arka
رایان سامانه آرکا

C-Prot

معرفی C-Prot Endpoint Security

www.arka.ir
www.c-prot.com
021-91300476

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 VB100 گروه تحقیقاتی Virus Bulletin شده است.

ویژگیهای فنی C-Prot Endpoint Security

- رعایت الزامات ابلاغی مرکز مدیریت راهبردی افتا در خصوص ضوابط سامانه‌ها و سکوهای خارجی
- موافقت با شرایط پیشنهادی افتا در خصوص ضوابط سامانه ها و سکوهای خارجی
- قدرت تشخیص بالا به لطف استفاده از هوش مصنوعی پیشرفته
- سبک (سربار گزاری بسیار کم)
- کسب امتیازات بالا در آزمون های Virus Bulletin و سایر آزمونهای مستقل
- کنسول مدیریتی پیشرفته با مدیریت آسان
- تشخیص منفی کاذب(False positive) بسیار پایین(در نتیجه بدون پیام های آزار دهنده)

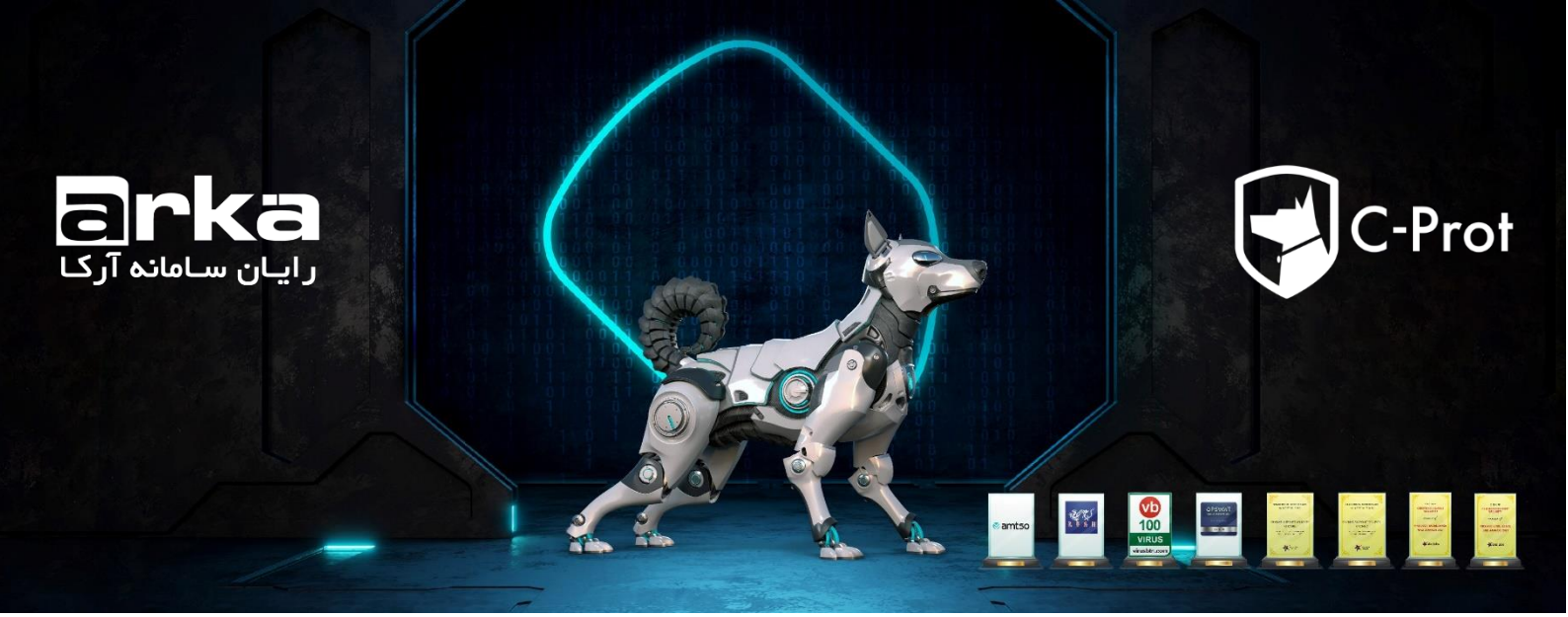
ویژگی‌های تجاری

- پشتیبانی فنی از طریق تیم شرکت آرکا در ایران و در صورت نیاز از طریق تیم پشتیبانی شرکت مادر
- وجود نمایندگی رسمی و پشتیبانی همه جانبه و نبود واسط
- اقتصادی بودن C-Prot نسبت به رقبای خود و وجود تخفیف 70% بدلیل نمایندگی انحصاری شرکت رایان سامانه آرکا

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.



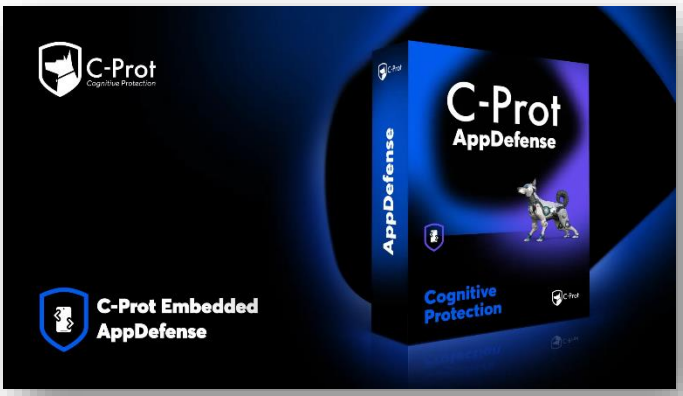
درباره‌ی C-Prot

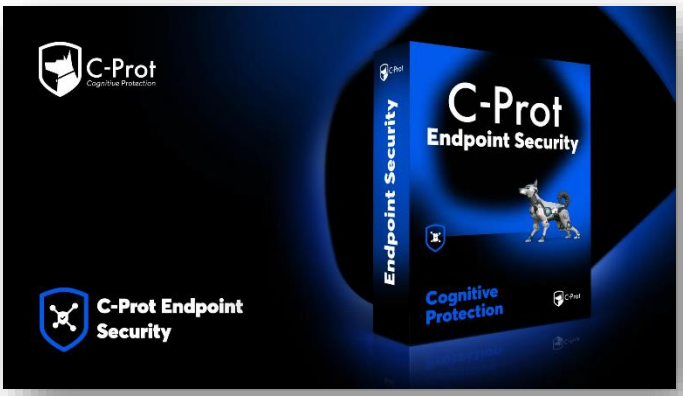
C-Prot توسعه دهنده محصولات امنیتی است که مشکلات امنیت سایبری کاربران را با روش‌های نوآورانه حل می‌کنند و تجربه کاربری را در اولویت قرار می‌دهند. این محصولات امنیت سایبری در حفاظت از زیرساخت‌های حیاتی مانند صنعت دفاع، مخابرات، انرژی، بانکداری، بهداشت، حمل‌ونقل و مالی استفاده می‌شوند.

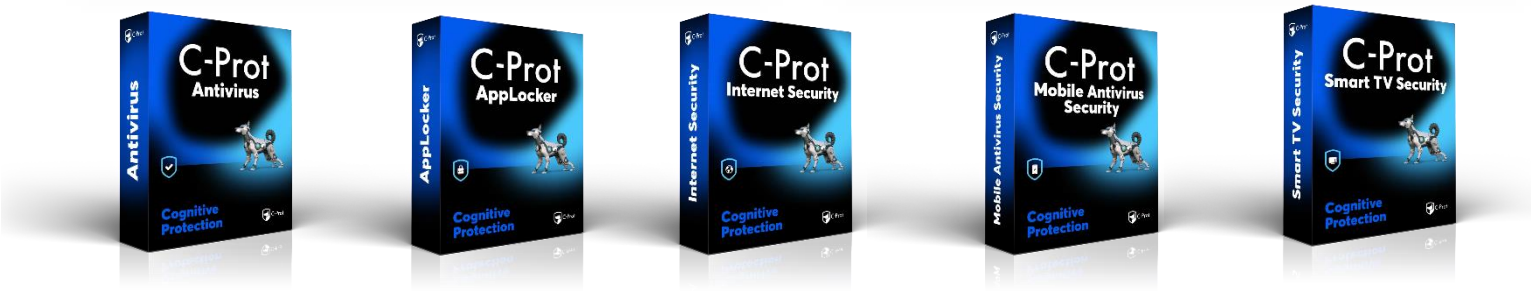
C-Prot دارای جوایز معتبر OPSWAT، STARCHECK، SKD AWARDSو VB100 است که فقط تعداد کمی از شرکت‌ها در جهان موفق به کسب آن‌ها شده‌اند.

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







Virus Bulletin
Covering the global threat landscape
VB100 TEST REPORT

vb 100 VIRUS virusbtn.com

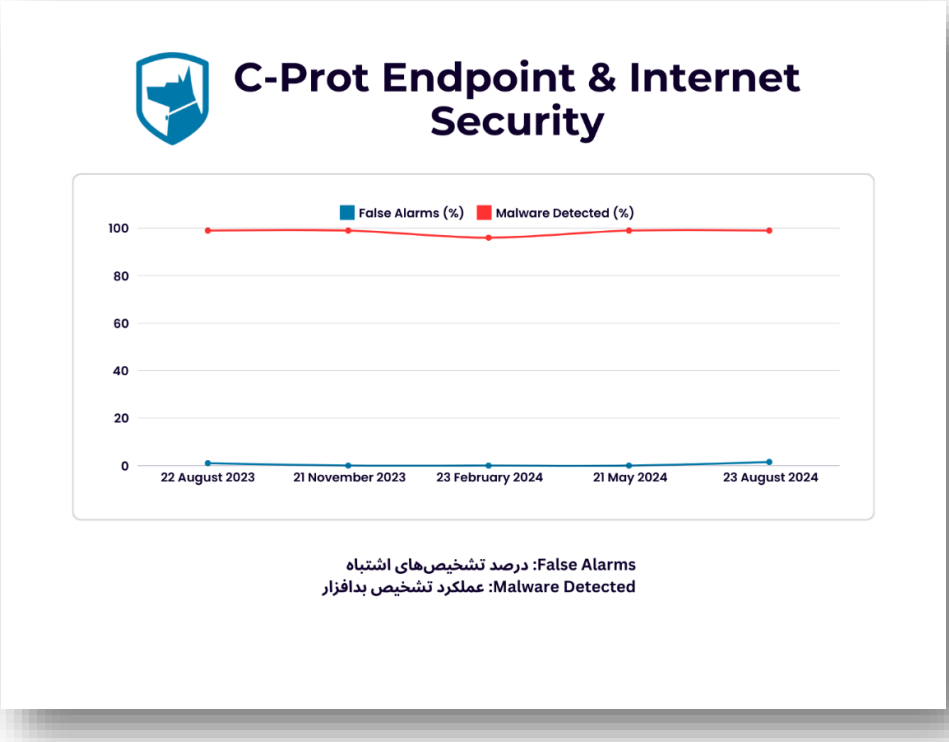
Test result
Test passed

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

1. **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.
2. **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.
3. **سازگاری بالا** :نرم‌افزارهای C-Prot بر روی سیستم‌عامل‌های مختلف با کارایی و سازگاری کامل اجرا شده‌اند که امتیاز بالایی در آزمون کسب کرده است.
4. **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 آموزشی

1. **آموزش مجازی:**
   - برگزاری وبینارها و دوره‌های آنلاین
   - دوره‌های آموزشی تعاملی برای بهبود مهارت‌های امنیتی
   - دسترسی به منابع آموزشی آنلاین مانند ویدئوهای آموزشی، مقالات و مستندات
2. **آموزش حضوری:**
   - برگزاری کارگاه‌های آموزشی و سمینارهای تخصصی در محل‌های مختلف
   - آموزش‌های سفارشی برای تیم‌ها و سازمان‌ها
   - جلسات آموزشی عملی و شبیه‌سازی حملات و تهدیدات امنیتی
   - پشتیبانی حضوری در طول دوره‌های آموزشی برای اطمینان از درک بهتر مطالب

این خدمات می‌توانند نیازهای مختلف کاربران را در زمینه امنیت سایبری و استفاده بهینه از محصولات C-Prot پوشش دهند.

خدمات پشتیبانی

1. **پشتیبانی فنی ۷/۲۴** :تیم ما همیشه در دسترس است تا به شما در رفع مشکلات فنی و پاسخگویی به سوالات مرتبط با محصولات C-Prot کمک کند.
2. **پشتیبانی از راه دور** :ما از طریق ابزارهای پشتیبانی از راه دور، مشکلات شما را به سرعت شناسایی و برطرف می‌کنیم تا به حداقل رساندن زمان قطعی و مشکلات سیستمی کمک کنیم.
3. **مشاوره و راهنمایی شخصی** :خدمات مشاوره‌ای اختصاصی به شما کمک می‌کند تا به بهترین نحو از ویژگی‌های محصولات C-Prot استفاده کنید و بهترین شیوه‌ها را برای حفظ امنیت اطلاعات خود بیاموزید.
4. **آموزش و مستندات جامع** :دسترسی به منابع آموزشی آنلاین و راهنماهای جامع برای کمک به شما در استفاده بهینه از نرم‌افزارهای C-Prot فراهم است.
5. **ارتقاء و به‌روزرسانی‌های منظم** :ما به صورت دوره‌ای آپدیت‌های امنیتی و ویژگی‌های جدید را به سیستم شما ارائه می‌دهیم تا از آخرین تهدیدات سایبری محافظت شوید.

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.

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

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

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

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

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.

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.

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: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی: ۱۵۳۱۶۴۵۹۱۸
info@arka.ir
www.arka.ir
رایان سامانه آرکا

C-Prot Embedded AppDefense

برای ارائه محافظت سبک و جاسازی‌شده (Embedded SDK) برای برنامه‌های شما در برابر همه تهدیدات، مجموعه‌ای از ویژگی‌ها و ابزارهای امنیتی برتر را می‌توان به کار برد.

ویژگی‌های برتر

تشخیص تماس‌های مشکوک
تماس‌های دریافتی از شماره‌های ناشناخته، مشکوک یا تلاش‌های تقلب شناسایی می‌شود.

ضد بدافزار
تشخیص بدافزارهای موجود روی دستگاه شما انجام می‌شود.

تشخیص شبیه‌ساز
تعیین می‌شود که آیا برنامه روی یک دستگاه واقعی اجرا می‌شود یا خیر.

اثر انگشت‌گیری دستگاه
یک شناسه دیجیتال منحصر به فرد برای دستگاه‌های شما ایجاد می‌کند.

بخش‌های استفاده

مراکز اقامت
این صنعت اطمینان حاصل می‌کند که اطلاعات شخصی و مالی مشتریان به صورت ایمن پردازش می‌شود.

دولت
این ابزار می‌تواند برای حفاظت از داده‌های حساس موجود در برنامه‌های موبایل توسعه یافته توسط دولت‌ها، وزارت‌های دفاع و مؤسسات عمومی استفاده شود.

