# معرفی محصول Padvish DLP

شرکت نرم افزاری امن پرداز

**سطح محرمانگی: عادی**

شرکت نرم افزاری
امن پرداز

نسخه ۱.۱
بهار ۱۴۰۵

# فهرست مطالب

فهرست مطالب

# ۱. مقدمه

در عصر حاضر، اطلاعات به عنوان ارزشمندترین دارایی راهبردی سازمان‌ها شناخته می‌شوند. تولید، پردازش و تبادل این داده‌ها در بستر فناوری اطلاعات انجام می‌گیرد و حفاظت از آن‌ها در برابر دسترسی‌های غیرمجاز و نشت احتمالی، به یکی از اولویت‌های اصلی مدیران ارشد امنیت اطلاعات تبدیل شده است؛ چرا که پیامدهای ناشی از نقض داده‌ها می‌تواند خسارات جبران‌ناپذیری برای سازمان‌ها به همراه داشته باشد.

بر اساس گزارش‌های معتبر امنیتی در سطح جهانی، یکی از متداول‌ترین حملات سایبری، هدفگیری داده‌های حساس سازمان و تهدید به افشای آن‌هاست. علاوه بر این، نشت اطلاعات (خواه ناشی از فعالیت‌های مخرب داخلی یا اشتباهات کاربران) نیز خطری جدی محسوب می‌شود. عوامل مذکور لزوم به‌کارگیری راهکارهای جامع حفاظت از اطلاعات را بیش از پیش ضروری ساخته است.

شرکت نرم‌افزاری امن‌پرداز برای مقابله با این تهدیدات، راهکار Padvish DLP را ارائه کرده است. این محصول با بهره‌گیری از قابلیت مدیریت حقوق دیجیتال (DRM) مبتنی بر رمزنگاری پیشرفته و تعریف سیاست‌های دسترسی پویا دسترسی به اطلاعات سازمان‌ها را مدیریت می‌نماید.

Padvish DLP با استفاده از معماری رمزنگاری نامتقارن، امنیت داده‌ها را در سطح فایل تضمین می‌کند. در این معماری، کلید خصوصی به‌صورت امن در سرور مدیریتی سازمان نگهداری شده و کلید عمومی در اختیار کلاینت‌های مجاز قرار می‌گیرد. بدین ترتیب، هر سند تولیدشده در کلاینت، به‌طور خودکار و شفاف از دید کاربر رمزگذاری می‌شود و تنها با اخذ مجوز از سرور مرکزی و مطابق با سیاست‌های تعریف‌شده، قابل بازیابی است.

از مزایای کلیدی این راهکار، عدم نیاز به تغییر در فرآیندهای کاری کاربران نهایی است. کاربران می‌توانند با استفاده از نرم‌افزارهای متداول (نظیر Microsoft Office، Adobe PDF و سایر برنامه‌های مورد اعتماد) به کار خود ادامه دهند، در حالی که رمزنگاری و نظارت بر دسترسی به‌صورت کاملاً شفاف در پس‌زمینه انجام می‌پذیرد.

مقدمه

علاوه بر این، تمهیدات امنیتی گسترده‌ای برای جلوگیری از نشت داده (حتی توسط کاربران داخلی) در نظر گرفته شده است. از جمله این اقدامات می‌توان به محدودیت در پرینت، تهیه اسکرین شات از صفحه و تهیه کپی از محتوا به خارج از محیط اسناد محافظت‌شده اشاره کرد. لازم به ذکر است که تبادل داده بین اسناد امن و نیز چاپ برای کاربران مجاز، بدون محدودیت و به سهولت امکان‌پذیر است.

این سند، به معرفی جامع محصول Padvish DLP، ویژگی‌های فنی و قابلیت‌های کلیدی آن خواهد پرداخت.

# ۲. قابلیت‌های فنی

قابلیت‌های محصول Padvish DLP در چهار حوزه زیر دسته‌بندی می‌شود:

- محافظت داده در پردازش (Data in Use)
- محافظت داده در انتقال (Data in Motion)
- محافظت داده در ذخیره‌ساز (Data at Rest)
- قابلیت‌های سازگاری و مدیریتی (Management)

## ۲٫۱. محافظت از داده‌ها در حالت پردازش (Data in Use)

محصول Padvish DLP با به‌کارگیری مکانیزم‌های کنترلی پیشرفته، از داده‌های سازمان در حین پردازش و استفاده فعال محافظت می‌نماید. این راهکار با اعمال سیاست‌های امنیتی یکپارچه در لایه‌های مختلف زیر، مانع از نشت اطلاعات در حین کار کاربران می‌شود:

- کنترل ابزارهای جانبی (Device Control)
- کنترل برنامه‌های کاربردی (Application Control)
- کنترل انتقال فایل (File Transfer Control)
- کنترل عملیات پرینت (Print Control)
- کنترل حافظه موقت (Clipboard Control)
- محافظت در برابر تهیه اسکرین شات از صفحه (Screenshot Protection)
- نظارت بر مولفه‌های سخت‌افزاری و نرم‌افزاری (Hardware/Software Monitoring)

تمامی این قابلیت‌ها به صورت متمرکز و مبتنی بر سیاست‌های تعریف‌شده سازمانی عمل نموده و امکان نظارت، کنترل و گزارش‌گیری جامع از فعالیت‌های کاربران را در اختیار مدیران امنیت اطلاعات قرار می‌دهد.

