C-Prot
Cognitive Protection

arka
رایان سامانه آرکا

C-Prot

Endpoint Security Platform

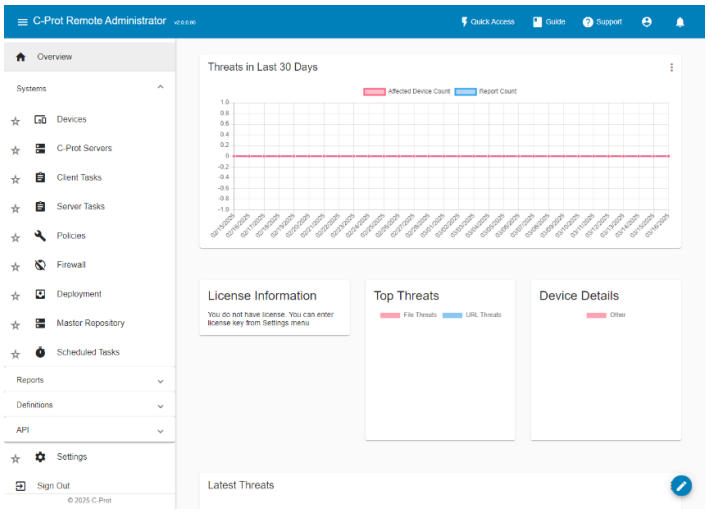
AV/EDR

چرا C-Prot؟

C-Prot یک شرکت پیشرو در حوزه امنیت سایبری است که خدمات و محصولات نوآورانه‌ای برای محافظت از داده‌ها و سیستم‌ها ارائه می‌دهد. این شرکت با تمرکز برEndpoint Security و AppDefense به کسب‌وکارها و سازمان‌ها در بخش‌های مختلف مانند مخابرات، مالی، بهداشت، تجارت الکترونیک و شرکت‌های بزرگ کمک می‌کند تا تهدیدات سایبری را شناسایی و خنثی کنند. C-Prot با استفاده از فناوری‌های پیشرفته، امنیت دیجیتال را به سطحی جدید ارتقا داده و راهکارهای مبتنی بر هوش مصنوعی و تحلیل داده ارائه می‌دهد. محصول Endpoint Security شرکت C-Prot، به دلیل کیفیت طراحی بالا، موفق به گذراندن آزمون‌های مختلف جهانی، خصوصا آزمون VB۱۰۰ گروه تحقیقاتی Virus Bulletinشده است. **در کمال خوشبختی به اطلاع میرساند محصول C-Prot Endpoint Security با رعایت الزامات مرکز مدیریت راهبردی افتای ریاست جمهوری، موفق به کسب مجوز افتا و ارائه خدمات به تمامی سازمان های دولتی و خصوصی شده است.** لازم به‌ذکر است شرکت رایان سامانه آرکا با بیش از ۲۰ سال سابقه در ارائه راهکارهای جامع امنیت و با سابقه داشتن نمایندگی انحصاری آویرا و جی دیتا به مدت بیش از ۱۵ سال، تجربه پشتیبانی و ارائه محصولات آنتی‌ویروس سازمانی به بیش از ۲۵۰۰ مشتری در ایران را داراست.

ویژگیهای و مزایای C-Prot Endpoint Security

- **دارای مجوز افتا:** با رعایت الزامات مرکز افتا، محصول C-Prot Endpoint Security موفق به کسب مجوز افتا شده است.
- تأییدیه لازم برای استفاده در زیرساخت‌های حیاتی، سازمان‌های دولتی و شرکت‌های خصوصی
- قدرت تشخیص بالا به لطف استفاده از هوش مصنوعی پیشرفته
- مصرف بسیار کم منابع سخت‌افزاری
- کسب امتیازات A و +A در آزمون های بین‌المللی مانند Virus Bulletin
- کنسول مدیریتی پیشرفته با مدیریت آسان
- تشخیص منفی کاذب (کمتر از ۱٪) و در نتیجه بدون پیام های آزار دهنده
- پشتیبانی فنی از طریق تیم شرکت آرکا در ایران و در صورت نیاز از طریق تیم پشتیبانی شرکت مادر
- ارائه لایسنس رسمی بنام مشتری
- این محصول دارای تخفیف ۷۰٪ برای مشتریان آموزشی و دانشگاهی و ۴۰٪ برای مشتریان دولتی میباشد.
- مدیریت کامل فرآیند مهاجرت از آنتی‌ویروس قبلی به طور حرفه‌ایی و خودکار



شرکت رایان سامانه آرکا به‌عنوان نماینده انحصاری C-Prot در ایران، مسئولیت عرضه، استقرار و پشتیبانی این محصول را بر عهده دارد. مدیران این شرکت دریافت مجوز افتا را گامی مهم در جهت افزایش سطح امنیت سایبری کشور و توسعه استفاده از راهکارهای استاندارد و تأییدشده در سازمان‌های ایرانی می‌دانند.

ویژگی های برجسته‌ی C-Prot

ویژگی‌های فنی

۱. امنیت و تشخیص تهدیدات
- قدرت تشخیص بالا به لطف استفاده از هوش مصنوعی پیشرفته
- یادگیری ماشین (Machine Learning) برای شناسایی الگوهای پیچیده حمله
- تحلیل رفتاری (Behavioral Analysis) برای کشف تهدیدات ناشناخته و نوظهور
- حفاظت پیشرفته از حملات روز صفر (Zero-Day Protection)
- تشخیص منفی کاذب (False Positive) بسیار پایین - بدون پیام‌های آزاردهنده
- نظارت و هشدار لحظه‌ای
- شناسایی مبتنی بر امضا (Signature-based Detection)برای تهدیدات شناخته‌شده

۲. عملکرد و کارایی
- سبک و کم‌حجم - سربار بسیار کم بر روی سیستم
- تأثیر ناچیز بر منابع - حفظ کامل بهره‌وری کاربران
- موتور اسکن سریع و دقیق با الگوریتم‌های بهینه‌شده
- به‌روزرسانی خودکار و هوشمند پایگاه داده تهدیدات
- اجرای بهینه حتی بر روی سیستم‌های قدیمی‌تر

۳. مدیریت و کنترل
- کنسول مدیریتی پیشرفته با مدیریت آسان
- رابط کاربری ساده و شهودی - قابل استفاده برای کاربران غیرمتخصص
- مدیریت متمرکز تمام نقاط پایانی از یک نقطه
- نصب و استقرار از راه دور
- گزارش‌گیری جامع و قابل تنظیم
- سیاست‌گذاری امنیتی انعطاف‌پذیر برای بخش‌های مختلف سازمان

٤. اعتبار بین‌المللی
- کسب امتیازات بالا در آزمون‌های بین‌المللی مانندVirus Bulletin
- تأیید شده توسط مراجع معتبر امنیتی جهانی
- سابقه اثبات‌شده در حفاظت از سازمان‌های بزرگ

ویژگی‌های عمومی

۱. مجوزها و تأییدیه‌های رسمی
- دارای مجوز رسمی افتا - رعایت کامل الزامات مرکز افتا
- تأییدیه لازم برای استفاده در زیرساخت‌های حیاتی کشور
- مجاز برای سازمان‌های دولتی و شرکت‌های خصوصی
- ارائه لایسنس رسمی به نام مشتری

۲. پشتیبانی کامل و حرفه‌ای
- پشتیبانی فنی تخصصی از طریق تیم متخصص شرکت آرکا در ایران
- دسترسی به تیم پشتیبانی شرکت مادر در صورت نیاز
- پشتیبانی ۲۴ ساعته و ۷ روز هفته
- ارائه مستندات کامل به زبان فارسی
- آموزش و راه‌اندازی توسط کارشناسان داخلی

۳. مزایای اقتصادی و تخفیفات ویژه
- تخفیف ۷۰٪ برای مشتریان آموزشی و دانشگاهی
- تخفیف ۴۰٪ برای مشتریان دولتی
- قیمت‌گذاری منصفانه و رقابتی با توجه به بازار داخلی
- عدم وابستگی به پرداخت‌های ارزی و تحریم‌ها
- کاهش هزینه‌های نگهداری در بلندمدت

٤. انعطاف‌پذیری و سازگاری
- مقیاس‌پذیری بالا - از کسب‌وکارهای کوچک تا سازمان‌های بزرگ
- سیاست‌های امنیتی سفارشی‌سازی‌شده برای نیازهای مختلف
- ادغام بی‌درز با زیرساخت‌های IT موجود
- سازگاری کامل با استانداردهای امنیتی ملی
- قابلیت استقرار در شبکه‌های محدود و منقطع

شرکت رایان سامانه آرکا نماینده انحصاری C-Prot در ایران

تمامی محصولات C-Prot به صورت مستقیم و با گارانتی اصالت از طریق شرکت آرکا ارائه می‌شوند. ما با تحلیل نیازهای سازمان‌ها و کسب‌وکارها، راهکارهای سفارشی و متناسب با چالش‌های امنیتی آنان ارائه می‌دهیم. ما راهکارهای C-Prot را با نیازها و الزامات بومی و منطقه‌ای سازگار کرده‌ایم تا بهترین تجربه ممکن را برای مشتریان فراهم کنیم.