تولید
حفاظت از امنیت برنامه‌های موبایل مورد استفاده در بخش تولید در دنیای دیجیتال را تضمین می‌کند.

مالی
این ابزار به بانک‌ها، موسسات مالی و شرکت‌های مشابه امکان می‌دهد تا به طور ایمن از اطلاعات مالی مشتریان خود محافظت کنند.

خرده‌فروشی
شبکه‌های خرده‌فروشی، به ویژه آن‌هایی که دارای قابلیت خرید درون برنامه‌ای هستند، اطمینان حاصل می‌کنند که اطلاعات پرداخت مشتریان به صورت ایمن پردازش می‌شود.

حمل و نقل
شرکت‌هایی که خدمات وسایل نقلیه ارائه می‌دهند، به ویژه خدمات اجاره و اشتراک‌گذاری وسایل نقلیه، تاکسی و خدمات مشابه، از حفاظت اطلاعات شخصی مشتریان خود اطمینان حاصل می‌کنند.

arka
رایان سامانه آرکا

محافظت از برنامه‌های جاسازی‌شده

توسعه‌دهندگان نرم‌افزار به راحتی می‌توانند در پروژه‌های موجود خود یا فرآیندهای توسعه برنامه‌های جدید ادغام شوند. این ابزار با ویژگی‌های پیشرفته تشخیص تهدید و جلوگیری از نفوذ تجهیز شده است. این ویژگی‌ها به طور فعال از برنامه‌ها در برابر فعالیت‌های مخرب محافظت می‌کنند و داده‌های کاربران را امن نگه می‌دارند. این ابزار راه‌حلی برای همه ذینفعانی است که می‌خواهند امنیت برنامه‌های موبایل را افزایش دهند. این ابزار نرم‌افزارهای keylogger را تشخیص می‌دهد، بدافزارهایی که هر کلیک کاربر را ثبت می‌کنند مسدود می‌کند و به صورت مداوم کاربر را نظارت می‌کند. با استفاده از C-Prot Remote Administrator می‌توانید برنامه‌های خود را از هر جایی مدیریت کنید. این ابزار مدیریت می‌تواند تشخیص دهد که آیا برنامه‌های موجود در دستگاه‌های شما در حالت دیباگ اجرا می‌شوند و آیا روی دستگاه روت شده یا جیلبریک شده اجرا می‌شوند یا خیر. این ابزار به شما کمک می‌کند تشخیص دهید که آیا هنگام استفاده از برنامه، خواننده صفحه نمایش روشن است، آیا برنامه روی یک دستگاه واقعی اجرا می‌شود و آیا از صفحه نمایش اسکرین‌شات گرفته می‌شود. همچنین بررسی می‌کند که کد SDK اجرا شده در زمان اجرا تغییر نکرده و کد مخرب اضافه نشده است. شما همچنین می‌توانید تعیین کنید که آیا گواهی استفاده شده در ارتباط با سرور امن است یا خیر. می‌توانید فهرست دستگاه‌های خود، سیستم عامل استفاده شده، آدرسIP ، اطلاعات برند و مدل را مشاهده کنید. این یک راه‌حل جامع است که برای اطمینان از امنیت برنامه‌های موبایل شما و ارائه محافظت در برابر بدافزارها توسعه یافته است.

ضد Keylogger نرم‌افزار ضد Keylogger که هر ضربه کلیدی که می‌زنید را ثبت می‌کند و به طور مداوم شما را نظارت می‌کند، شناسایی می‌شود.	✔
کنسول مدیریت مرکزی تمام نقاط انتهایی خود را از هر جایی با استفاده از C-Prot Remote Administrator که می‌تواند به صورت ابری یا در محل استفاده شود، مدیریت کنید.	✔
ضد دیباگینگ تشخیص می‌دهد که برنامه در حالت دیباگ اجرا می‌شود.	✔
تشخیص روت/جیلبریک تعیین می‌شود که آیا برنامه روی دستگاه روت یا جیلبریک شده اجرا می‌شود یا خیر.	✔
کنترل اسکرین‌شات تشخیص می‌دهد که آیا هنگام استفاده از برنامه، اسکرین‌شات گرفته می‌شود یا خیر.	✔
ضد تزریق بررسی می‌شود که کد SDK اجرا شده در زمان اجرا تغییر نکرده و هیچ کد مخربی اضافه نشده باشد.	✔
SSL-Pinning تعیین می‌کند که آیا گواهی در ارتباط با سرور امن است یا خیر.	✔
فهرست دستگاه‌ها شما می‌توانید فهرست دستگاه‌های خود، سیستم‌عاملی که استفاده می‌کنند، اطلاعات IP مورد استفاده در ارتباطات، برند و مدل را مشاهده کنید.	✔
تشخیص پوشش (Overlay Detection) ویژگی تشخیص پوشش تشخیص می‌دهد که آیا کاربران در هنگام استفاده از برنامه پوششی روی صفحه نمایش خود دارند یا خیر. پوشش‌ها (Overlays) برای دسترسی به اطلاعات شخصی و مالی کاربران استفاده می‌شوند. این ویژگی با شناسایی چنین حملاتی، تجربه کاربری امنی را فراهم می‌کند.	✔
تشخیص نقش مشکوک(Suspicious Role Detection) در هنگام استفاده از برنامه، تماس‌های ناشناخته و مشکوک یا تلاش‌های تقلب شناسایی می‌شوند.	✔

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
info@arka.ir www.arka.ir
arka رایان سامانه آرکا

C-Prot Endpoint Security

Advanced protection that can be managed on-premises or in the cloud with a single application against all threats.

Top Features

Anti-Malware
Protects computers, servers and mobile devices in your organization against risks from viruses, trojans, worms and ransomware.

External Media Management:
You can limit or control the use of undefined external devices (USB drives, CD/DVD drives, external hard drives, etc.).

Central Management Console
Manage all your endpoints from anywhere with C-Prot Remote Administrator, available as cloud-based or on-prem.

Policy Management:
You can configure multiple policies with different values. An application may run under different settings for different administrative groups.

Sectors Used

Finance:
Develops endpoint protection solutions for organisations providing financial services, including banks, financial institutions and insurance companies.

Government:
Provides protection against cyber threats that government and public sector organisations may face in the digital world.

Healthcare:
Provides security against cyber threats in the digital world to protect patients' medical records and personal health information.

Education:
The C-Prot Endpoint Security product has been developed to protect the information of educational institutions, students and staff against cyber attacks.

Critical Infrastructure:
Protects against cyber threats in the digital world to prevent power outages in power generation, transmission, utilities and critical infrastructure.

Retail:
Provides protection in the digital world to safeguard customer data and payment information.

Manufacturing:
Provides security in the digital world to prevent interruptions in production processes and defend against industrial espionage.

Telecommunications:
Telecommunications companies and internet service providers can use this to protect their computers at endpoints.

ENDPOINT SECURITY

C-Prot Endpoint Security prevents the risks posed by all kinds of viruses, spyware, trojans, worms, adware and other threats while enabling you to use your devices with high performance. It continues to protect you on the internet thanks to Internet and e-mail protection. It provides full protection to your device with its intuitive protection technology feature. In an enterprise environment, you can use C-Prot Endpoint Security with C-Prot Remote Administrator to easily manage multiple client workstations, apply your policies and policies, and configure them remotely from any network computer.

Highlights

★ ★ ★ ★ ★

Advanced Machine Learning Technology
It offers superior protection technology by utilizing the latest machine learning developed against new and unidentified malware.

Distributed Update Structure
Create multiple distribution points to avoid putting extra load on the servers while updating the application and signature database.

Internet-Using Applications
Instantly see the internet traffic of the applications and block the application you want.

Phishing and Fraud Protection
It provides high-level protection against malicious websites that want to capture your sensitive data such as your username, password, banking or credit card information.

Online Payment Protection
It prevents hacking of your credit card information and financial data while conducting an online transaction on devices in your institution.

Botnet Protection
It protects devices in your organization from being misused as part of an infected computer network or as a "botnet".

Anti-Theft
It helps you track and locate your devices in case of loss or theft.

Self-Defense
C-Prot's self-defense feature provides a defense mechanism against malware or other harmful activities from disabling C-Prot.

E-mail Protection
Keeps and blocks spam or malicious e-mails out of your inbox. Thus, it prevents your employees from clicking on harmful e-mails and ensures protection against phishing attacks.

Patch Management
Strengthen security with automatic patch management; possible in software, operating systems, and applications. reduce the risk of security vulnerabilities.

Spyware Detection
It provides protection against malicious software that collects the information of devices in your organization without permission.

Low Resource Consumption
It uses system resources efficiently and protects your computer without slowing down.

Firewall
C-Prot Endpoint Security offers an integrated firewall. This firewall monitors network traffic and blocks harmful or unwanted connections. It also ensures the security of data entering and leaving your organization's network.

Mobile Threat Protection
It provides comprehensive protection by detecting spyware, viruses and other malicious applications on mobile devices in your organization.

C-Prot will continue to keep you safe in the digital world with a wide range of high-tech cybersecurity products, from smart televisions to mobile devices, while maintaining its commitment to providing it's customers with the best endpoint protection products.

C-Prot
cprotglobal
cprotglobal
cprot
Known more at **https://www.c-prot.com**

C-Prot Embedded AppDefense

Provide lightweight, embedded SDK protection for your applications against all threats.

Top Features

Anti-Malware
Detection of malicious software present on your device is performed.

Emulator Detection
It is determined whether the application works on a real device.

Device Fingerprinting
Creates a unique digital fingerprint identifier for your devices.

Suspicious Call Detection
Calls from unknown, suspicious numbers or fraud attempts are detected.

Sectors Used

Finance:
It enables banks, financial institutions and similar companies to securely protect their customers' financial information.

Retail:
Retail networks, especially those with in-app shopping capabilities, ensure that their customers' payment information is processed securely.

Transportation:
Companies offering vehicle services, especially rental and sharing services, Taxi and similar services ensure the protection of their customers' personal information.

Hospitality:
It ensures that the personal and financial information of its customers is processed securely.

Government:
It can be used to protect sensitive data contained in mobile applications developed by governments, ministries of defence and public institutions.

Manufacturing:
Ensures the security of mobile applications used in the manufacturing sector in the digital world.

EMBEDDED APPDEFENSE

Application developers can be easily integrated into their existing projects or new application development processes. It is equipped with advanced threat detection and intrusion prevention features. These features proactively protect applications against malicious activity and keep user data secure. It offers a solution for all stakeholders who want to increase mobile application security. It detects keylogger software, blocks malware that records every keystroke of the user and continuously monitors the user. With C-Prot Remote Administrator you can manage your applications from anywhere. This management tool can detect whether the apps on your devices are running in debug mode and determine whether they are running on a rooted/jailbroken device. It helps you determine whether the screen reader is turned on while using the application, whether it is running on a real device, and whether screenshots are taken. It also checks that the running SDK code has not been modified at runtime and that no malicious code has been added. You can also determine whether the certificate used in communication with the server is secure. You can view the list of your devices, the operating system used, IP address, brand and model information. It is a comprehensive solution developed to ensure the security of your mobile applications and provide protection against malware.

Anti-Keylogger Keylogger software that records every keystroke you make and continuously monitors you is detected.	✔
Central Management Console Manage all your endpoints from anywhere with C-Prot Remote Administrator, which can be used as cloud-based or On-prem.	✔
Anti-Debugging It detects that the application is running in debug mode.	✔
Root/Jailbreak Detection It is determined whether the application is running on a Root/Jailbroken device.	✔
Screenshot Control Detects when a screenshot is taken while using the application.	✔
Anti-Injection It is checked that the running SDK code is not changed at runtime and that no malicious code is added.	✔
SSL-Pinning It determines whether the certificate is secure in communication with the server.	✔
Device List You can view the list of your devices, the operating system it uses, the iP information it uses while communicating, the brand and model.	✔
Overlay Detection The Overlay detection feature detects whether users have an overlay on their screen when using an application. Overlay attacks are used to capture users' personal and financial data. It provides a secure user experience by detecting such attacks.	✔
Suspicious Call Detection While using the application, calls from unknown, suspicious numbers or fraud attempts are detected.	✔

C-Prot will continue to keep you safe in the digital world with a wide range of high-tech cybersecurity products, from smart televisions to mobile devices, while maintaining its commitment to providing it's customers with the best endpoint protection products.

C-Prot
cprotglobal
cprotglobal
cprot
Known more at **https://www.c-prot.com**

رایان سامانه آرکا

C-Prot

کاتالوگ محصولات C-Prot

www.arka.ir
www.c-prot.com
021-91300476

C-Prot

کاتالوگ محصولات C-Prot

arka
رایان سامانه آرکا

نماینده انحصاری C-Prot در ایران

C-Prot
Cognitive Protection

arka
رایان سامانه آرکا

درباره‌ی C-Prot

C-Prot محصولات منحصر به فردی در زمینه امنیت سایبری توسعه می‌دهد که مشکلات امنیتی کاربران را با روش‌های نوآورانه حل می‌کند، تجربه کاربری را در اولویت قرار می‌دهد، قابلیت استفاده در پلتفرم‌های مختلف را دارد و به بازار جهانی جذب می‌شود. محصولات امنیت سایبری که این شرکت توسعه داده است، عمدتاً در صنایع دفاعی، ارتباطات الکترونیکی، انرژی، بانکداری و مالی، خدمات عمومی حیاتی و بخش حمل و نقل استفاده می‌شوند.

C-Prot جوایزی مانند OPSWAT، STARCHECK، SKD AWARDS و VB100 را با بالاترین معیارهایی که تنها تعداد کمی از شرکت‌های جهان دارا هستند، دریافت کرده است.

C-Prot عضو گروه کارشناسان اروپایی برای امنیت فناوری اطلاعات، شورای استانداردهای امنیتی PCI ، سازمان آزمون ضد بدافزار، انجمن پژوهشگران ضد ویروس آسیایی و کلاستر امنیت سایبری ترکیه است.

جوایز و عضویت‌ها

OPSWAT Platinum

C-Prot دارای گواهینامه معتبر OPSWAT Platinum است که یکی از بالاترین استانداردها در جهان به شمار می‌رود و اولین و تنها نرم‌افزار آنتی‌ویروس در ترکیه است که این گواهینامه را دریافت کرده است.

VB100

C-Prot برای شانزدهمین بار موفق به دریافت گواهینامه "VB100" برای محصولات مصرفی و شرکتی خود از سازمان مستقل تست و گواهی‌دهی Virus Bulletin مستقر در بریتانیا شد.

با نرخ شناسایی نزدیک به ۱۰۰٪، C-Prot موفقیت بین‌المللی خود را دوباره به نمایش گذاشت و در میان معدود شرکت‌های جهانی قرار گرفت که این گواهینامه معتبر را کسب کرده‌اند.

Starcheck

C-Prot برای چهارمین بار موفق به دریافت گواهینامه "STARCHECK" شد. پس از انجام تست‌های جامع توسط آزمایشگاه تست و گواهی‌دهی مستقل SKD Labs در سال‌های ۲۰۲۰، ۲۰۲۱، ۲۰۲۲ و ۲۰۲۳ با نرخ شناسایی بدافزار ۹۹/۹۹٪، شناسایی ۱۰۰٪ باج‌افزار و نرخ اشتباه صفر درصد، C-Prot این شایستگی را برای محصولات شرکتی و مصرفی خود به دست آورد.