در ادامه به معرفی هر یک از این قابلیت‌ها می‌پردازیم.

### ۲/۱/۱. کنترل ابزارهای جانبی (Device Control)

وظیفه مولفه کنترل ابزارهای جانبی، نظارت و مدیریت جامع بر اتصال کلیه دستگاه‌های ذخیره‌سازی و ارتباطی به سیستم‌های سازمان می‌باشد. این قابلیت طیف گسترده‌ای از تجهیزات را پوشش داده و امکان اعمال سیاست‌های امنیتی دقیق را فراهم می‌نماید.

#### ۲/۱/۱/۱. ابزارهای جانبی قابل مدیریت

لیست انواع ابزارهایی که در این محصول کنترل می‌شود شامل موارد زیر است:

| | | | | |
|---|---|---|---|---|
| USB Storages | Optical Disks | Floppy Disks | Bluetooth Devices | Infrared Devices |
| Portable Devices | Scanners | Capture Cards | WebCams | Internal Network Adapters |
| External Network Adapters | Internal WiFi Adapters | External WiFi Adapters | Modems | Printers |

#### ۲/۱/۱/۲. امکان تعیین قواعد پیشرفته

در کنار سیاست‌های پایه، سامانه کنترل ابزارهای جانبی پادویش از قواعد پیشرفته و مبتنی بر شناسه‌های دقیق دستگاه پشتیبانی می‌نماید. این قابلیت امکان اعمال کنترل‌های بسیار جزئی و سفارشی را برای مدیران امنیت فراهم می‌سازد.

- تطبیق دقیق نام ابزار(Device Name)
- تطبیق بخشی از نام ابزار(Device Name)
- تطبیق دقیق شناسه ابزار(Device ID)
- تطبیق بخشی از شناسه ابزار(Device ID)
- تطبیق ابزارهای دارای تگ مشخص (تگ‌گذاری شده توسط ادمین)
- تطبیق شناسه سازنده و شناسه محصول (مخصوص USB Storage)

### ۲/۱/۱/۳. انواع عملیات

در قاعده‌گذاری پیشرفته امکان تعریف واکنش‌های زیر وجود دارد:

- Allow and log (اتصال مجاز)
- Read-only and log (اتصال فقط خواندنی – امکان‌پذیر در هر سه نوع دستگاه USB Storage، Optical Disk و Portable Device)
- Block and log (جلوگیری و لاگ‌برداری)
- Block and lock-screen (قفل صفحه تا زمانی که ابزار غیرمجاز از سیستم جدا شود)
- Block and password-protected lock-screen (قفل صفحه پسورددار –در این حالت جدا کردن ابزار یا حتی ریست کردن سیستم برای باز شدن قفل صفحه کافی نیست و حتماً باید سیستم توسط ادمین از قفل خارج شود)
- Block and restart (ریستارت سیستم در صورت اتصال ابزار غیرمجاز)
- Block and shutdown (خاموش کردن سیستم در صورت اتصال ابزار غیرمجاز)

### ۲/۱/۱/۴. بانک ابزار (Device Bank)

بانک ابزار در پادویش DLP به عنوان یک مخزن متمرکز، اطلاعات جامعی از کلیه ابزارهای جانبی متصل به سیستم‌های تحت پوشش شبکه را جمع‌آوری و مدیریت می‌نماید. این قابلیت، دید کاملی از اکوسیستم دستگاه‌های متصل به سازمان در اختیار مدیران امنیت قرار می‌دهد.

قابلیت‌های کلیدی بانک ابزار:

۱. مشاهده لیست کامل ابزارهای متصل شده به همراه تاریخ اولین و آخرین اتصال و اطلاعات کلاینت مرتبط
۲. اعطا یا لغو مجوز دسترسی برای دستگاه‌ها به سادگی
۳. امکان تگ‌گذاری و گروه‌بندی ابزارها برای استفاده در قواعد کنترل دسترسی
۴. تعریف نام‌های قابل فهم برای دستگاه‌ها به جای استفاده از شناسه‌های فنی (مانند «فلش بخش مالی» به جای Transcend_8GB_2349123)

### ۲/۱/۱/۵. ابزارهای مورد اعتماد (Trusted Devices)

قابلیت ابزارهای مورد اعتماد، مدیریت دستگاه‌های مجاز در سازمان را به‌طور چشمگیری ساده‌سازی می‌کند. این ویژگی به مدیران سیستم امکان می‌دهد تا:

۱. با یک کلیک در بخش بانک ابزار یا از طریق پنل مدیریت، دستگاه‌ها را مجاز نمایند.
۲. بدون نیاز به تعریف حجم وسیعی از قواعد پیشرفته، مجموعه بزرگی از ابزارهای جانبی را کنترل کنند.
۳. در صورت مفقود شدن یا عدم استفاده از ابزارهای مورد اعتماد در بازه زمانی مشخص، از طریق گزارش‌های خودکار مطلع شوند.