شرکت آرکا با بهره‌گیری از تجربه و دانش متخصصان داخلی و حمایت از فناوری‌های پیشرفتهC-Prot، مأموریت دارد که امنیت سایبری کاربران در ایران را به سطحی جهانی ارتقاء دهد.


C-Prot | Authorized Exclusive Distributor

We confirm that

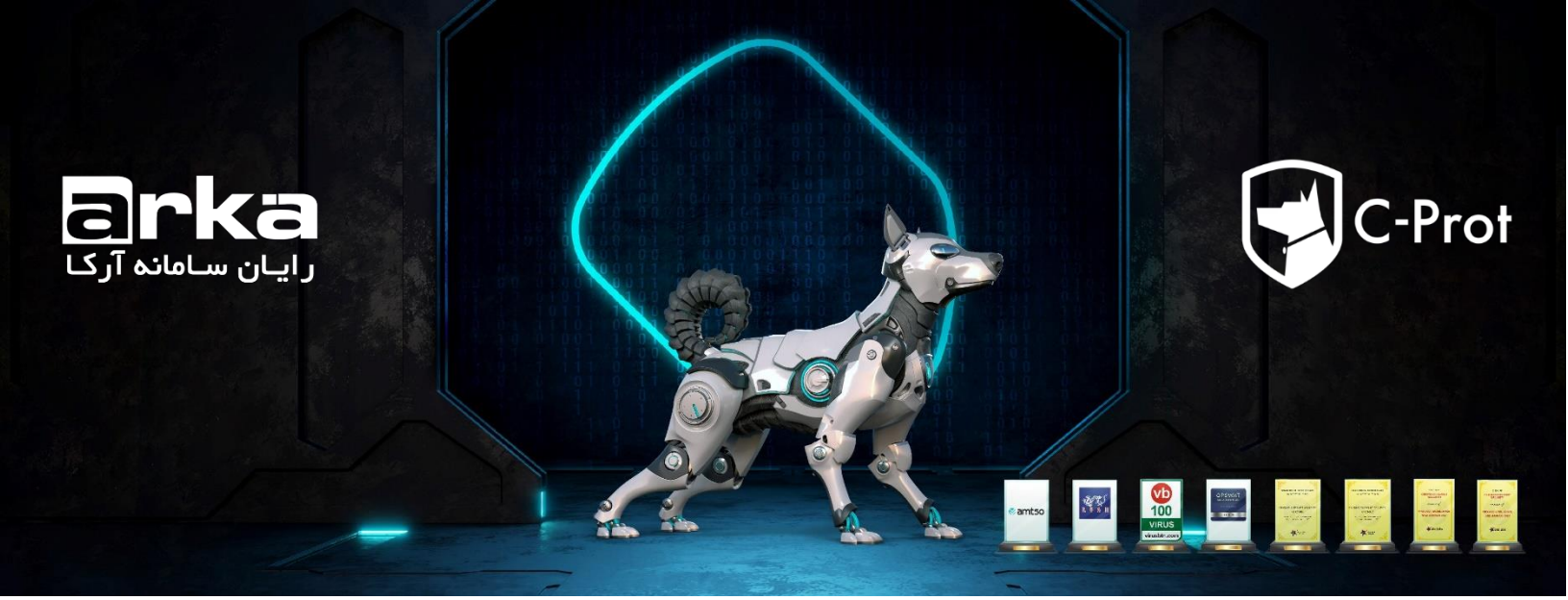
Rayan Samaneh Arka

is trusted to fully manage their business chanel/market and provide C-Prot sales program to their partners.

S.Bilgehan ÜSTÜNDAĞ
CEO

C-Prot UK Limited
Gf150 214 Baker Street, Enfield,
London,United Kingdom,EN1 3JT
c-prot.com info@c-prot.com

01/01/2029
This certifocate os valid for 5 years.
Territory: Iran



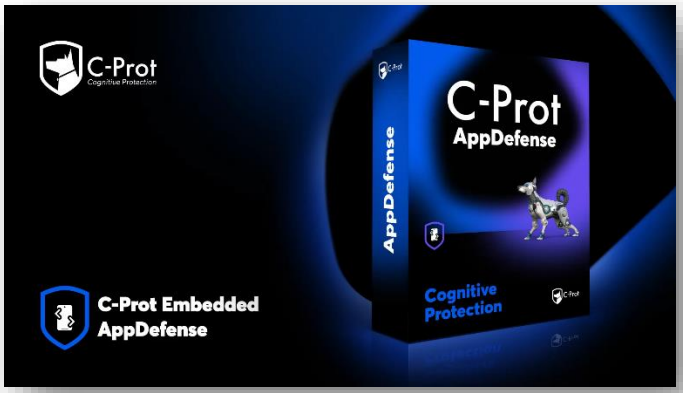
درباره‌ی C-Prot

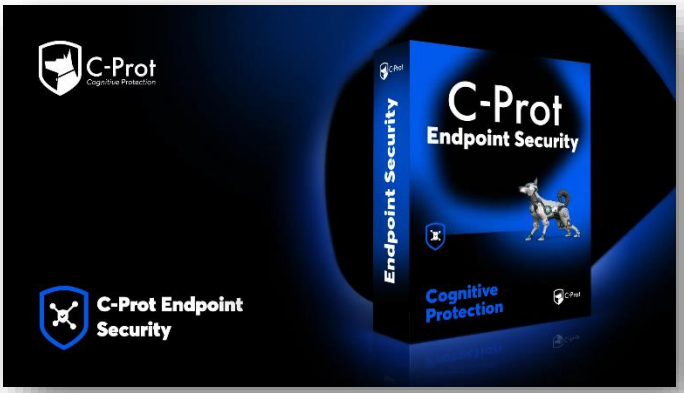
C-Prot توسعه دهنده محصولات امنیتی است که مشکلات امنیت سایبری کاربران را با روش‌های نوآورانه حل می‌کنند و تجربه کاربری را در اولویت قرار می‌دهند. این محصولات امنیت سایبری در حفاظت از زیرساخت‌های حیاتی مانند صنعت دفاع، مخابرات، انرژی، بانکداری، بهداشت، حمل‌ونقل و مالی استفاده می‌شوند.

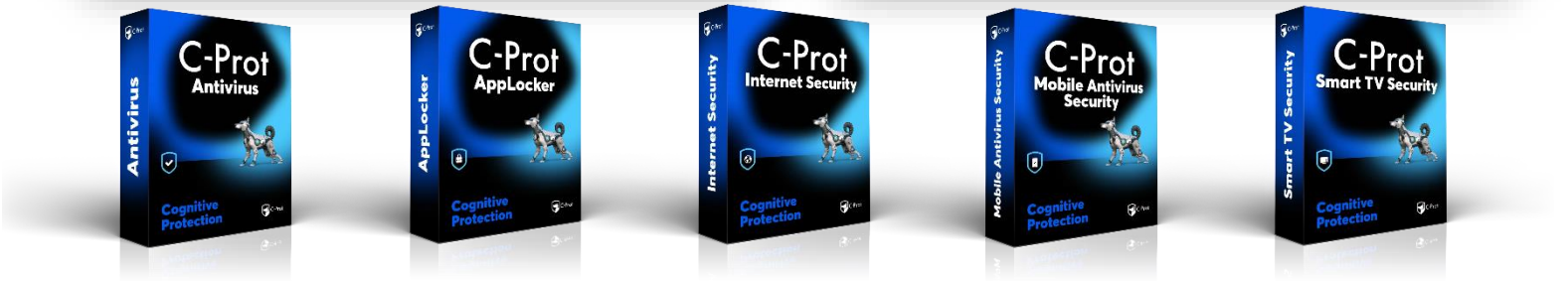
C-Prot دارای جوایز معتبر OPSWAT، STARCHECK، SKD AWARDS و VB100 است که فقط تعداد کمی از شرکت‌ها در جهان موفق به کسب آن‌ها شده‌اند.

C-Prot عضو گروه European Expert Group for IT-Security، شورای استانداردهای امنیتی "PCI Security Standards Council"، سازمان استانداردهای تست ضدبدافزار "Anti-Malware Testing Standards Organization" و انجمن محققان آنتی‌ویروس آسیایی "Association of Asian Antivirus Researchers" سی‌پروت همچنان با ارائه طیف گسترده‌ای از محصولات پیشرفته امنیت سایبری، از تلویزیون‌های هوشمند تا دستگاه‌های تلفن همراه، شما را در دنیای دیجیتال ایمن نگه خواهد داشت.

محصولات C-Prot







محصولات

C-Prot محصولات امنیت سایبری را توسعه می‌دهد که از فناوری‌های پیشرفته هوش مصنوعی و یادگیری ماشین استفاده می‌کنند و از سیستم‌عامل‌های مختلفی مانند اندروید، ویندوز، لینوکس، macOS، iOS و HarmonyOS پشتیبانی می‌کنند، که این محصولات را قابل استفاده در پلتفرم‌های مختلف می‌سازد.