SKD Awards Product Excellence

C-Prot در سال‌های ۲۰۲۲ و ۲۰۲۳ موفق به دریافت جایزه "PRODUCT EXCELLENCE SKD AWARDS" برای محصولات حفاظت از نقاط پایانی فردی، شرکتی و موبایل شد.

C-Prot به عنوان اولین و تنها شرکت در ترکیه که این جایزه را برای دو سال متوالی دریافت کرده، در گروه منتخب شرکت‌های جهانی قرار دارد که به دلیل برتری در این دسته‌ها شناخته شده‌اند.

SKD Special Award

C-Prot با دریافت "جایزه ویژه SKD برای برتری محصول" در هر دو دسته حفاظت از نقاط پایانی فردی و شرکتی، مورد تقدیر قرار گرفت.

Deloitte Fast50

C-Prot رشد چشمگیر ۹۴۶٪ را در سه سال گذشته به دست آورد و موفق به دریافت جایزه "دوم‌ها" شدDeloitte Fast50.

Deloitte Technology Fast50 2023

C-Prot با قرار گرفتن در فهرست Deloitte Technology Fast50 2023 ، شایستگی قابل توجهی به دست آورد که یک موفقیت بزرگ محسوب می‌شود.

AMTSO

C-Prot به عنوان تنها شرکت نرم‌افزاری از ترکیه پذیرفته شده است که به عضویت سازمان استانداردهای آزمون ضد بدافزار جهانی (AMTSO) درآمده است.
AMTSO یک سازمان بین‌المللی غیرانتفاعی است که در سال ۲۰۰۸ تأسیس شده و هدف آن رسیدگی به نیازهای بهبود کیفیت، ارتباط‌پذیری و بی‌طرفی در متدولوژی‌های آزمون ضد بدافزار است.

EICAR

C-Prot عضو گروه کارشناسان اروپایی برای امنیت فناوری اطلاعات (EICAR) است. یک سازمان جهانی مستقر در اروپا در زمینه امنیت رایانه. این شرکت همچنین تنها شرکت نرم‌افزاری از ترکیه است که به عضویت این سازمان پذیرفته شده است. EICAR که در سال ۱۹۹۱ تأسیس شد، یک پلتفرم مستقل و بی‌طرف برای کارشناسان امنیت فناوری اطلاعات در زمینه‌های علم، تحقیق، توسعه، کاربرد و مدیریت فراهم می‌آورد.

AVAR

C-Prot به تنها شرکت نرم‌افزاری از ترکیه تبدیل شده که به عضویت AVAR (انجمن پژوهشگران آنتی ویروس آسیایی) درآمده است. AVAR بر روی منطقه آسیا تمرکز دارد و با کارشناسان برجسته از ۱۸ کشور همکاری می‌کند.

PCI SSC

C-Prot به عنوان یک سازمان مشارکت‌کننده در "شورای استانداردهای امنیتی(PCI SSC) "PCI ، به همکاری برای ارتقاء امنیت داده‌های پرداخت در سطح جهانی پرداخته است PCI SSC .رهبری یک تلاش جهانی برای بهبود امنیت پرداخت‌ها از طریق ارائه استانداردهای امنیتی داده‌های منعطف و مؤثر را بر عهده دارد.

SAHA استانبول

در سال ۲۰۲۲، C-Prot به عنوان عضو "SAHA استانبول – کلاستر دفاع، هوافضا و فضا" پذیرفته شد، که هدف آن افزایش میزان بومی‌سازی در صنعت دفاعی، هوافضا و فضا ترکیه و تقویت رقابت‌پذیری بین‌المللی است. این عضویت از توسعه توانمندی‌های فناوری و صنعتی در میان اعضا پشتیبانی کرده و همکاری برای ایجاد یک اکوسیستم قوی را ترویج می‌کند.

HTK

C-Prot عضو "کلاستر فناوری‌های ارتباطات" است که در سال ۲۰۱۷ با حمایت OSTIM و سازمان تنظیم مقررات و ارتباطات رادیویی (BTK) تأسیس شد.

کلاستر امنیت سایبری ترکیه

C-Prot عضو "کلاستر امنیت سایبری ترکیه" است که در سال ۲۰۱۷ با مشارکت تمام نهادهای دولتی مرتبط، نمایندگان بخش خصوصی و دانشگاه‌ها، و با حمایت ریاست جمهوری صنایع دفاعی و دفتر تحول دیجیتال تأسیس شد. هدف این کلاستر توسعه اکوسیستم بومی امنیت سایبری است.

جایزه "شرکت با بیشترین صادرات"

C-Prot در سومین اجلاس بخش که توسط کلاستر امنیت سایبری ترکیه برگزار شد، جایزه "شرکت با بیشترین صادرات" را دریافت کرد.

محصول درخشان در بازار جهانی

C-PROT جایزه "محصول درخشان در بازار جهانی"

C-Prot در چهارمین اجلاس بخش که توسط کلاستر امنیت سایبری ترکیه برگزار شد، با جایزه "محصول درخشان در بازار جهانی" مورد تقدیر قرار گرفت.

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

C-Prot Internet Security

حفاظت پیشرفته در برابر تمام تهدیدات با یک برنامه واحد.

• مزایای اصلی

حفاظت از میکروفن/دوربین
هنگامی که برنامه‌ها به میکروفن یا دوربین شما دسترسی پیدا می‌کنند، به شما هشدار می‌دهد و به شما این امکان را می‌دهد که از دسترسی غیرمجاز جلوگیری کنید.

حفاظت در زمان واقعی
تهدیدات را در زمان واقعی شناسایی می‌کند و از آسیب رسیدن به دستگاه شما جلوگیری می‌کند.

حفاظت در برابر باج‌افزار
مال‌ورهایی که داده‌های شما را رمزگذاری می‌کنند شناسایی و خنثی می‌کند و دسترسی ایمن به فایل‌های شما را تضمین می‌کند.

حفاظت از اینترنت
دسترسی به وب‌سایت‌های مخرب را مسدود کرده و به طور خودکار فایل‌های دانلودی از اینترنت را اسکن می‌کند.

• حوزه‌های استفاده

استفاده شرکتی :کسب‌وکارهای کوچک و متوسط از **C-Prot** برای حفاظت از رایانه‌ها و شبکه‌های خود در برابر تهدیدات آنلاین استفاده می‌کنند.

استفاده فردی **C-Prot** :برای محافظت از امنیت آنلاین کودکان، تأمین امنیت تجربه بازی و حفاظت از تراکنش‌های بانکی شما استفاده می‌شود.

بهداشت و درمان :بیمارستان‌ها و موسسات بهداشتی از **C-Prot** برای محافظت از سوابق پزشکی و اطلاعات بهداشتی شخصی بیماران استفاده می‌کنند.

تجارت الکترونیک :فروشگاه‌های آنلاین از **C-Prot** برای حفاظت از اطلاعات مشتریان و داده‌های پرداخت استفاده می‌کنند.

مخابرات :شرکت‌های مخابراتی از **C-Prot** برای تأمین امنیت دیجیتال کارکنان و زیرساخت‌های خود استفاده می‌کنند.

مالی :بانک‌ها و ارائه‌دهندگان خدمات مالی از **C-Prot**برای محافظت از حساب‌های مشتریان و داده‌های مالی استفاده می‌کنند.

INTERNET SECURITY

محصول امنیتی اینترنتی C-Prot، آنتی‌ویروس، حفاظت قوی در برابر بدافزارها، باج‌افزارها و جاسوس‌افزارها ارائه می‌دهد، در حالی که ویژگی‌های حفاظت از میکروفون و دوربین شما را از دسترسی غیرمجاز به داده‌های حساس‌تان محافظت می‌کنند. ویژگی حفاظت از ایمیل امنیت آنلاین شما را با مسدود کردن پیوست‌های مضر و حملات فیشینگ تقویت می‌کند. علاوه بر این، فایروال یک لایه اضافی از دفاع در برابر تهدیدات آنلاین فراهم می‌آورد.

• ویژگی‌های برجسته

نظارت بر وضعیت درایو دیسک
به‌طور مداوم عملکرد، وضعیت و دمای هارد دیسک‌های داخلی و خارجی شما را نظارت می‌کند. در صورت شناسایی هرگونه مشکل، بلافاصله اعلان دریافت می‌کنید.

مصرف کم منابع
منابع سیستم را به‌طور کارآمد استفاده کرده و از رایانه شما محافظت می‌کند بدون اینکه باعث کند شدن آن شود.

شبکه امنیتی C-Prot
محافظت سطح بالا برای دستگاه‌های شما ارائه می‌دهد و امنیت اضافی از طریق فناوری محافظت ابری فراهم می‌آورد.

حفاظت هیوریستیک
اسکن رفتاری رفتار مشکوک یا مخرب بدافزارها را شناسایی کرده و حفاظت چندلایه‌ای برای دستگاه شما فراهم می‌کند

دفاع شخصی
ویژگی دفاع شخصی C-Prot مکانیزمی برای دفاع در برابر بدافزارها یا سایر فعالیت‌های مخربی است که قصد دارند C-Protرا غیرفعال کنند.

حفاظت در برابر بات‌نت
C-Prot از دستگاه شما در برابر استفاده از آن به عنوان بخشی از شبکه‌های کامپیوتری آلوده یا "بات‌نت" محافظت می‌کند. این ویژگی امنیت دستگاه شما را تقویت کرده و اقدامات پیشگیرانه در برابر فعالیت‌های مخرب اتخاذ می‌کند.

حفاظت در برابر استخراج ارز دیجیتال
C-Prot به‌طور مؤثر منابع رایانه شما را مدیریت کرده و از فعالیت‌های استخراج ارز دیجیتال جلوگیری می‌کند. این اطمینان می‌دهد که استفاده از دستگاه شما هم امن و هم بهینه باشد، و شما را از تقلب‌های مربوط به ارز دیجیتال محافظت می‌کند.

ضد بدافزار
محافظت از رایانه شما در برابر ویروس‌ها، جاسوس‌افزارها و سایر نرم‌افزارهای مخرب.

فناوری C-Prot Boost
پیکربندی خودکار منابع سخت‌افزاری و نرم‌افزاری برای استفاده بهینه از عملکرد دستگاه شما.

حفاظت از ایمیل
ایمیل‌های ناخواسته یا مخرب را از صندوق ورودی شما دور نگه می‌دارد و پیوست‌ها را به‌طور خودکار اسکن می‌کند.

حفاظت از شبکه‌های اجتماعی
از خطراتی که ممکن است از پلتفرم‌های شبکه‌های اجتماعی مانند فیس‌بوک، ایکس (توئیتر سابق) و اینستاگرام به وجود آید، پیشگیری می‌کند.

دانلود ایمن
به‌طور خودکار فایل‌های دانلود شده از اینترنت را اسکن می‌کند.

حفاظت در برابر فیشینگ و تقلب
محافظت درجه یک در برابر وب‌سایت‌های مخربی که قصد دارند اطلاعات حساس شما را سرقت کنند، مانند نام کاربری، رمز عبور، اطلاعات بانکی یا کارت اعتباری.

شناسایی جاسوس‌افزار
محافظت در برابر نرم‌افزارهای مخربی که بدون اجازه اطلاعات را از دستگاه شما جمع‌آوری می‌کنند.

گزارش تهدیدات
خلاصه‌ای از تهدیدات شناسایی شده و اطلاعات بیشتر را ارائه می‌دهد.

C-Prot Smart TV Security

حفاظت پیشرفته در برابر تمام تهدیدات برای تلویزیون‌های هوشمند فراهم می‌کند.

• مزایای اصلی

اسکن برنامه‌ریزی شده
شما می‌توانید اسکن برای شناسایی بدافزار را در تلویزیون خود با مشخص کردن هر روز یا زمان خاصی از هفته آغاز کنید.

آنتی‌ویروس و ضد جاسوس‌افزار
تلویزیون هوشمند شما را در برابر ویروس‌ها، جاسوس‌افزارها و سایر نرم‌افزارهای مخرب محافظت می‌کند.

فایروال
ترافیک اینترنتی و فعالیت‌های شبکه‌ای برنامه‌های نصب شده روی دستگاه را نظارت می‌کند.

محافظت از دستگاه USB
تلویزیون هوشمند شما را در برابر بدافزاری که ممکن است از طریق دستگاه‌های ذخیره‌سازی USB وارد شود، محافظت می‌کند.

• حوزه‌های استفاده

بهداشت و درمان:
مؤسسات بهداشتی از آن برای تأمین امنیت اطلاعات پزشکی روی تلویزیون‌های هوشمند موجود در اتاق‌های انتظار یا اتاق‌های بیماران استفاده می‌کنند.

حمل و نقل:
برای تأمین امنیت تلویزیون‌های هوشمند در مراکز حمل و نقل مانند فرودگاه‌ها، ایستگاه‌های قطار و پایانه‌های اتوبوس استفاده می‌شود.

سرگرمی:
برای تأمین امنیت تلویزیون‌های هوشمند در مکان‌های سرگرمی در دنیای دیجیتال استفاده می‌شود.

استفاده فردی:
برای تأمین امنیت تلویزیون‌های هوشمند در خانه، هنگام خرید آنلاین، تماشای فیلم و سریال یا استفاده از شبکه‌های اجتماعی استفاده می‌شود.

آموزش:
مدارس و مؤسسات آموزشی از آن برای تأمین امنیت تلویزیون‌های هوشمند استفاده می‌کنند.

صنعت مهمان‌نوازی:
در تلویزیون‌های هوشمند اتاق‌های هتل‌ها برای ارائه تجربه دیجیتال امن به مهمانان استفاده می‌شود.

SMART TV SECURITY

C-Prot Smart TV Security یک برنامه امنیتی آنتی‌ویروس جایزه‌برنده است که به‌طور خاص برای امنیت تلویزیون‌های هوشمند که بر روی سیستم‌عامل Android TV اجرا می‌شوند، طراحی شده و اولویت آن عملکرد بالا و مصرف کم منابع است. به لطف فناوری حفاظت در زمان واقعی، این برنامه به‌طور خودکار شما را در برابر بدافزارها، باج‌افزارها، حملات فیشینگ، جاسوس‌افزارها و سایر نرم‌افزارهای مخرب محافظت می‌کند.

ویژگی‌های برجسته

مصرف کم منابع
منابع سیستم شما را به‌طور مؤثر استفاده می‌کند و دستگاه شما را بدون کاهش سرعت محافظت می‌کند.

حفاظت هورسیتیک
محافظت در برابر بدافزارهای جدید و ناشناخته را فراهم می‌کند.

به‌روزرسانی خودکار
به‌روزرسانی خودکار برای مقابله با تهدیدات جدید در طول دوره اعتبار مجوز شما ارائه می‌دهد.

اسکن هوشمند
حفاظت در زمان واقعی با اسکن تمام برنامه‌های در حال اجرا روی تلویزیون هوشمند شما فراهم می‌شود.