### ۲/۱/۲. کنترل انتقال فایل (File Transfer Control)

این مولفه که با عنوان SDC- Software and Device Control نیز شناخته می‌شود، یکی از مولفه های اصلی در این راهکار به حساب آمده و وظیفه کنترل و محدودسازی دسترسی نرم‌افزارها و کاربران به دستگاه‌های جانبی از نوع USB Storage را بر عهده دارد. لازم به ذکر است که سیاست‌های این مولفه بعد از مولفه‌های Device Control و Application Control اعمال می‌شود.

این مولفه خود به دو بخش کنترل و نظارت تقسیم می‌شود.

#### ۲/۱/۲/۱. بخش کنترل انتقال فایل

در این بخش کاربر می‌تواند قواعدی با توجه به هر ۶ سرفصل زیر تعیین کند:

۱. چه کسانی (کاربران و گروه‌های اکتیودایرکتوری) مجاز به کار کردن با دستگاه‌های جانبی هستند؟
۲. چه چیزی (برحسب شناسه یا مشخصات دستگاه جانبی) مجاز به استفاده می‌باشد؟
۳. کجا (در کدام سیستم یا گروه از سیستم‌ها) اجازه استفاده از دستگاه‌های جانبی وجود دارد؟
۴. کدام نرم‌افزارها (برحسب اطلاعات سازنده، محصول یا هش کامل فایل) مجاز به دسترسی به دستگاه‌های جانبی هستند؟
۵. چه زمانی (در ساعات کاری یا خارج از آن) اجازه دسترسی وجود دارد؟
۶. چه فایل‌هایی (برحسب نام فایل) اجازه انتقال به/از دستگاه جانبی را دارند؟

تمام موارد فوق در قالب یک سیاست واحد و متمرکز تعیین می‌شود و بدین ترتیب امکان تعریف قواعد مختلف وجود خواهد داشت.

**۲/۱/۲/۲. بخش نظارت بر انتقال فایل**

بخش Volume Log نیز که در این مولفه تعبیه شده مسئول ثبت جامع فراداده‌های مربوط به ابزارهای جانبی (از انواع حافظه‌های USB و دیسک‌های نوری) و فایل‌های انتقالی به/از آن‌ها می‌باشد.

حالات کاری شامل موارد زیر است:

۱. Mount/Unmount Log

- فقط اتصال و قطع شدن ابزار لاگ می‌شود. اطلاعاتی شامل برچسب درایو، حجم کلی و مصرف شده، تاریخ و کاربر پشت سیستم و ...

۲. Mount/Unmount + Write Log

- علاوه بر موارد قبل، فراداده هر فایلی که روی فلش نوشته شود لاگ می‌شود. اطلاعاتی شامل نام و سایز فایل، تاریخ ساخت، تغییر، دسترسی و ...

۳. Mount/Unmount + Write + Read Log

- علاوه بر موارد قبل، فراداده هر فایلی که روی فلش نوشته و یا خوانده شود نیز لاگ می‌شود.

سطوح مختلف لاگ‌برداری، امکان نظارت و کنترل دقیق بر جریان تبادل اطلاعات را مطابق با نیازهای امنیتی سازمان فراهم می‌نماید.

**۲/۱/۳. کنترل برنامه (Application Control)**

این مولفه با اعمال سیاست‌های دسترسی پیشرفته، اجرای برنامه‌های غیرمجاز در محیط سازمان را مسدود می‌نماید. قاعده‌گذاری در این بخش بر اساس معیارهای زیر انجام می‌پذیرد:

۱. بر اساس شرکت سازنده (By Company)
۲. بر اساس محصول خاص (By Product)
۳. بر اساس محتوای برنامه (By Content)

۲،۱،۳،۱. **بانک برنامه‌ها** (Application Inventory Discovery)

این قابلیت با تشکیل یک بانک متمرکز از کلیه برنامه‌های نصب‌شده روی کلاینت‌های سراسر شبکه، بستری جامع برای اعمال سیاست‌های کنترلی دقیق فراهم می‌نماید.

۲/۱/۴. **کنترل پرینت (Print Control)**

سیستم کنترل پرینت در پادویش DLP امکان مدیریت جامع عملیات پرینت در شبکه را ارائه می‌دهد:

۱. مدیریت دسترسی: امکان مسدودسازی یا مجاز نمودن عملیات پرینت بر اساس دستگاه (سیستم) و چاپگر
۲. ثبت و پایش: امکان لاگ‌برداری کامل از فراداده‌های پرینت شامل تاریخ، کاربر، سیستم، نام چاپگر، عنوان سند و تعداد صفحات

۲/۱/۵. **نظارت بر مولفه‌های سخت‌افزاری و نرم‌افزاری (HW/SW Monitoring)**

این بخش امکان پایش کامل تجهیزات و نرم‌افزارهای سازمان را فراهم می‌نماید:

۱. پایش سخت‌افزار: جمع‌آوری و نظارت بر اطلاعات سخت‌افزاری مطابق با ساختار Device Manager ویندوز
۲. مدیریت نرم‌افزار: گردآوری و کنترل اطلاعات نرم‌افزارهای نصب‌شده مطابق با ساختار Programs and Features

کلیه اطلاعات جمع‌آوری‌شده در این بخش قابلیت جستجو و تحلیل پیشرفته را برای مدیران امنیت فراهم می‌نماید.

