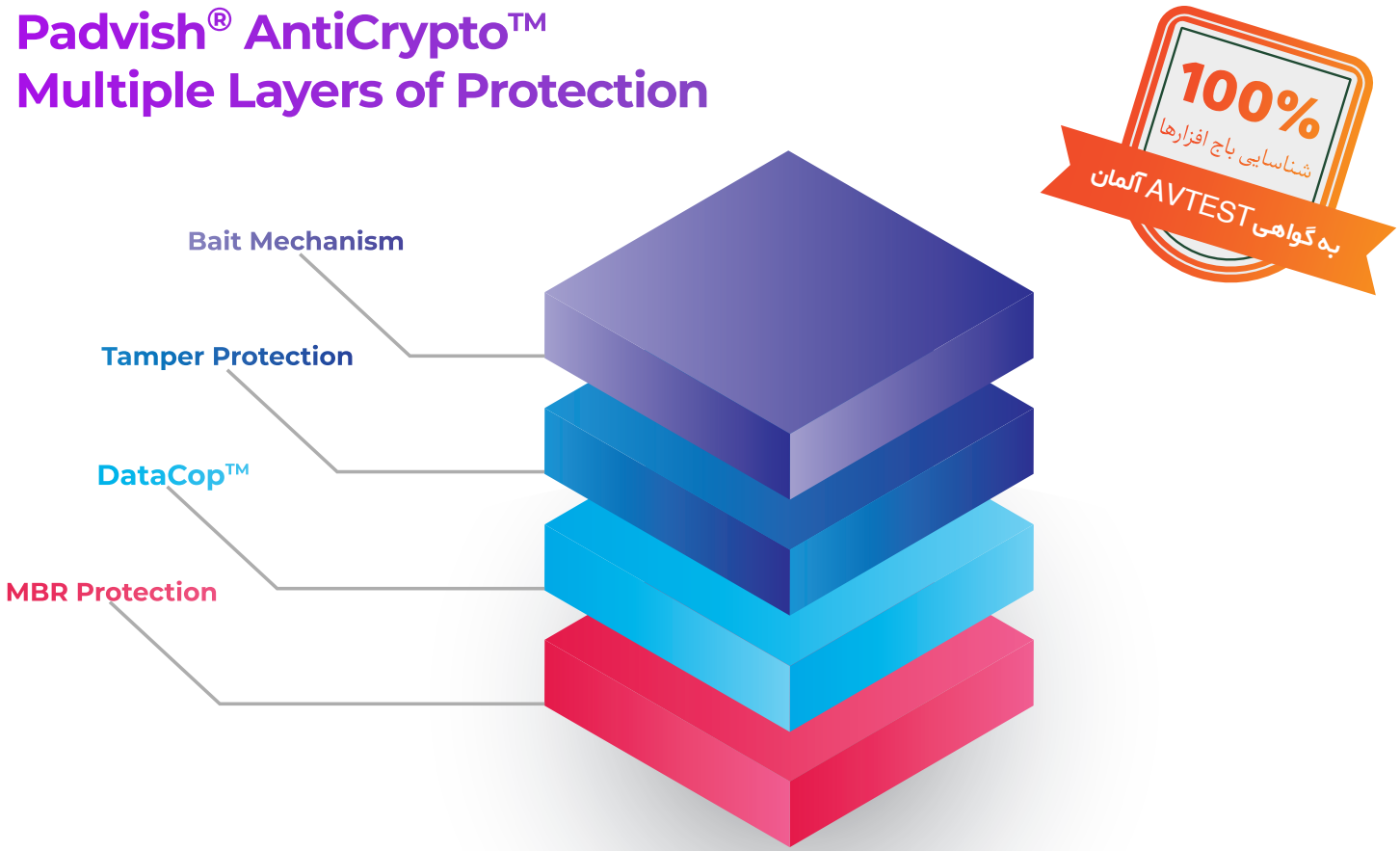
۲. لایه‌ی داده‌بان: روزی دوبار از کل اطلاعات شما پشتیبان گرفته و از حذف شدن این بکاپ‌ها نیز جلوگیری می‌کند. پشتیبان‌گیری ظرف چند ثانیه و تنها با مصرف ۵٪ از حجم هر درایو انجام می‌گیرد و حتی نیازی به تنظیمات یا کار خاصی از سمت شما نیست.

۳. لایه‌ی محافظت MBR: برخی باج‌افزارها با آلوده کردن MBR قبل از بوت ویندوز بالا آمده و هارد را رمز می‌کنند. پادویش جلوی تغییر MBR را گرفته و از این رو هم جلوی این باج‌افزارها را می‌گیرد و هم جلوی روت‌کیت‌های آلوده‌کننده‌ی MBR گرفته می‌شود.

۴. لایه‌ی طعمه گذاری: پادویش برای باج‌افزارها چند فایل طعمه قرار می‌دهد تا هرگاه باج‌افزاری قصد رمز کردن فایل‌های شما را داشت، به جای فایل‌ها به سراغ این طعمه‌ها رفته و همانجا در دام ضدباج‌گیر پادویش گرفتار شود!

این مکانیزم چندلایه، در تست حملات واقعی، گواهی تشخیص ۱۰۰% باج‌افزارها را از آزمایشگاه AV-TEST آلمان دریافت کرده است.