اسکن خودکار
هنگامی که یک برنامه جدید نصب می‌کنید، قبل از اجرای آن به‌طور خودکار توسط C-Prot Smart TV Security اسکن می‌شود.

دانلود امن
با اسکن خودکار فایل‌های دانلود شده از اینترنت، امنیت شما را تضمین می‌کند.

تنظیمات پیشرفته
شما می‌توانید تنظیمات حفاظت خود را شخصی‌سازی کرده، به‌روزرسانی‌ها را مدیریت کرده و اسکن‌های برنامه‌ریزی شده اختیاری را با استفاده از گزینه‌های تنظیمات پیشرفته فعال کنید.

قرنطینه
هنگامی که بدافزار شناسایی می‌شود، می‌تواند از طریق فرایندهای حذف یا قرنطینه نرم‌افزار مخرب را ایزوله کرده و به شما این امکان را می‌دهد که فایل‌هایی که ایمن می‌دانید را بازیابی کنید.

سهولت استفاده
Google Play Store را باز کرده، به جستجوی C-Prot Smart TV Security بپردازید و برنامه را دانلود کنید. شما می‌توانید از نسخه رایگان لذت ببرید یا برای دسترسی به ویژگی‌های اضافی، به نسخه پریمیوم ارتقا دهید.

C-Prot Web Protection

محافظت در برابر وب‌سایت‌های مخرب، تبلیغات و ردیاب‌های تحلیلی فراهم می‌کند.

• مزایای اصلی

تحلیل لینک
امکان علامت‌گذاری آدرس‌های اینترنتی به عنوان ایمن یا ناامن را فراهم می‌کند.

پشتیبانی از مرورگرهای متعدد
برای مرورگرهای مبتنی بر کرومیوم (گوگل کروم، یاندکس براوزر، اپرا، اج و غیره) قابل دسترسی است.

محافظت در برابر فیشینگ
شما را از حملات فیشینگ در وب‌سایت‌های مخرب محافظت می‌کند.

مسدودسازی پیشرفته تبلیغات
شما می‌توانید تمام ردیاب‌های تبلیغاتی، پاپ‌آپ‌ها و تبلیغات را مسدود کنید.

• حوزه‌های استفاده

استفاده شرکتی:
کسب‌وکارهای کوچک و متوسط می‌توانند از راه‌حل‌های C-Protبرای محافظت از کامپیوترها و شبکه‌های خود در برابر ویروس‌ها، جاسوس‌افزارها و تهدیدات آنلاین استفاده کنند.

استفاده شخصی:
C-Prot ایمنی آنلاین کودکان شما را تضمین می‌کند و از بازی‌ها و تراکنش‌های بانکی شما محافظت می‌کند. این برنامه تمام جنبه‌های زندگی دیجیتال شما را امن می‌سازد.

مالی:
بانک‌ها و ارائه‌دهندگان خدمات مالی حساب‌های مشتریان و داده‌های مالی حساس را ایمن نگه می‌دارند.

تجارت الکترونیک:
فروشگاه‌های آنلاین از C-Prot برای تأمین امنیت اطلاعات مشتریان و داده‌های پرداخت استفاده می‌کنند.

مخابرات:
شرکت‌های مخابراتی و ارائه‌دهندگان خدمات اینترنتی ایمنی دیجیتال هم کارکنان و هم زیرساخت‌های خود را با استفاده از C-Prot تضمین می‌کنند.

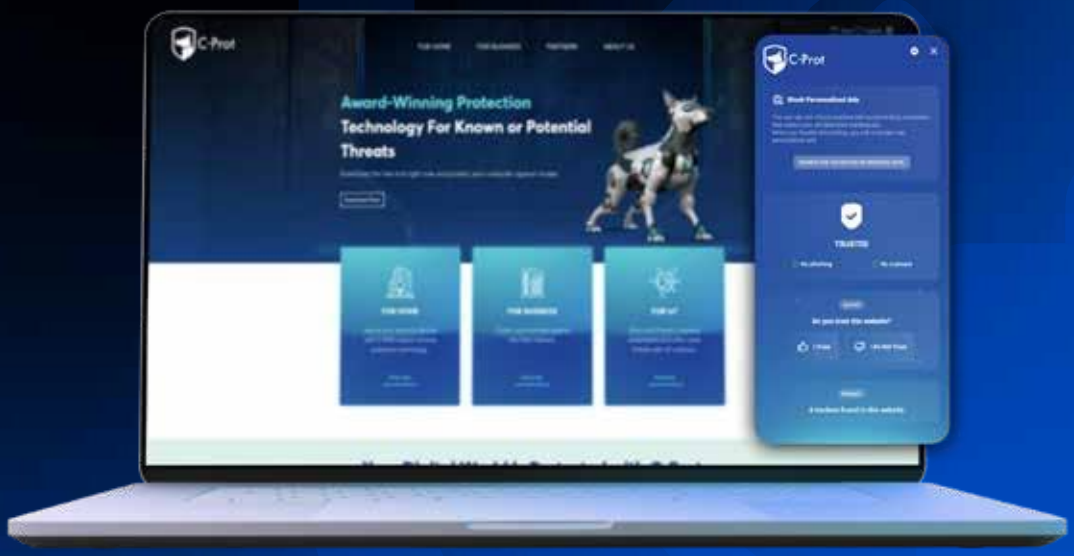
بهداشت و درمان:
بیمارستان‌ها و مؤسسات بهداشتی سوابق پزشکی و داده‌های شخصی سلامت بیماران را در برابر تهدیدات سایبری محافظت می‌کنند.

WEB PROTECTION

با C-Prot Web Protection از تقلب‌های آنلاین، وب‌سایت‌های مخرب، تبلیغات و ردیاب‌های تحلیلی که شما را آنلاین نظارت می‌کنند، در امان بمانید.

ویژگی‌های برجسته

- ✔ **پشتیبانی از مرورگرهای متعدد**
  می‌تواند با مرورگرهای مبتنی بر کرومیوم (گوگل کروم، یاندکس براوزر، اپرا، اج و غیره) استفاده شود.
- ✔ **مصرف کم منابع**
  با ویژگی مسدودسازی تبلیغات، استفاده ازCPU ، حافظه و ترافیک شبکه را کاهش می‌دهد و از این طریق مصرف مؤثر دستگاه و ترافیک شبکه شما را تضمین می‌کند.
- ✔ **مسدودسازی پیشرفته تبلیغات**
  C-Prot Web Protectionردیاب‌های تبلیغاتی را در وب‌سایت‌هایی که بازدید می‌کنید شناسایی کرده و وب‌سایت‌هایی که شما را ردیابی می‌کنند به شما نشان می‌دهد. این ویژگی حریم خصوصی شما را با جلوگیری از ردیابی فعالیت‌های آنلاین شما محافظت می‌کند.
- ✔ **تحلیل لینک**
  C-Prot Web Protectionقابلیت تحلیل قابلیت اطمینان وب‌سایت‌هایی که قصد دارید از آن‌ها بازدید کنید را دارد و لینک‌های بالقوه مضر یا ناامن را شناسایی می‌کند. این امر تجربه آنلاین ایمن‌تری را برای شما تضمین می‌کند.
- ✔ **عملکرد بالا**
  بارگذاری صفحات را سرعت می‌بخشد و پهنای باند را ذخیره می‌کند.
- ✔ **محافظت در برابر فیشینگ**
  C-Prot Web Protectionدر برابر حملات فیشینگ محافظت فراهم می‌کند. این برنامه وب‌سایت‌های مخرب و تلاش‌های فیشینگ بالقوه را شناسایی کرده و از داده‌های شخصی شما محافظت می‌کند.
- ✔ **خاموش کردن مجوزهای تبلیغات**
  C-Prot Web Protection گزینه‌ای برای غیرفعال کردن مجوزهای تبلیغاتی ارائه می‌دهد. این امکان به شما می‌دهد تا مجوزهای تبلیغاتی را خاموش کرده و از دستگاه و حریم خصوصی آنلاین خود محافظت کنید.



C-Prot Endpoint Security

حفاظت پیشرفته در برابر تمام تهدیدات با یک برنامه واحد، که قابل مدیریت به‌صورت محلی یا ابری است.

• مزایای اصلی

مدیریت رسانه‌های خارجی
با **C-Prot Endpoint Security** ، می‌توانید استفاده از دستگاه‌های خارجی تعریف‌نشده) درایوهای **USB** ، درایوهای **CD/DVD**، هارد دیسک‌های خارجی و غیره (را محدود یا کنترل کنید.

ضد بدافزار
C-Prot Endpoint Securityبه‌طور مؤثر از نقطه‌های پایانی کسب‌وکار شما در برابر ویروس‌ها، جاسوس‌افزارها و سایر نرم‌افزارهای مخرب محافظت می‌کند.

سیاست‌های امنیتی
از طریق کنسول مدیریت**C-Prot Security Center** ، می‌توانید پسوندهای فایل، مسیرهای فایل و آدرس‌های وب را به لیست سفید یا سیاه اضافه کرده و به‌صورت گروهی یا دستگاهی آن‌ها را مجاز یا مسدود کنی

کنسول مدیریت مرکزی
با کنسول مدیریت که می‌تواند به‌صورت ابری یا محلی استفاده شود، می‌توانید بسته‌های **C-Prot** را مستقر کرده، وظایف و سیاست‌های امنیتی را مدیریت کرده و به‌سرعت به مشکلات یا تهدیدات روی نقاط پایانی پاسخ دهید.

• حوزه‌های استفاده

دولت:
در برابر تهدیدات سایبری که سازمان‌های دولتی و بخش عمومی ممکن است در دنیای دیجیتال با آن‌ها مواجه شوند، محافظت فراهم می‌کند.

آموزش:
امنیت برای محافظت از اطلاعات دانش‌آموزان و کارکنان در مؤسسات آموزشی در برابر تهدیدات سایبری فراهم می‌کند.

خرده‌فروشی:
در دنیای دیجیتال امنیت فراهم می‌کند تا از داده‌های مشتریان و اطلاعات پرداخت محافظت شود.

مخابرات:
شرکت‌های مخابراتی و ارائه‌دهندگان خدمات اینترنتی می‌توانند از راه‌حل‌های **C-Prot** برای محافظت از دستگاه‌های نقطه پایانی استفاده کنند.

مالی:
راه‌حل‌های حفاظت از نقطه پایانی برای سازمان‌های ارائه‌دهنده خدمات مالی، مانند بانک‌ها، مؤسسات مالی و شرکت‌های بیمه توسعه می‌دهد.

بهداشت و درمان:
در برابر تهدیدات سایبری در دنیای دیجیتال امنیت فراهم می‌کند تا سوابق پزشکی بیماران و اطلاعات شخصی سلامت آن‌ها محافظت شود.

زیرساخت‌های حیاتی:
در برابر تهدیدات سایبری در زیرساخت‌های حیاتی مانند تولید، انتقال و خدمات انرژی محافظت فراهم می‌کند تا از خاموشی‌های برق جلوگیری شود.

تولید:
در دنیای دیجیتال امنیت فراهم می‌کند تا از اختلالات در فرآیندهای تولید جلوگیری شود و در برابر جاسوسی صنعتی دفاع کند.

ENDPOINT SECURITY

C-Prot Endpoint Security امنیت حداکثری با عملکرد بالا را در دستگاه‌های شما فراهم می‌کند. این برنامه تهدیداتی مانند ویروس‌ها، جاسوس‌افزارها، تروجان‌ها، کرم‌ها، تبلیغات‌افزارها و روت‌کیت‌ها را خنثی می‌کند. ویژگی‌های حفاظت از اینترنت و ایمیل، امنیت را در محیط‌های آنلاین تقویت می‌کنند. با استفاده از فناوری‌های پیشرفته یادگیری ماشین و حفاظت هورسیتیک، دفاع جامع را ارائه می‌دهد.

C-Prot Security Centerبه شما این امکان را می‌دهد که تمام نقاط پایانی را از طریق یک کنسول مدیریت مرکزی، چه به‌صورت ابری و چه محلی، مدیریت کنید. ویژگی‌هایی مانند حفاظت از پرداخت آنلاین، شناسایی جاسوس‌افزارها و حفاظت در برابر فیشینگ، داده‌های حساس شما را ایمن می‌کنند. ماژول‌هایHIPS ، حفاظت از میکروفن و وب‌کم، و شناسایی دسترسی از راه دور لایه‌های امنیتی اضافی فراهم می‌کنند. این امکان مدیریت ایستگاه‌های کاری و اجرای سیاست‌های امنیتی در محیط‌های شرکتی را آسان‌تر می‌کند.

ویژگی‌های برجسته

دفاع خودکار
مکانیزم دفاع خودکار C-Prot از شما در برابر بدافزار یا فعالیت‌های مخرب که تلاش می‌کنند C-Prot را غیرفعال کنند، محافظت می‌کند.

محافظت از ایمیل
کارمندان شما را از حملات فیشینگ محافظت کرده و ایمیل‌های هرزنامه و مخرب را مسدود می‌کند.

مدیریت وصله‌ها
آسیب‌پذیری‌های امنیتی در نرم‌افزارها، سیستم‌عامل‌ها و برنامه‌ها را از طریق مدیریت خودکار وصله‌ها به حداقل می‌رساند.

تشخیص جاسوس‌افزار
از نرم‌افزارهای مخربی که تلاش دارند به طور غیرمجاز به سازمان شما دسترسی پیدا کنند، محافظت می‌کند.

مصرف کم منابع
بدون کاهش عملکرد دستگاه شما، با استفاده بهینه از منابع سیستم، حفاظت امنیتی ارائه می‌دهد..

فایروال
فایروال یکپارچه، ترافیک شبکه را نظارت کرده و با مسدود کردن اتصالات مخرب، امنیت داده‌های شما را تضمین می‌کند.

افزونه محافظت وبC-Prot
با افزونه محافظت وبC-Prot ، شما را از کلاهبرداری‌های آنلاین و وب‌سایت‌های حاوی بدافزار محافظت کرده و یک تجربه مرور امن را تضمین می‌کند.

فناوری یادگیری ماشین پیشرفته
با استفاده از فناوری یادگیری ماشین، از دستگاه شما در برابر بدافزارهای جدید و ناشناخته محافظت می‌کند و محافظت آنتی‌ویروسی برنده جوایز را ارائه می‌دهد.

معماری به‌روزرسانی توزیع‌شده
نقاط توزیع مختلفی ایجاد می‌کند تا بار سرورها را کاهش دهد در حین به‌روزرسانی برنامه و پایگاه داده امضای آن.

محافظت از میکروفن/دوربین
هنگامی که برنامه‌ها به میکروفن یا دوربین شما دسترسی پیدا می‌کنند، به شما هشدار می‌دهد و به شما این امکان را می‌دهد تا دسترسی‌های غیرمجاز را مسدود کنید.

پاک‌کن فایل
اطلاعات خود را بدون باقی‌گذاشتن هیچ ردی با استفاده از روش‌های حذف بین‌المللی پاک کنید.

