راد پژوهان ماندگار

اینترنت امن، بدون ریسک

سامانه کریدور

دسترسی امن به اینترنت برای سازمان‌های حساس

اینترنت بدون اتصال مستقیم



چالش و راهکار

چرا دسترسی مستقیم به اینترنت یک ریسک امنیتی است؟

تهدیدات رایج

- حملات فیشینگ و بدافزار
- نشت اطلاعات به خارج از سازمان
- آلودگی ایستگاه‌های کاری
- تهدیدات ناشی از کاربران داخلی
- عبور تهدیدات از کنترل‌های سنتی

سامانه کریدور با جداسازی کامل نشست اینترنت از ایستگاه کاری، امکان استفاده امن از اینترنت را بدون هیچ ارتباط مستقیمی فراهم می‌کند. کاربر تنها تصویر مرورگر ایزوله را مشاهده می‌کند و هیچ محتوای فعال اینترنتی وارد ایستگاه کاری نمی‌شود.

دسترسی با کریدور



مرورگر امن کانتینری



بدون ارتباط مستقیم



انتقال پیکسل بجای دیتا



مهار همه تهدیدات + محافظت سازمانی

امنیت واقعی بدون اتصال مستقیم

دسترسی سنتی



اتصال مستقیم اینترنت



ورود بدافزار و دور زدن کنترل‌ها با فیشینگ



نشت داده‌ها



تهدیدات داخلی

ریسک بالا برای سازمان

CORRIDOR

CORRIDOR
NETWORK ISOLATOR

معماری کریدور

سامانه کریدور، مبتنی بر مفهوم Zero-Trust و فناوری‌های جداسازی مرورگر (Browser Isolation)، Docker Container و پراکسی، توسعه و به بازار عرضه گردیده است. این راهکار، خطر مرور وب را به خارج از سازمان منتقل کرده و تمام تعاملات وب در کانتینرهای docker و در یک محیط ایزوله اجرا می‌شوند و تنها استریمی از تصاویر به مرورگر کاربر ارسال می‌شود.

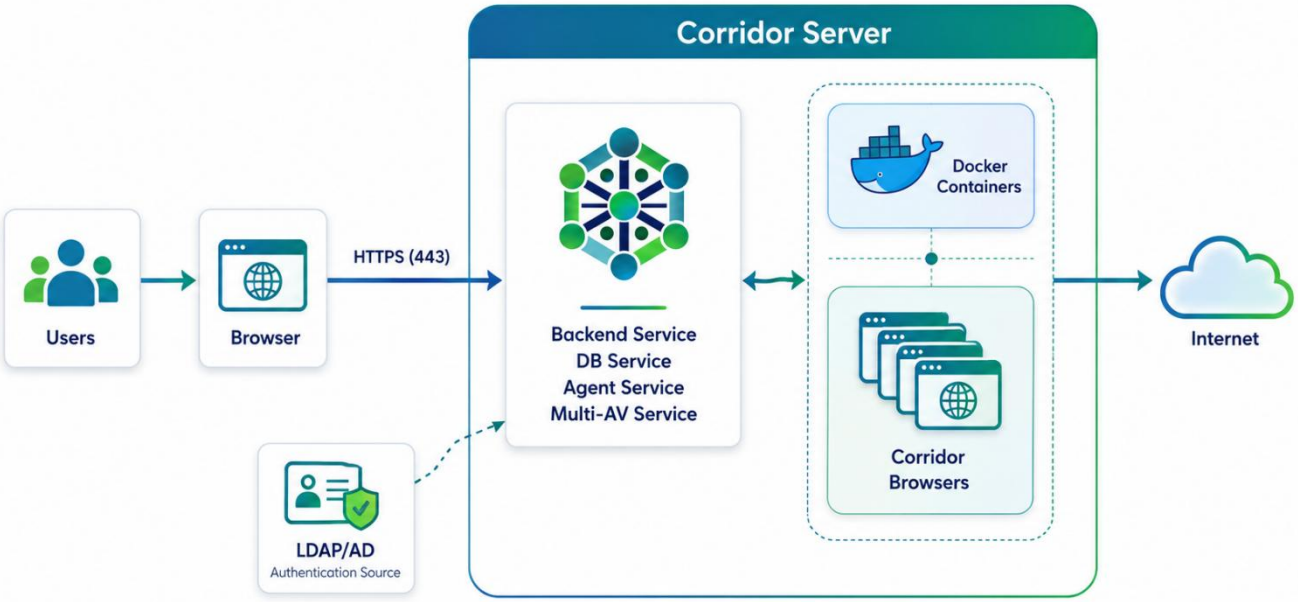
در حالت پیش فرض امکان انتقال فایل های دانلود شده توسط کاربر در محیط کریدور به کلاینت وی وجود ندارد. در صورت اجازه این امر طبق سیاست های امنیتی تعریف شده، پس از درخواست کاربر، ابتدا فایل توسط Multi-AV اسکن شده و در صورت نبود آلودگی، به کلاینت کاربر منتقل می شود.