Padvish® AntiCrypto™
Multiple Layers of Protection



به راحتی آب خوردن

به راحتی آب خوردن

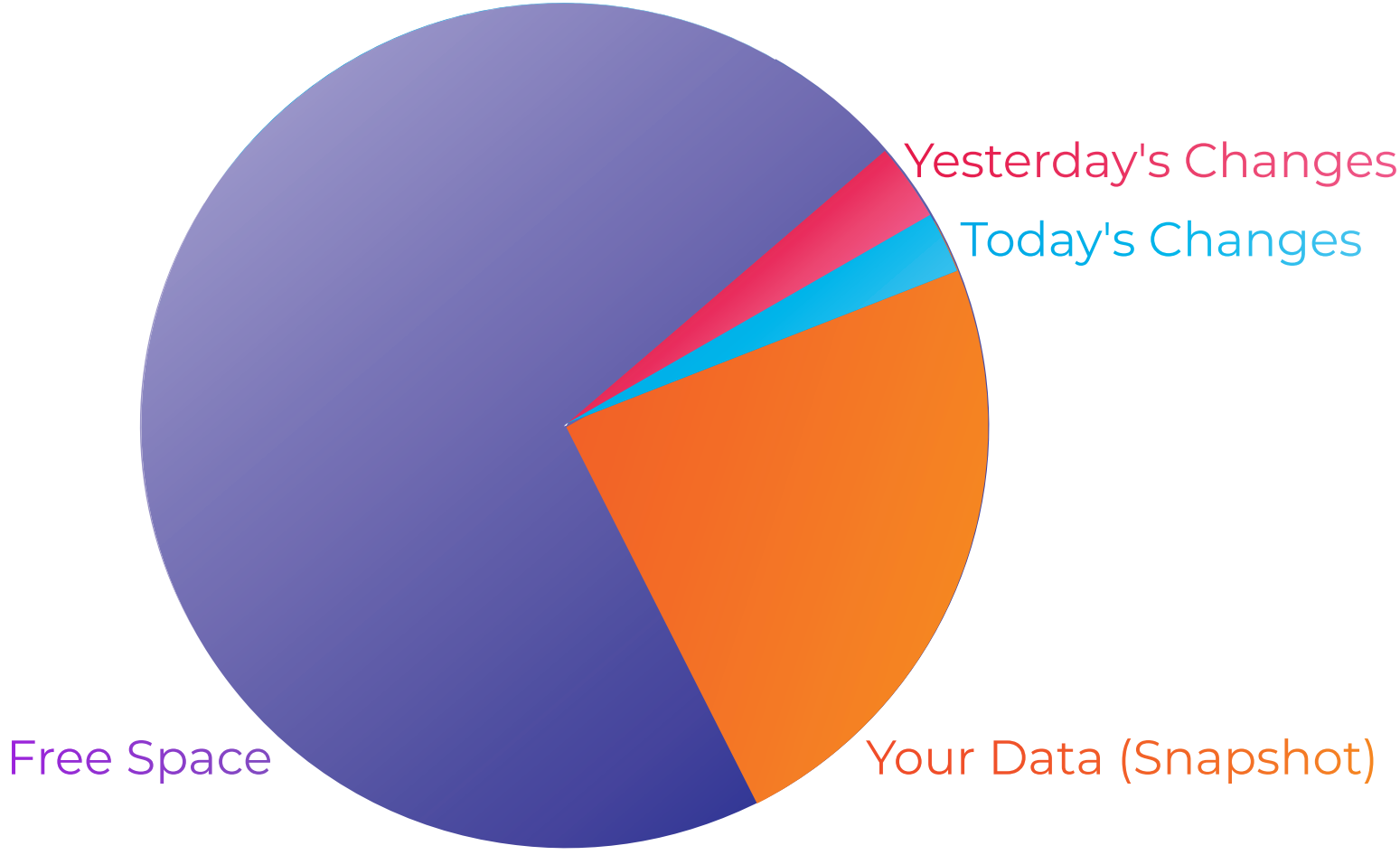
روزی دو بار پشتیبان گرفتن از کل اطلاعات کم است؟

با پادویش هیچوقت حسرت حذف یک سند مهم یا دسترسی به نسخه قبلی آن را نخواهید داشت. چرا که داده‌بان پادویش به صورت کاملا خودکار و ظرف چند ثانیه همه‌ی اطلاعات شما را پشتیبان گرفته و آنها را در برابر اتفاقات نرم‌افزاری و بدافزاری بیمه می‌کند.

داده‌بان پادویش با سازگاری با آخرین تکنولوژی VSS ویندوز و با حداقل سربار (کمتر از ۵٪ حجم درایو) اطلاعات شما را روزی دو بار پشتیبان‌گیری می‌کند و می‌توانید هر لحظه اطلاعات خود را به نسخه‌های قبلی بازگردانی کنید و یا آنها را با هم مقایسه کنید.

داده‌بان پادویش بخشی از تکنولوژی ممتاز ضدباج‌گیر محسوب می‌شود و نشان می‌دهد پادویش صرفا یک آنتی‌ویروس خوب نیست. چرا که هیچ آنتی‌ویروسی چنین امکانی را در اختیار شما نمی‌گذارد.

Padvish® DataCop™
Backup using 5% of drive, in 5 seconds



خیالت راحت، فلش بزن!