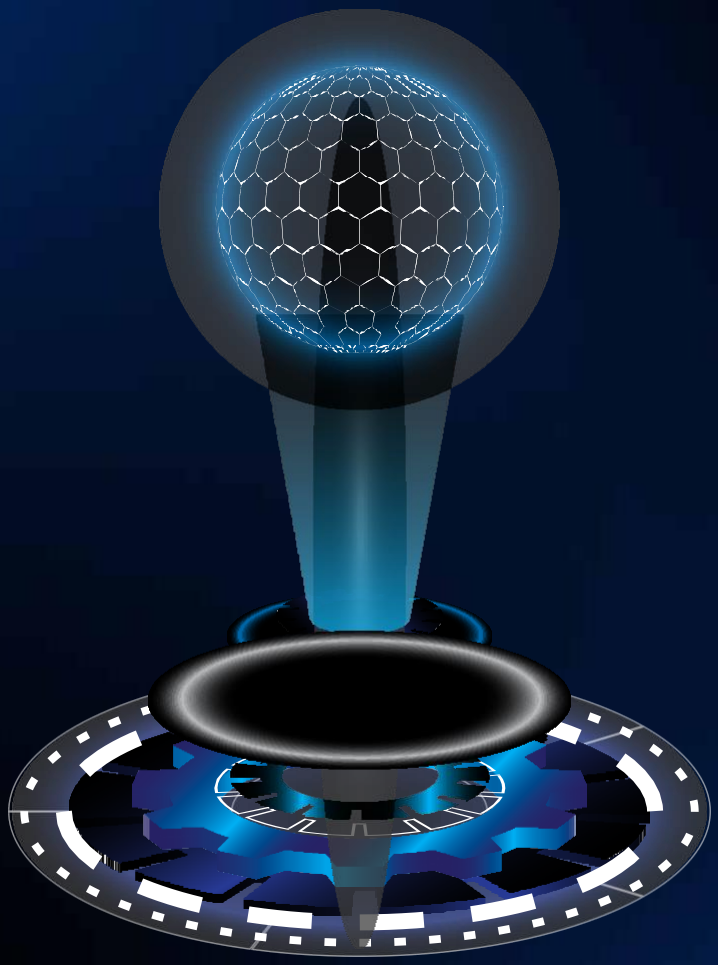
محافظت از پرداخت آنلاین
اطلاعات کارت اعتباری و داده‌های مالی شما را در هنگام انجام تراکنش‌های آنلاین محافظت می‌کند.

محافظت در برابر بات‌نت
از دستگاه‌های شما در برابر تبدیل شدن به بخشی از شبکه‌های مخرب بات‌نت محافظت می‌کند.

شناسایی دسترسی از راه دور
برنامه‌های نصب‌شده روی رایانه شما را که هکرها می‌توانند برای کنترل دستگاه یا سرقت اطلاعات شخصی شما استفاده کنند، شناسایی می‌کند.

C-Prot Threat Intelligence Portal

یکپارچه‌سازی جریان‌های داده تهدید به‌روزرسانی شده به طور مداوم در برنامه‌های امنیتی مانند SIEM



• مزایای اصلی

تحلیل فایل و هش
تمام تهدیدات را از طریق تحلیل‌های دینامیک، استاتیک و رفتاری با استفاده از سیستم اعتبار جهانی ابری شناسایی می‌کند.

تحلیل بدافزار
اطلاعات دقیق در مورد ابزارها، تاکتیک‌ها و انواع حملاتی که توسط مهاجمین سایبری استفاده می‌شود، ارائه می‌دهد

هوش تهدید و تحلیل
تهدیدات، نمونه‌های بدافزار و آسیب‌پذیری‌ها را با ارائه هوش تهدید به‌روزرسانی‌شده به‌طور مداوم نظارت می‌کند.

دسترسی به API
APIهایی فراهم می‌کند که به تیم‌های امنیتی یا ابزارهای خودکار امکان دسترسی به هوش تهدید و تولید پاسخ‌های خودکار را می.

• حوزه‌های استفاده

دولت:
حفاظت در برابر تهدیدات سایبری که سازمان‌های دولتی و بخش عمومی ممکن است در دنیای دیجیتال با آن‌ها مواجه شوند.

آموزش:
حفاظت از اطلاعات دانش‌آموزان و کارکنان در مؤسسات آموزشی در برابر تهدیدات سایبری فراهم می‌کند.

خرده‌فروشی:
حفاظت در دنیای دیجیتال برای حفظ اطلاعات مشتریان و اطلاعات پرداخت.

مخابرات:
شرکت‌های مخابراتی و ارائه‌دهندگان خدمات اینترنتی می‌توانند از راه‌حل‌های C-Prot برای حفاظت از دستگاه‌های نقطه پایانی استفاده کنند.

مالی:
راه‌حل‌های حفاظت از نقطه پایانی برای سازمان‌های ارائه‌دهنده خدمات مالی مانند بانک‌ها، موسسات مالی و شرکت‌های بیمه را توسعه می‌دهد.

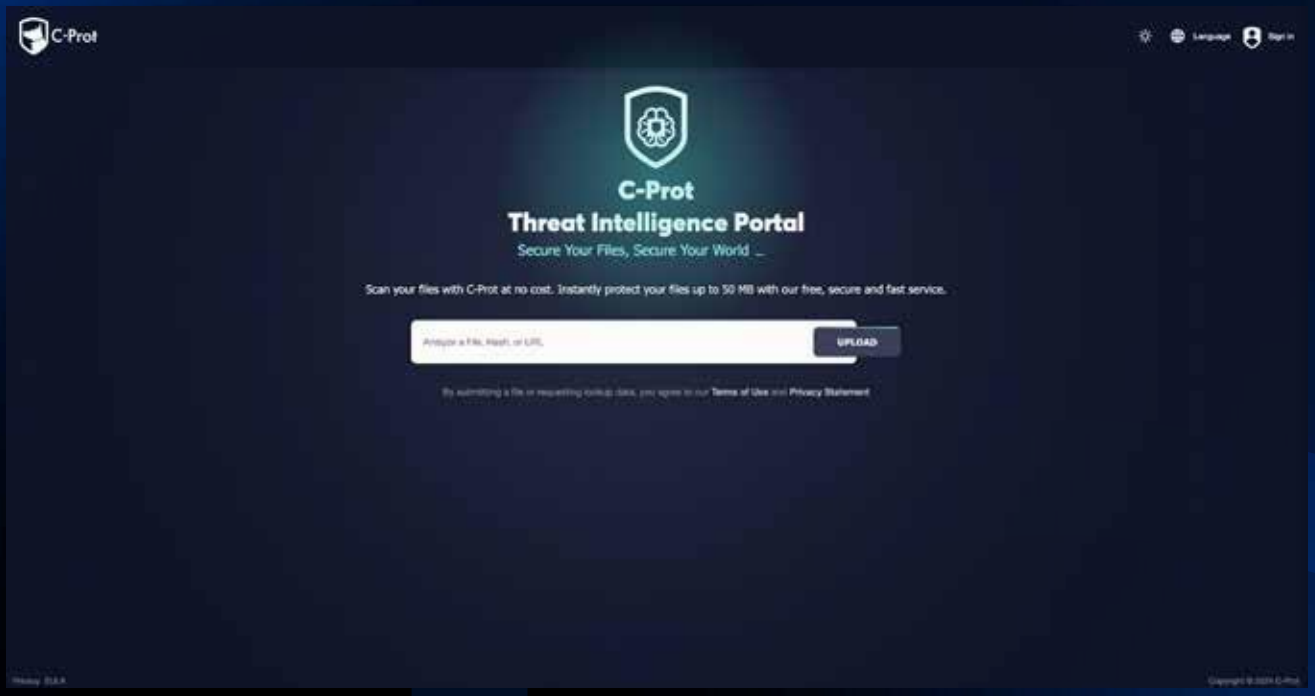
بهداشت و درمان:
حفاظت در برابر تهدیدات سایبری در دنیای دیجیتال برای حفظ سوابق پزشکی بیماران و اطلاعات شخصی سلامت آن‌ها فراهم می‌کند.

زیرساخت‌های حیاتی:
حفاظت در برابر تهدیدات سایبری در زیرساخت‌های حیاتی مانند تولید انرژی، انتقال و خدمات برای جلوگیری از قطع برق فراهم می‌کند.

ساخت‌وساز:
حفاظت در دنیای دیجیتال برای جلوگیری از اختلالات در فرآیندهای تولید و دفاع در برابر جاسوسی صنعتی فراهم می‌کند.

THREAT INTELLIGENCE PORTAL

پورتال اطلاعات تهدید C-Prot یک سرویس وب است که دسترسی به اطلاعات تهدیدات سایبری را فراهم می‌کند. این پورتال امکان تحلیل شاخص‌های مشکوک تهدید مانند فایل‌ها، هش‌های فایل، آدرس‌های IP و آدرس‌های وب را فراهم می‌کند. سازمان‌ها می‌توانند تهدیدات بالقوه را شناسایی کرده و اقدامات احتیاطی لازم را انجام دهند. وضعیت تهدیدات خود را ارزیابی کرده و به‌طور پیشگیرانه حملات هدفمند را شناسایی کنید.



ویژگی‌های برجسته

★★★★★

اطلاعات تهدید جهانی
اطلاعات جامع تهدیدات را شامل الگوهای حمله، انواع بدافزارها، تحلیل حملات و سایر اطلاعات مرتبط با تهدیدات فراهم می‌کند.

تحلیل بدافزار
اطلاعات دقیق در مورد شاخص‌های خاص بدافزارها مربوط به ابزارها، تاکتیک‌ها و انواع حملات استفاده‌شده توسط مهاجمان سایبری را فراهم می‌کند.

تحلیل فایل و هش
تهدیدات پیشرفته را با استفاده از فناوری‌های پیشرفته تشخیص، شامل تحلیل‌های داینامیک، استاتیک و رفتاری، همراه با یک سیستم اعتبارسنجی ابری جهانی، شناسایی می‌کند.

اطلاعات تهدید استراتژیک و عملیاتی
امکان تحلیل دقیق وضعیت تهدیدات را فراهم می‌آورد و به شما کمک می‌کند روند تهدیدات را درک کرده و حملات خاص را از پیش پیش‌بینی کنید. با بینش‌هایی در مورد رفتارها و زیرساخت‌های مهاجمان، مکانیسم‌های دفاعی خود را تقویت می‌کند.

C-Prot Device Fingerprint

تعریف بازدیدکنندگان وب و موبایل خود با دقیق‌ترین پلتفرم شناسایی دستگاه.

• مزایای اصلی

یکپارچگی آسان برای توسعه‌دهندگان
با افزودن سریع **SDK** اثر انگشت دیجیتال **C-Prot** به برنامه‌های ابری یا محل استقرار خود، به راحتی یکپارچه شوید.

اثر انگشت دیجیتال منحصر به فرد
C-Protبا استفاده از الگوریتم‌های خاص، اثر انگشت دیجیتال منحصر به فردی برای هر کاربر که از دستگاه‌های وب و موبایل وارد می‌شود، ایجاد می‌کند.

تشخیص سفر سریع
تغییرات موقعیت مکانی که در بازه زمانی تعریف‌شده در پنل مدیریت انجام شده‌اند را شناسایی می‌کند

شناسایی تغییر کشور، شهر و منطقه زمانی
زمانی که کاربران از مکانی متفاوت (کشور، شهر، منطقه زمانی) نسبت به اطلاعات جلسه قبلی خود وارد می‌شوند، شناسایی می‌شود.

• حوزه‌های استفاده

تبلیغات
برای شناسایی و تقسیم‌بندی مخاطبان استفاده می‌شود. اطمینان حاصل می‌کند که تبلیغات درست به کاربران مناسب نشان داده می‌شود و به جلوگیری از تقلب در تبلیغات کمک می‌کند.

مالی:
بانک‌ها و مؤسسات مالی امنیت حساب‌ها را با شناسایی دستگاه‌های کاربران تقویت می‌کنند. همچنین می‌توان از آن برای تقویت فرآیندهای شناسایی تقلب و احراز هویت استفاده کرد.

رمزارز:
تقلب‌های مرتبط با ارزهای دیجیتال را شناسایی می‌کند که سعی در سرقت داده‌های حساب و انتقال وجوه به کیف پول‌های خود دارند، با دقت نزدیک به ۱۰۰٪.

مراکز درمانی
امنیت و کنترل دسترسی در خدمات بهداشت و درمان فراهم می‌کند. فرآیندهای احراز هویت و مجوز را تقویت می‌کند و از محرمانگی داده‌های پزشکی محافظت می‌کند.

بازیهای آنلاین:
از تکنیک‌های رایج تقلب در بازی‌ها و کازینو، مانند پر کردن خودکار اعتبارنامه‌ها، استراتژی‌های تقلب و دیگر فعالیت‌های غیرقانونی محافظت می‌کند.

فروش اینترنتی:
کاربران مشکوک را که از پلتفرم تجارت الکترونیک بازدید می‌کنند، با دقت نزدیک به ۱۰۰٪ شناسایی می‌کند.

DEVICE FINGERPRINT

C-Prot Device Fingerprint یک راه‌حل است که برای شناسایی ایمن کاربران در وب‌سایت‌ها و تجزیه و تحلیل ترافیک وب توسعه یافته است. این راه‌حل با شناسایی کاربران از طریق یک شناسه دستگاه منحصر به فرد با دقت نزدیک به ۱۰۰٪، امنیت بالایی را تضمین کرده و در عین حال تجربه کاربری را نیز بهبود می‌بخشد.

ویژگی‌های برجسته

تشخیص اتصال ریموت
C-Prot Device Fingerprintکاربران را که از طریق برنامه‌های اتصال دسکتاپ ریموت مانند AnyDesk و TeamViewer وارد می‌شوند شناسایی می‌کند.

تشخیص جعل شناسه دستگاه
اطلاعات اپلیکیشن ممکن است در دستگاه‌های روت‌شده تغییر کند. این ویژگی تشخیص می‌دهد که آیا اطلاعات تغییر کرده است یا همچنان اصلی باقی‌مانده است.

تشخیص استفاده از تب ناشناس
کاربرانی که در حالت مرور ناشناس به وب‌سایت‌ها دسترسی پیدا می‌کنند شناسایی می‌شوند.

تشخیص ربات
تعیین می‌کند که آیا مرورگر توسط یک ربات مانند Seleniumیا یک انسان واقعی استفاده می‌شود.

تشخیص استفاده از ابزارهای خودکار
درخواست‌هایی که توسط ابزارهای خودکار وب برای هدف قرار دادن آدرس‌های اینترنتی ارسال می‌شود شناسایی می‌شود.

کنسول مدیریت مرکزی
با C-Prot Security Center که می‌تواند به صورت ابری یا در محل استفاده شود، شما می‌توانید همه دستگاه‌های نقطه پایانی خود را مدیریت کنید و از هر جایی آن‌ها را کنترل کنید.

تشخیص کاربران متعدد
ورود چندین کاربر از یک مرورگر شناسایی می‌شود.

تشخیص کاربران مخرب
کاربران مخرب با ویژگی‌هایی مانند مناطق زمانی ناسازگار، استفاده از حالت ناشناس و پروکسی‌ها شناسایی می‌شوند.