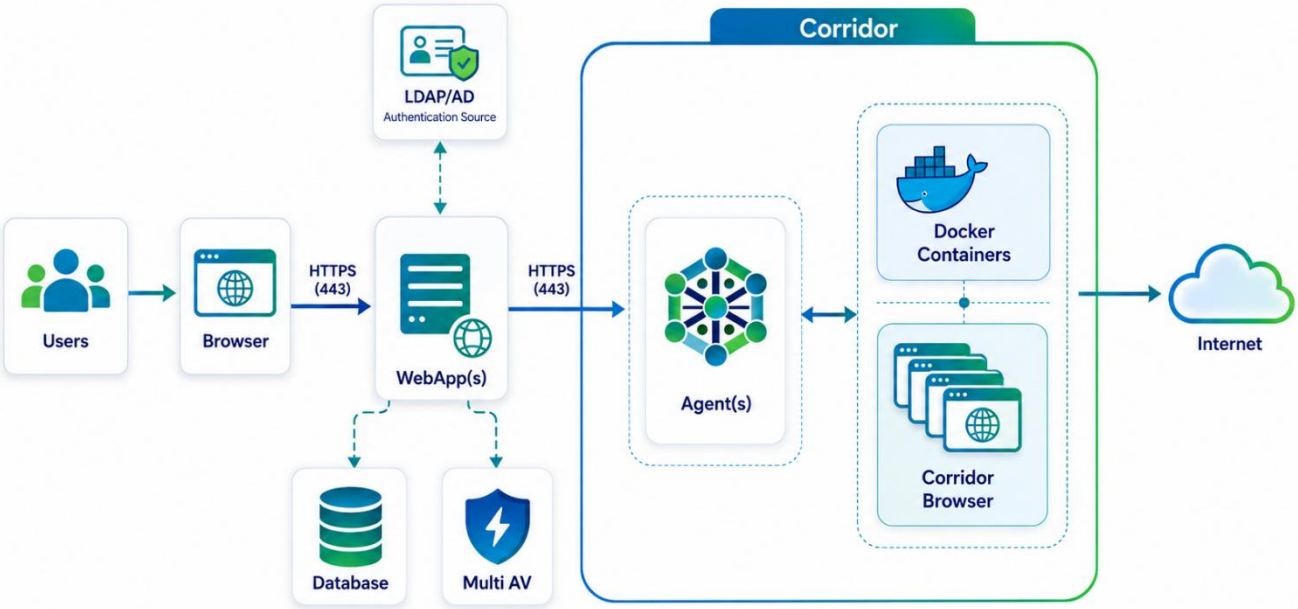


مدل استقرار

سامانه جداساز کریدور هم بر بستر فیزیکی و هم مجازی قابل پیاده سازی می‌باشد.
با توجه به پیاده سازی سامانه بصورت میکروسرویس، هم بصورت Single Server و هم Multi Server قابل استقرار می باشد.



معماری Single Server



معماری Multi Server

CORRIDOR

قابلیت‌های کلیدی کریدور

- پیاده سازی در بستر Container-Docker
- دسترسی به اینترنت در یک محیط ایزوله و امن
- قابلیت استفاده از انواع مرورگر
- اجرای بسیار سریع و آسان و بدون نیاز به تغییر در شبکه سازمان
- عدم نیاز به نصب افزونه مجزا در کلاینت کاربران
- واسط کاربری مبتنی بر فناوری های HTML5 و Websocket
- ارتباط کاربران تنها از طریق ارتباط امن و رمزگذاری‌شده توسط پروتکل TLS (HTTPS)
- امکان اکانتینگ بر مبنای حجم مصرفی، پهنای باند و مدت استفاده
- قابلیت کنترل فایل‌های دانلودی و آپلودی به تفکیک گروه کاربری بر مبنای MIME-Type، Extension و Size

- اسکن فایل‌های دانلود/ آپلود شده با استفاده از Multi-AV
- قابلیت مدیریت و کنترل وبکم، میکروفن و ...
- قابلیت واترمارکینگ
- امکان ضبط نشست
- قابلیت فیلترینگ وب مبتنی بر لیست سفید/سیاه
- امکان تعیین سطح دسترسی به کاربر
- امکان آنالیز فعالیت کاربران
- امکان گروه‌بندی کاربران و اعمال قوانین روی گروه‌ها
- مشاهده و کنترل لاگ های سیستم
- مدیریت بهینه منابع
- تعیین روزها و ساعات مجاز کاری
- تعیین آدرس‌های مجاز کاربران
- قابلیت احراز هویت دوعاملی TOTP