خیالت راحت، فلش بزن!

چقدر هنگام زدن فلش‌های جدید به سیستم خود محتاط هستید؟

چند بار تاکنون نگران آلوده شدن دیسک‌های فلش خود و انتقال آلودگی به سیستم خود بوده‌اید؟

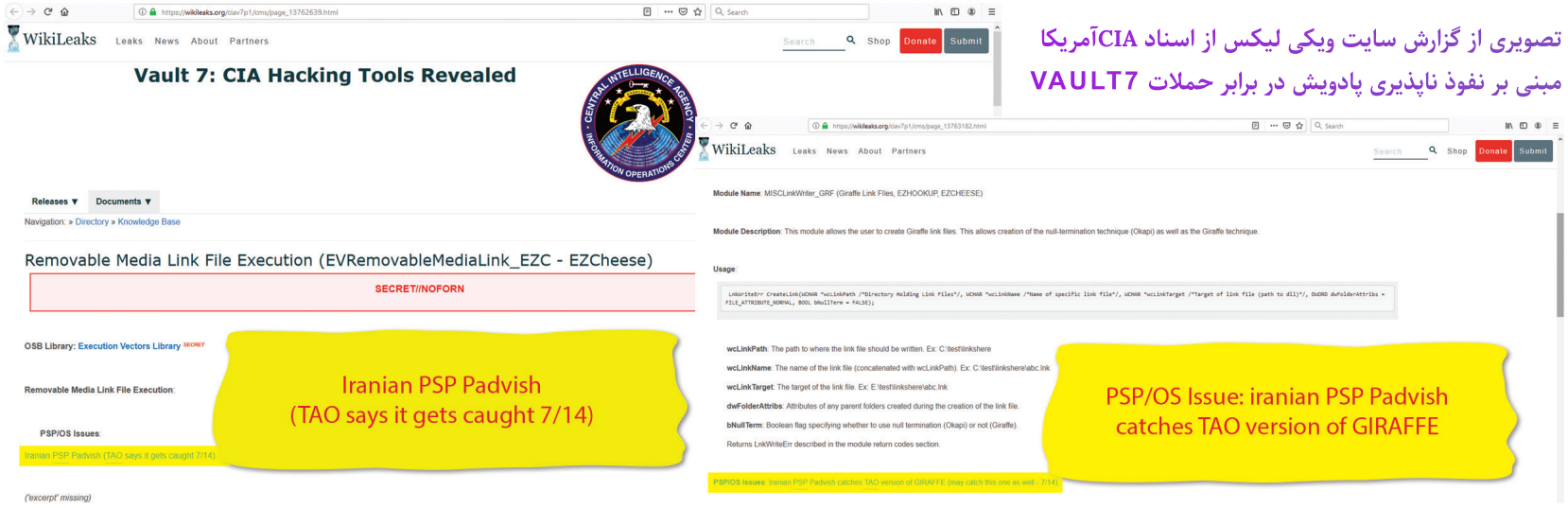
چقدر نگران آلوده شدن سیستم‌ها و شبکه‌ی خود از طریق فلش‌های ویروسی کاربران هستید؟

بسیاری از بدافزارها از طریق فلش منتقل می‌شوند، اما با پادویش نیازی به نگرانی در این زمینه نیست. چرا که حتی اگر فلش شما به ویروس جدیدی آلوده است که توسط هیچ آنتی‌ویروسی قابل شناسایی نیست، باز هم سیستم شما آلوده نمی‌شود.

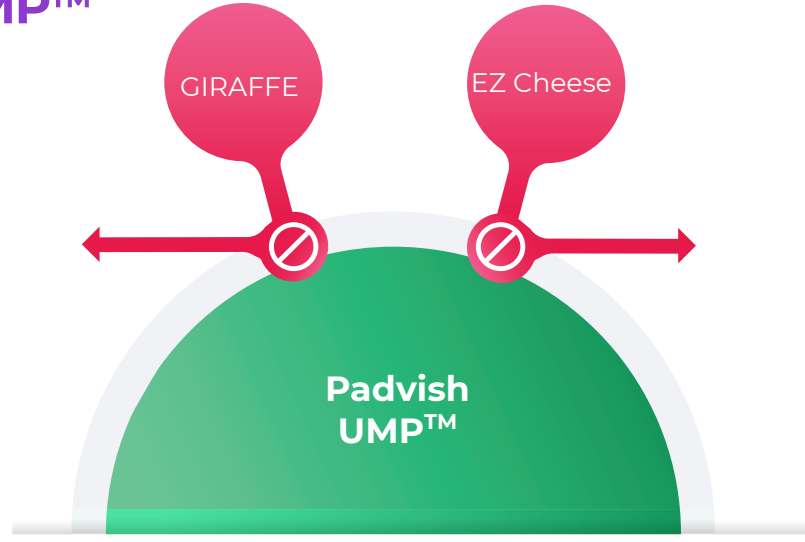
مولفه UMP™ (USB Malware Protection) پادویش با برخی محصولات مبتنی بر autorun و مانند آن متفاوت بوده و حتی بدافزارهایی را که این ابزارها قادر به شناسایی آنها نیستند نیز متوقف می‌کند.

حتی استاکس‌نت و فلِیم هم نمی‌توانند از طریق فلش، سیستم شما را آلوده کنند!