تشخیص استفاده از VPN و پروکسی
با تجزیه و تحلیل آدرس IP کاربر، مشخص می‌شود که آیا آدرس مربوط به یک سرور VPN یا پروکسی است.

- پارامترهایWebGL
- دستگاه‌های رسانه‌ای، داده‌هایDirectX
- عامل کاربری(User Agent) ، سیستم عامل، پلتفرم، منطقه زمانی و غیره
- فونت‌ها، پلاگین‌ها، زبان دستگاه، نوع MIMEو غیره
- اثر انگشتCanvas
- ردیابی کوکی‌ها و پارامترهای دیگر

C-Prot Fraud Prevention

جلوگیری از تقلب و ارائه تجربه دیجیتال بدون درز برای مشتریان خود.

مزایای اصلی

آنتی‌مالور
تکنولوژی آنتی‌ویروس برنده جایزه **C-Prot** با شناسایی نرم‌افزارهای جاسوسی، ویروس‌ها و برنامه‌های مخرب دیگر، محافظت جامع را فراهم می‌آورد.

الگوریتم‌های شناسایی تقلب
C-Prot از الگوریتم‌های پیشرفته شناسایی تقلب، یادگیری ماشین و اطلاعات تهدید **C-Prot** برای تشخیص اینکه آیا یک تزریق بی‌ضرر است یا مخرب، استفاده می‌کند.

تشخیص خدمات دسترسی
این ویژگی به‌طور پیشگیرانه استفاده غیرمجاز از خدمات دسترسی توسط نرم‌افزارهای مخرب یا برنامه‌های تهدیدآمیز را شناسایی می‌کند.

تشخیص روت/جیل‌بریک
این سیستم شناسایی می‌کند که آیا برنامه روی دستگاهی که روت یا جیل‌بریک شده است اجرا می‌شود.

حوزه‌های استفاده

بهداشت و درمان:
سوابق بهداشتی را امن می‌کند، تلاش‌های فیشینگ را شناسایی می‌کند و تقلب در نسخه‌های دارویی را تشخیص می‌دهد.

سفر:
رزروهای سفر را امن می‌کند، اطلاعات کارت مشتری را محافظت می‌کند و تلاش‌های فیشینگ را شناسایی می‌کند.

ارتباطات:
تلاش‌های فیشینگ را شناسایی می‌کند، از تقلب حساب جلوگیری می‌کند و اطلاعات مشترکین را محافظت می‌کند.

مالی:
امنیت مالی را در تراکنش‌های بانکی آنلاین افزایش می‌دهد، تلاش‌های فیشینگ را شناسایی می‌کند و بدافزارها را مسدود می‌کند.

تجارت الکترونیک:
از تقلب در تجارت الکترونیک جلوگیری می‌کند، پرداخت‌های مشتریان را امن می‌سازد و تلاش‌های فیشینگ را شناسایی می‌کند.

بیمه:
از تقلب جلوگیری می‌کند، ادعاهای تقلبی بیمه را شناسایی می‌کند و اطلاعات مشتریان را امن می‌سازد.

FRAUD PREVENTION

حفاظت با استفاده از SDK موبایل

تشخیص پوشش (Overlay Detection)
تشخیص می‌دهد که آیا بر روی صفحه نمایش کاربران در حین استفاده از یک اپلیکیشن، پوشش (یک پنجره که بر روی پنجره‌های دیگر قرار می‌گیرد) وجود دارد یا خیر.
تشخیص مجوزهای اندروید به‌صورت زنده:
مجوزهای حیاتی دستگاه‌های کاربر را به‌صورت آنی مانیتور می‌کند و امنیت را با مسدود کردن عملیات اپلیکیشن‌های پرخطر هنگام شناسایی مجوزهای مشکوک اندروید افزایش می‌دهد.
آنتی-کی‌لاگر (Anti-Keylogger)
نرم‌افزارهای کی‌لاگر که هر ضربه‌ای که وارد می‌کنید را ثبت و شما را به‌طور مداوم نظارت می‌کنند، شناسایی می‌شود.
آنتی-دباگینگ (Anti-Debugging)
تشخیص می‌دهد که آیا اپلیکیشن در حالت دیباگ در حال اجرا است یا خیر.
تشخیص شبیه‌ساز (Emulator Detection)
معلوم می‌کند که آیا اپلیکیشن بر روی دستگاه واقعی در حال اجرا است یا بر روی شبیه‌ساز.
آنتی-اینژکشن (Anti-Injection)
بررسی می‌کند که آیا کد SDK در حال اجرا تغییر کرده است یا خیر و اطمینان حاصل می‌کند که کدی مخرب وارد نشده است.
نظارت بر اپلیکیشن پیش‌فرض پیامک:(Monitoring the Default SMS Application)
فعالیت‌های غیرعادی در اپلیکیشن‌های پیامک را ردیابی می‌کند.

حفاظت با استفاده از Web SDK

تشخیص اسکریپت‌های مخرب:(Malicious Script Detection)
پیشگیری از تقلب زمانی که یک اسکریپت مخرب از جاوااسکریپت برای تغییر داده‌های وارد شده توسط کاربر (برای مثال، مبلغ تراکنش یا گیرنده پرداخت) استفاده می‌کند، شناسایی می‌کند.

تشخیص بات‌ها:(Bot Detection)

پیشگیری از تقلب C-Prot به‌طور مؤثر بات‌ها را مسدود می‌کند و تفاوت بین اقدامات کاربر و اقداماتی که توسط اسکریپت‌ها تولید شده‌اند را تشخیص می‌دهد.

ماژول پراکسی پیشگیرانه:(Preventive Proxy Module)

ماژول تخصصی پراکسی پیشگیرانه برای جلوگیری از فعالیت‌های پیشرفته بات‌ها طراحی شده است و با شناسایی فعالیت‌های مخرب، امنیت را افزایش می‌دهد.

حفاظت در برابر حملات مهندسی اجتماعی:(Social Engineering Protection)
C-Prot حفاظت جامع در برابر حملات مهندسی اجتماعی فراهم می‌کند. این سیستم احراز هویت پیشرفته ارائه می‌دهد، تعاملات مشکوک را نظارت می‌کند و از سایت‌های فیشینگ محافظت می‌کند. با استفاده از اطلاعات تهدید در زمان واقعی و جستجوی تهدید دستی، امکان ایجاد سیاست‌هایی برای کاهش مؤثر تلاش‌های تقلب فراهم می‌آید.
اطلاعات تهدید در زمان واقعی:(Real-Time Threat Intelligence)
C-Prot از طریق پایگاه‌های داده تهدید به‌روز و تحلیل‌های مداوم، بینش‌هایی در مورد زیرساخت‌های تقلب فراهم می‌آورد. این اطمینان می‌دهد که تدابیر مقابله با حملات مهندسی اجتماعی همواره به‌روز هستند و امکان شناسایی و خنثی‌سازی سریع تاکتیک‌های جدیدی که توسط تقلب‌کنندگان به کار گرفته می‌شود، فراهم می‌آید.
تشخیص تقلب در شناسه تماس در سطح برنامه:(Detecting Caller ID Spoofing at the Application Level)
C-Prot قابلیت تشخیص تماس‌های تقلبی در سطح برنامه موبایل را فراهم می‌کند. هم در پلتفرم‌های اندروید و هم iOS امکان جمع‌آوری متادیتاهای مرتبط با تماس‌ها در حین استفاده از برنامه موبایل برای کاربر نهایی وجود دارد. با مجوزهای خاص، برنامه‌های اندرویدی می‌توانند تاریخچه تماس‌ها، شماره تلفن‌ها، مدت زمان تماس و نوع تماس را بخوانند و حتی این داده‌ها را در حین تماس جمع‌آوری کنند.

FRAUD PREVENTION

C-Prot Fraud Prevention یک راه‌حل جامع است که برای جلوگیری از تقلب دیجیتال، محافظت از هویت دیجیتال کاربران و مسدود کردن فعالیت‌های مخرب ربات‌ها طراحی شده است. این راه‌حل به طور مؤثر در زمان واقعی در کانال‌های موبایل و وب عمل می‌کند و از فناوری‌های یادگیری ماشین، اثر انگشت‌گذاری دستگاه و داده‌های متنی مربوط به جلسات کاربری استفاده می‌کند. در حالی که امنیت کاربر را تقویت می‌کند، C-Prot Fraud Prevention روش‌های پیشرفته‌ای برای شناسایی سریع و جلوگیری از تلاش‌های تقلبی ارائه می‌دهد.

ویژگی‌های برجسته

★★★★★

تشخیص تقلب مرورگر
شناسایی می‌کند که آیا اطلاعات مرورگری که کاربر استفاده می‌کند واقعی است یا دستکاری شده است، زیرا جزئیات مرورگر قابل تغییر هستند.

تشخیص تماس مشکوک
هنگام استفاده از برنامه، تماس‌هایی از شماره‌های ناشناس، شماره‌های مشکوک یا تلاش‌های تقلبی شناسایی می‌شود.

تشخیص / VPN پروکسی
مشخص می‌کند که آیا کاربر از طریق یک VPN به اینترنت متصل است یا خیر.

تشخیص تقلب(SMIPhishing) SMS
شناسایی می‌کند که آیا اطلاعات مربوط به تقلب SMS در گوشی کاربر وجود دارد یا خیر.

تشخیص مرورگرTor
شناسایی می‌کند که آیا کاربر از مرورگر Tor استفاده می‌کند یا خیر.

تشخیص تغییر سیم کارت
مشخص می‌کند که آیا سیم کارت در دستگاه کاربر وجود دارد و آیا سیم کارت تغییر کرده است.

تشخیص تغییر کشور، شهر و منطقه زمانی
شناسایی می‌کند که آیا کاربران در موقعیتی خارج از کشور، شهر و منطقه زمانی ثبت شده در ورودهای قبلی خود قرار دارند یا خیر.

تشخیص سفر سریع
پنل تشخیص می‌دهد که آیا تغییر موقعیت مکانی در یک بازه زمانی مشخص رخ داده است.

تشخیص چند حساب کاربری در دستگاه
هنگامی که گوشی ثبت‌شده در دستگاه کاربر وارد می‌شود، افراد استفاده‌کننده از حالت مهمان نیز شناسایی می‌شوند.

تشخیص جعل هویت دستگاه
مشخص می‌کند که آیا اطلاعات برنامه در دستگاه‌های روت شده تغییر کرده است، زیرا این اطلاعات می‌تواند تغییر کند.

اثر انگشت دستگاه
یک هویت منحصر به فرد برای دستگاه‌های موبایل یا وب تولید می‌کند.

تشخیص اتصال از راه دور
تشخیص می‌دهد که آیا دستگاه از طریق برنامه‌های دسکتاپ از راه دور در حال دسترسی است یا اینکه به‌طور مستقیم توسط کاربر استفاده می‌شود..

C-Prot Embedded AppDefense

ارائه حفاظت سبک و یکپارچه با استفاده از SDK برای برنامه‌های شما در برابر تمام تهدیدات.

مزایای اصلی

شناسایی شبیه‌ساز
تشخیص می‌دهد که آیا برنامه روی دستگاه واقعی اجرا می‌شود یا خیر.

آنتی‌مالور
تهدیدات نرم‌افزاری موجود در دستگاه شما را شناسایی می‌کند.

شناسایی تماس مشکوک
تماس‌های ناشناخته و مشکوک را شناسایی می‌کند.

اثر انگشت‌گیری دستگاه
یک شناسه منحصر به فرد دیجیتال برای دستگاه‌های شما ایجاد می‌کند.

حوزه‌های استفاده

اقامت
تراکنش‌های پرداختی که در برنامه‌های موبایلی هتل‌ها و شرکت‌های گردشگری انجام می‌شود را ایمن می‌کند.

دولت
اطلاعات حساس را در برنامه‌های موبایلی موسسات عمومی و وزارتخانه‌های دفاع محافظت می‌کند.

تولید
امنیت برنامه‌های موبایلی مورد استفاده در بخش تولید را تضمین می‌کند.

مالی
اطلاعات مالی مشتریان را در برنامه‌های موبایلی بانک‌ها و موسسات مالی ایمن نگه می‌دارد.

خرده‌فروشی
پرداخت‌هایی که از طریق برنامه‌های موبایلی انجام می‌شود را ایمن می‌کند.

حمل و نقل
اطلاعات مشتریان را در برنامه‌های موبایلی شرکت‌های اجاره، اشتراک و تاکسی محافظت می‌کند.

EMBEDDED APPDEFENSE

C-Prot Embedded AppDefense به توسعه‌دهندگان برنامه‌های موبایل، مؤسسات مالی، شرکت‌های تجارت الکترونیک، سازمان‌های دولتی و بسیاری دیگر این امکان را می‌دهد تا برنامه‌های موبایل خود را در برابر تهدیدات شناخته‌شده و در حال ظهور محافظت کنند. این راه‌حل مؤثر SDK به شما کمک می‌کند تا برنامه‌های موبایل خود را به‌صورت ایمن به مشتریان خود تحویل دهید و از داده‌ها و حریم خصوصی آن‌ها محافظت کنید. با ارائه حفاظت در زمان واقعی، این سیستم در برابر بدافزارها و سایر تهدیدات امنیتی دفاع می‌کند. علاوه بر این، به شما این امکان را می‌دهد که وضعیت امنیتی برنامه خود را نظارت کرده و در صورت لزوم مداخله کنید. بدین ترتیب، شما می‌توانید تجربه‌ای امن‌تر برای کاربران خود فراهم کرده و برنامه‌های موبایل خود را بر پایه امنیت بنا کنید.

ویژگی‌های برجسته

- **آنتی‌کی‌لاگر**
  نرم‌افزارهای کی‌لاگر که هر ضربه کلیدی شما را ضبط کرده و به‌طور مداوم شما را نظارت می‌کنند، شناسایی می‌شوند.
- **کنسول مدیریت مرکزی**
  تمامی دستگاه‌های انتهایی خود را از هر مکانی با استفاده از C-Prot Security Center مدیریت کنید، که به‌صورت راه‌حل مبتنی بر ابر یا محلی در دسترس است.
- **آنتی‌دیباگینگ**
  شناسایی می‌کند که آیا برنامه در حالت دیباگ در حال اجرا است یا خیر.
- **تشخیص روت/جیل‌بریک**
  شناسایی می‌کند که آیا برنامه بر روی دستگاهی که روت یا جیل‌بریک شده است، در حال اجرا است.
- **تشخیص اسکرین‌شات**
  شناسایی می‌کند که آیا در حین استفاده از برنامه اسکرین‌شات گرفته شده است.
- **آنتی‌انجکشن**
  بررسی می‌کند که آیا کد SDK در زمان اجرا تغییر کرده و کد مخربی به آن وارد شده باشد.
- **SSL-Pinning**
  شناسایی می‌کند که آیا گواهی‌نامه در هنگام ارتباط با سرور امن است یا خیر.
- **لیست دستگاه‌ها**
  شما می‌توانید فهرست دستگاه‌های خود را مشاهده کرده، سیستم‌عامل مورد استفاده، اطلاعات IP برای ارتباط، برند و مدل دستگاه‌ها را بررسی کنید.
- **تشخیص اورلی**
  شناسایی می‌کند که آیا در حین استفاده از برنامه، پنجره‌ای بر روی صفحه‌نمایش قرار گرفته باشد.
- **تشخیص تماس مشکوک**
  تماس‌ها از شماره‌های ناشناخته، شماره‌های مشکوک یا تلاش‌های تقلبی را در حین استفاده از برنامه شناسایی می‌کند.