• محصولات سازمانی

- C-Prot Endpoint Security
- C-Prot Endpoint Mobile Security
- C-Prot Threat Intelligence Portal
- C-Prot Cyber Security Kiosk
- C-Prot Device Fingerprint
- C-Prot Embedded AppDefense
- C-Prot Fraud Prevention

• محصولات خانگی

- C-Prot Antivirus
- C-Prot Internet Security
- C-Prot Prime Security
- C-Prot Web Protection
- C-Prot Mobile Antivirus Security
- C-Prot Smart Tv Security
- C-Prot AppLocker
- C-Prot Parental Control
- C-Prot VPN
- C-Prot QR Scanner

Virus Bulletin
Covering the global threat landscape
VB100 TEST REPORT

vb 100 VIRUS virusbtn.com

Test result
Test passed

Certification
Clean
Diversity

آزمون‌های **VB100** توسط سازمان **Virus Bulletin** برگزار می‌شوند و یکی از معتبرترین ارزیابی‌ها در حوزه امنیت سایبری و آنتی‌ویروس‌ها محسوب می‌شوند. این آزمون‌ها بر اساس توانایی نرم‌افزارهای امنیتی در شناسایی بدافزارها، عملکرد بدون هشدارهای اشتباه (False Positives) و سازگاری با سیستم‌عامل‌ها ارزیابی می‌شوند.

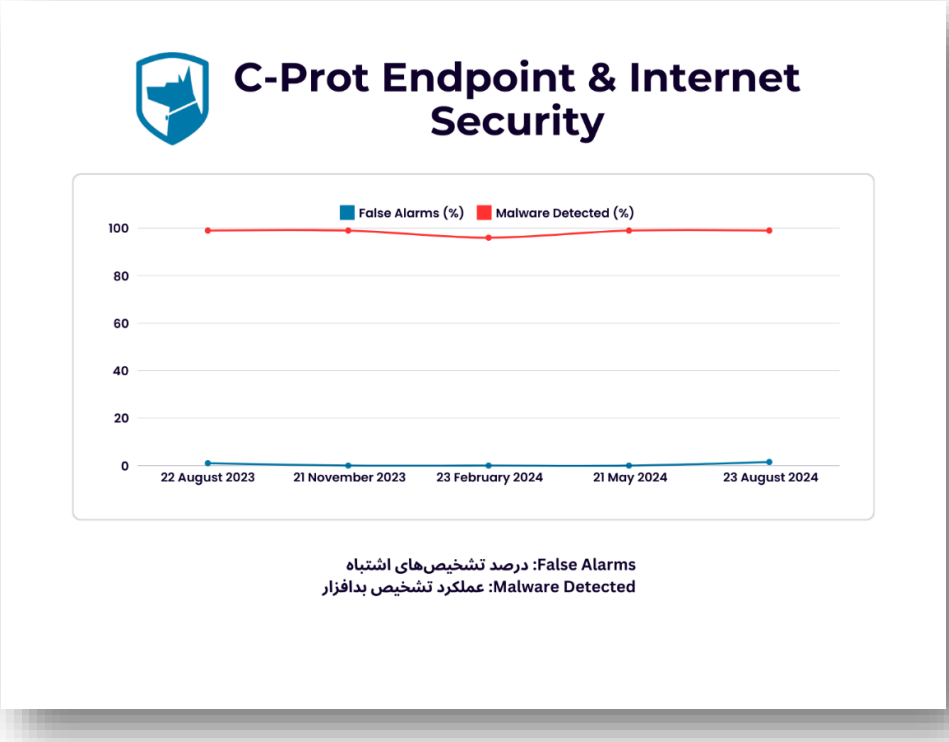
نتایج آزمون VB100 برای C-Prot

۱. **نرخ تشخیص بالا** :محصولات C-Prot در آزمون‌های VB100 توانسته‌اند با نرخ تشخیص بسیار بالا، بدافزارهای شناخته‌شده را شناسایی و مسدود کنند. این نشان‌دهنده قدرت بالای موتور امنیتی این شرکت است.

۲. **عدم هشدارهای اشتباه (False Positives)** :یکی از مهم‌ترین معیارهای آزمون VB100، جلوگیری از هشدارهای نادرست است. محصولات C-Prot در این زمینه عملکرد بسیار مطلوبی داشته‌اند و تعداد کمی هشدار اشتباه تولید کرده‌اند.

۳. **سازگاری بالا** :نرم‌افزارهای C-Prot بر روی سیستم‌عامل‌های مختلف با کارایی و سازگاری کامل اجرا شده‌اند که امتیاز بالایی در آزمون کسب کرده است.

٤. **جوایز متعدد** :نتایج درخشان در آزمون VB100 به C-Prot این امکان را داده است که جایگاه معتبری در بین شرکت‌های پیشرو در امنیت سایبری داشته باشد.



C-Prot

arka
رایان سامانه آرکا

خدمات جامع C-Prot

۱. خدمات مهاجرت و استقرار هوشمند

- **انتقال یکپارچه و بدون وقفه:**

C-Prot فرایند کامل جایگزینی آنتی‌ویروس قبلی را به صورت حرفه‌ای و خودکار مدیریت می‌کند. تیم متخصص ما تمامی تنظیمات، سیاست‌های امنیتی، استثنائات و پیکربندی‌های سفارشی شما را استخراج و به دقت پشتیبان‌گیری می‌نماید. سپس با استفاده از ابزارهای تخصصی، آنتی‌ویروس قبلی به طور کامل حذف شده و agent های C-Prot با انتقال کامل کانفیگ‌ها نصب می‌گردند.

- **ویژگی‌های کلیدی مهاجرت:**
  - حفظ سرمایه‌گذاری قبلی :تمامی سیاست‌ها، لیست سفید/سیاه، قوانین فایروال و تنظیمات امنیتی به پلتفرم جدید منتقل می‌شوند.
  - بدون خلأ امنیتی :انتقال به گونه‌ای طراحی شده که حفاظت سازمان شما در هیچ لحظه‌ای قطع نمی‌شود.
  - استقرار خودکار و متمرکز :نصب و پیکربندی بر روی تمامی سیستم‌ها بدون نیاز به دخالت دستی انجام می‌شود.
  - آزمون و اعتبارسنجی جامع :پس از استقرار، کلیه قابلیت‌ها به دقت تست می‌شوند تا از عملکرد بهینه اطمینان حاصل شود.
  - شفافیت کامل :گزارش تفصیلی از تمامی مراحل و وضعیت به مدیریت IT ارائه می‌گردد.

۲. خدمات پشتیبانی پیشرفته

- پشتیبانی فنی ۷/۲۴
  - تیم متخصص ما همواره در دسترس شماست. در هر ساعتی از شبانه‌روز، هفت روز هفته، برای رفع مشکلات فنی، پاسخگویی به سؤالات تخصصی و حل چالش‌های امنیتی، می‌توانید بر پشتیبانی فوری ما حساب کنید.
- پشتیبانی از راه دور
  - با استفاده از ابزارهای پیشرفته پشتیبانیRemote ، کارشناسان ما به سرعت به سیستم‌های شما دسترسی یافته و مشکلات را در کمترین زمان ممکن شناسایی و برطرف می‌کنند. این رویکرد، زمان قطعی سرویس و اختلالات عملیاتی را به حداقل می‌رساند.
- مشاوره تخصصی و راهنمایی شخصی‌سازی‌شده
  - خدمات مشاوره‌ای اختصاصی ما به شما کمک می‌کند تا از تمام قابلیت‌های C-Prot بهره کامل ببرید. کارشناسان امنیتی ما بهترین شیوه‌ها، استراتژی‌های حفاظتی و راهکارهای بهینه‌سازی را متناسب با نیازهای منحصر به فرد سازمان شما ارائه می‌دهند.

C-Prot

arka
رایان سامانه آرکا

(ادامه خدمات جامع C-Prot)

- منابع آموزشی و مستندات جامع
  - مجموعه کامل راهنماهای فنی، ویدئوهای آموزشی، مقالات تخصصی و مستندات گام‌به‌گام به شما امکان می‌دهد تا به طور مستقل از ویژگی‌های پلتفرم بهره‌برداری کنید. پایگاه دانش آنلاین ما همواره به‌روز و در دسترس است.

- ارتقاء و به‌روزرسانی‌های هوشمند
  - سیستم به‌روزرسانی خودکار C-Prot، به صورت دوره‌ای و بدون ایجاد وقفه، آخرین آپدیت‌های امنیتی، تعاریف تهدیدات جدید و ویژگی‌های پیشرفته را بر روی سیستم‌های شما نصب می‌کند تا همواره از بالاترین سطح حفاظت برخوردار باشید.