۲/۱/۶. **کنترل حافظه موقت (Clipboard Control)**

این مولفه با اعمال سیاست‌های امنیتی پیشرفته، از نشت اطلاعات از طریق حافظه موقت (کلیپ‌بورد) جلوگیری می‌نماید. قابلیت‌های کلیدی این بخش شامل:

- مسدودسازی عملیات کپی/پیست از برنامه‌های مجاز (حاوی اسناد محرمانه) به غیرمجاز
- اجازه کپی/پیست بین دو برنامه مجاز (دو سند محرمانه) وجود دارد.
- اجازه کپی/پیست بین دو برنامه غیرمجاز وجود دارد.

- اجازه کپی/پیست از برنامه غیرمجاز به برنامه مجاز (سند محرمانه) نیز وجود دارد.
- امکان تعریف استثنا برای کاربران و برنامه‌های مجاز

### ۲/۱/۷. محافظت در برابر تصویربرداری از صفحه (Screenshot Protection)

این قابلیت با به کارگیری مکانیزم‌های پیشرفته، از نشت اطلاعات از طریق تهیه اسکرین‌شات از اسناد محرمانه جلوگیری می‌نماید.

- جلوگیری از ثبت تصویر برنامه‌های مجاز (حاوی اسناد محرمانه) توسط اسکرین‌شات ( Print Screen) و نرم‌افزارهای مشابه
- امکان تعریف استثنا برای کاربران و برنامه‌های مجاز

## ۲/۲. محافظت داده در انتقال (Data in Motion)

محصول Padvish DLP با به‌کارگیری مجموعه‌ای از قابلیت‌های پیشرفته، از داده‌های سازمان در حین انتقال بر روی شبکه محافظت می‌نماید. این راهکار با ایجاد لایه‌های امنیتی چندگانه، مانع از نشت اطلاعات از طریق کانال‌های ارتباطی می‌شود.

۱. شبکه‌های مورد اعتماد (Trusted Network)
۲. تشخیص اتصال اینترنت (Internet Connection Detection)
۳. کنترل وب (Web Control)
۴. دیوار آتش (Firewall)
۵. Attack Blocker

### ۲/۲/۱. شبکه‌های مورد اعتماد (Trusted Network)

یکی از مخاطرات امنیتی قابل توجه در محیط‌های سازمانی، تغییر فیزیکی اتصال شبکه و اتصال مستقیم سیستم‌ها به دستگاه‌های غیرمجاز (از طریق اتصال Back-to-Back) جهت انتقال داده‌ها می‌باشد. از آنجایی که در این سناریو هیچ ابزار جانبی به سیستم متصل نمی‌شود، مکانیزم‌های کنترل ابزار قادر به شناسایی و جلوگیری از این تهدید نیستند.

قابلیت شبکه‌های مورد اعتماد در پادویش DLP با تشخیص پویای شبکه سازمان و مسدودسازی اتصال به شبکه‌های غیرمجاز، این تهدید را خنثی می‌نماید. این سیستم با اعتبارسنجی مشخصات شبکه متصل، از برقراری ارتباط در محیط‌های غیرمطمئن جلوگیری می‌کند.

خصوصیات قابل استفاده در قاعده‌گذاری:

۱. DNS server IP addresses
۲. WINS server IP addresses
۳. DHCP IP addresses
٤. Default gateway IP addresses
٥. Default gateway MAC addresses

عملیات قابل تعریف در برابر اتصال غیرمجاز:

- ثبت رویداد (Log Only): ثبت اخطار در سیستم گزارش‌دهی
- مسدودسازی (Block): قطع ارتباط شبکه به صورت خودکار
- مسدودسازی و اعلان (Block and Notify User): قطع ارتباط و نمایش پیام هشدار به کاربر

این رویکرد پیشگیرانه، امنیت داده‌ها را در سطح شبکه فیزیکی تضمین نموده و از انتقال غیرمجاز اطلاعات حتی در صورت دسترسی فیزیکی به تجهیزات جلوگیری می‌نماید.

### ۲/۲/۲. تشخیص اتصال اینترنت (Internet Connection Detection)

یکی از الزامات اساسی در سیاست‌گذاری امنیتی، کنترل و محدودسازی دسترسی سیستم‌ها به اینترنت است. قابلیت تشخیص اتصال اینترنت در این محصول، هرگونه نقض این سیاست را – صرف نظر از روش اتصال – به سرعت شناسایی و گزارش می‌نماید.

مکانیزم عملکرد:

- این قابلیت مبتنی بر تحلیل رفتار ترافیک شبکه عمل می‌نماید. به محض مشاهده هرگونه تبادل داده با شبکه اینترنت، سیستم به صورت خودکار فعال شده و رویداد را ثبت می‌کند.