EMBEDDED APPDEFENSE

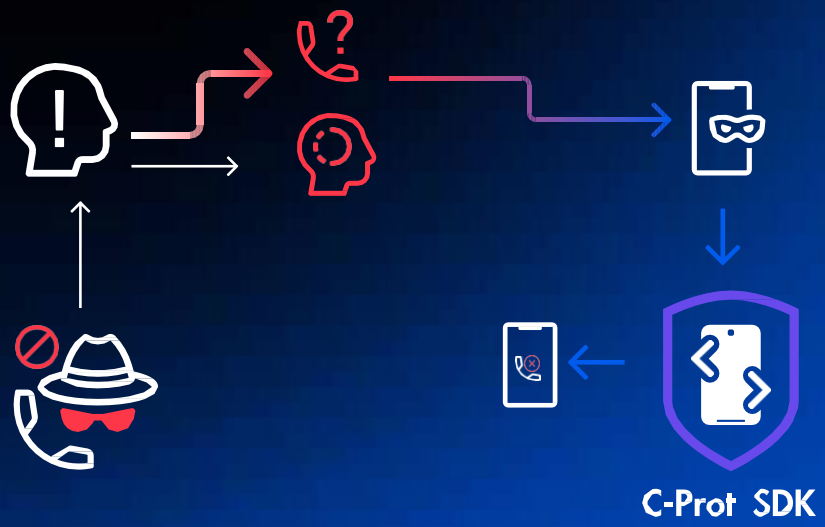
ماژول تشخیص تماس مشکوک

C-Prot با استفاده از ماژول تشخیص تماس مشکوک، حفاظت پیشرفته‌ای در برابر تقلب‌های هویت‌سازی فراهم می‌کند. با بهره‌گیری از تماس‌های VOIP و پروتکل‌های تأییدSTIR/SHAKEN ، این سیستم به‌طور مؤثر تماس‌های تقلبی را شناسایی کرده و اطمینان حاصل می‌کند که کاربران از تماس‌هایی که با هویت‌های جعلی انجام می‌شود، در امان هستند.

ویژگی ها	اصول کار	حالت فعال	حالت غیرفعال
شناسایی تماس‌های مشکوک	تماس‌های ورودی بررسی می‌شوند و تماس‌هایی که ویژگی‌هایی مانند شماره‌های ناشناخته یا تماس‌های اسپم دارند، به عنوان مشکوک علامت‌گذاری می‌شوند		
مسدودسازی در پس‌زمینه	به محض شناسایی تماس‌های مشکوک، SDKبه طور خودکار این تماس‌ها را در پس‌زمینه مسدود می‌کند و تهدیدات بالقوه را بدون نیاز به دخالت کاربر از بین می‌برد.		
استفاده از پروتکل‌های STIR/SHAKEN	ویژگی تأیید STIR/SHAKEN C-Prot یک مکانیزم امنیتی است که برای جلوگیری از جعل شناسه تماس در تماس‌ها طراحی شده و محیط ارتباطی امنی را تضمین می‌کند.		
تحلیل داده‌های پیشرفته و شناسایی ناهنجاری‌ها	C-Prot فعالیت‌های تماس‌هایی که از الگوهای عادی انحراف دارند را با استفاده از تحلیل داده‌های کلان و تکنیک‌های شناسایی ناهنجاری‌ها به دقت بررسی می‌کند.		
کنترل‌های لیست سیاه	C-Prot کاربران را از تهدیدات بالقوه با ادغام لیست‌های سیاهی که شامل شماره‌های معروف کلاهبرداری یا کلاهبرداری هستند، محافظت می‌کند و به طور خودکار تماس‌های این شماره‌ها را شناسایی و مسدود می‌کند.		
یادگیری ماشین و هوش مصنوعی	از الگوریتم‌های یادگیری ماشین و هوش مصنوعی برای یادگیری الگوهای تماس عادی و شناسایی فعالیت‌های غیرعادی استفاده می‌کند. این قابلیت به آن اجازه می‌دهد تا به طور مؤثر از فعالیت‌های کلاهبرداری جلوگیری کند.		

تشخیص جعل شناسه تماس در سطح برنامه

C-Prot این قابلیت را فراهم می‌کند که تماس‌های تقلبی را در سطح برنامه موبایل شناسایی کند. پلتفرم‌های اندروید وiOS امکان جمع‌آوری متادیتاهای مربوط به تماس‌ها را در حین تعامل کاربران نهایی با برنامه موبایل فراهم می‌کنند. با مجوزهای خاص، برنامه‌های اندروید می‌توانند تاریخچه تماس، شماره تلفن‌ها، مدت زمان تماس، نوع تماس‌ها و حتی این داده‌ها را در حین برقراری تماس جمع‌آوری کنند.



C-Prot Cyber Security Kiosk

این به‌عنوان یک افسر امنیت دیجیتال طراحی شده است که دستگاه‌های رسانه قابل حمل را نظارت می‌کند.

مزایای اصلی

کنسول مدیریت مرکزی
C-Prot Security Centerتجربه‌ای کاربردی از مدیریت با ویژگی‌های مدیریتی کاربرپسند ارائه می‌دهد.

محافظت در برابر ویروس‌ها و بدافزارها
حفاظت در برابر ویروس‌ها، جاسوس‌افزارها و سایر نرم‌افزارهای مخرب را فراهم می‌کند.

گزارش‌دهی دقیق
شما می‌توانید گزارش‌های اسکن دستگاه‌های رسانه قابل حمل را به‌راحتی از کیوسک یا کنسول مدیریت مشاهده کنید.

کنترل کامل با سیاست‌های امنیتی
با تعریف سیاست‌های قابل سفارشی از طریق کنسول مدیریت، می‌توانید رفتار دستگاه‌های رسانه قابل حمل را نظارت کنید.

حوزه‌های استفاده

مالی:
در ورودی بانک‌ها و مؤسسات مالی قرار می‌گیرد تا از حفاظت ایمن اطلاعات مالی مشتریان آن‌ها اطمینان حاصل کند.

حمل و نقل:
می‌تواند برای فراهم کردن حفاظت در برابر تهدیدات سایبری از طریق قرارگیری در نقاط حیاتی سازمان‌های فعال در زمینه‌هایی مانند خطوط هوایی، راه‌آهن‌ها، بنادر و بزرگراه‌ها استفاده شود.

مخابرات:
حفاظت در برابر تهدیدات سایبری که ممکن است از طریق دستگاه‌های رسانه قابل حمل وارد شود، از طریق قرارگیری در نقاط حیاتی سازمان‌هایی مانند شرکت‌های مخابراتی و ارائه‌دهندگان خدمات اینترنتی فراهم می‌کند.

زیرساخت‌های حیاتی:
برای محافظت از سازمان‌ها در برابر تهدیدات سایبری از طریق قرارگیری در نقاط حیاتی شرکت‌های انرژی و ارائه‌دهندگان زیرساخت‌ها استفاده می‌شود.

دولت:
می‌تواند برای فراهم کردن حفاظت در برابر تهدیدات سایبری از طریق قرارگیری در نقاط حیاتی دولت‌ها، وزارتخانه‌های دفاع و مؤسسات عمومی استفاده شود.

صنعت **دفاعی:**
دستگاه‌های قابل حملUSB) ها، هارددیسک‌های خارجی، گوشی‌های هوشمند و غیره (کارکنان فعال در زیرساخت‌های حیاتی مانند صنعت دفاعی را اسکن کرده و تهدیدات بالقوه را شناسایی می‌کند.

CYBER SECURITY KIOSK

کیوست امنیت سایبری C-Prot برای بازرسی و مدیریت دستگاه‌های رسانه قابل جابجایی در برابر بدافزارها طراحی شده است. این محصول ابزارهای لازم را به مدیران فناوری اطلاعات ارائه می‌دهد تا امنیت دیجیتال دستگاه‌ها در یک سازمان را تضمین کنند. با پنل مدیریت کاربرپسند خود، این امکان را فراهم می‌آورد تا تهدیدات بالقوه شناسایی شده و تدابیر پیشگیرانه انجام شود، که باعث تقویت وضعیت امنیتی سازمان می‌شود.

★★★★★

ویژگی‌های برجسته

✔ **پاک‌سازی تهدیدات خودکار و قرنطینه**
کیوست امنیت سایبری C-Prot به‌طور خودکار تهدیدات و فایل‌های مخرب شناسایی‌شده در حین اسکن را پاک‌سازی یا قرنطینه می‌کند.

✔ **کنسول مدیریت مرکزی**
با C-Prot Security Center ، می‌توانید تمام دستگاه‌های خود را از هر مکانی مدیریت کنید. این راه‌حل در نسخه‌های ابری و محلی در دسترس است.

✔ **دستگاه‌های رسانه پشتیبانی‌شده**
از انواع رسانه قابل حمل مانندUSB ، Type-C، CD، DVD، Blu-Ray، خوانندگان کارت و کارت‌های SD پشتیبانی می‌کند.

✔ **دستگاه رسانه قابل اعتماد**
فقط دستگاه‌های رسانه قابل حمل از پیش تعریف‌شده و تأیید شده به‌طور ایمن می‌توانند در داخل سازمان استفاده شوند. این امر از دسترسی دستگاه‌های رسانه قابل حمل ناشناخته یا بالقوه خطرناک به شبکه شرکتی جلوگیری می‌کند.

✔ **راه‌حل ترجیحی**
کیوست امنیت سایبری C-Prot یک راه‌حل معتبر برای ایمن‌سازی رسانه‌های قابل حمل در بخش‌های مختلف از جمله مالی، بهداشت، آموزش و خدمات عمومی است.

✔ **سفارشی‌سازی**
گزینه‌های قابل سفارشی‌سازی برای رابط کاربری و تنظیمات زبان در دسترس است تا نیازهای کاربر را برآورده کند.

✔ **پشتیبانی فنی**
پشتیبانی آنلاین ۷/۲۴

C-Prot
Cognitive Protection

arka
رایان سامانه آرکا

www.c-prot.com
www.arka.ir

رایان سامانه آرکا

C-Prot

نتایج آزمون‌های VirusBulletin

www.arka.ir
www.c-prot.com
021-91300476

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

C-Prot

C-Prot Endpoint Security

August 23, 2024

Test result

Test passed

A+

Detection grade

Grade A+

Certification

99.79% malware detected

Clean

0.006% false alarms

Quick Summary

Product version

1.0.0.498

Test date:

August 1, 2024

Test methodology

VB100 1.5 Link

Test platform

Microsoft Windows 10 Pro N, 64-bit, 10.0.19045

Executive summary

We tested **C-Prot Endpoint Security** (version 1.0.0.498) on August 1, 2024, on Microsoft Windows 10 Pro N, 64-bit, 10.0.19045, as per the 1.5 version of the VB100 methodology.

The tested product has successfully met the VB100 test criteria, with a malware detection grade of A+.

Test criteria:

- The product must detect at least 75.00% of all test cases in the Certification set (malicious samples).
- The product must not generate more than 0.05% false alarms in the Clean set (legitimate program samples).

Where to find more details

For detailed test results, please consult the rest of the report. You may also find the links below useful for up-to-date information on how to interpret the report data.

- **Report reader's guide** Link
  Everything you find in this report, explained.
- **Testing methodology, version 1.5** Link
  Learn exactly how we test.
- **VB100 on the web** Link
  VB100 news and certified products.

AMTSO Standard Compliance

Virus Bulletin executed this test in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization. The compliance status can be verified on the **AMTSO website**.

Test sets and product response

The VB100 test uses multiple sets of malicious and clean test cases to verify the ability of the tested product to detect malware, and to do so without generating false alarms for legitimate programs.

AT A GLANCE

CERTIFICATION	CLEAN
Description	**Description**
Common and prevalent Windows malware recently observed in the the wild.	A random selection of some widely and less widely used legitimate program files.
Type	**Type**
Outcome	**Outcome**
Pass	**Pass**
Detection rate	**False alarm rate**
99.79%	**0.006%**
Best possible outcome: **100.00%** Requirement: >= **75.00%**	Best possible outcome: **0.00%** Requirement: <= **0.05%**

DETAILED TEST RESULTS

Total cases tested	**Total cases tested**
1,917	**100,000**
Cases detected	**Cases with false alarm**
1,913	**6**
Cases missed	**Cases without false alarm**
4	**99,994**

TEST SET COMPOSITION

Windows PE executables	**Windows PE executables**
1,917	**29,723**
Other file types	**Other file types**
0	**70,277**

Report notes

Report notes contain complementary information that may be of interest to the report reader. Likewise, anyextraordinary circumstance—particularly, those that may affect the test results—are recorded in these notes.

All measurements in this report are based on-demand scanning of samples, either because the product does not offer real-time protection, or its real-time protection is not compatible with the VB100 test methodology. No further information is available at this time.

Virus Bulletin Ltd

Manor House, Office 6,
Howbery Business Park

Wallingford OX10 8BA,
United Kingdom

+44 20 3920 6348

editorial@virusbulletin.com

https://www.virusbulletin.com/

Head of Testing: Péter Karsai

Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu, Bálint Tanos

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

C-Prot

C-Prot Endpoint Security

May 21, 2024

Test result

Test passed

A+

Detection grade

Grade A+

Certification

99.76% malware detected

Clean

0.002% false alarms

Quick Summary

Product version

1.0.0.498

Test period:

May 2, 2024 - May 3, 2024

Test methodology

VB100 1.5 Link

Test platform

Microsoft Windows 10 Pro N, 64-bit, 10.0.19044

Executive summary

We tested **C-Prot Endpoint Security** (version 1.0.0.498) between May 2, 2024 and May 3, 2024, on Microsoft Windows 10 Pro N, 64-bit, 10.0.19044, as per the 1.5 version of the VB100 methodology.

The tested product has successfully met the VB100 test criteria, with a malware detection grade of A+.

Test criteria:

- The product must detect at least 75.00% of all test cases in the Certification set (malicious samples).
- The product must not generate more than 0.05% false alarms in the Clean set (legitimate program samples).

Where to find more details

For detailed test results, please consult the rest of the report. You may also find the links below useful for up-to-date information on how to interpret the report data.

- **Report reader's guide** Link
  Everything you find in this report, explained.
- **Testing methodology, version 1.5** Link
  Learn exactly how we test.
- **VB100 on the web** Link
  VB100 news and certified products.

AMTSO Standard Compliance

Virus Bulletin executed this test in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization. The compliance status can be verified on the **AMTSO website**.

Test sets and product response

The VB100 test uses multiple sets of malicious and clean test cases to verify the ability of the tested product to detect malware, and to do so without generating false alarms for legitimate programs.