۳. خدمات آموزشی تخصصی

- **آموزش مجازی**
  - وبینارهای تخصصی :برگزاری منظم جلسات آنلاین در خصوص آخرین تهدیدات سایبری و نحوه مقابله با آن‌ها
  - دوره‌های تعاملی :آموزش‌های گام‌به‌گام برای ارتقای مهارت‌های تیم امنیتی و **IT** شما
  - پلتفرم یادگیری آنلاین :دسترسی نامحدود به کتابخانه جامع شامل ویدئوها، مقالات و راهنماهای فنی
  - گواهینامه‌های معتبر :اخذ مدارک تخصصی پس از اتمام موفقیت‌آمیز دوره‌های آموزشی
- **آموزش حضوری**
  - کارگاه‌های عملی :برگزاری جلسات تخصصی در محل سازمان با تمرکز بر نیازهای واقعی شما
  - آموزش سفارشی‌سازی‌شده :طراحی برنامه‌های آموزشی متناسب با سطح دانش و نقش تیم‌های مختلف
  - شبیه‌سازی حملات :تمرین عملی مواجهه با تهدیدات واقعی در محیط کنترل‌شده
  - پشتیبانی حضوری :همراهی کارشناسان در طول دوره برای درک عمیق‌تر مفاهیم و حل مسائل پیچیده

تعهد ما به موفقیت شما

خدمات جامع **C-Prot** طیف کاملی از نیازهای امنیت سایبری سازمان‌ها را پوشش می‌دهد. از لحظه تصمیم‌گیری برای استفاده از **C-Prot** تا پیاده‌سازی، آموزش، بهره‌برداری و پشتیبانی مستمر، تیم ما در کنار شماست تا اطمینان حاصل کنیم که زیرساخت امنیتی شما همواره در بالاترین سطح کارایی قرار دارد.

arka
رایان سامانه آرکا

C-Prot

بروشور C-Prot Endpoint Security

امنیت اندپوینت سی-پروت

C-Prot Endpoint Security

حفاظت پیشرفته که می‌تواند در محل یا در ابر مدیریت شود با یک برنامه تنها در برابر تمام تهدیدها.

ویژگی های ممتاز

External Media Management:
شما می‌توانید استفاده از دستگاه‌های خارجی ناشناخته را محدود یا کنترل کنید. (درایوهایUSB ، درایوهایCD/DVD ، هاردهای خارجی و غیره)

Anti-Malware:
حفاظت از کامپیوترها، سرورها و دستگاه‌های تلفن همراه در سازمان شما در برابر خطراتی از ویروس‌ها، تروجان‌ها، کرم‌ها و رنسوم‌ور است.

Policy Management:
شما می‌توانید چندین سیاست با ارزش‌های مختلف پیکربندی کنید. یک برنامه ممکن است با تنظیمات مختلف برای گروه‌های مدیریتی مختلف اجرا شود.

Central Management Console:
همهٔ نقاط پایانی خود را از هر کجا با مدیریت از راه دور C-Prot، در دسترس به صورت مبتنی بر ابر یا در محل، مدیریت کنید.

بخش های مورد استفاده

Government:
این شرکت حفاظت را در برابر تهدیدات سایبری که دولت و سازمان‌های بخش عمومی ممکن است در دنیای دیجیتال با آنها روبه‌رو شوند، فراهم می‌کند.

Finance:
این شرکت راه‌حل حفاظت از نقاط پایانی برای سازمان‌های ارائه‌دهنده خدمات مالی از جمله بانک‌ها، موسسات مالی و شرکت‌های بیمه توسعه می‌دهد.

Education:
محصول امنیتی C-Prot Endpoint Security برای حفاظت از اطلاعات مؤسسات آموزشی، دانشجویان و کارکنان در برابر حملات سایبری توسعه یافته است.

Healthcare:
این شرکت امنیت را در برابر تهدیدات سایبری در جهان دیجیتال فراهم می‌کند تا پرونده‌های پزشکی بیماران و اطلاعات شخصی سلامت را محافظت کند.

Retail:
این شرکت در دنیای دیجیتال حفاظت از داده‌های مشتری و اطلاعات پرداخت را فراهم می‌کند تا آنها را محافظت کند.

Critical Infrastructure:
این شرکت در جهان دیجیتال در برابر تهدیدات سایبری محافظت انجام می‌دهد تا از وقوع قطعی برق در تولید برق، انتقال، امکانات عمومی و زیرساخت‌های حیاتی جلوگیری کند.

Telecommunications:
شرکت‌های مخابراتی و ارائه دهندگان خدمات اینترنت می‌توانند از این ابزار برای حفاظت از کامپیوترهای خود در نقاط پایانی استفاده کنند.

Manufacturing:
این شرکت امنیت را در دنیای دیجیتال ارائه می‌دهد تا از وقوع وقفه در فرآیندهای تولید جلوگیری کرده و در برابر جاسوسی صنعتی دفاع کند.

ENDPOINT SECURITY

C-Prot Endpoint Security جلوی خطرات ایجاد شده توسط انواع ویروس‌ها، جاسوس‌نرم‌افزارها، تروجان‌ها، کرم‌ها، ادوئرها و سایر تهدیدات را می‌گیرد در حالی که به شما اجازه می‌دهد دستگاه‌های خود را با عملکرد بالای اچ‌وان اچ استفاده کنید. این به شما ادامه حفاظت در اینترنت را به واسطهٔ حفاظت از اینترنت و ایمیل می‌دهد. این ویژگی تکنولوژی حفاظتی بازهم به دستگاه شما حفاظت کاملی ارائه می‌دهد. در محیط شرکتی، شما می‌توانید از C-Prot Endpoint Security همراه با C-Prot Remote Administratorبرای مدیریت آسان ایستگاه‌های کاری چندگانه مشتری، اعمال سیاست‌ها و تنظیم آنها را از دور از هر کامپیوتر در شبکه استفاده کنید.

دفاع از خود
ویژگی دفاع شخصی C-Prot از مکانیزم دفاعی در برابر نرم‌افزارهای مخرب یا فعالیت‌های مضر دیگر که باعث غیرفعال شدن C-Prot می‌شوند، فراهم می‌کند.

تکنولوژی یادگیری ماشینی پیشرفته
این فناوری حفاظت برتری را ارائه می‌دهد که با استفاده از آخرین یادگیری ماشینی توسعه یافته در برابر بدافزارهای جدید و شناسایی نشده به کار می‌رود.

امنیت ایمیل
این ویژگی باعث می‌شود ایمیل‌های اسپم یا مخرب از صندوق پستی شما دور نگه داشته و مسدود شود. این کار باعث می‌شود که کارمندان شما نتوانند بر روی ایمیل‌های مضر کلیک کنند و از حملات فیشینگ جلوگیری می‌کند.

ساختار به‌روزرسانی توزیع‌شده
ایجاد نقاط توزیع چندگانه برای جلوگیری از افزودن بار اضافی بر روی سرور در حال به‌روزرسانی برنامه و پایگاه داده امضا.

مدیریت پچ
تقویت امنیت با مدیریت خودکار پچ که در سیستم‌عامل‌ها و برنامه‌ها امکان‌پذیر است، باعث کاهش ریسک آسیب‌پذیری‌های امنیتی می‌شود.

برنامه‌های استفاده‌کننده از اینترنت
به‌صورت فوری ترافیک اینترنتی برنامه‌ها را مشاهده کرده و برنامه‌های دلخواه را مسدود کنید.

شناسایی جاسوسی
این حفاظت را در برابر نرم‌افزارهای مخرب که اطلاعات دستگاه‌های موجود در سازمان شما را بدون اجازه جمع‌آوری می‌کنند، فراهم می‌کند.

محافظت در برابر فیشینگ و کلاهبرداری
این فناوری حفاظت سطح بالا را در برابر وب‌سایت‌های مخرب که قصد دارند اطلاعات حساس شما مانند نام کاربری، رمز عبور، اطلاعات بانکی یا کارت اعتباری را به دست آورند، ارائه می‌دهد.

مصرف پایین منابع
این از منابع سیستم به صورت کارآمد استفاده می‌کند و کامپیوتر شما را بدون کاهش سرعت محافظت می‌کند.

محافظت در برابر پرداخت‌های آنلاین
این جلوگیری می‌کند از هک شدن اطلاعات کارت اعتباری و اطلاعات مالی شما در هنگام انجام تراکنش‌های آنلاین روی دستگاه‌های موجود در موسسه‌ی شما.

فایروال
C-Prot Endpoint Security یک دیواره آتش یکپارچه ارائه می‌دهد. این دیواره آتش ترافیک شبکه را نظارت می‌کند و اتصالات مضر یا ناخواسته را مسدود می‌کند. همچنین اطمینان می‌دهد که امنیت داده‌های وارد شده و خارج شده از شبکه سازمان شما حفظ می‌شود.

محافظت در برابر شبکه‌های زامبی
این موجودیت‌ها را از سوءاستفاده به عنوان بخشی از یک شبکه‌ی کامپیوتری آلوده یا به عنوان یک شبکه زامبی محافظت می‌کند.

حفاظت در برابر تهدیدات تلفن همراه
این امنیت جامع را با شناسایی جاسوسی، ویروس‌ها و برنامه‌های مخرب دیگر در دستگاه‌های تلفن همراه در سازمان شما فراهم می‌کند.

ضدسرقت
این به شما کمک می‌کند تا در صورت از دست رفتن یا دزدیده شدن، دستگاه‌های خود را پیدا و موقعیت آن‌ها را پیگیری کنید.

رایان سامانه آرکا، با بیش از بیست سال سابقه ارائه آنتی ویروس های سازمانی، نماینده انحصاری C-Prot در ایران.