- این رویکرد پیشرفته، امکان نظارت جامع بر دسترسی به اینترنت را بدون ایجاد بار اضافی روی شبکه فراهم نموده و هرگونه تلاش برای نقض سیاست‌های دسترسی را در لحظه شناسایی می‌کند.

### ۲/۲/۳. کنترل وب (Web Control)

مؤلفه کنترل وب در پادویش DLP، با نظارت و کنترل دسترسی به منابع اینترنتی، از برقراری ارتباط با دامنه‌ها و وب‌سایت‌های غیرمجاز جلوگیری می‌نماید. این سامانه، محتوای تبادل شده در پروتکل‌های اصلی زیر را برای شناسایی و مسدودسازی اتصالات غیرمجاز تحلیل می‌کند:

۱. HTTP
۲. HTTPS
۳. DNS

این قابلیت در حالت‌های عملیاتی زیر قابل تنظیم و فعال‌سازی است:

۱. **لیست سیاه (Blacklist)**: در این حالت، دسترسی به دامنه‌های مشخص شده در لیست، مسدود شده و ارتباط با سایر دامنه‌ها آزاد است.
۲. **لیست سفید (Whitelist)**: در این حالت، تنها دسترسی به دامنه‌های مشخص شده در لیست مجاز بوده و ارتباط با هر دامنه دیگر به طور کامل مسدود می‌شود.
۳. **ثبت رویداد (Logging)**: این گزینه می‌تواند به همراه هر یک از حالت‌های فوق استفاده شود تا از تمامی تلاش‌های ارتباطی، گزارش‌گیری جامع انجام پذیرد.
۴. **قابلیت تطبیق الگو (Pattern Matching)**: علاوه بر تعریف دقیق دامنه‌ها، این مؤلفه از تطبیق بخشی از نام دامنه نیز پشتیبانی می‌نماید. برای مثال:

- مسدودسازی تمام زیردامنه‌های یک سایت:. telegram.org*
- مسدودسازی تمام دامنه‌هایی که با یک کلمه خاص شروع می‌شوند: mail.*

این رویکرد انعطاف‌پذیر، امکان اعمال سیاست‌های امنیتی دقیق و مقیاس‌پذیر را برای کنترل ترافیک وب سازمان فراهم می‌سازد.

### ۲/۲/۴. دیوار آتش (Firewall)

پادویش مجهز به یک دیوار آتش دو لایه مبتنی بر معماری ویندوز می‌باشد که حفاظت جامعی در سطوح مختلف شبکه ارائه می‌نماید:

لایه‌های دیوار آتش:

- لایه ۳ (Stateless Firewall)
  - قرارگیری در پایین‌ترین لایه هسته ویندوز و مستقیماً بر روی درایور کارت شبکه
  - کنترل بسته‌های ورودی و خروجی بر مبنای فیلتر بسته (Packet-based)
- لایه ۷ (Stateful Firewall)
  - استقرار در بالاترین لایه هسته ویندوز و قبل از برنامه‌های کاربردی
  - نظارت و کنترل اتصالات ورودی و خروجی بر اساس برنامه (Connection-based)

### ۲/۲/۵. مسدود کننده حملات Attack Blocker

این مولفه در صورت تشخیص رفتار مشکوک و/یا بدافزاری در شبکه، از ارتباط سیستم آلوده با سیستم مجهز به پادویش و ادامه حمله جلوگیری می‌کند.

به عنوان مثال اگر سیستمی در شبکه فاقد پادویش بوده و آلوده به باج‌افزار شود و تلاش کند که فایل‌های سیستم‌های مجهز به پادویش را رمز نماید، این مولفه فعال شده و جلوی این حمله و هر نوع اتصال سیستم آلوده را – تا زمانی که پاکسازی شود – می‌گیرد.

## ۲/۳. محافظت از داده‌ها در حالت ذخیره‌سازی (Data at Rest)

محصول Padvish DLP با ارائه سه قابلیت تخصصی، از داده‌های ذخیره‌شده در رسانه‌های مختلف در برابر دسترسی غیرمجاز، نشت، و تخریب محافظت می‌نماید. این لایه از حفاظت با هدف اطمینان از محرمانگی، یکپارچگی و در دسترس‌پذیری اطلاعات، حتی در صورت سرقت یا دسترسی فیزیکی به حامل‌های داده است.

قابلیت‌های کلیدی:

۱. پشتیبان‌گیری سریع و کم‌حجم Padvish DataCop™
۲. ضدباج‌افزار Anti Ransomware
۳. قابلیت مدیریت دسترسی به اطلاعات Information Rights Management

### ۲/۳/۱. پشتیبان‌گیری سریع و کم‌حجم (Padvish DataCop™)

قابلیت انحصاری Padvish DataCop™، با هدف محافظت از داده‌های کاربران و اطمینان از بازیابی سریع و مطمئن اطلاعات طراحی شده است. این سامانه با بهره‌گیری از فناوری‌های پیشرفته، به‌صورت کاملاً خودکار از داده‌ها پشتیبان‌گیری نموده و نسخه‌های پشتیبان را در برابر تهدیدات سایبری مدرن محافظت می‌نماید.

