



معرفی C-Prot Endpoint Security



www.arka.ir

www.C-prot.com

021 9130 0476



021 8280 5911

This page is intentionally leave blank.

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 بر Endpoint 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، خصوصاً 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 سکوهاى خارجی
- موافقت با شرایط پیشنهادی افتا در خصوص ضوابط سامانه‌ها و سکوهاى خارجی
- قدرت تشخیص بالا به لطف استفاده از هوش مصنوعی پیشرفته
- سبک (سربار گزاری بسیار کم)
- کسب امتیازات بالا در آزمون‌های Virus Bulletin و سایر آزمون‌های مستقل
- کنسول مدیریتی پیشرفته با مدیریت آسان
- تشخیص منفی کاذب (False positive) بسیار پایین (در نتیجه بدون پیام‌های 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 پیشرفته C-Prot، مأموریت دارد که امنیت سایبری کاربران در ایران را به سطحی جهانی ارتقاء دهد.





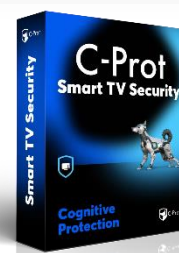
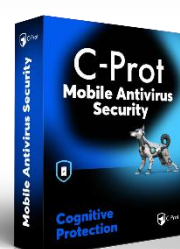
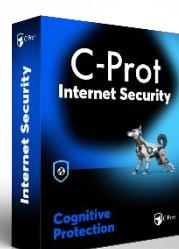
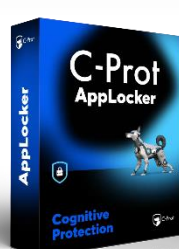
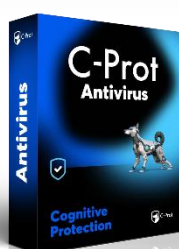
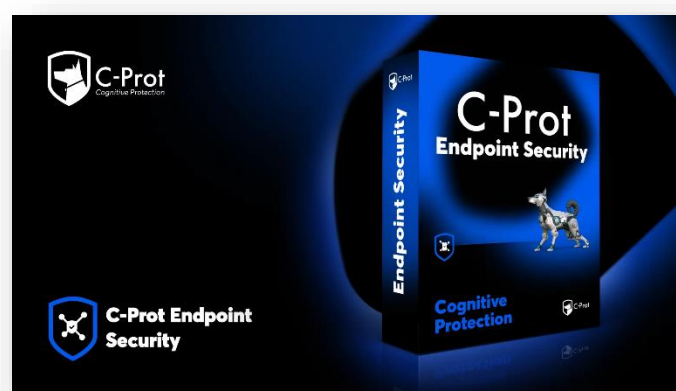
درباره‌ی C-Prot

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 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



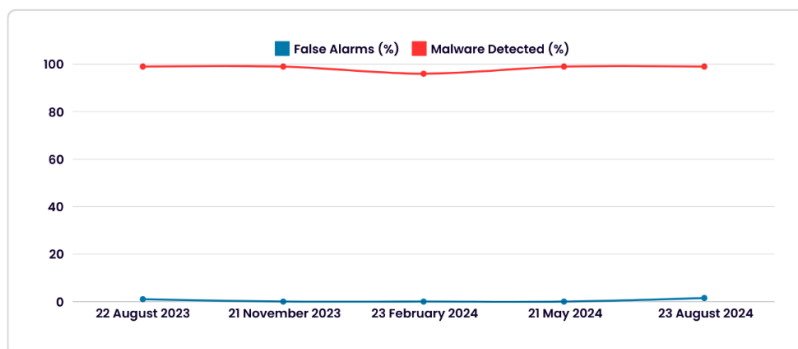
آزمون‌های VB100 توسط سازمان Virus Bulletin برگزار می‌شوند و یکی از معتبرترین ارزیابی‌ها در حوزه امنیت سایبری و آنتی‌ویروس‌ها محسوب می‌شوند. این آزمون‌ها بر اساس توانایی نرم‌افزارهای امنیتی در شناسایی بدافزارها، عملکرد بدون هشدارهای اشتباه (False Positives) و سازگاری با سیستم‌عامل‌ها ارزیابی می‌شوند.

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 Endpoint & Internet Security



False Alarms: درصد تشخیص‌های اشتباه
Malware Detected: عملکرد تشخیص بدافزار



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.

This page is intentionally leave blank.



کاتالوگ محصولات C-Prot



www.arka.ir

www.C-prot.com

021 9130 0476



021 8280 5911

This page is intentionally leave blank.

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 100٪، 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.



Starccheck

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 2020، 2021، 2022 و 2023 با نرخ شناسایی بدافزار 99.99٪، شناسایی 100٪ 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 2022 و 2023 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 946% را در سه سال گذشته به دست آورد و موفق به دریافت جایزه "دومها" شد Deloitte 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 2008 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 1991 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 18 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 2022، C-Prot به عنوان عضو SAHA "استانبول – کلاستر دفاع، هوافضا و فضا" پذیرفته شد، که هدف آن افزایش میزان بومی سازی در صنعت دفاعی، هوافضا و فضا ترکیه و تقویت رقابت پذیری بین المللی است. این عضویت از توسعه توانمندی های فناوری و صنعتی در میان اعضا پشتیبانی کرده و همکاری برای ایجاد یک اکوسیستم قوی را ترویج می کند.



HTK

C-Prot عضو "کلاستر فناوری های ارتباطات" است که در سال 2017 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 2017 با مشارکت تمام نهادهای دولتی مرتبط، نمایندگان بخش خصوصی و دانشگاه ها، 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، iOS، macOS و HarmonyOS پشتیبانی می‌کنند، که این محصولات را قابل استفاده در پلتفرم‌های مختلف می‌سازد.

● محصولات سازمانی



● محصولات خانگی





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 دلودی 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 می‌کند.



ضد بدافزار

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



مصرف کم منابع

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



فناوری C-Prot Boost

پیکربندی خودکار منابع سخت‌افزاری و نرم‌افزاری برای استفاده بهینه از عملکرد دستگاه شما.



شبکه امنیتی C-Prot

محافظت سطح بالا برای دستگاه‌های شما ارائه می‌دهد و امنیت اضافی از طریق فناوری محافظت ابری فراهم می‌آورد.



حفاظت از ایمیل

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



حفاظت هیوریستیک

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



حفاظت از شبکه‌های اجتماعی

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



دفاع شخصی

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



دانلود ایمن

به‌طور خودکار فایل‌های دانلود شده از اینترنت را اسکن می‌کند.



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 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.



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.



گزارش تهدیدات

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





C-Prot Web Protection

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



• مزایای اصلی



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



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



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



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

• حوزه‌های استفاده



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.



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



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



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



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



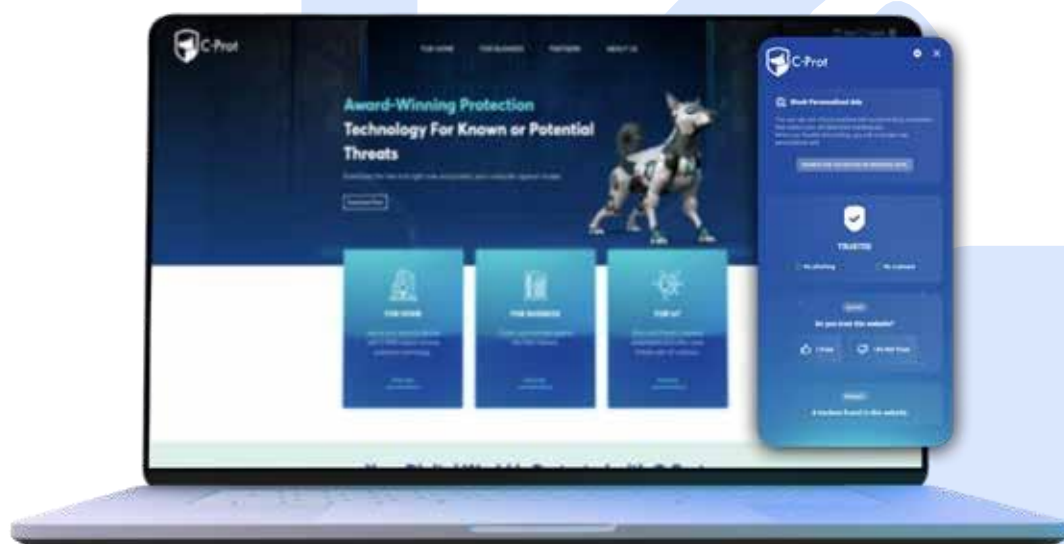
مخابرات:
شرکت‌های مخابراتی و ارائه‌دهندگان خدمات اینترنتی ایمنی دیجیتال هم کارکنان و هم زیرساخت‌های خود را با استفاده از **C-Prot** تضمین می‌کنند.

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 براورزر، اپرا، اج و غیره) استفاده شود.
✓	مصرف کم منابع با ویژگی مسدودسازی تبلیغات، استفاده از CPU، 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 Protection ردیاب‌های 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 Protection قابلیت 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 Protection در 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 به صورت محلی یا ابری است.



• مزایای اصلی



ضد بدافزار

C-Prot Endpoint Security به طور مؤثر از نقطه های پایانی کسب و کار شما در برابر ویروس ها، جاسوس افزارها و سایر نرم افزارهای مخرب محافظت می کند.



مدیریت رسانه های خارجی

با **C-Prot Endpoint Security**، می توانید استفاده از دستگاه های خارجی تعریف نشده (درایوهای USB، درایوهای CD/DVD، هارد دیسک های خارجی و غیره) را محدود یا کنترل کنید.



کنسول مدیریت مرکزی

با کنسول مدیریت که می تواند به صورت ابری یا محلی استفاده شود، می توانید بسته های **C-Prot** را مستقر کرده، وظایف و سیاست های امنیتی را مدیریت کرده و به سرعت به مشکلات یا تهدیدات روی نقاط پایانی پاسخ دهید.



سیاست های امنیتی

از طریق کنسول مدیریت **C-Prot Security Center**، می توانید پسوند های فایل، مسیرهای فایل و آدرس های وب را به لیست سفید یا سیاه اضافه کرده و به صورت گروهی یا دستگاهی آن ها را مجاز یا مسدود کنی

• حوزه های استفاده



مالی:

راه حل های حفاظت از نقطه پایانی برای سازمان های ارائه دهنده خدمات مالی، مانند بانک ها، مؤسسات مالی و شرکت های بیمه توسعه می دهد.



دولت:

در برابر تهدیدات سایبری که سازمان های دولتی و بخش عمومی ممکن است در دنیای دیجیتال با آن ها مواجه شوند، محافظت فراهم می کند.



بهداشت و درمان:

در برابر تهدیدات سایبری در دنیای دیجیتال امنیت فراهم می کند تا سوابق پزشکی بیماران و اطلاعات شخصی سلامت آن ها محافظت شود.



آموزش:

امنیت برای محافظت از اطلاعات دانش آموزان و کارکنان در مؤسسات آموزشی در برابر تهدیدات سایبری فراهم می کند.



زیرساخت های حیاتی:

در برابر تهدیدات سایبری در زیرساخت های حیاتی مانند تولید، انتقال و خدمات انرژی محافظت فراهم می کند تا از خاموشی های برق جلوگیری شود.



خرده فروشی:

در دنیای دیجیتال امنیت فراهم می کند تا از داده های مشتریان و اطلاعات پرداخت محافظت شود.



تولید:

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



مخابرات:

شرکت های مخابراتی و ارائه دهندگان خدمات اینترنتی می توانند از راه حل های **C-Prot** برای محافظت از دستگاه های نقطه پایانی استفاده کنند.

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 هورسیتیگ، دفاع جامع را ارائه می‌دهد.

C-Prot Security Center به شما این امکان را می‌دهد که تمام نقاط پایانی را از طریق یک کنسول مدیریت مرکزی، چه به صورت 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. ماژول‌های **HIPS**، 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 وب C-Prot

با افزونه محافظت وب C-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

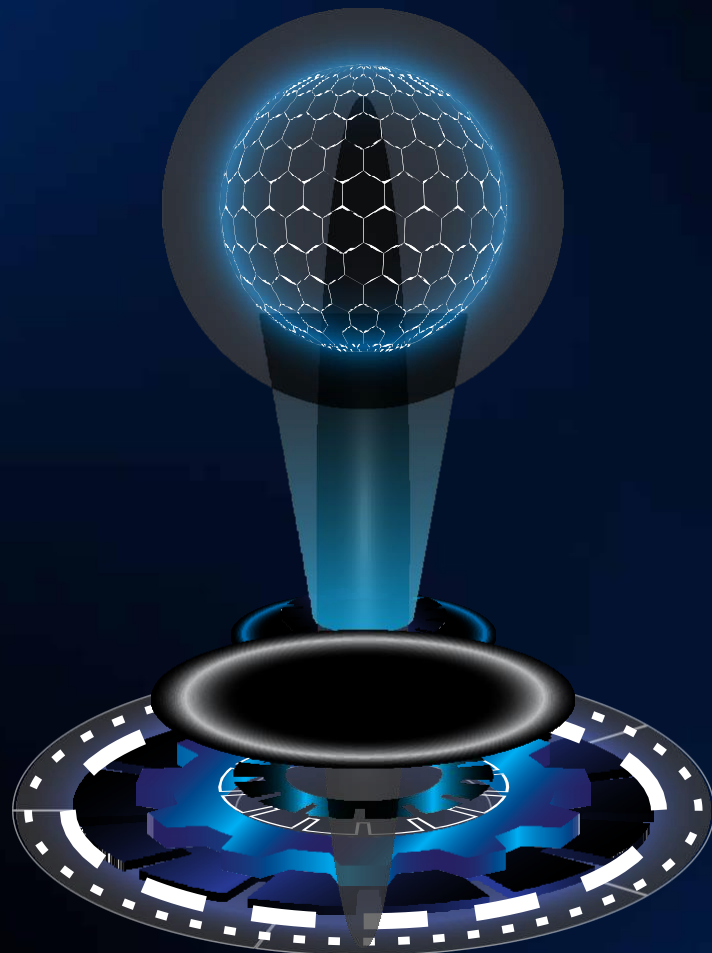
برنامه‌های نصب‌شده روی رایانه شما را که هرکدام می‌توانند برای کنترل دستگاه یا سرقت اطلاعات شخصی شما استفاده کنند، شناسایی می‌کند.





C-Prot Threat Intelligence Portal

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



• مزایای اصلی



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 می‌دهد.



تحلیل قابل 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.

• حوزه‌های استفاده



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.



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.

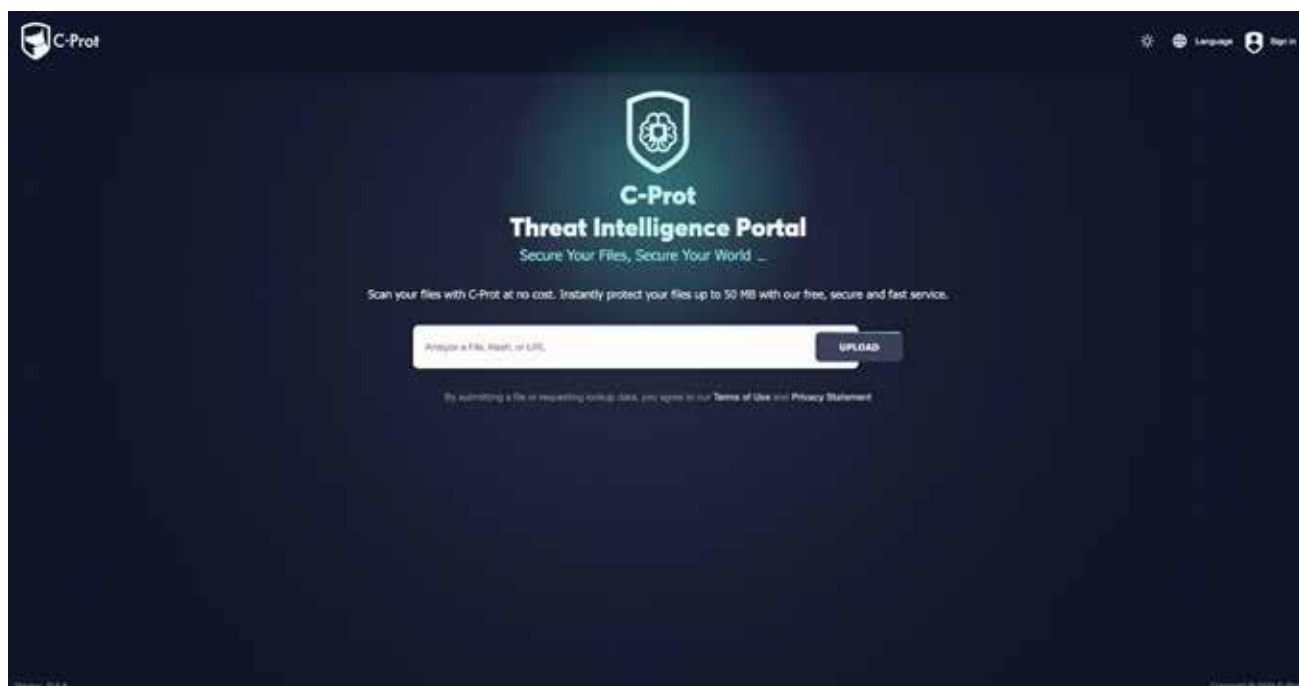


مخابرات

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

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.



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 دینامیک، 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



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



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



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.



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

حوزه‌های استفاده



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.



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.



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.



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 100٪.



فروش اینترنتی:

کاربران مشکوک را که از پلتفرم تجارت الکترونیک بازدید می‌کنند، با دقت نزدیک به 100٪ شناسایی می‌کند.



بازیهای آنلاین:

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

DEVICE FINGERPRINT

C-Prot Device Fingerprint یک راه حل است که برای شناسایی ایمن کاربران در وبسایتها و تجزیه و تحلیل ترافیک وب توسعه یافته است. این راه حل با شناسایی کاربران از طریق یک شناسه دستگاه منحصر به فرد با دقت نزدیک به 100٪، امنیت بالایی را تضمین کرده و در عین حال تجربه کاربری را نیز بهبود می بخشد.

ویژگی های برجسته

تشخیص اتصال ریموت

C-Prot Device Fingerprint کاربران را که از طریق برنامه های اتصال دسکتاپ ریموت مانند AnyDesk و TeamViewer وارد می شوند شناسایی می کند.

تشخیص استفاده از تب ناشناس

کاربرانی که در حالت مرور ناشناس به وبسایتها دسترسی پیدا می کنند شناسایی می شوند.

تشخیص استفاده از ابزارهای خودکار

درخواست هایی که توسط ابزارهای خودکار وب برای هدف قرار دادن آدرس های اینترنتی ارسال می شود شناسایی می شود.

تشخیص کاربران متعدد

ورود چندین کاربر از یک مرورگر شناسایی می شود.

تشخیص جعل شناسه دستگاه

اطلاعات اپلیکیشن ممکن است در دستگاه های روت شده تغییر کند. این ویژگی تشخیص می دهد که آیا اطلاعات تغییر کرده است یا همچنان اصلی باقی مانده است.

تشخیص ربات

تعیین می کند که آیا مرورگر توسط یک ربات مانند Selenium یا یک انسان واقعی استفاده می شود.

کنسول مدیریت مرکزی

با C-Prot Security Center می تواند به صورت ابری یا در محل استفاده شود، شما می توانید همه دستگاه های نقطه پایانی خود را مدیریت کنید و از هر جایی آنها را کنترل کنید.

تشخیص کاربران مخرب

کاربران مخرب با ویژگی هایی مانند مناطق زمانی ناسازگار، استفاده از حالت ناشناس و پروکسی ها شناسایی می شوند.

تشخیص استفاده از VPN و پروکسی

با تجزیه و تحلیل آدرس IP کاربر، مشخص می شود که آیا آدرس مربوط به یک سرور VPN یا پروکسی است.

پارامترهای WebGL

دستگاه های رسانه ای، داده های DirectX

عامل کاربری (User Agent)، سیستم عامل، پلتفرم، منطقه زمانی و غیره

فونت ها، پلاگین ها، زبان دستگاه، نوع MIME و غیره

اثر انگشت Canvas

ردیابی کوکی ها و پارامترهای دیگر





C-Prot Fraud Prevention

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



مزایای اصلی

آنتی مالور

تکنولوژی آنتی ویروس برنده جایزه C-Prot با شناسایی نرم افزارهای جاسوسی، ویروس ها و برنامه های مخرب دیگر، محافظت جامع را فراهم می آورد.



الگوریتم های شناسایی تقلب

C-Prot از الگوریتم های پیشرفته شناسایی تقلب، یادگیری ماشین و اطلاعات تهدید C-Prot برای تشخیص اینکه آیا یک تزریق بی ضرر است یا مخرب، استفاده می کند.



تشخیص خدمات دسترسی

این ویژگی به طور پیشگیرانه استفاده غیرمجاز از خدمات دسترسی توسط نرم افزارهای مخرب یا برنامه های تهدیدآمیز را شناسایی می کند.



تشخیص روت/جیل بریک

این سیستم شناسایی می کند که آیا برنامه روی دستگاهی که روت یا جیل بریک شده است اجرا می شود.



حوزه های استفاده

بهداشت و درمان:

سوابق بهداشتی را امن می کند، تلاش های فیشینگ را شناسایی می کند و تقلب در نسخه های دارویی را تشخیص می دهد.



سفر:

رزروهای سفر را امن می کند، اطلاعات کارت مشتری را محافظت می کند و تلاش های فیشینگ را شناسایی می کند.



ارتباطات:

تلاش های فیشینگ را شناسایی می کند، از تقلب حساب جلوگیری می کند و اطلاعات مشترکین را محافظت می کند.

مالی:

امنیت مالی را در تراکنش های بانکی آنلاین افزایش می دهد، تلاش های فیشینگ را شناسایی می کند و بدافزارها را مسدود می کند.



تجارت الکترونیک:

از تقلب در تجارت الکترونیک جلوگیری می کند، پرداخت های مشتریان را امن می سازد و تلاش های فیشینگ را شناسایی می کند.



بیمه:

از تقلب جلوگیری می کند، ادعاهای تقلبی بیمه را شناسایی می کند و اطلاعات مشتریان را امن می سازد.

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 به صورت زنده:
مجوزهای حیاتی دستگاه‌های کاربر را به صورت آنی مانیتور می‌کند و امنیت را با مسدود کردن عملیات اپلیکیشن‌های پرخطر هنگام شناسایی مجوزهای مشکوک اندروید افزایش می‌دهد.
آنتی-کی لاگر (Anti-Keylogger)
نرم افزارهای کی لاگر که هر ضربه‌ای که وارد می‌کنید را ثبت و شما را به طور مداوم نظارت می‌کنند، شناسایی می‌شود.
آنتی-دباکینگ (Anti-Debugging)
تشخیص می‌دهد که آیا اپلیکیشن در حالت دیباگ در حال اجرا است یا خیر.
تشخیص شبیه ساز (Emulator Detection)
معلوم می‌کند که آیا اپلیکیشن بر روی دستگاه واقعی در حال اجرا است یا بر روی شبیه ساز.
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 پیش فرض 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 به طور 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 به روز و تحلیل‌های مداوم، بینش‌هایی در مورد زیرساخت‌های تقلب فراهم می‌آورد. این اطمینان می‌دهد که تدابیر مقابله با حملات مهندسی اجتماعی همواره به روز 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 راه حل جامع است که برای جلوگیری از تقلب دیجیتال، محافظت از هویت دیجیتال کاربران و مسدود کردن فعالیت های مخرب ربات ها طراحی شده است. این راه حل به طور مؤثر در زمان واقعی در کانال های موبایل و وب عمل می کند و از فناوری های یادگیری ماشین، اثر انگشت گذاری دستگاه و داده های متنی مربوط به جلسات کاربری استفاده می کند. در حالی که امنیت کاربر را تقویت می کند، C-Prot Fraud Prevention روش های پیشرفته ای برای شناسایی سریع و جلوگیری از تلاش های تقلبی ارائه می دهد.

ویژگی های برجسته



تشخیص تقلب مرورگر



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

تشخیص تماس مشکوک



هنگام استفاده از برنامه، تماس هایی از شماره های ناشناس، شماره های مشکوک یا تلاش های تقلبی شناسایی می شود.

تشخیص / VPN پروکسی



مشخص می کند که آیا کاربر از طریق یک VPN به اینترنت متصل است یا خیر.

تشخیص تقلب (SMIPhishing) SMS



شناسایی می کند که آیا اطلاعات مربوط به تقلب SMS در گوشی کاربر وجود دارد یا خیر.

تشخیص مرورگر Tor



شناسایی می کند که آیا کاربر از مرورگر Tor استفاده می کند یا خیر.

تشخیص تغییر سیم کارت



مشخص می کند که آیا سیم کارت در دستگاه کاربر وجود دارد و آیا سیم کارت تغییر کرده است.

تشخیص تغییر کشور، شهر و منطقه زمانی



شناسایی می کند 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 می دهد که آیا تغییر موقعیت مکانی در یک بازه زمانی مشخص رخ داده است.

تشخیص چند حساب کاربری در دستگاه



هنگامی که گوشی ثبت شده در دستگاه کاربر وارد می شود، افراد استفاده کننده از حالت مهمان نیز شناسایی می شوند.

تشخیص جعل هویت دستگاه



مشخص می کند که آیا اطلاعات برنامه در دستگاه های روت شده تغییر کرده است، زیرا این اطلاعات می تواند تغییر کند.

اثر انگشت دستگاه



یک هویت منحصر به فرد برای دستگاه های موبایل یا وب تولید می کند.

تشخیص اتصال از راه دور



تشخیص می دهد که آیا دستگاه از طریق برنامه های دسکتاپ از راه دور در حال دسترسی است یا اینکه به طور مستقیم توسط کاربر استفاده می شود...



C-Prot Embedded AppDefense

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



مزایای اصلی



آنتی‌مالور

تهدیدات نرم‌افزاری موجود در دستگاه شما را شناسایی می‌کند.



شناسایی شبیه‌ساز

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



اثر انگشت‌گیری دستگاه

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



شناسایی تماس مشکوک

تماس‌های ناشناخته و مشکوک را شناسایی 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 تأیید STIR/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.

ویژگی‌ها	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، SDK به‌طور 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 C-Prot STIR/SHAKEN 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 به‌طور 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 به‌طور 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 و iOS 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.



This page is intentionally leave blank.



نتایج آزمون‌های VirusBulletin



www.arka.ir

www.C-prot.com

021 9130 0476



021 8280 5911

This page is intentionally leave blank.

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT



C-Prot

C-Prot Endpoint Security



August 23, 2024



Test result
Test passed



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

August 23, 2024

VB100 TEST REPORT



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](#).

August 23, 2024

VB100 TEST REPORT



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

Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT



C-Prot

C-Prot Endpoint Security



May 21, 2024



Test result
Test passed



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

DETAILED TEST RESULTS

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

TEST SET COMPOSITION

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

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 تمامی استان‌های 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 توانیدی را به مشتریان خود ارائه کرده است. از جمله محصولات تولیدی این شرکت می‌توان به مواردی مانند آرکاگیت که یک فایروال بومی با امکانات کامل و جامع و اینترنت اکانتینگ کامل است اشاره کرد. همچنین چاپان، نرم‌افزاری برای مدیریت چاپ در شبکه، pamArka محصول بومی برای مدیریت دسترسی ادمین (PAM)، از دیگر محصولات تولیدی شرکت رایان سامانه آرکا است.

محصولات و راهکارهای رایان سامانه آرکا



آدرس دفتر مرکزی: تهران، خیابان شهید بهشتی، خ پاکستان، کوچه 4 پلاک 11 واحد 7
مرکز تماس: +98 (21) 8280 591 +98 (21) 9130 0476

دفتر تبریز: چهارراه منصور، برج ابریشم، طبقه 6، واحد 8
تلفن: +98 (41) 3559 5230

✉ info@arka.ir 🌐 www.arka.ir
☎ WhatsApp: +989919003219
📠 Telegram: rayansamanarka
📷 Instagram: rayansamanarka
🌐 LinkedIn: rayan-samaneh-arka

لینک دانلود کاتالوگ: https://files.arka.ir/brochure/all_about_c-prot.pdf