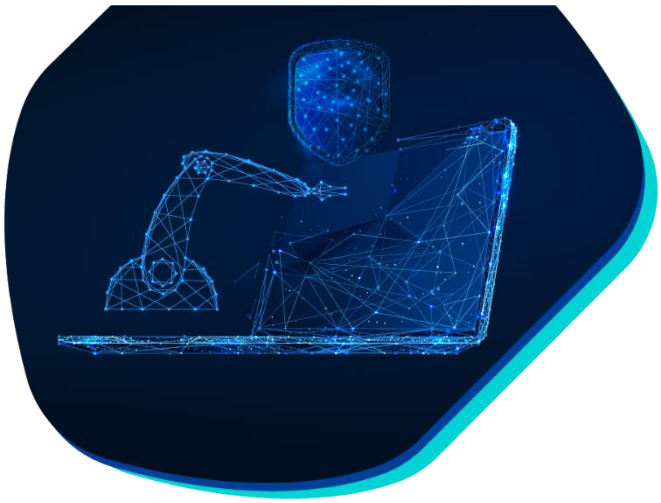
C-Prot با یک مجموعه گسترده از محصولات امنیت سایبری پیشرفته، از تلویزیون‌های هوشمند تا دستگاه‌های تلفن همراه، ادامه می‌دهد تا شما را در دنیای دیجیتال ایمن نگه دارد، همچنین به عهده‌داری از ارائه بهترین محصولات حفاظت از نقاط پایانی به مشتریان خود پایبند می‌ماند.

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۰۲۱-۹۱۳۰۰۴۷۶ | دورنگار: ۰۲۱-۸۸۸۰۴۹۶۱ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
info@arka.ir
www.arka.ir
رایان سامانه آرکا

arka
رایان سامانه آرکا

C-Prot

بروشور C-Prot EDR



راهکار C-Prot EDR (تشخیص و پاسخ به نقاط پایانی)

راهکار C-Prot EDR(تشخیص و پاسخ به نقاط پایانی) تهدیدات را به‌طور آنی با استفاده از تله‌متری عمیق نقاط پایانی، مشاهده در زمان واقعی و تحلیل‌های رفتاری شناسایی می‌کند. با قابلیت‌های پاسخ خودکار خود، حملات پیشرفته را به سرعت متوقف می‌کند و به تیم‌های امنیتی این امکان را می‌دهد که در کوتاه‌ترین زمان ممکن به حوادث واکنش نشان دهند.

- تحلیل عمیق حملات
- پاسخ خودکار
- تشخیص تهدیدات پیشرفته

دریافت قدرت تشخیص تهدیدات در سطح سازمانی و پاسخ خودکار

C-Prot EDR (تشخیص و پاسخ به نقاط پایانی) حملات مدرن را در زمان واقعی از طریق تحلیل‌های رفتاری، موتورهای تشخیص مبتنی بر هوش مصنوعی و قابلیت‌های پاسخ خودکار شناسایی و مسدود می‌کند. با دید تله‌متری عمیق، همبستگی حملات و تحلیل مبتنی بر داستان، این سیستم به تیم‌های امنیتی امکان می‌دهد تا به سرعت و به طور مؤثر به حوادث واکنش نشان دهند.

۱. تهدیدات با سرعت ماشین

مهاجمان اکنون می‌توانند با استفاده از اتوماسیون و هوش مصنوعی، در عرض چند میلی‌ثانیه به سیستم‌ها نفوذ کنند. در حالی‌که راهکارهای سنتی در برابر این سرعت کارایی لازم را ندارند، تحلیل‌های رفتاری و محافظت خودکار C-Prot EDR تهدیدات را به‌صورت بلادرنگ متوقف می‌کند.

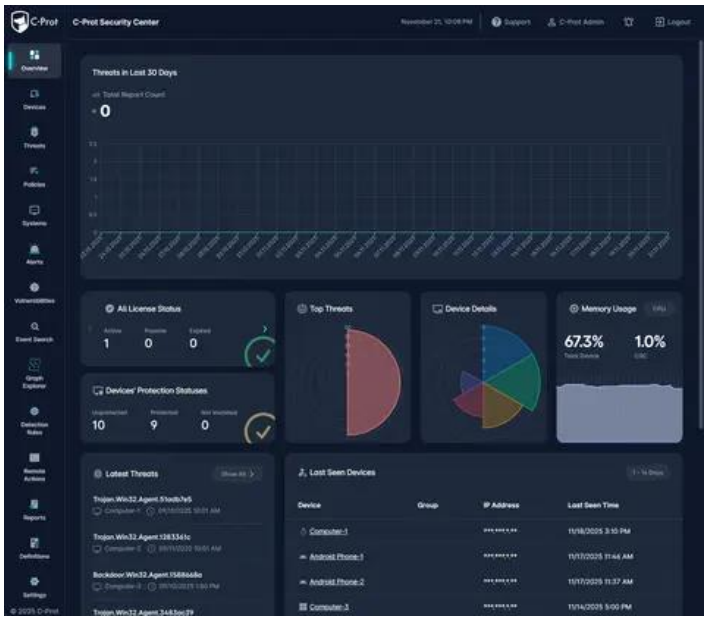
۲. سطوح حمله گسترده‌تر و همگرا

سطوح نقاط پایانی، هویت و شبکه هر روز بیش از پیش به هم متصل و درهم‌تنیده می‌شوند. این همگرایی، دیدپذیری را کاهش می‌دهد و جابه‌جایی پنهانی مهاجمان را آسان‌تر می‌کند .(تشخیص و پاسخ به نقاط پایانی) C-Prot EDR با یک عامل واحد، دید یکپارچه‌ای در همه لایه‌ها—از نقاط پایانی تا فعالیت‌های مرتبط با هویت—فراهم می‌سازد.

۳. تیم‌های SOC تحت فشار و اضافه‌بار

امروزه تیم‌های SOC با پیچیدگی رو به افزایش و منابع رو به کاهش دست‌وپنجه نرم می‌کنند. این فشار، تصمیم‌گیری سریع و مدیریت مؤثر رخدادها را دشوارتر می‌کند C-Prot Deep Black AI .با قابلیت‌هایی مانند پرس‌وجوی زبان طبیعی، خلاصه‌سازی خودکار، همبستگی (Correlation)و پیشنهادهای هوشمند، بار کاری تحلیل‌گران را به‌طور چشمگیری کاهش می‌دهد.

تهدیدات پیشرفته را با محافظت خودکار و دید عمیق متوقف کنید



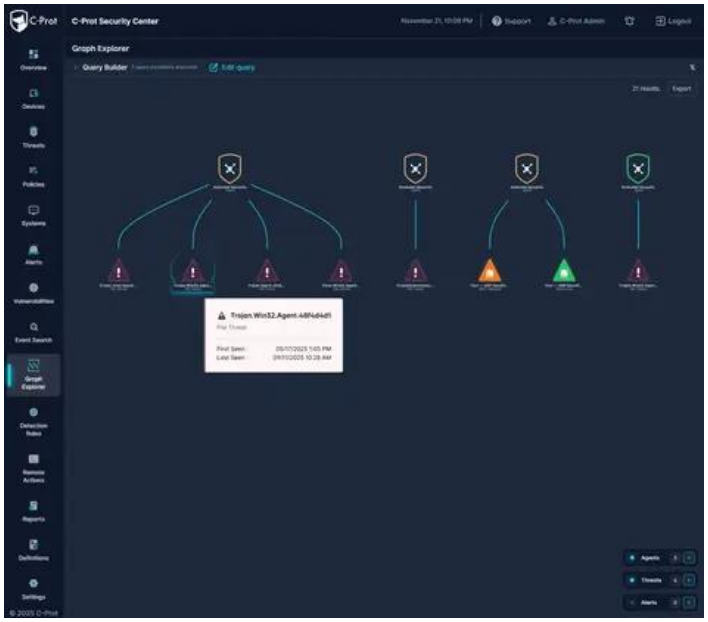
پیشگیری با سرعت ماشین :موتورهای هوش مصنوعی رفتاری و ایستای C-Prot فعالیت‌های مشکوک را پیش از اجرا شناسایی می‌کنند و بدافزارهای مدرن را به‌صورت بلادرنگ مسدود می‌سازند.

تشخیص فوری باجافزار :تحلیل‌های رفتاری، الگوهای غیرعادی رمزگذاری و حرکت جانبی (Lateral Movement) را بلافاصله شناسایی می‌کنند؛ C-Prot EDR (تشخیص و پاسخ به نقاط پایانی) تلاش‌های رمزگذاری فایل، فعالیت‌های فیشینگ و عملیات فرماندهی‌وکنترل (C۲) را مسدود می‌کند.

دید جامع از طریق تله‌متری یکپارچه :این راهکار تمام تله‌متری نقاط پایانی—از رخدادهای سیستمی تا حملات مبتنی بر هویت—را در یک زمینه امنیتی واحد تجمیع می‌کند. فعالیت‌های پردازه، فایل، حافظه، رجیستری و هویت در همان لایه دیدپذیری نمایش داده می‌شوند تا تحلیل‌گران بتوانند تهدیدات حیاتی را در یک نگاه تشخیص دهند.

محافظت چندسکویی C-Prot :محافظتی آماده برای تهدیدات روز-صفر (Zero-Day) روی دستگاه‌های iOS و Android در برابر فیشینگ، بدافزار، ارتقای سطح دسترسی (Privilege Escalation)و حملات مرد میانی (MITM) ارائه می‌دهد.