AT A GLANCE

CERTIFICATION	CLEAN
Description	**Description**
Common and prevalent Windows malware recently observed in the the wild.	A random selection of some widely and less widely used legitimate program files.
Type	**Type**
Outcome	**Outcome**
Pass	**Pass**
Detection rate	**False alarm rate**
99.76%	**0.002%**
Best possible outcome: **100.00%** Requirement: >= **75.00%**	Best possible outcome: **0.00%** Requirement: <= **0.05%**

DETAILED TEST RESULTS

Total cases tested	**Total cases tested**
1,659	**100,000**
Cases detected	**Cases with false alarm**
1,655	**2**
Cases missed	**Cases without false alarm**
4	**99,998**

TEST SET COMPOSITION

Windows PE executables	**Windows PE executables**
1,659	**30,110**
Other file types	**Other file types**
0	**69,890**

Report notes

Report notes contain complementary information that may be of interest to the report reader. Likewise, anyextraordinary circumstance—particularly, those that may affect the test results—are recorded in these notes.

During this test, no such notes were generated.

Virus Bulletin Ltd

Manor House, Office 6,
Howbery Business Park

Wallingford OX10 8BA,
United Kingdom

+44 20 3920 6348

editorial@virusbulletin.com

https://www.virusbulletin.com/

Head of Testing: Péter Karsai

Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu, Bálint Tanos

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

C-Prot

C-Prot Endpoint Security

February 23, 2024

Test result

Test passed

B

Detection grade

Grade B

Certification

96.58% malware detected

Clean

0.003% false alarms

Quick Summary

Product version

1.0.0.498

Test date:

February 2, 2024

Test methodology

VB100 1.5 Link

Test platform

Microsoft Windows 10 Pro N, 64-bit, 10.0.19044

Executive summary

We tested **C-Prot Endpoint Security** (version 1.0.0.498) on February 2, 2024, on Microsoft Windows 10 Pro N, 64-bit, 10.0.19044, as per the 1.5 version of the VB100 methodology.

The tested product has successfully met the VB100 test criteria, with a malware detection grade of B.

Test criteria:

- The product must detect at least 75.00% of all test cases in the Certification set (malicious samples).
- The product must not generate more than 0.05% false alarms in the Clean set (legitimate program samples).

Where to find more details

For detailed test results, please consult the rest of the report. You may also find the links below useful for up-to-date information on how to interpret the report data.

- **Report reader's guide** Link
  Everything you find in this report, explained.
- **Testing methodology, version 1.5** Link
  Learn exactly how we test.
- **VB100 on the web** Link
  VB100 news and certified products.

AMTSO Standard Compliance

Virus Bulletin executed this test in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization. The compliance status can be verified on the **AMTSO website**.

Test sets and product response

The VB100 test uses multiple sets of malicious and clean test cases to verify the ability of the tested product to detect malware, and to do so without generating false alarms for legitimate programs.

AT A GLANCE

CERTIFICATION	CLEAN
Description	Description
Common and prevalent Windows malware recently observed in the the wild.	A random selection of some widely and less widely used legitimate program files.
Type	Type
Outcome	Outcome
Pass	**Pass**
Detection rate	False alarm rate
96.58%	**0.003%**
Best possible outcome: **100.00%** Requirement: >= **75.00%**	Best possible outcome: **0.00%** Requirement: <= **0.05%**

DETAILED TEST RESULTS

Total cases tested	Total cases tested
1,986	**100,000**
Cases detected	Cases with false alarm
1,918	**3**
Cases missed	Cases without false alarm
68	**99,997**

TEST SET COMPOSITION

Windows PE executables	Windows PE executables
1,986	**30,127**
Other file types	Other file types
0	**69,873**

Report notes

Report notes contain complementary information that may be of interest to the report reader. Likewise, anyextraordinary circumstance—particularly, those that may affect the test results—are recorded in these notes.

During this test, no such notes were generated.

Virus Bulletin Ltd

Manor House, Office 6,
Howbery Business Park

Wallingford OX10 8BA,
United Kingdom

+44 20 3920 6348

editorial@virusbulletin.com

https://www.virusbulletin.com/

Head of Testing: Péter Karsai

Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu, Bálint Tanos

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

C-Prot

C-Prot Endpoint Security

November 21, 2023

Test result

Test passed

A+ Detection grade

Grade A+

Certification

99.78% malware detected

Clean

0.003% false alarms

Quick Summary

Product version

1.0.0.498

Test date:

November 2, 2023

Test methodology

VB100 1.5 Link

Test platform

Microsoft Windows 10 Pro N, 64-bit, 10.0.19044

Executive summary

We tested **C-Prot Endpoint Security** (version 1.0.0.498) on November 2, 2023, on Microsoft Windows 10 Pro N, 64-bit, 10.0.19044, as per the 1.5 version of the VB100 methodology.

The tested product has successfully met the VB100 test criteria, with a malware detection grade of A+.

Test criteria:

- The product must detect at least 75.00% of all test cases in the Certification set (malicious samples).
- The product must not generate more than 0.05% false alarms in the Clean set (legitimate program samples).

Where to find more details

For detailed test results, please consult the rest of the report. You may also find the links below useful for up-to-date information on how to interpret the report data.

- **Report reader's guide** Link
  Everything you find in this report, explained.
- **Testing methodology, version 1.5** Link
  Learn exactly how we test.
- **VB100 on the web** Link
  VB100 news and certified products.

AMTSO Standard Compliance

Virus Bulletin executed this test in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization. The compliance status can be verified on the **AMTSO website**.

Test sets and product response

The VB100 test uses multiple sets of malicious and clean test cases to verify the ability of the tested product to detect malware, and to do so without generating false alarms for legitimate programs.

AT A GLANCE

CERTIFICATION	CLEAN
Description	**Description**
Common and prevalent Windows malware recently observed in the the wild.	A random selection of some widely and less widely used legitimate program files.
Type	**Type**
Outcome	**Outcome**
Pass	**Pass**
Detection rate	**False alarm rate**
99.78%	**0.003%**
Best possible outcome: **100.00%** Requirement: >= **75.00%**	Best possible outcome: **0.00%** Requirement: <= **0.05%**

DETAILED TEST RESULTS

Total cases tested	**Total cases tested**
1,844	**99,999**
Cases detected	**Cases with false alarm**
1,840	**3**
Cases missed	**Cases without false alarm**
4	**99,996**

TEST SET COMPOSITION

Windows PE executables	**Windows PE executables**
1,844	**30,081**
Other file types	**Other file types**
0	**69,918**

Report notes

Report notes contain complementary information that may be of interest to the report reader. Likewise, anyextraordinary circumstance—particularly, those that may affect the test results—are recorded in these notes.

During this test, no such notes were generated.

Virus Bulletin Ltd

Manor House, Office 6,
Howbery Business Park

Wallingford OX10 8BA,
United Kingdom

+44 20 3920 6348

editorial@virusbulletin.com

https://www.virusbulletin.com/

Head of Testing: Péter Karsai

Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu, Bálint Tanos

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

C-Prot

C-Prot Endpoint Security

August 22, 2023

Test result

Test passed

A

Detection grade

Grade A

Certification

99.35% malware detected

Clean

0.005% false alarms

Quick Summary

Product version

1.0.0.498

Test date:

August 3, 2023

Test methodology

VB100 1.4 Link

Test platform

Microsoft Windows 10 Pro N, 64-bit, 10.0.19044

Executive summary

We tested **C-Prot Endpoint Security** (version 1.0.0.498) on August 3, 2023, on Microsoft Windows 10 Pro N, 64-bit, 10.0.19044, as per the 1.4 version of the VB100 methodology.

The tested product has successfully met the VB100 test criteria, with a malware detection grade of A.

Test criteria:

- The product must detect at least 75.00% of all test cases in the Certification set (malicious samples).
- The product must not generate more than 0.05% false alarms in the Clean set (legitimate program samples).

Where to find more details

For detailed test results, please consult the rest of the report. You may also find the links below useful for up-to-date information on how to interpret the report data.

- **Report reader's guide** Link
  Everything you find in this report, explained.
- **Testing methodology, version 1.4** Link
  Learn exactly how we test.
- **VB100 on the web** Link
  VB100 news and certified products.

Test sets and product response

The VB100 test uses multiple sets of malicious and clean test cases to verify the ability of the tested product to detect malware, and to do so without generating false alarms for legitimate programs.

AT A GLANCE

CERTIFICATION	CLEAN
Description	Description
Common and prevalent Windows malware recently observed in the the wild.	A random selection of some widely and less widely used legitimate program files.
Type	Type
Outcome	Outcome
Pass	**Pass**
Detection rate	False alarm rate
99.35%	**0.005%**
Best possible outcome: **100.00%** Requirement: >= **75.00%**	Best possible outcome: **0.00%** Requirement: <= **0.05%**

DETAILED TEST RESULTS

Total cases tested	Total cases tested
1,987	**100,000**
Cases detected	Cases with false alarm
1,974	**5**
Cases missed	Cases without false alarm
13	**99,995**

TEST SET COMPOSITION

Windows PE executables	Windows PE executables
1,987	**29,837**
Other file types	Other file types
0	**70,163**

Report notes

Report notes contain complementary information that may be of interest to the report reader. Likewise, any extraordinary circumstance—particularly, those that may affect the test results—are recorded in these notes.

During this test, no such notes were generated.

Virus Bulletin Ltd

Manor House, Office 6,
Howbery Business Park

Wallingford OX10 8BA,
United Kingdom

+44 20 3920 6348

editorial@virusbulletin.com

https://www.virusbulletin.com/

Head of Testing: Péter Karsai

Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu, Bálint Tanos

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

C-Prot

C-Prot Endpoint Security

May 22, 2023

Test result

Test passed

A

Detection grade

Grade A

Certification

98.94% malware detected

Clean

0.005% false alarms

Quick Summary

Product version

1.0.0.498

Test date:

May 2, 2023

Test methodology

VB100 1.4 Link

Test platform

Microsoft Windows 10 Pro N, 64-bit, 10.0.19044

Executive summary

We tested **C-Prot Endpoint Security** (version 1.0.0.498) on May 2, 2023, on Microsoft Windows 10 Pro N, 64-bit, 10.0.19044, as per the 1.4 version of the VB100 methodology.

The tested product has successfully met the VB100 test criteria, with a malware detection grade of A.

Test criteria:

- The product must detect at least 75.00% of all test cases in the Certification set (malicious samples).
- The product must not generate more than 0.05% false alarms in the Clean set (legitimate program samples).

Where to find more details

For detailed test results, please consult the rest of the report. You may also find the links below useful for up-to-date information on how to interpret the report data.

- **Report reader's guide** Link
  Everything you find in this report, explained.
- **Testing methodology, version 1.4** Link
  Learn exactly how we test.
- **VB100 on the web** Link
  VB100 news and certified products.

Test sets and product response

The VB100 test uses multiple sets of malicious and clean test cases to verify the ability of the tested product to detect malware, and to do so without generating false alarms for legitimate programs.

AT A GLANCE

CERTIFICATION	CLEAN
Description	**Description**
Common and prevalent Windows malware recently observed in the the wild.	A random selection of some widely and less widely used legitimate program files.
Type	**Type**
Outcome	**Outcome**
Pass	**Pass**
Detection rate	**False alarm rate**
98.94%	**0.005%**
Best possible outcome: **100.00%** Requirement: >= **75.00%**	Best possible outcome: **0.00%** Requirement: <= **0.05%**

DETAILED TEST RESULTS

Total cases tested	**Total cases tested**
1,975	**99,998**
Cases detected	**Cases with false alarm**
1,954	**5**
Cases missed	**Cases without false alarm**
21	**99,993**

TEST SET COMPOSITION

Windows PE executables	**Windows PE executables**
1,975	**29,985**
Other file types	**Other file types**
0	**70,013**

Report notes

Report notes contain complementary information that may be of interest to the report reader. Likewise, any extraordinary circumstance—particularly, those that may affect the test results—are recorded in these notes.

During this test, no such notes were generated.

Virus Bulletin Ltd

Manor House, Office 6,
Howbery Business Park

Wallingford OX10 8BA,
United Kingdom

+44 20 3920 6348

editorial@virusbulletin.com

https://www.virusbulletin.com/

Head of Testing: Péter Karsai

Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu, Bálint Tanos

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

C-Prot

C-Prot Endpoint Security

February 20, 2023

Test result

Test passed

A+ Detection grade

Grade A+

Certification

99.74% malware detected

Clean

0.002% false alarms

Quick Summary

Product version

1.0.0.498

Test date:

February 1, 2023

Test methodology

VB100 1.4 Link

Test platform

Microsoft Windows 10 Pro N, 64-bit, 10.0.19044

Executive summary

We tested **C-Prot Endpoint Security** (version 1.0.0.498) on February 1, 2023, on Microsoft Windows 10 Pro N, 64-bit, 10.0.19044, as per the 1.4 version of the VB100 methodology.

The tested product has successfully met the VB100 test criteria, with a malware detection grade of A+.

Test criteria:

- The product must detect at least 75.00% of all test cases in the Certification set (malicious samples).
- The product must not generate more than 0.05% false alarms in the Clean set (legitimate program samples).

Where to find more details

For detailed test results, please consult the rest of the report. You may also find the links below useful for up-to-date information on how to interpret the report data.

- **Report reader's guide** Link
  Everything you find in this report, explained.
- **Testing methodology, version 1.4** Link
  Learn exactly how we test.
- **VB100 on the web** Link
  VB100 news and certified products.

Test sets and product response

The VB100 test uses multiple sets of malicious and clean test cases to verify the ability of the tested product to detect malware, and to do so without generating false alarms for legitimate programs.

AT A GLANCE

CERTIFICATION	CLEAN
Description	**Description**
Common and prevalent Windows malware recently observed in the the wild.	A random selection of some widely and less widely used legitimate program files.
Type	**Type**
Outcome	**Outcome**
Pass	**Pass**
Detection rate	**False alarm rate**
99.74%	**0.002%**
Best possible outcome: **100.00%** Requirement: >= **75.00%**	Best possible outcome: **0.00%** Requirement: <= **0.05%**

DETAILED TEST RESULTS

Total cases tested	**Total cases tested**
1,900	**100,000**
Cases detected	**Cases with false alarm**
1,895	**2**
Cases missed	**Cases without false alarm**
5	**99,998**

TEST SET COMPOSITION

Windows PE executables	**Windows PE executables**
1,900	**30,142**
Other file types	**Other file types**
0	**69,858**

Report notes

Report notes contain complementary information that may be of interest to the report reader. Likewise, any extraordinary circumstance—particularly, those that may affect the test results—are recorded in these notes.

During this test, no such notes were generated.

Virus Bulletin Ltd

Manor House, Office 6,
Howbery Business Park

Wallingford OX10 8BA,
United Kingdom

+44 20 3920 6348

editorial@virusbulletin.com

https://www.virusbulletin.com/

Head of Testing: Péter Karsai

Security Test Engineers: Adrian Luca, Csaba Mészáros, Ionuţ Răileanu, Bálint Tanos

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin