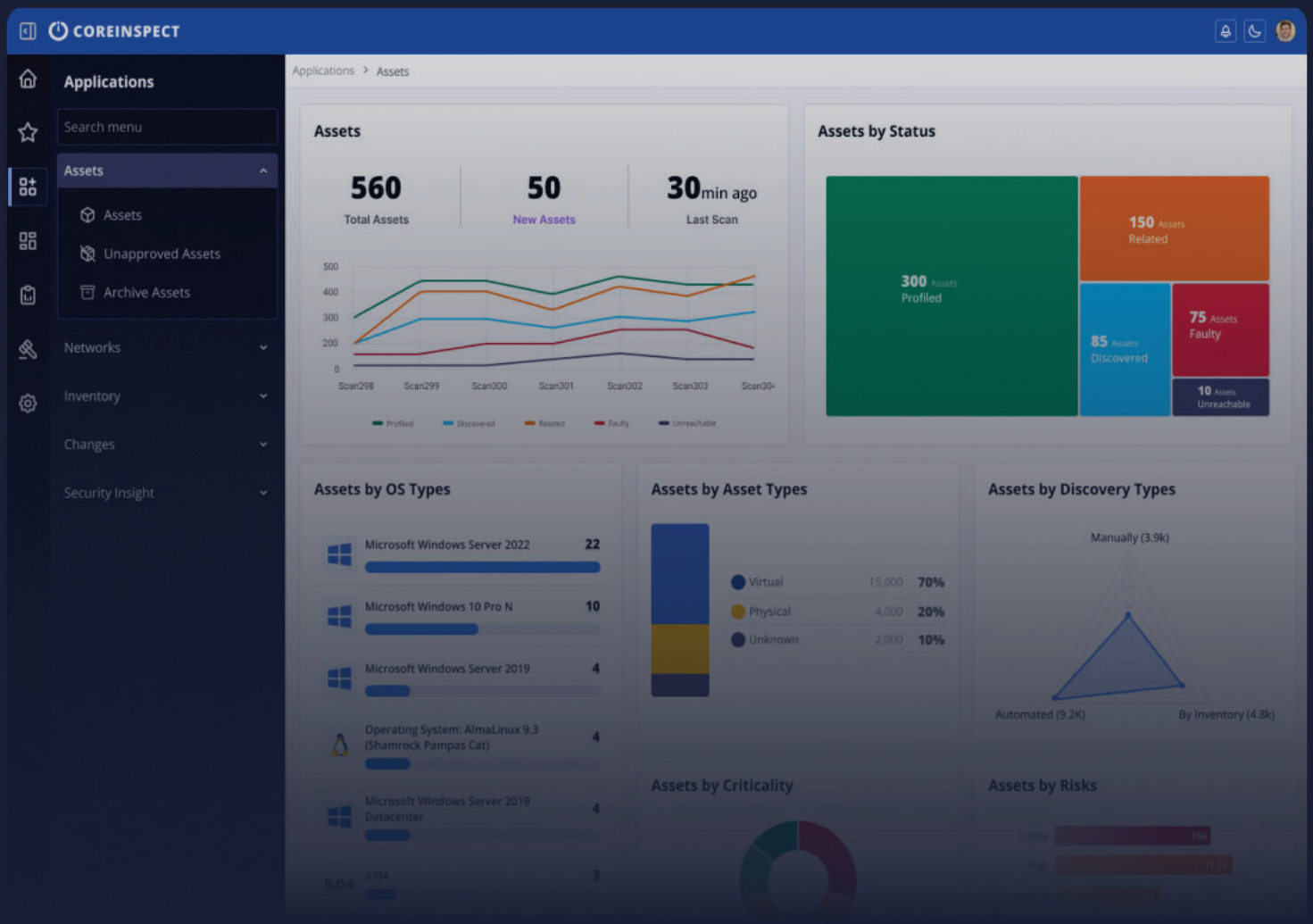
Core Inspect

Cyber Security Asset Management

سامانه بومی مدیریت دارایی‌های سایبری

کوراینسپکت سامانه‌ای کاملا بومی، با هدف مدیریت دارایی‌های سایبری سازمان (CSAM) است که تمامی مراحل طراحی و تولید آن توسط شرکت بهین راهکار صورت پذیرفته است. این سامانه با توانایی کشف و ذخیره سازی خودکار دارایی‌های سازمان به همراه جزئیات آنها، یک نمای ۳۶۰ درجه از تمامی موجودیت‌های سایبری سازمان ارائه می دهد.

WWW.BEHINRAHKAR.COM



نسخه ۲.۲ ـ آذر ۱۴۰۳

معـــرفی ســـامـانه

مقـدمـه

شناسایی دارایی های سایبری گام اول و لازمه ایجاد امنیت در حوزه فناوری اطلاعات است. پیاده سازی گام های امنیتی در سازمان برای محافظت از دارایی ها زمانی معنی پیدا می کند که بدانیم از چه چیزی می خواهیم محافظت کنیم.

کوراینسپکت با شناسایی دارایی های سازمان و دسته بندی آن‌ها در قالب مولفه های ذاتی و کسب و کاری، علاوه بر کمک در پیاده سازی امنیت، موجب تسهیل در پایش عملکرد و برنامه ریزی جهت بهبود وضعیت عملیاتی دارایی های سازمان می گردد.

چـــالش‌هـای پیـش روی سـازمان‌ها در حـوزه مدیـریت دارایی‌های ســایبری

شنـاسـایی تمـــام دارایـی‌هـای فعـــال ســـازمان

یکی از اصلی ترین دلایل تاخیر و یا شکست پروژه های ISMS در کشور، عدم تهیه به موقع لیستی دقیق و بروز از دارایی های سازمان است. با در نظر داشتن اینکه در اجرای اغلب پروژه های ISMS در سازمان های بزرگ با تعداد زیادی از دارایی های سایبری مواجهه هستیم، تهیه لیست های جزیره ای توسط دپارتمان های مختلف دیتاسنتر، شبکه، نرم افزار و ... از طریق ابزارهای متفاوت و یا بصورت دستی، نه تنها موجب ایجاد یک لیست یکپارچه نمی گردد که سازمان را در برزورسانی آن نیز دچار چالش می کند

بروزرسـانی لیـست تعـداد و جزئیـــات دارایی‌هـای سـازمان

پس از تهیه لیست اولیه دارایی های سازمان و جزئیات آنها، ثبت دقیق تغییرات، نگهداری سوابق و بروزرسانی مستمر لیست با توجه به فرکانس بالای تغییرات دارایی ها در سازمان ها، فرآیندی پر چالش برای مدیران فناوری اطلاعات و امنیت می باشد.

جمـع آوری دقیـق و قـابل اطمینان، جزئیـــات دارایی‌هـا

لیست دارایی های تهیه شده توسط کارشناسان سازمان همواره وابسته به دقت کارشناسی است که اطلاعات را جمع آوری می کند و در نهایت اطمینان به گزارش تهیه شده همیشه با در نظر گرفتن ضریب خطای انسانی همراه است.

آمـاده سـازی پیش نیازهای اجـرایی سـایر ابـزار هـای امنیتی

سطح پوشش ابزارهای مدیریت شبکه و امنیت همواره به عنوان فاکتور اصلی در پیاده سازی و استقرار یک محصول در سازمان ها در نظر گرفته می شود. دغدغه عدم اطمینان از افزودن همه تجهیزات در سامانه های مدیریت شبکه و امنیت چالشی هست که مدیران فناوری با توجه به تغییرات مستمر شبکه و سرویس ها، همیشه با آن مواجه هستند.

معـــرفی ســـامـانه

چـــالش‌هـای پیـش روی سـازمان‌ها در حـوزه مدیـریت دارایی‌های ســایبری

کنتـرل دارایی‌هـا، در شبکه‌هایی با گستره وسیع جغـرافیـایی

کنترل دارایی های فعال در شبکه به لحاظ سخت افزاری (افزودن یا حذف اقلام سخت افزاری)، نرم افزاری (نصب یا حذف پکیج های نرم افزاری) و همچنین دسترسی (اتصال و یا قطع ارتباط) به شبکه همیشه از چالشهای پیش روی مدیران فناوری اطلاعات و امنیت در سازمان‌هایی با شبکه های بزرگ و پراکنده در سطح کشور می باشد.

اطمینـــان از پیـــروی از سیـــاست‌هـــای امنیتـــی

بررسی مستمر و حصول اطمینان از پیاده سازی سیاستهای امنیتی سازمان در حوزه مدیریت دارایی مانند نصب یا عدم نصب نرم افزاری ها مورد نظر و یا عدم وجود نسخه آسیب پذیر برخی نرم افزارهای مجاز و ...، در سطح کل شبکه سازمان همواره جزئی از دغدغه های مدیران فناوری اطلاعات و امنیت می باشد.

کـوراینسپـــکت چه مـــزیتی بـــرای کسـب و کار شمـــا دارد؟

اطلاعـــات دقیـق و بـــروز از دارایی‌هـــا

فـــرآیند خـــودکار کشـف، واکشـــی و ثبت جزئیـــات دارایی‌ها به صـورت دوره‌ای و در بازه‌هـــای زمـــانی کـوتاه منجـــر به جمـع آوری اطلاعـــاتی دقیـــق و بـــروز از تمـــامی دارایی‌هـــای ســـازمـان و تولیـــد گزارشـــاتی جامـع و تحلیلـــی بـــرای آن‌ها می گـــردد.

کاهـــش هـــزینه‌هـــا

کشـــف و ذخیـره سـازی خودکار جزئیات دارایی‌ها در سطوح مختلف و نگهـــداری سابقـــه آن‌ها مـــوجب کاهـــش هـزینه‌ها در بـــرنامه ریـزی و ایجـــاد نقشـــه راه در خصـــوص بهینـــه سازی فـــرآینـــدهای مدیـــریت شبکه و امنیت می گـــردد.

مـــدیـــریت آســـانتـــر تـغییـــرات

ثبت خـودکار و لحظه‌ای تغییرات هـر دارایی در سطـوح مختلف سخـت افزار، نرم افزار، شبکه و کاربران و ارسال هشدار از طریق کانال های مرسوم تیکت، ایمیل و پیامک امکان پیگیری تغییرات را برای سازمان تسهیل می نماید.

ارتقـــاء سطـــح امنیـــت

پایش مستمر سیاستهای امنیت سازمان و اعلام در لحظه هرگونه نقض سیاست در سطوح مختلف هر دارایی، باعث اطمینان از انطباق آنها با معیارهای در نظر گرفته شده و در نهایت ارتقاء سطح امنیت می گردد.

مـــدیـــریت متـــمرکـــز دارایـــی‌هـــا

معماری توزیع پذیر و قابلیت Low-Config/No-Config سامانه موجب استقرار سریع و بی نقص سامانه در شبکه های بزرگ شده و اطلاعات دارایی ها را در کمترین زمان ممکن در کنسول مدیریتی جمع آوری و برای اقدامات بعدی مهیا می نماید.

انـــطبـــاق پـــذیـــری

ایجاد سیاستهای دلخواه برای دارایی ها در سطوح مختلف، امکان انطباق با چارچوب ها و استانداردهایی از قبیل ISO ۲۷۰۰۱ و NIST و پایش مستمر آنها را برای سازمان به ارمغان می آورد

قابلیت‌هـــای کـــوراینسپـــکت

سامانه کوراینسپکت قابلیتهای کاربردی بسیاری را برای مشتریان در سطح Enterprise ارائه می دهد تا آنها بتوانند بهترین انتخاب را برای محافظت ار دارایی های سازمان خود در نظر بگیرند.

۱ کشف خودکار دارایی‌ها بصورت دوره‌ای و بازه‌های زمانی کوتاه

۲ جمع آوری جزئیات دارایی‌ها در کلیه سطوح سخت افزار، نرم افزار، شبکه و کاربر

۳ ثبت تغییرات و ارائه گزارشات پیشرفته در خصوص سوابق دارایی‌ها

۴ بهره مندی از اسکنرهای اختصاصی شرکت بهین راهکار

۵ امکان تعریف سیاست‌های امنیتی در سطوح مختلف دارایی و شبکه

۶ ارائه قابلیتهای مدیریت آدرس ها (IPAM)

۷ ارسال هشدار از طریق کانال‌های مرسوم (تیکت، ایمیل، پیامک)

۸ ارسال خودکار هشدار بر اساس سیاست‌های از پیش تعریف شده

۹ بهره مندی از طیف وسیعی از آداپتورهای اتصال به دارایی‌ها و استخراج جزئیات آن‌ها

۱۰ تعدد گزارشات و داشبوردهای طبقه بندی شده

۱۱ امکان تعریف برچسب‌های دلخواه و الصاق خودکار آن‌ها به دارایی‌ها

۱۲ امکان تهیه خروجی از داشبوردها و گزارشات در فرمت‌های مرسوم نظیر اکسل

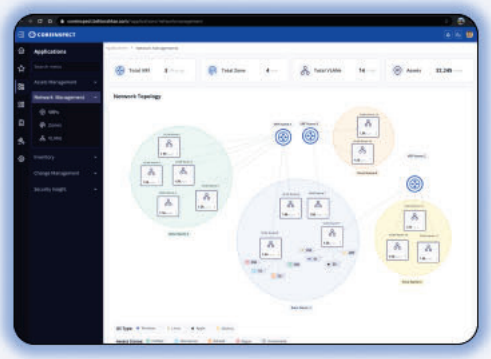
۱۳ ایجاد گزارشات سفارشی توسط کاربر و زمانبندی خودکار اجرا و ارسال آن‌ها

۱۴ ایجاد داشبوردهای سفارشی توسط کاربر

۱۵ تعریف اطلاعات موقعیت مکانی، مدیر، مالک و ... برای دارایی

۱۶ اجرای آسیب پذیری پسیو در صورت یکپارچگی با سامانه کورتیس

۱۷ اولویت بندی دارایی‌ها بر اساس میزان حساسیت آنها



مشاهده لحظه به لحظه وضعیت دارایی‌های سازمان با کوراینسپکت

مـــزایای رقـابتی کـورااینسپـــکت

برخی از ویژگی‌های اصلی کوراینسپکت به‌عنوان یک سامانه CSAM:

۱ اکتشـــاف و استخـــراج جزئیـات دارایی‌هـا

پـشتیبـانی همـــزمـــان از هـــر دو روش Agent-base و Agentless در تمـامی فـــرآیـنـدهـــای اکـتـشـاف و استخـراج جزئیات دارایـی ها

۲ حـداقل سطـح دستـرسی به دارایی هـــا

پیروی از اصول Zero-Trust و Least Privilege Access در تمامی فرآیندهای اکتشاف و واکشی جزئیات د ارایی ها

۳ جمـــع آوری جزئیـات دارایـی‌هـــا

واکـــشی جزئیـات دارایی‌هـــا در ۵ سطـح : نـــرم افـــزار، سخـــت افـــزار، کاربـــران، سیستـــم عامـل، تنظیمـات شبکه

۴ کشـــف دارایـی‌هـــا به صـــورت دوره ای

انجـام فـــرآیـنـد اکتشـاف به صـورت دوره ای و در بـازه‌هـــای زمـانی قابـل تنظیـم توسط مدیر سامانه (حداقل هر ۵ دقیقه)

۵ حـــداقل ســـربار (Overhead) در شبـــکه

انجـام فـرآیـنـد اکتشـــاف بـدون ایـجاد اختـــلال یا تغـــییـــر محســـوس در عمـــلکـــرد شبـــکه ســـازمـــان، با ســـربـــار ۸ کیلـوبایـت به ازای کشـــف هـــر ۱۰،۰۰۰ آدرس IP

۶ ارائـــه گزارشـــات پیشـــرفته تغییـــرات دارایـی‌هـا

ثبـــت و گـــزارش تـغیـیـرات در سطـح دارایـی‌هـــا، از جـمـلـه سخت‌افـزار، نـرم‌افـزار، ســرویـس، سیستـم عـامـل، کارت شبـــکه و ســایر مولـفه‌های مـرتبط

۷ سـرعت بی نظیـر در اکتشـاف دارایی‌هـــای ســـازمـــان

اکـتـشـاف آدرس‌هـــای IP فعال در شبکه با صـرف تنهـــا ۳۰ ثانیـــه زمـان به ازای کشـــف هـــر ۱۰،۰۰۰ آدرس IP

۸ ارسـال Notification از طریق تمـام کانال‌هـــا

قـــابلیـــت اتصـــال به ســـرور ایمیـــل، درگـــاه پیـــامک (SMS gateway) و سامانه‌های تیکتینـگ برای ارسال اعـلان‌ها به کاربران.

۹ تعـریف و انتصـاب اتوماتیـک برچسب‌هـــای شخصـی

قابلیـت تعـریف فیلتـــر و اختصـاص اتوماتیـک بـرچسب به دارایی‌ها بـــر اساس ویـژگی‌های شخصی، سرویـس‌های کسب و کار و مـوقعیـت جغـرافیایی، جهـت دستـه‌بندی و تعییـــن ارتبـــاطات دارایـــی‌ها

۱۰ پـــورت اسکنـــرهای اختصـــاصی

اکتشـــاف ســـریع پـورت‌های پـاسخـگوی دارایـی‌هـــا در شبـــکه سازمان توسـط پـورت اسـکنرهـــای خـاص منظوره و اختصـاصی شـرکت بهیـــن راهـــکار

۱۱ تعـــریف سیـــاستهـــای امنیتـــی

قـــابلیـــت تعـریف سیـاستهـــای امنیتـــی در صـــورت حضـــور یا عـدم حضـــور نـــرم‌افـــزارهای خـــاص بـــر روی سیـستـم‌ها و ارســـال پیغـام‌های اخـطار به مـدیر سـامـانه در صـــورت نقـــض سیـــاستهـــا

۱۲ گـزارشات و نمـودارهـای طبقه بنـــدی شـــده دارایی‌هـــا

وجـود نمـودارهـــا و گـــزارشـــات طبـقـــه بنـــدی شـده پیـش فـرض در کلیه سـطوح اطـلاعات دارایی‌هـــا بـراساس نـوع تجهیـز، سیستـم عامـــل، تنـــوع سخـــت افـزار، مجـازی یا سخـت افزاری، سـرور یا کلاینت ، میـزان آسیب پذیری و ...

۱۳ طیـــف گستـــرده ای از آداپـتـــورهـــای اتصـــال

پـــشتیبـــانی از بیـــش از ۷۰ آداپتـــور بـــرای اتصـــال و اینـــونتـــوری تجهـیـزات مختـــلف

۱۴ گـــزارش دهـــی مـــتنـــوع

قابلیـــت دریافت خروجی با فرمت های مختلف نظیر Excel از تمامی گزارش‌ها و فیلترهای سامانه

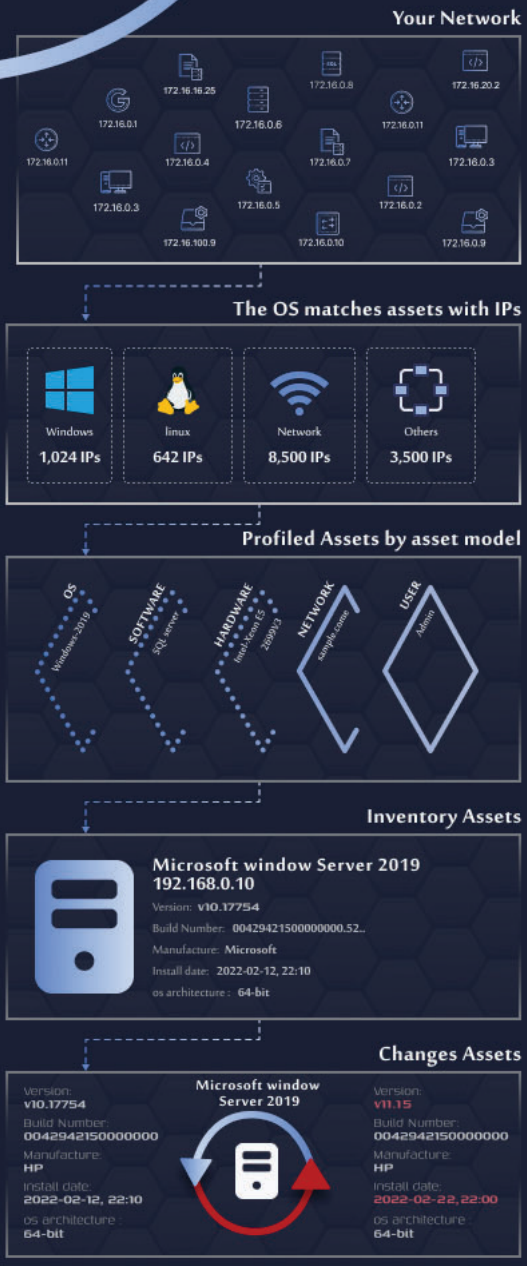
۱۵ ارائـه IPAM (IP Address Management) خـودکار

ارائـــه گـــزارش در مـــورد تمـــامی VLANهای ســـازمان به همـــراه تعـــداد IPهـــای فعـــال در هـــر VLAN و میـــزان اشغـــال فضای VLANها

۱۶ پـشتیبانی از تمامی پروتـکل های استـــاندارد ارتبـــاطی

پـشتیبـانی از پروتـــکل‌های SNMP V1، SNMP V2C، SNMP V3 و WMI، SSH، Telnet، REST-API، SOAP-API و ...

کورااینسپکت چگونه کار میکند؟



شناسایی تمامی IP های فعال در شبکه

کورااینسپکت با اتصال به تجهیزات شبکه سازمان نظیر سوییچ‌های لایه ۳ و یا روترها، در حداقل زمان ممکن (کمتر از ۳۰ ثانیه) تمامی آدرس IPهای فعال در شبکه سازمان را در کشف و ذخیره می کند.

دسته بندی IP های فعال

پس از کشف IP آدرس های فعال در شبکه سازمان، سامانه به وسیله آداپتورهای مختلف اقدام به دسته بندی دارایی ها براساس پروتکل های پاسخگوی دارایی ها نظیر WMI، SSH، HTTP، HTTPS و ... می کند.

اتصال به دارایی و کشف جزئیات هر دارایی

در قدم بعدی سامانه پس از شناسایی خودکار نوع دارایی بوسیله آداپتورهای مختص آن دارایی و Credential متناسب با هر دارایی که توسط مدیر شبکه تنظیم شده به آن دارایی متصل شده و اطلاعات دارایی را دریافت و ذخیره می کند.

ذخیره سازی جزئیات دارایی ها

با الصاق آداپتورهای اینونتوری به دارایی های مدیریت شده، اطلاعات دارایی ها در ۵ سطح سیستم عامل، سخت افزار، نرم افزار، کاربران و تنظیمات کارت شبکه آنها واکشی و در سامانه ذخیره می شود.

شناسایی تغییرات دارایی ها

در نهایت با توجه به انجام دوره ای فرآیند کشف و اینونتوری دارایی ها، پس از هر انجام دوره، تمامی تغییرات نسبت به دوره های قبل تشخیص داده شده و ذخیره می شود.

کورااینسپکت مناسب چه سازمان هایی است؟

۱- سازمان های بزرگ با تعداد دارایی‌ها زیاد که به کنترل دارایی ها و تهیه گزارشات دقیق و بروز در مورد آن‌ها اهمیت می دهند.

۲- سازمان‌هایی با دفاتر مختلف و وسعت جغرافیایی که نظارت بر دارایی‌ها برای آن‌ها دشوار است.

۳- سازمان‌هایی که با فرکانس بالای تغییرات در سطوح سخت افزار و نرم افزار مواجه هستند.

۴- سازمان‌هایی که بدنبال انطباق و اخذ گواهینامه‌های استانداردهای امنیتی هستند.

معمـاری سـامانه و نیازمندی‌های سخت افزاری

سامانه کوراینسپکت از اجزاء (کامپوننت ها) های مختلفی تشکیل شده است. برخی از آنها بسته به نوع لایسنس نیازمندیهای سخت افزاری متفاوتی دارند. کلیه این اجزاء بر روی بستر مجازی قابل پیاده سازی می باشند.

App For each 3,500 Profiled Assets	
Component	**Enterprise**
Physical appliance	**Provided by Vendor**

CoreInspect_Explorer (OVA) For each 10k (Network Node) or 3,500 Devices	
PROCESSOR	**6 Core (>=2.4 GHz) | (12 vCPUs or Threads)**
MEMORY	**32 GB**
STORAGE	**300 GB(SAS 10k or higher)**
NIC	**1 Gb Ethernet or higher**

Identity Gateway For each 10k (Network Node) or 3,500 Devices	
PROCESSOR	**4 threads**
MEMORY	**16 GB**
STORAGE	**50 GB**
NIC	**2 NICs (Gb Ethernet or higher)**

Update Proxy For each 10k (Network Node) or 3,500 Devices	
PROCESSOR	**4 Core**
MEMORY	**8 GB**
STORAGE	**50 GB**
NIC	**1 Gb Ethernet or higher**

لایـسنـس کـوراینسپــکت

لایسنس سامانه کورایسنپکت بر اساس تعداد IP های قابل کشف در شبکه و یا تعداد دارایی هایی که نیاز به مدیریت دارند محاسبه می گردد. جدول زیر لایسنس های پیش فرض را نمایش می دهد.

Managed IPs	Total IPs
1k	**3K**
2k	**6K**
3k	**9K**
4k	**12K**
5k	**15K**
7k	**21K**

Managed IPs	Total IPs
10k	**30K**
12k	**36K**
15k	**45K**
17k	**51K**
20k	**60K**
25k	**75K**

Managed IPs	Total IPs
30k	**90K**
35k	**105K**
40k	**120K**
45k	**135K**
50k	**150K**
60k	**180K**

Managed IPs	Total IPs
70k	**210K**
80k	**240K**
90k	**270K**
100k	**300K**

خـــدمات پشـتیبـانـی

با بهره گیری از خدمات پشتیبانی کوراینسپکت می‌توانید با مراجعه به آدرس https://support.behinrahkar.com در کمترین زمان به متخصصین پشتیبانی فنی دسترسی داشته باشید. در جدول زیر خدمات قابل ارائه در دو سطح پایه و پیشرفته آورده شده است.

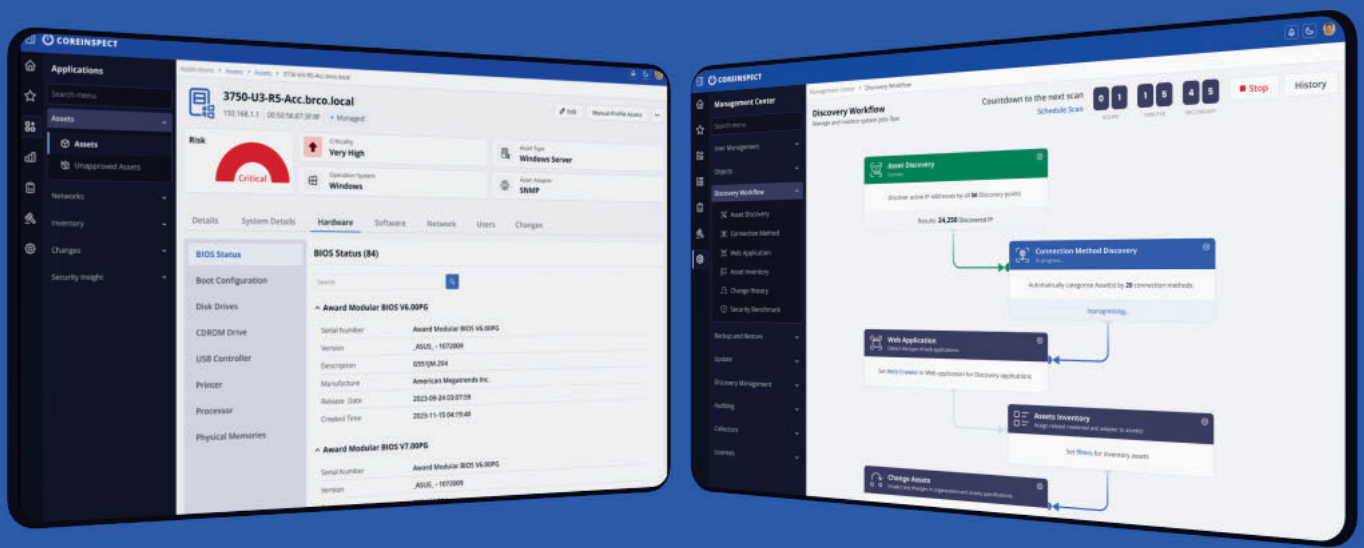
خـدمـات	پـایه	پیـشرفـته
پـشتیبـانی از طـریق تیکـت	✓	✓
پـشتیبـانی در زمـان اداری (۸x۵)	✓	✓
دسـتـرسی به پایـگاه دانـش (KB)	✓	✓
پـشتیبـانی جهـت رفـع باگ (مطابق SLA)	✓	✓
تـولید داشبـورد/گـزارش/پالیسی شخصی سـازی شده (مطابق SLA)		✓

پـشـتـیـبـانی پـایـه

این سطح از پشتیبانی که بصورت پیش فرض در فروش تمامی محصولات لحاظ می شود، صرفا در قبال رفع باگهای احتمالی سامانه ارائه می گردد. در پشتیبانی پایه ارائه سایر خدمات پس از فروش شامل تدوین داشبوردها، گزارشات و یا پالسی های شخصی سازی شده مستلزم محاسبه نفر/ساعت و پرداخت هزینه می باشد.

پـشـتـیـبـانی پیـشرفـتـه

این سـطح پـشتیبانی عـلاوه بـر رفـع مشـکلات سیـستمی (مطابـق SLAهای پشـتـیـبانی پایه)، شامل بـرخی خدمات پشتیبـانی شخصی سـازی شده میباشد.



Core Inspect
Cyber Security Asset Management

در مسیر امنیت در هر قدم کنار شما هستیم.

۰۲۱-۴۱۸۷۸۰۰۰

info@behinrahkar.com

https://behinrahkar.com/coreinspect

تهران خیابان کریمخان زند، خیابان استاد نجات الهی (ویلا)، کوچه رضا مقدسی (بیمه)، پلاک ۲۴

بهین راهکار
راهکارهای جامع امنیت فناوری اطلاعات