رخدادها را با پاسخ مبتنی بر هوش مصنوعی سریع‌تر حل‌وفصل کنید

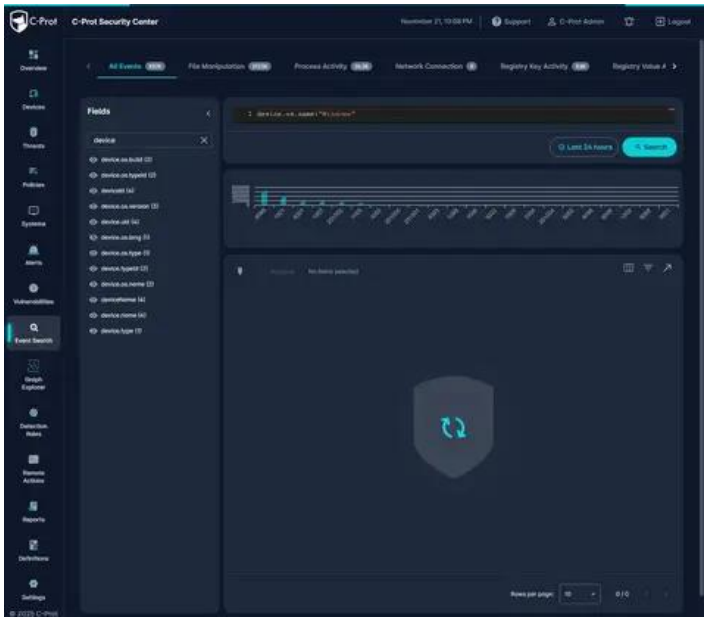


اصلاح خودکار و رفع مشکل با یک کلیک C-Prot EDR :(تشخیص و پاسخ به نقاط پایانی) به‌طور خودکار به تهدیدات شناسایی‌شده واکنش نشان می‌دهد و ظرف چند ثانیه اقداماتی مانند پایان‌دادن به پردازه‌ها(Process Kill) ، ایزوله‌سازی شبکه، بازگردانی (Rollback)و اعمال سیاست‌ها را انجام می‌دهد.

نمایش کل زنجیره حمله با Storyline: فناوری C-Prot Storyline به‌صورت خودکار تله‌متری نقاط پایانی، هویت و شبکه را به یک زنجیره حمله زمینه‌مند تبدیل می‌کند. تحلیل‌گران می‌توانند از طریق یک تایم‌لاین گرافیکی واحد، منشأ تهدید و نحوه پیشروی آن در محیط را دنبال کنند.

تحلیل زمینه‌مند و اولویت‌بندی :هشدارها به‌طور خودکار در میان فعالیت‌های پردازه، فایل، هویت و شبکه همبسته‌سازی (Correlate)شده و بر اساس شدت رتبه‌بندی می‌شوند. تهدیدات حیاتی برجسته می‌گردند تا تیم‌های SOC فوراً تشخیص دهند کدام رخدادها نیاز به رسیدگی فوری دارند.

امنیت را با عامل یکپارچه و کم‌اثر C-Prot بهینه کنید

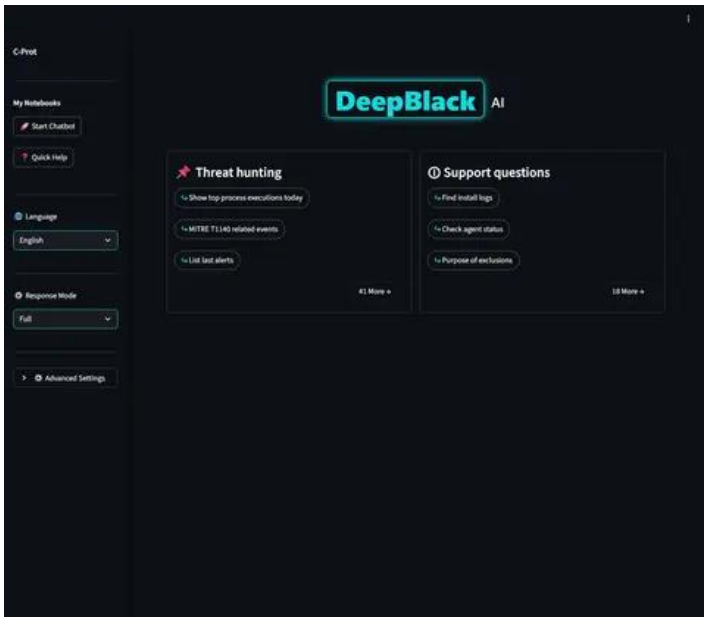


عامل واحد، معماری ساده‌تر C-Prot EDR :تحلیل‌های رفتاری و محافظت مبتنی بر هویت را در قالب یک عامل هوشمند C-Prot Agent یکپارچه می‌کند. این کار مشکلات عملکردی ناشی از چندعامل را حذف می‌کند، مدیریت نقاط پایانی را ساده‌تر می‌سازد و پیچیدگی عملیاتی را کاهش می‌دهد.

کارایی بالا در همه پلتفرم‌ها C-Prot Agent :طوری بهینه شده که همان سطح امنیت و عمق تله‌متری را درWindows ، macOS، Linuxو سیستم‌عامل‌های موبایل ارائه دهد. دیدپذیری یکنواخت و محافظت برابر را در تمام پلتفرم‌ها تضمین می‌کند.

معماری سبک، بیشترین بهره‌وری :طراحی آن مصرف CPU و حافظه را پایین نگه می‌دارد، در حالی‌که فعالیت‌های پردازه، فایل، شبکه و هویت را در حد میلی‌ثانیه تحلیل می‌کند. دیدپذیری نقاط پایانی را افزایش می‌دهد بدون اینکه کارایی سیستم افت کند و از تداوم محافظت دستگاه‌ها اطمینان می‌دهد.

تیم‌های امنیتی را با هوش خودکار مبتنی بر AI توانمند کنید



شکار تهدید با زبان طبیعی :باDeep Black AI ، تحلیل‌گران می‌توانند به تمام تله‌متری—از جمله داده‌های پردازه، لاگ‌ها، رویدادهای هویتی و فعالیت شبکه—با زبان طبیعی دسترسی داشته باشند. این قابلیت شکار تهدید را بدون نیاز به نوشتن کوئری‌های پیچیده سریع‌تر می‌کند و بینش‌های حیاتی را ظرف چند ثانیه آشکار می‌سازد.

خلاصه‌سازی خودکار و تحلیل هدایت‌شده Deep Black AI :
هشدارها را به‌طور خودکار خلاصه می‌کند، یافته‌های کلیدی را برجسته می‌سازد و پیشنهاد می‌دهد کدام مؤلفه در گام بعدی بررسی شود. این کار یک جریان تحقیق زمینه‌مند ایجاد کرده و سرعت تصمیم‌گیری تحلیل‌گران را به‌طور محسوسی افزایش می‌دهد.

مدل‌های AI امنیت‌محور با کاهش خطا :مدل‌های امنیت‌محور هوش مصنوعی C-Prot با تمرکز بر دقت، قابلیت اتکا و الزامات ممیزی سازمانی طراحی شده‌اند. این مدل‌ها ریسک نتایج گمراه‌کننده یا پرنویز را کاهش می‌دهند و به تحلیل‌گران کمک می‌کنند تصمیم‌های سریع‌تر و دقیق‌تری بگیرند .

• مقایسه راهکارهای EDR

معیار	C-Prot EDR	Symantec EDR	ESET (PROTECT + EDR)	Kaspersky EDR
تمرکز محصول	EDR محور با تحلیل رفتار و پاسخ اتوماتیک	EDR Enterprise با ادغام در سبد Broadcom	پلتفرم کامل EPP + EDR سبک	تشخیص و پاسخ به تهدیدها در پایان‌نقطه‌ها با ابزارهای تحلیلی
تشخیص تهدیدات پیچیده	خیلی خوب – رفتارشناسی AI محور	عالی – هوش تهدیدات جهانی + تحلیل ML قوی	خیلی خوب – تشخیص پیشرفته و اعلان به‌موقع	خوب – ML و رفتارشناسی با دید وسیع
Threat Hunting	جستجو با زبان طبیعی مبتنی بر AI	امکانات حرفه‌ای و گسترده	امکانات خوب جهت تحقیقات دستی	امکانات پایه
واکنش خودکار (Response)	ایزوله‌سازی، Kill Process، Rollback خودکار	قرنطینه، مهار، پاسخ متمرکز	واکنش سریع و گزارش	قرنطینه و مهار تهدیدها
دید و گزارش‌گیری	Timeline و Storyline تحلیلی	داشبورد مدیریتی پیشرفته	گزارش‌های قابل فهم و دقیق	دید کلی و تحلیل رویدادها
سهولت استقرار / مدیریت	طراحی آسان و سبک	پیچیده‌تر اما حرفه‌ای	نسبتاً ساده و سبک	ساده‌تر در مقایسه با Enterprise بزرگ
مصرف منابع Endpoint	سبک و بهینه	بالا در استقرار Enterprise	کم تا متوسط	متوسط
مقیاس‌پذیری در سازمان‌های بزرگ	مناسب	بسیار مناسب	مناسب	متوسط
یکپارچگی با دیگر ابزارها	محدودتر – تمرکز روی EDR داخلی	بسیار قوی با SIEM، SOAR، DLP و...	خوب با برخی ابزارها	متوسط
پشتیبانی پلتفرم‌ها	Windows, macOS, Linux, Mobile	Windows, macOS, Linux	Windows, macOS, Linux,	Windows, macOS, Linux
بهینه برای سازمان‌های کوچک/متوسط	☆☆☆☆	☆☆	☆☆☆☆	☆☆
بهینه برای سازمان‌های بزرگ(Enterprise)	☆☆☆☆☆	☆☆☆☆	☆☆☆	☆☆

- **کسب بالاترین امتیاز در آزمون‌های EDR-Telemetry توسط C-Prot EDR**

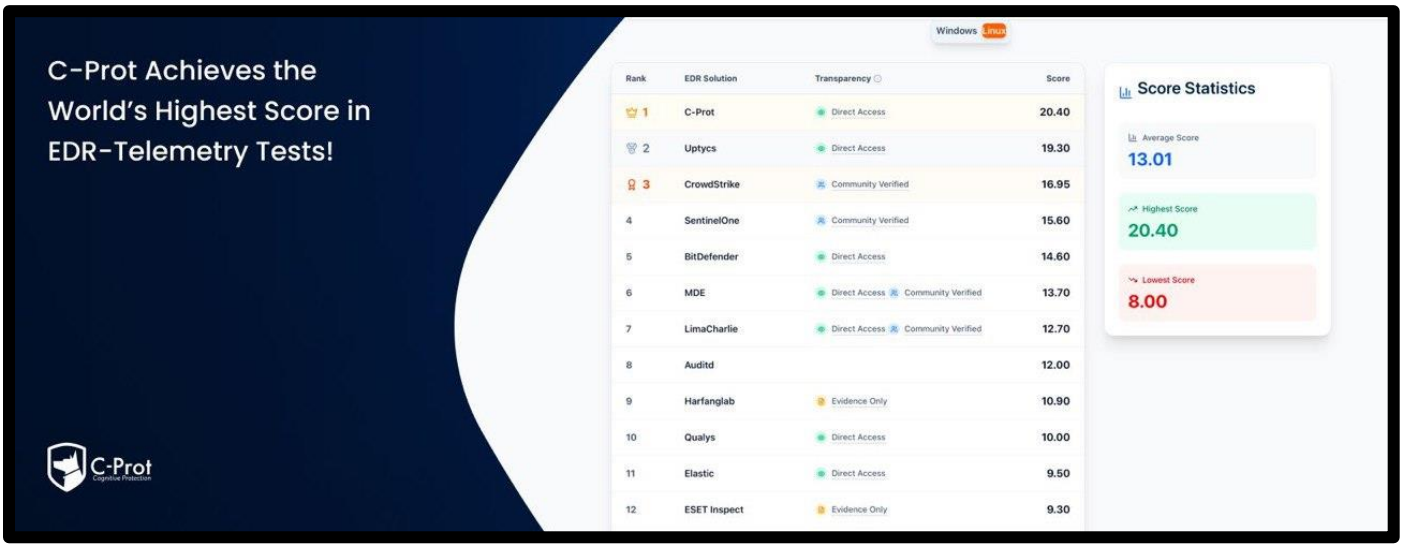
محصول نسل جدید حفاظت از نقاط پایانی شرکت سی‌پروت با نام **C-Prot EDR**، پس از ارزیابی‌های انجام‌شده توسط پلتفرم مستقل و شفاف **EDR-Telemetry**، بالاترین امتیاز را در میان محصولات EDR در سراسر جهان به دست آورد.

در آزمون EDR-Telemetry، محصول C-Prot EDR امتیاز **۲۰٫۴۰** را کسب کرد که به‌طور قابل‌توجهی بالاتر از میانگین جهانی فعلی **۱۳٫۰۱** است و در رتبه نخست تمامی محصولات EDR مورد ارزیابی قرار گرفت. این نتیجه، شاخصی قوی و به‌صورت مستقل تأییدشده از عمق تله‌متری، میزان شفافیت رویدادها و کیفیت مهندسی C-Prot EDR به شمار می‌رود.

کسب جایگاه نخست جهانی توسط C-Prot EDR در این ارزیابی نشان می‌دهد که این محصول صرفاً یک راهکار امنیتی برای شناسایی تهدیدات نیست، بلکه یک محصول EDR بالغ و پیشرفته است که تله‌متری عمیق، دید گسترده و قابلیت‌های عملیاتی قدرتمندی را ارائه می‌دهد.

در چارچوب پلتفرم امنیت نقاط پایانیC-Prot ، این شرکت قابلیت‌های آنتی‌ویروس نسل جدید (AV) و EDR را به‌صورت یکپارچه و از طریق معماری تک‌اِیجنت ارائه می‌دهد و به این ترتیب، نخستین و تنها تولیدکننده داخلی در ترکیه است که AV و EDR را به‌عنوان یک محصول یکپارچه امنیت نقاط پایانی عرضه می‌کند. این رویکرد یکپارچه، مزایای قابل‌توجهی در عملکرد و بهره‌وری عملیاتی به همراه دارد.

این دستاورد، چشم‌انداز C-Prot برای تبدیل‌شدن به یک محصول مرجع شناخته‌شده در سطح جهانی در حوزه فناوری‌های EDR را بیش از پیش تقویت می‌کند.



C-Prot EDR

Endpoints remain the most critical entry point for attacks targeting corporate networks. However, modern attacks have become far more automated, faster, and increasingly difficult to detect. As endpoint- and identity-based attack surfaces continue to converge, legacy and siloed security solutions are no longer capable of keeping pace with these evolving threats. Despite the growing scope and complexity of the threat landscape, security teams are expected to achieve higher efficiency with fewer resources. The C-Prot Endpoint Security Platform is a comprehensive EPP and EDR solution designed to protect endpoints against advanced, high-velocity attacks.

Built on a single-agent architecture, it delivers AI-driven automated protection, threat detection, and response capabilities across endpoints, servers, and identities. When combined with DeepBlack AI, the platform significantly accelerates incident prioritization, in-depth analysis, threat hunting, and rapid response workflows—elevating the overall effectiveness of security operations to an advanced level.

Key Benefit

- Protect endpoints in real time using artificial intelligence.
- Detect threats autonomously with minimal human intervention.
- Respond to threats automatically or with a single click.
- Defend against ransomware using behavioral and static AI models, while detecting suspicious activities instantly.
- Full compatibility with Windows, macOS, and Linux platforms.
- Advanced AI-powered analysis assistant for security operations: DeepBlack AI.
- One-click remediation and rollback capabilities.
- Correlate incidents and generate visual incident timelines using Storyline technology.
- Mobile endpoint protection support for iOS and Android.
- User-controlled, instant security updates that do not require system restarts, ensuring protection against emerging threats.

C-Prot EDR

Stop Attacks with Unmatched Protection, Detection, and Visibility

Protect against malware through autonomous prevention capabilities, and detect ransomware and zero-day exploits using behavioral AI models—without requiring human intervention. Gain real-time visibility and receive critical alerts across the entire threat spectrum, from system-level attacks to identity-based threats.

Minimize Disruption with Real-Time Response and Automated Remediation

Leverage Storyline technology to connect related events and gain a complete view of attack activity. Automatically correlate and prioritize alerts across devices, identities, and vulnerabilities. Respond to threats either autonomously or with a single click, and rapidly restore systems using rollback capabilities.

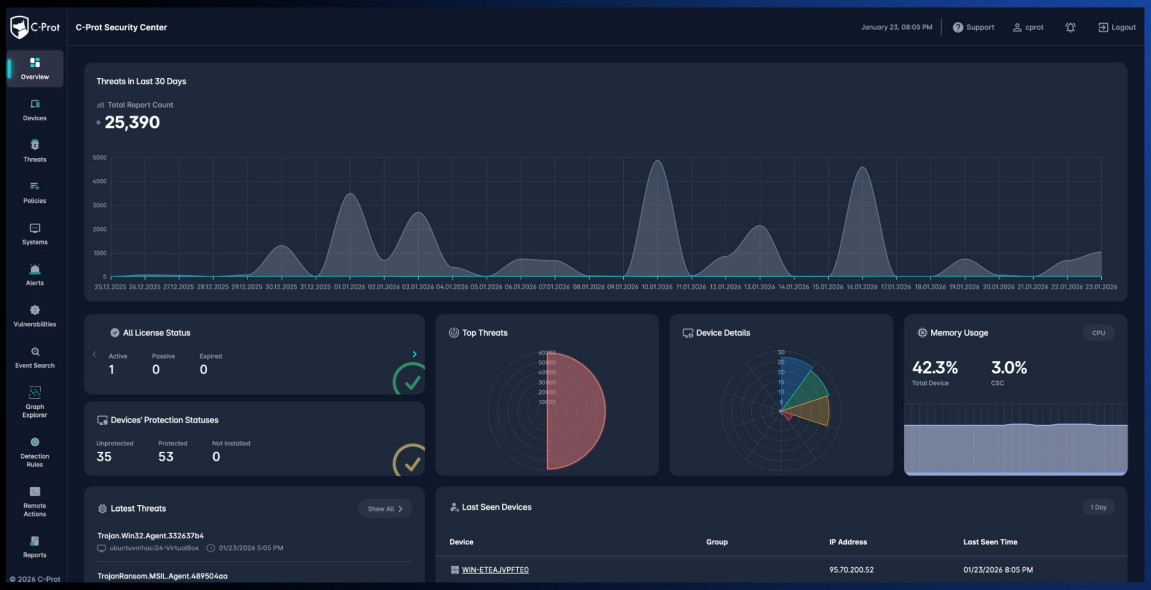
Stay in Control with a Lightweight, Unified Agent

Experience comprehensive security through a unified architecture that combines EDR capabilities and identity protection in a single package. The lightweight, autonomous agent is specifically designed to minimize end-user impact while limiting kernel-level interactions for enhanced stability and performance.