ویژگی‌های کلیدی:

- پشتیبان‌گیری کاملاً خودکار: انجام عملیات پشتیبان‌گیری بدون نیاز به هیچ‌گونه تنظیم یا مداخله دستی از سوی کاربر- این ویژگی بر اساس سیاست‌های سازمان قابل تنظیم می‌باشد.
- سرعت فوق‌العاده: انجام فرآیند پشتیبان‌گیری سریع، بدون ایجاد اختلال در روند کاری کاربران
- بهینه‌سازی حافظه: مصرف تنها ۵٪ از فضای دیسک برای ذخیره‌سازی پشتیبان‌ها (قابل تنظیم توسط ادمین شبکه) از آنجایی‌که فناوری مورد استفاده بر اساس تهیه تصویر (Snapshot) کار می‌کند، هیچ داده‌ای کپی نمی‌شود، بلکه تنها تغییرات داده‌ها ذخیره می‌شوند، لذا مصرف حافظه آن بسیار پایین است.
- محافظت امنیتی: ایمن‌سازی نسخه‌های پشتیبان در برابر بدافزارها، باج‌افزارها و هرگونه دستکاری نرم‌افزاری
- فناوری پایه: بهره‌گیری از سرویس VSS ویندوز برای ایجاد snapshotهای یکپارچه و مطمئن
- این قابلیت، راهکاری جامع برای تضمین در دسترس‌پذیری و بازیابی داده‌های حیاتی سازمان ارائه می‌نماید.

### ۲/۳/۲. ضد باج‌افزار (Anti-Ransomware)

ضد باج‌افزار پادویش یک راهکار امنیتی پیشرفته و کاملاً مبتنی بر تشخیص رفتاری است که با تحلیل و مانیتورینگ بلادرنگ رفتار نرم‌افزارها، اقدامات مخرب باج‌افزارها را شناسایی و خنثی می‌نماید.

ویژگی‌های کلیدی این لایه محافظتی:

- حفاظت چندلایه: ارائه محافظت چندلایه در برابر طیف وسیعی از تهدیدات باج‌افزاری
- تشخیص مبتنی بر رفتار: توانایی شناسایی باج‌افزارهای نوظهور و ناشناخته (Zero-day) بدون اتکا به امضاهای از پیش تعریف شده
- استقلال از به‌روزرسانی: عدم نیاز ضروری به به‌روزرسانی پایگاه داده برای شناسایی نمونه‌های جدید
- تأییدیه بین‌المللی: دارنده گواهی معتبر AV-TEST آلمان برای شناسایی ٪۱۰۰ باج‌افزارها
- قابلیت طعمه‌گذاری (Honeypot): امکان ایجاد فایل‌های طعمه با نام‌های قابل سفارشی‌سازی برای جذب و شناسایی زودهنگام فعالیت باج‌افزار
- مدیریت استثناها: امکان تعریف رفتارهای سالم و شناخته‌شده جهت جلوگیری از اخطارهای کاذب و تطبیق‌پذیری بهتر با محیط‌های عملیاتی
- مقابله با باج‌افزارهای پیچیده: توانایی تشخیص باج‌افزارهای بوت‌کیت پیچیده (مانند Petya)
- این مولفه با تمرکز بر تحلیل هوشمند رفتارها، از رمزنگاری غیرمجاز و قفل‌سازی داده‌های سازمان به طور مؤثر جلوگیری می‌کند.

### ۲/۳/۳. مدیریت حقوق دیجیتال (DRM)

مدیریت دسترسی به اطلاعات با رمز کردن فایل‌ها و اسناد موجود در سیستم‌ها، مانع نشت اطلاعات سازمان می‌شود. این رمزکردن به نحوی انجام می‌شود که اطلاعات در هیچ محلی غیر از شبکه سازمان قابل بازگشایی نیست. به این ترتیب دیگر نیازی به نگرانی از اینکه اطلاعات از شبکه خارج بشود یا خیر وجود ندارد، چرا که اطلاعات خارج شده صرفاً کدهای بی‌معنی بوده و قابل استفاده نخواهد بود.

ویژگی‌های کلیدی:

- فایل‌های اسناد به محض ساخته شدن رمز شده و با کلید رمزنگاری نامتقارن محافظت می‌شوند.

- از دید کاربر و نرم‌افزارها رمزنگاری کاملاً شفاف بوده و وجود آن اصلاً احساس نمی‌شود.
- در مقابل تهدیداتی مانند دزدی فیزیکی هارد یا ذخیره‌ساز، خروج داده از طریق فلش و ابزار جانبی، ایمیل کردن، آپلود کردن، کپی کردن و ... داده‌ها مصون خواهند بود.
- امکان مدیریت کلید رمزنگاری به صورت متمرکز
- امکان توزیع کلید در ساختار درختی زیرمجموعه‌ها
- امکان تعریف برنامه‌های مورد اعتماد جهت بازگشایی اسناد
- امکان محدودسازی و محافظت از برنامه‌های مورد اعتماد و اطلاعات درون آنها
- جلوگیری از نشت اطلاعات از طریق کپی/پیست یا اسکرین‌شات
- تعیین سیاست‌های دسترسی برحسب:
  - سیستم
  - کاربر یا گروه ویندوزی
  - نوع سند
  - برنامه کاربردی مجاز
  - تعریف زمان انقضای دسترسی
- امکان عملکرد در صورت قطعی موقت از سرور کلید

### ۲/۳/۳/۱. معماری و مکانیزم رمزنگاری

این سیستم مبتنی بر رمزنگاری نامتقارن با استفاده از جفت کلید عمومی و خصوصی عمل می‌کند:

- کلید عمومی سرور به تمامی کلاینت‌های مجاز توزیع می‌شود.
- کلید خصوصی به صورت امن و متمرکز روی سرور کلید سازمان نگهداری می‌شود.

### ۲/۳/۳/۲. فرآیند رمزگذاری

- اسناد بلافاصله پس از ایجاد، به صورت شفاف و خودکار رمزگذاری می‌شوند.
- هر فایل با یک کلید یکتا رمز می‌شود.
- این کلید یکتا خود با استفاده از کلید عمومی سرور رمزگذاری شده و در هدر فایل رمزشده ذخیره می‌گردد.

- حتی خود سازنده سند نیز بدون دریافت مجوز از سرور DRM نخواهد توانست فایل را باز کند.

### ۲/۳/۳/۳. فرآیند اعطای دسترسی و رمزگشایی

هنگامی که یک برنامه مجاز سعی در باز کردن یک سند محافظت‌شده دارد:

- کلاینت پادویش درخواست رمزگشایی را به سرور ارسال می‌کند.
- این درخواست شامل کلید یکتا رمزشده از هدر فایل است.
- سرور با اعتبارسنجی درخواست بر اساس سیاست‌های تعریف‌شده، در صورت تایید، کلید یکتا را با کلید خصوصی خود رمزگشایی کرده و برای کلاینت ارسال می‌نماید.
- تنها پس از دریافت این کلید، سند قابل دسترسی خواهد بود.

### ۲/۳/۳/۴. مولفه‌های سیاست‌گذاری پیشرفته

سیاست‌های دسترسی بر اساس مولفه‌های زیر به صورت دینامیک تعریف و اعمال می‌شوند:

| مولفه | توضیحات |
|---|---|
| **چه کسی** | تعیین کاربر یا گروه‌های کاربری ویندوز |
| **چه چیزی** | تعیین نوع اسناد (بر اساس فرمت محتوای فایل) |
| **کجا** | تعیین سیستم‌های مجاز |
| **چه زمانی (When)** | تعریف زمان انقضای دسترسی به سند |
| **چگونه (How)** | تعریف برنامه‌های مورد اعتماد (Trusted Applications) |

### ۲/۳/۳/۵. مدیریت کلید و معماری توزیع‌شده

- امکان مدیریت متمرکز کلیدهای رمزنگاری توسط مدیر سیستم
- قابلیت توزیع کلید سازمانی در ساختار درختی سرورهای مدیریتی
- بهینه‌سازی برای به حداقل رساندن تاخیر و ایجاد تعادل بین امنیت و کارایی

### ۲/۳/۳/۶. عملکرد در حالت آفلاین

در صورت قطعی موقت اتصال کلاینت از سرور کلید، کاربر قادر به انجام عملیات زیر خواهد بود:

| عملیات | امکان عملکرد | توضیحات |
|---|---|---|
| **ایجاد و ذخیره اسناد جدید** | ✓امکان‌پذیر | رمزگذاری با استفاده از کلید عمومی کش‌شده محلی |
| **باز کردن اسناد قبلاً دیده‌شده** | ✓امکان‌پذیر (تا زمان مشخص) | مدیر شبکه تعیین می‌کند کاربران تا چه زمانی مجاز به کش کردن کلیدهای یکتا هستند. کلیدها به صورت رمزشده برای هر کاربر و با اعتبار زمانی محدود نگهداری می‌شوند. |
| **باز کردن اسناد جدید** | ×غیرممکن | کلید یکتای فایل در کش محلی موجود نیست، لذا فایل‌های سازمان که در زمان اتصال به سرور باز نشده‌اند قابل بازگشایی نیستند. |

## ۲/۴. قابلیت‌های سازگاری و مدیریتی (Management)

### ۲/۴/۱. امکانات کنسول مدیریتی

کنسول مدیریتی پادویش، ابزار مدیر شبکه برای نصب، مدیریت و نظارت بر محصولات پادویش است. این کنسول قابلیت‌های متنوعی از کشف و استخراج اطلاعات رایانه‌های شبکه و ضدویروس نصب شده روی آنها، نصب از راه دور، گرفته تا گروه‌بندی خودکار سیستم‌ها و اعمال تنظیمات متناسب هر گروه، ارسال تسک‌ها و انجام عملیات روی کلاینت‌ها، و نهایتاً تولید و مشاهده انواع گزارش‌های تجمیعی قابل سفارشی‌سازی را به مدیران شبکه ارائه می‌دهد. از نظر قابلیت استقرار نیز کنسول مدیریتی پادویش با دارا بودن امکان نصب به صورت ساختار سلسله‌مراتبی و گزارش‌های تجمیعی، تمهیدات انجام شده در بحث ترافیک شبکه و به‌روزرسانی P2P و بسیاری قابلیت‌های دیگر، امکان کنترل هر تعداد کلاینت در شبکه‌های گسترده و با پراکندگی جغرافیایی بالا را به خوبی پشتیبانی می‌کند.

### ۲/۴/۲. ویژگی‌های اصلی کنسول مدیریتی

۱. مدیریت کلیه مولفه‌ها و محصولات از طریق یک ایجنت و یک کنسول واحد

۲. ساختار سلسله‌مراتبی در کنسول‌های مدیریتی و امکان مستر/اسلیو
۳. گروه‌بندی کلاینت‌ها و اعمال تنظیمات به هر گروه
۴. تعریف گروه‌بندی خودکار برحسب مشخصاتی مانند سیستم عامل، حجم رم، و ...
۵. اکتشاف سیستم‌های فاقد ایجنت
۶. نصب از راه دور خودکار ایجنت
۷. سینک تنظیمات در ساختار سلسله مراتبی
۸. پشتیبانی از VDI
۹. مدیریت کلاینت‌ها از طریق فلش آفلاین
۱۰. گزارش‌های آماری قابل سفارشی‌سازی
۱۱. داشبورد قابل سفارشی‌سازی
۱۲. مدیریت دسترسی کاربران به کنسول مدیریتی
۱۳. مدیریت رویدادها:
- ارسال رویداد به Syslog
- ارسال رویداد به صورت فرمان به URL
- ارسال رویداد به ایمیل

### ۲/۴/۳. امکانات ایجنت

۱. محافظت از خود
۲. عملکرد کامل در Safe Mode
۳. ارسال پیام به کاربران
۴. خاموش کردن/ریستارت سیستم از راه دور
۵. غیرفعال کردن موقت محافظت‌ها
۶. آپگرید نسخه ایجنت از راه دور
۷. حذف ایجنت از راه دور

# ۳. جمع بندی

در عصر حاضر که داده‌ها به عنوان ارزشمندترین دارایی راهبردی سازمان‌ها شناخته می‌شوند، حفاظت جامع و چندلایه از اطلاعات در تمامی حالات (پردازش، انتقال و ذخیره‌سازی) به ضرورتی اجتناب‌ناپذیر تبدیل شده است. راهکار یکپارچه Padvish DLP با بهره‌گیری از معماری پیشرفته و رویکرد مبتنی بر سیاست‌گذاری متمرکز، پاسخی کامل و اثربخش به این چالش‌های امنیتی ارائه می‌نماید.

**مزایای راهبردی محصول:**

**۱. پوشش کامل چرخه حیات اطلاعات**

- در حالت پردازش (Data in Use): از طریق قابلیت‌های پیشرفته‌ای شامل کنترل ابزارهای جانبی، کنترل برنامه، نظارت بر مولفه‌های سخت‌افزاری و نرم‌افزاری و ...
- در حالت انتقال (Data in Motion): با به‌کارگیری دیوار آتش دو لایه، کنترل وب، شبکه‌های مورد اعتماد
- در حالت ذخیره‌سازی (Data at Rest): توسط راهکارهای رمزنگاری، پشتیبان‌گیری و محافظت پیشرفته در برابر باج‌افزار

**۲. مدیریت متمرکز و یکپارچه**

- ارائه کنسول مدیریتی واحد برای نظارت و کنترل سیاست‌های امنیتی
- امکان اعمال سیاست‌های یکسان در سطح سازمان
- قابلیت گزارش‌گیری جامع

**۳. انعطاف‌پذیری و سازگاری**

- توانایی تطبیق با محیط‌های پیچیده سازمانی
- امکان سفارشی‌سازی سیاست‌ها بر اساس نیازمندی‌های خاص
- سازگاری کامل با زیرساخت‌های موجود

### ۴. کارایی و شفافیت عملیاتی

- عملکرد بدون اختلال در فرآیندهای کسب‌وکار
- رابط کاربری یکپارچه با سایر محصولات پادویش برای مدیریت آسان و جلوگیری از نصب ایجنت‌های متعدد

### سخن پایانی

راهکار Padvish DLP با ترکیب هوشمندانه فناوری‌های پیشرفته امنیتی و رویکرد مدیریت متمرکز، نه تنها به عنوان یک راهکار امنیتی، بلکه به عنوان سرمایه‌ای راهبردی در راستای تحقق امنیت پایدار داده‌ها عمل می‌نماید. این محصول سازمان‌ها را قادر می‌سازد تا از دارایی‌های دیجیتال خود در برابر تهدیدات داخلی و خارجی محافظت نموده و با کاهش ریسک عملیاتی و حفظ اعتبار سازمانی به فعالیت خود ادامه دهند.