تصویری از گزارش سایت ویکی لیکس از اسناد CIAآمریکا
مبنی بر نفوذ ناپذیری پادویش در برابر حملات VAULT7



Padvish® UMP™



برای سازمان‌های بزرگ

مدیریت شبکه‌های بزرگ و با پراکندگی جغرافیایی بالا پیچیدگی‌های خاص خود را داشته و نیازمند راهکارهای با قابلیت انعطاف بالا و ویژگی‌های خاص می‌باشد.

- حجم بالای کلاینت‌ها؛ راهکار مناسب باید توانایی کار با تعداد بالای کلاینت‌ها و مدیریت آنها را داشته باشد.
- انعطاف‌پذیری و سازگاری با چارت سازمانی و ساختار مدیریت IT سازمان
- پراکندگی جغرافیایی و دور بودن کلاینت‌ها از سرور مدیریتی خود
- محدودیت پهنای باند ارتباطی بین نقاط و شعب مختلف
- محدودیت امکانات سخت‌افزاری و تجهیزات در برخی نقاط
- سخت بودن گزارش‌گیری جامع و قابل اتکا از کل سیستم‌های شبکه

پادویش تجربه‌ی نصب و مدیریت انواع شبکه‌های بزرگ از چند هزار تا چند ده هزار کاربر شامل وزارتخانه‌ها، دانشگاه‌ها، بانک‌ها و سازمان‌های بزرگ دولتی و خصوصی را دارا می‌باشد و برای این موضوع امکانات ویژه‌ای ارائه می‌دهد.

برخی از امکانات پادویش برای سازمان‌های بزرگ:

- امکان تعریف سلسله مراتبی کنسول‌های مدیریتی پادویش
- انجام عملیات مختلف از توزیع لایسنس و به‌روزرسانی تا انجام تنظیمات و دریافت گزارش‌های تجمیعی در کل ساختار سلسله مراتبی
- حداقل استفاده از پهنای باند و قابلیت مدیریت زمان و نحوه توزیع به‌روزرسانی
- امکان توزیع کلاینت به کلاینت (P2P) به‌روزرسانی به صورت خودکار یا سفارشی
- امکان تعریف سطوح دسترسی مختلف برای کاربران و ادمین‌های کنسول مدیریتی
- امکان تقسیم وظایف و گروه‌های کلاینت‌ها بین ادمین‌های کنسول مدیریتی
- انواع روش‌های خودکارسازی از کشف و نصب کلاینت‌ها، تا گروه‌بندی خودکار، حذف کلاینت‌های بلااستفاده، گزارش‌گیری و ...
- امکان پایش و یافتن سیستم‌عامل‌های آسیب‌پذیر بحرانی و یافتن وصله‌های امنیتی مورد نیاز برای هر سیستم

مدیریت یکپارچه هر تعداد کلاینت، از یک نقطه

توزیع بار، توزیع مسئولیت، تجمیع نظارت

در شبکه‌های بزرگ، تعداد بالای کلاینت‌ها، وجود یک ساختار مدیریتی را در واحد IT ایجاب می‌کند. این موضوع در هر سازمان و با توجه به شرایط ویژه آن به نحو متفاوت و متناسبی تقسیم می‌گردد. اما مدیران واحد IT همواره لازم دارند که یک نظارت کامل و جامع بر روی کلاینت‌های کل سازمان داشته باشند.

کنسول مدیریتی پادویش از طریق امکان تعریف ساختار سلسله مراتبی و Master/Slave کردن سرورهای مدیریتی آنتی‌ویروس، انعطاف‌پذیری و جامعیت لازم را برای مدیران شبکه فراهم می‌کند:

- امکان تعریف Master/Slave سرورهای مدیریتی تا هر تعداد سطح لازم
- اطلاعات کلاینت‌ها و پردازش‌های لازم در هر سطح جداگانه انجام گرفته و بار کاری توزیع شده و ترافیک شبکه حداقل می‌گردد.
- در هر سطح مدیر و کاربران کنسول با سطح دسترسی مناسب جداگانه قابل تعریف بوده و می‌توانند مدیریت مجموعه خود را برعهده بگیرند.
- سطوح بالادستی (Master) کنترل کاملی بر زیرمجموعه خود داشته و در مورد همه تنظیمات، از نحوه تخصیص لایسنس گرفته تا کنترل کنسول و تنظیمات آن و دریافت گزارش‌های تجمیعی و غیرتجمیعی لازم از آنها، اختیار تام دارد.
- گزارش‌های تجمیعی، یک آمار واحد از کل ساختار سلسله مراتبی تا کلاینت‌های پایین‌ترین سطح را فراهم می‌کند، آن‌هم به صورت کاملا قابل سفارشی‌سازی.

امنیت واقعی، برای ساختار مجازی!

امروزه فواید مجازی‌سازی (Virtualization) در سادگی، انعطاف‌پذیری، سبکی و استفاده بهینه از تجهیزات و سخت‌افزارها به گونه‌ای است که کمتر شبکه‌ای را می‌توان یافت که گوشه‌ای از آن مجازی‌سازی انجام نشده باشد.

اما ساختارهای دسکتاپ مجازی (VDI) یک قدم جلوتر برداشته و خود کلاینت‌های شبکه را مجازی می‌کنند. این ساختارها اجازه می‌دهند به محض لاگین هر کاربر، یک ماشین مجازی به وی اختصاص یافته و سپس در زمان مقتضی کل ماشین مجازی حذف شده و دور انداخته شود. در این ساختارها به سبب متمرکزسازی عملیات کل کاربران بر روی مجموعه‌ای از سرورهای مرکزی و آمد و رفت بالای ماشین‌های مجازی، نیاز به راهکارهای خاص امنیتی وجود دارد.

نسخه‌های جدید پادویش با پشتیبانی از ساختار VDI امکانات محافظتی منحصربفرد پادویش را در محیط مجازی فراهم کرده و آنتی‌ویروسی سبک و سازگار را ارائه می‌دهد.

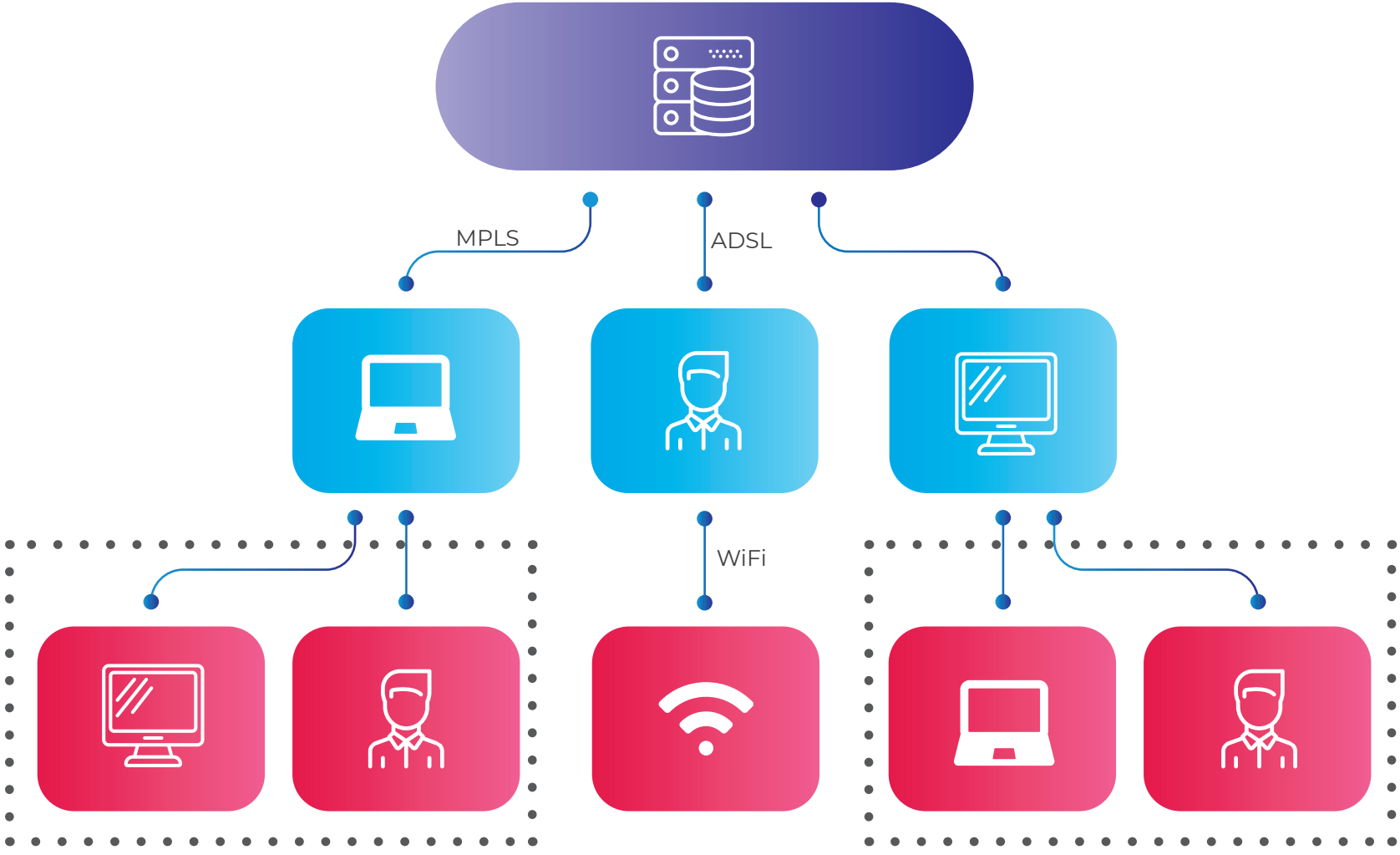
آپدیت رو از بغل دستی بگیر!

آپدیت رو از
بغل دستی بگیر!

توزیع به‌روزرسانی، بیشترین حجم ترافیک شبکه دارای ضدویروس را به خود اختصاص می‌دهد. این موضوع در شبکه‌های بزرگ و با پراکندگی بالا مانند شعب بانک‌ها که از یک طرف محدودیت پهنای باند داشته و بعضا امکان راه‌اندازی سرور جداگانه در هر شعبه را نیز ندارند به یک چالش تبدیل می‌شود. در پادویش علاوه بر کاهش حجم به‌روزرسانی از طریق الگوریتم‌های نوین تفاضلی و فشرده‌سازی آن و نیز مدیریت خودکار یا زمان‌بندی شده توزیع به‌روزرسانی، امکان تشخیص خودکار کلاینت‌های مستقر در یک subnet شبکه و توزیع بهینه به‌روزرسانی در بین آنها (P2P) وجود دارد. بدین ترتیب در هر بخش شبکه، تنها یکی از کلاینت‌ها آپدیت را از سرور دریافت کرده و سپس بین کلاینت‌های اطراف خود توزیع می‌کند.

اگرچه این فرآیند به صورت خودکار قابل انجام است، اما برخی ادمین‌ها با توجه به اشراف بر شرایط شبکه، تمایل دارند این تنظیمات را به صورت دقیق تعریف نمایند. به همین علت کنسول پادویش امکان نظارت دقیق بر این فرآیند را به طور کامل در اختیار ادمین قرار می‌دهد و در صورت انتخاب گزینه دستی، امکان تعریف گروه‌ها و کلاینت‌های توزیع کننده نیز وجود دارد.

Padvish® P2P Update Service



کنترل کامل حتی در Safe Mode

برخی کارهای کاربران تن هر ادمین شبکه‌ای را می‌لرزاند!

مراجعه به سایت‌های خطرناک، اتصال فلش و موبایل ویروسی به سیستم، اتصال کلاینت از طریق گوشی به اینترنت(!)، جابجا کردن ابزارهای جانبی سیستم‌های همدیگر در شبکه، سروگوش کشیدن در شبکه با انواع ابزارهای پویش شبکه، نصب انواع بازی‌ها یا پیام‌رسان‌ها، تلاش برای دور زدن سیاست‌های سازمان و ...

تشخیص بدافزار و امن‌سازی شبکه تنها رسالت کنسول آنتی‌ویروس نیست!

کنسول مدیریتی پادویش به مدیر شبکه اجازه می‌دهد سیاست‌های سازمان خود را در زمینه‌های استفاده از سیستم‌ها و شبکه تعیین کند. در برخی سازمان‌ها برای دسترسی به سایت‌های دانلود، سرگرمی، یا ایمیل و مانند آن محدودیت‌هایی تعریف شده است یا برای اجرای برنامه‌های آسیب‌پذیر یا آسیب‌زا ممنوعیت‌هایی وجود دارد که باید اعمال گردد.

کنترل وب پادویش با هدف سادگی کاربری و سرعت عملکرد طراحی شده و به مدیر شبکه اجازه می‌دهد سیاست‌های لازم را برای رایانه‌های شبکه‌ی خود اعمال نماید.

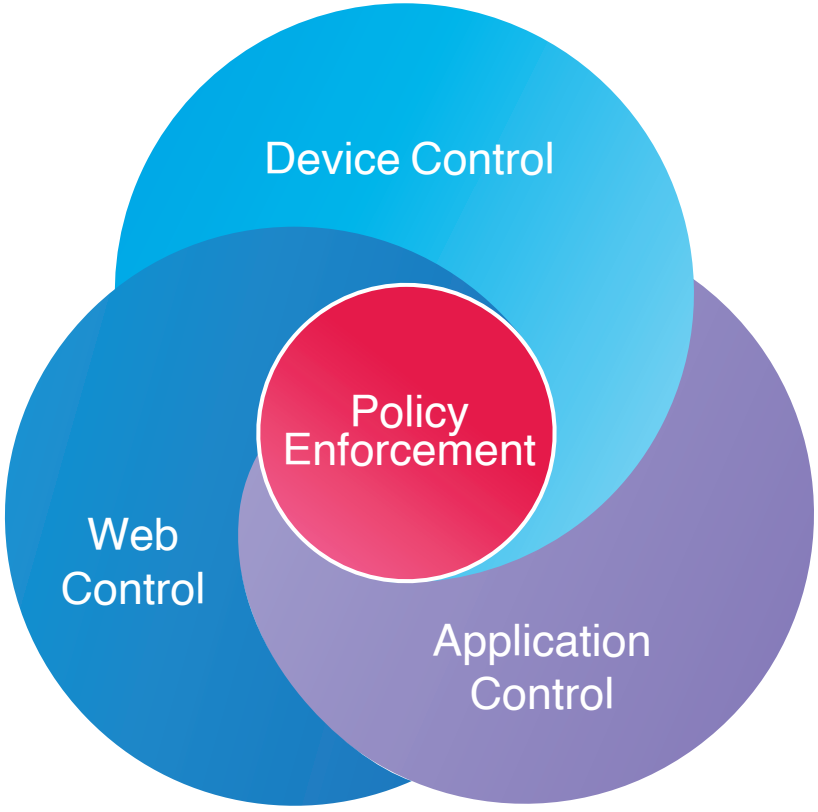
کنترل برنامه‌ی پادویش، با تشکیل خودکار بانک اطلاعاتی از نرم‌افزارهای موجود در کل شبکه (چه نصب شده و چه پرتابل) به شما اجازه می‌دهد اجرای نرم‌افزارهای خاصی (مانند ابزارهای تست نفوذ، بازی‌های رایانه‌ای و ...) را در شبکه محدود نمایید.

برخی سیستم‌ها نباید هرگز به شبکه اینترنت متصل شوند. با استفاده از قابلیت **تشخیص دسترسی به اینترنت پادویش**، بر اتصالات سیستم‌های رایانه‌ای کاربران نظارت کرده و در صورت اتصال به شبکه اینترنت، موضوع را لاگ‌برداری کرده و به مدیر شبکه اطلاع می‌دهد. در این قابلیت امکان تشخیص اتصال بدون مجوز کلاینت به اینترنت و گزارش‌گیری از ارتباطات اینترنتی مشاهده شده فراهم می باشد.

با قابلیت ویژه **مدیریت شبکه‌های مورد اعتماد پادویش**، اگر کاربری تلاش کند سیستم خود را به شبکه‌ای غیر از شبکه‌های مورد اعتماد تعریف شده متصل کند، ارتباطات شبکه وی مسدود شده و مدیر شبکه از این کار مطلع می‌گردد. فعال نمودن این قابلیت، سیستم‌ها را در برابر انتقال اطلاعات غیرمجاز از طریق تجهیزات شبکه و یا هاردهای NAS مصون می‌کند. با استفاده از این قابلیت می‌توانید شبکه‌های مورد اعتماد تعریف کنید، از دسترسی کلاینت‌ها به شبکه‌هایی بجز شبکه‌های مورد اعتماد تعریف شده جلوگیری نمایید و از موارد نقض سیاست‌های تعریف شده در شبکه‌های مورد اعتماد گزارش‌گیری جامع داشته باشید.

قابلیت **کنترل ابزار و جلوگیری از نشت اطلاعات پادویش**، یک بانک اطلاعاتی کامل از سخت‌افزارهای موجود در شبکه تهیه کرده و به شما اجازه می‌دهد از اتصال و کندن هر ابزاری مطلع شوید. به علاوه شما امکان محدود کردن ابزارهای مجاز اعم از فلش، هارداکسترنال، موبایل، مودم، و ... را نیز دارید. هر ابزار می‌تواند صرفا محدود شود، یا اینکه سیستم کاربر خاطی را قفل کرده و تا زمان کندن ابزار یا دخالت ادمین اجازه‌ی استفاده از سیستم به کاربر داده نشود.

خبر خوب اینکه برخلاف برخی محصولات خارجی، تمام این محافظت‌ها در Safe Mode هم برقرار است!



مدیریت آسیب‌پذیری سیستم عامل

روزانه به طور مستمر آسیب پذیری های جدیدی برای سیستم عامل ها اعلام می‌شود که برخی از این آسیب‌پذیری‌ها، بسیار حساس و بحرانی می‌باشند. این آسیب‌پذیری‌ها به مهاجمین اجازه می‌دهد به دنبال نفوذ به سیستم، دسترسی به اطلاعات با ارزش و ایجاد خرابکاری در سیستم‌عامل‌ها باشند.

به همین علت یکی از وظایف روزانه مدیر شبکه، بررسی شبکه، یافتن سیستم‌های آسیب‌پذیر و نصب وصله جهت رفع نقاط ضعف می‌باشد. پادویش با پویش آسیب‌پذیری‌های سیستم و گزارش آن به مدیر شبکه کمک می‌کند تا این فرآیند را سریع‌تر، راحت‌تر و دقیق‌تر انجام دهد.

مدیریت آسیب‌پذیری سیستم‌عامل شامل موارد زیر می‌باشد:

- گزارش جامع از نوع، میزان و گستردگی آسیب‌پذیری‌های موجود
- دسته‌بندی بر اساس میزان خطرناک بودن و مدت حیات آنها در سازمان
- بررسی جزئیات وصله‌های نصب شده و نصب نشده

- مناسب برای حفاظت از سازمان‌های بزرگ و دارای شبکه فناوری اطلاعات چند منظوره
- لایه‌های حفاظتی متنوع به منظور مقابله با جدیدترین تهدیدها
- پیاده سازی سریع با حداقل نیازمندی‌های سخت‌افزاری
- بهره‌گیری از تکنولوژی یادگیری ماشین در مواجهه با بدافزارهای پیچیده
- مدیریت آسیب‌پذیری‌های سراسر سازمان
- تکنولوژی ابر پادویش به منظور پاسخگویی سریع به تهدیدهای جدید
- سیستم گزارش‌دهی متنوع و کارا
- پیشگیری از اجرای نرم‌افزارهای منتخب

ایمیلی امن
بدون مزاحم

ایمیلی امن
بدون مزاحم

ایمیل‌های آلوده به انواع بدافزار و گسترش هرزنامه‌ها در فضای اینترنت به معضلی بزرگ تبدیل شده‌است. تبلیغات بیهوده و جعلی، بدافزارهای ایمیلی و انواع اسپمرها سالانه خسارت زیادی را به سازمان‌ها وارد می‌کنند.

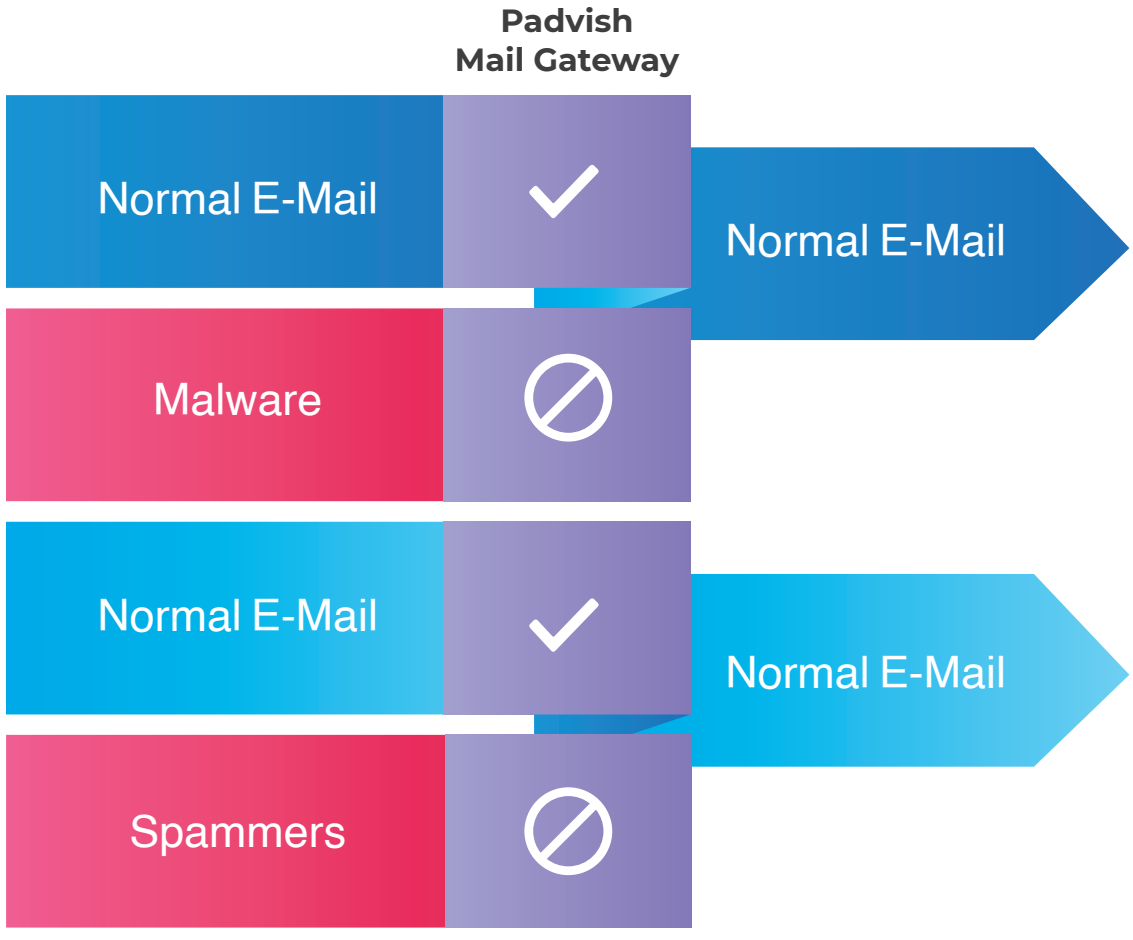
درگاه ایمیل پادویش، راهکاری قدرتمند و کارآمد در برابر هجوم آسیب‌های ایمیلی است.

این درگاه با فیلتر کردن مسیر ایمیل‌های ورودی، انواع بدافزارهای ایمیل شده به سازمان را شناسایی و مسدود می‌کند.

همچنین با شناسایی انواع هرزنامه‌ها از ورود حجم بالایی از ایمیل‌های بیهوده جلوگیری می‌کند.

نصب سریع و آماده سازی بسیار ساده و روان، تجربه ای لذت بخش از ایمیل‌ها و فضای نامه نگاری اینترنتی را برای شما فراهم می‌آورد.

Padvish® Mail Gateway System



کنسولی برای چند ادمین

کنسولی برای چند ادمین

چند ادمین در یک کنسول می‌گُنجند!

در برخی شبکه‌ها، به دلایل فنی و محدودیت‌های موجود، امکان اختصاص سرورهای مدیریتی برای بخش‌های مختلف وجود ندارد و همه کلاینت‌ها تحت یک کنسول مدیریت می‌شوند.

اما تقسیم کار بین ادمین‌ها ایجاب می‌کند که هر کس تنها کلاینت‌های تحت مدیریت خود را دیده و تنظیمات مربوط به آنها را انجام دهد.

همچنین ممکن است یک نفر وظیفه نصب و اتصال کلاینت‌ها را برعهده داشته و مدیریت تنظیمات کلاینت‌ها یا گزارش‌گیری به عهده کاربر دیگری قرار گیرد.

سیستم کنترل سطح دسترسی کاربران در کنسول مدیریتی پادویش به شما اجازه می‌دهد همه سناریوهای مختلف را پیاده‌سازی نمایید.

برای هر کاربر کنسول مدیریتی پادویش، سطوح دسترسی به جزء، قابل تعریف هستند؛ رویت کلاینت‌ها، تغییر تنظیمات، گزارش‌گیری و ...

همچنین امکان محدود کردن یک کاربر کنسول به رویت (و مدیریت) گروه‌های مشخصی از کلاینت‌ها وجود دارد. در این حالت یک ادمین، کلاینت‌های ادمین دیگر را ندیده و امکان تداخل در وظایف نیز وجود ندارد.

شرکت نرم‌افزاری امن پرداز®

Amnpardaz Soft®

@PadvishSecurity

www.padvish.com
www.amnpardaz.com