Accelerate Security Operations with Generative AI

Simplify threat hunting and incident investigations with natural language query support across first- and third-party data sources. DeepBlack AI accelerates SecOps workflows by automating rapid threat hunting, incident and outcome summaries, recommended follow-up questions, investigation notebooks, and analyst assistance.

End-to-End Threat Visibility and Response with C-Prot Security Center



AI-Powered Detection

Detect suspicious and malicious behavioral patterns in real time with high accuracy using advanced behavioral AI models.

Unified Agent and Correlation

Deliver comprehensive protection against endpoint- and identity-based attacks through a single, unified platform.

Accelerate with AI

Use DeepBlack AI to speed up incident prioritization, threat hunting, analysis, and response workflows.

Redefine your cybersecurity posture by integrating artificial intelligence, automation, and end-to-end visibility with C-Prot EDR.

Request a Demo

Tested by independent testing organizations.

C-Prot continues its commitment to providing its customers with the best cybersecurity products, and with the awards and certifications it has received globally, it will continue to ensure you stay safe in the digital world.

arka
رایان سامانه آرکا

C-Prot

جوایز بین‌المللی C-Prot

STARCHECK CERTIFICATE

NO. SKD ZS 2023-02-44-03

C-Prot Antivirus Security for Mobile

Anti-Malware

C-Prot

Valid until January 20, 2025

Certificate Query

skd labs

STARCHECK CERTIFICATE

NO. SKD ZS 2023-02-44-01

C-Prot Internet Security

Anti-Malware

C-Prot

Valid until January 20, 2025

Certificate Query

skd labs

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

vb 100 VIRUS virusbtn.com

C-Prot

C-Prot Endpoint Security

February 24, 2025

Test result
Test passed

Detection grade
Grade A

Certification
99.06% malware detected

Clean
0.008% false alarms

Quick Summary

Product version
1.0.0.498

Test date:
February 3, 2025

Test methodology
VB100 1.6

Test platform
Microsoft Windows 11 Pro, 64-bit, 10.0.26100

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

vb 100 VIRUS virusbtn.com

C-Prot

C-Prot Internet Security

February 24, 2025

Test result
Test passed

Detection grade
Grade A

Certification
99.06% malware detected

Clean
0.008% false alarms

Quick Summary

Product version
1.0.0.498

Test date:
February 5, 2025

Test methodology
VB100 1.6

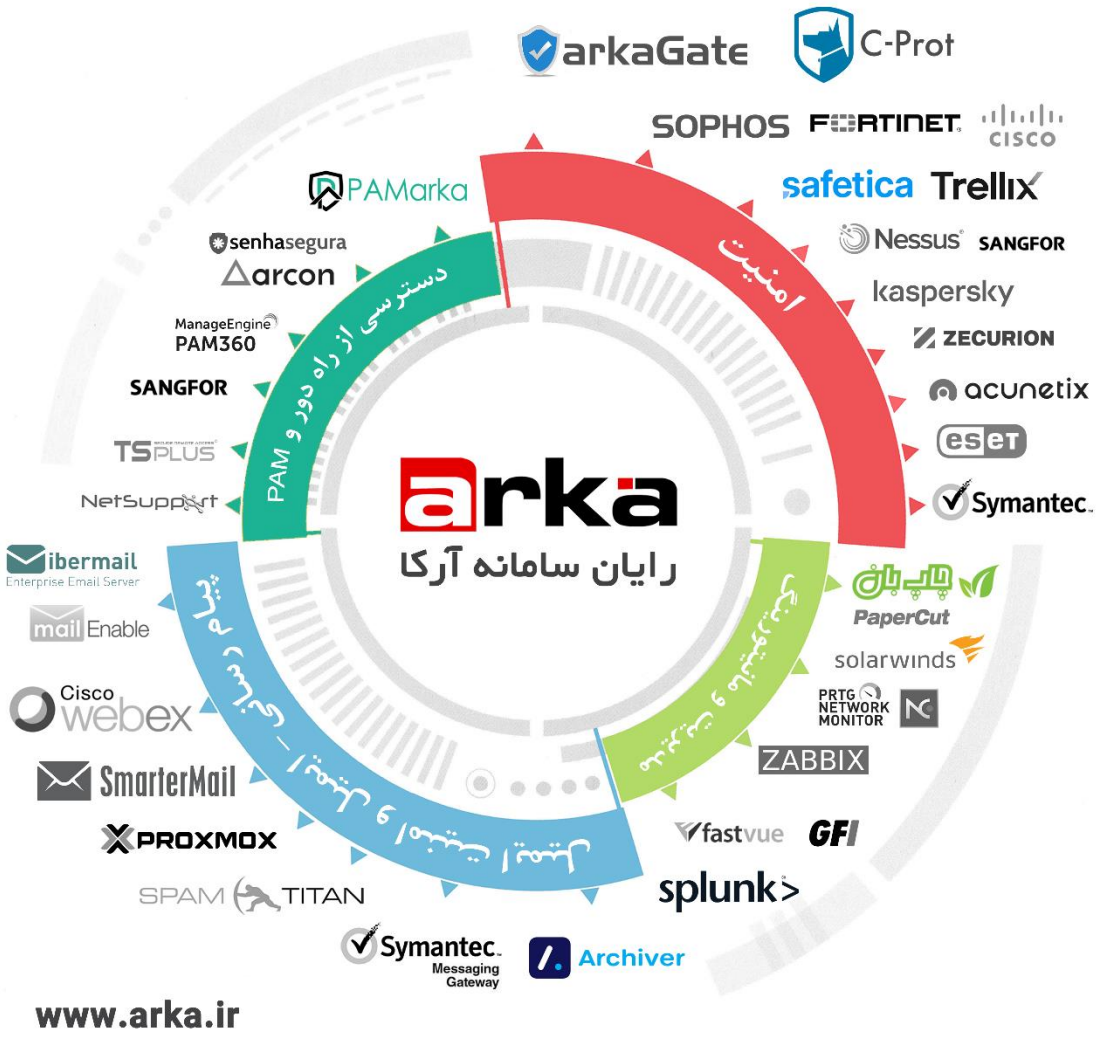
Test platform
Microsoft Windows 11 Pro, 64-bit, 10.0.26100

درباره آرکا

بهره‌مندی مشتریان ایرانی از آخرین فناوری‌ها و محصولات بروز در حوزه فناوری اطلاعات به خصوص در شاخه امنیت، یکی از اهداف شرکت رایان سامانه آرکا بوده است. در این راستا، این مجموعه از سال ۱۳۸۳ تاسیس یافته و با ارائه خدمات فنی و همچنین اخذ نمایندگی‌های محصولات شناخته شده در حوزه امنیت، مدیریت شبکه و ایمیل سرور، به ارائه خدمات به مشتریان ایرانی پرداخته است. جهت ارائه خدمات فروش و پس از فروش عالی، این شرکت در تمامی‌استان‌های کشور دارای نمایندگی بوده و افتخار همکاری با بیش از ۲۵۰۰ مشتری را در سراسر کشور داشته است.

به لطف متخصصان خبره کشور، این شرکت محصولاتی در زمینه‌های امنیت و مدیریت تولید کرده و پس از تست و ارزیابی و کسب مجوزهای لازم به خصوص از سازمان افتا، محصولات توایدی را به مشتریان خود ارائه کرده است. از جمله محصولات تولیدی این شرکت می‌توان به مواردی مانند آرکاگیت که یک فایروال بومی‌با امکانات کامل و جامع و اینترنت اکانتینگ کامل است اشاره کرد. همچنین چاپبان، نرم‌افزاری برای مدیریت چاپ در شبکه، pamArka محصول بومی‌برای مدیریت دسترسی ادمین (PAM)، از دیگر محصولات تولیدی شرکت رایان سامانه آرکا است.

محصولات و راهکارهای رایان سامانه آرکا



www.arka.ir

تماس با ما

آدرس دفتر مرکزی: تهران، خیابان شهید بهشتی، خ پاکستان، کوچه ٤ پلاک ١١ واحد ٧

مرکز تماس: ۵۹۱۱ ۸۲۸۰ (۲۱) ۹۸+ ۰٤٧٦ ۹۱۳۰ (۲۱) ۹۸+

دفتر تبریز: چهارراه منصور، برج ابریشم، طبقه ٦، واحد ٨

تلفن تماس: ۵۲۳۰ ۳۵۵۹ (٤١) ۹۸+

info@arka.ir www.arka.ir

WhatsApp: +۹۸۹۹۱۹۰۰۳۲۱۹

Telegram: rayansamanarka

Instagram: rayansamanarka

Linkedin: rayan-samaneh-arka

رایان سامانه آرکا

سایت آرکا

دانلود بروشور