CORRIDOR

مزایای سازمانی و کاربردها



CORRIDOR

مزایای کلیدی

کاهش ریسک آلودگی
حفاظت از شبکه داخلی در برابر تهدیدات اینترنتی

کاهش هزینه سخت افزار
راهکاری مقرون‌به‌صرفه با اجرای سریع

مقیاس‌پذیری بالا
بدون تغییر در معماری موجود شبکه

مدیریت متمرکز
کنترل یکپارچه سیاست‌ها و کاربران

کیوسک انتقال فایل امن کنکاش

درگاه امن دریافت، بررسی و تحویل فایل به سازمان



راهکاری سازمانی برای کنترل، پایش و ایمن‌سازی
فایل‌های ورودی در محیط‌های حساس
مناسب برای بانک‌ها، مؤسسات مالی، بیمه‌ها، سازمان‌های دولتی و شرکت‌های دارای شعبه

امنیت سایبری سازمانی | استقرار آفلاین | معماری سرویس‌گرا

هر فایل ورودی می‌تواند یک نقطه نفوذ به سازمان باشد!



سازمان‌ها به‌طور مداوم فایل دریافت می‌کنند، از مشتریان، پیمانکاران، شعب و نهادهای بیرونی، این فایل‌ها اغلب از طریق USB، دیسک خارجی، CD/DVD، کارت حافظه یا از روشهای دیگری منتقل می‌شوند. بدون فرآیند بازرسی کنترل‌شده، فایل‌های مخرب می‌توانند نقطه ورود بدافزار، باج‌افزار و تهدیدات سایبری باشند.

- CD / DVD
- USB
- کارت حافظه
- ...

ورود فایل به سازمان باید مبتنی بر اصل عدم اعتماد باشد.

کنکاش چگونه از ورود فایل آلوده جلوگیری می‌کند؟

هر فایل ورودی از یک فرآیند بازرسی چندلایه و ایزوله عبور می‌کند.
هیچ فایل مشکوکی مستقیماً وارد شبکه سازمان نمی‌شود.



تمام رویدادها ثبت، امضای دیجیتال شده و قابل ردگیری هستند.

بازرسی چندلایه

ترکیب Multi-AV، Sandbox و YARA برای شناسایی تهدیدات شناخته‌شده و ناشناخته

پالایش محتوا (CDR)

حذف ماکروها و محتوای فعال از فایل‌های اداری پیش از تحویل

قرنطینه خودکار

فایل‌های مشکوک به‌طور خودکار ایزوله و برای بررسی امنیتی نگهداری می‌شوند

ردگیری کامل

ثبت هش فایل، زنجیره امضای دیجیتال و لاگ‌های تغییرناپذیر برای هر رویداد

قابلیت‌های امنیتی و عملیاتی

ترکیب چندین لایه دفاعی برای اطمینان از سلامت فایل‌های ورودی
از شناسایی تهدید تا مدیریت متمرکز سازمانی

بررسی چندلایه فایل‌ها

- موتورهای چندگانه آنتی‌ویروس
- تحلیل Sandbox
- شناسایی YARA

پاکسازی فایل‌ها (CDR)

- حذف ماکروها و محتوای فعال
- کاهش ریسک فایل‌های اداری
- Content Disarm & Reconstruction



کنترل انتقال فایل

- پردازش مبتنی بر Workflow
- مکانیزم تأیید چندمرحله‌ای
- سیاست‌های قابل تنظیم

ثبت و ردگیری

- لاگ‌های تغییرناپذیر
- ردگیری هش فایل
- زنجیره امضای دیجیتال

خروج ایمن فایل

- احراز هویت گیرنده با OTP قبل از دانلود
- لینک دانلود امن با TTL
- CDR + Metadata Stripping قبل از ارسال

مدیریت سازمانی

- مدیریت متمرکز داده های امنیتی
- مدیریت متمرکز سرویس و کاربران
- پشتیبانی از چند کیوسک

یکپارچگی و استقرار

- استقرار On-Premise
- به‌روزرسانی آفلاین
- یکپارچه‌سازی SIEM
- پشتیبانی AD / LDAP / SSO

مزایای سازمانی

هر فایل پیش از ورود به سازمان، بررسی، پالایش و اعتبارسنجی می‌شود

کاهش ریسک آلودگی

- جلوگیری از ورود فایل‌های مخرب
- کاهش احتمال انتشار بدافزار در شبکه



سازگاری فرابخشی

- بانک‌ها و مؤسسات مالی
- بیمه‌ها
- سازمان‌های دولتی
- مراکز خدماتی دارای مراجعه‌کننده
- زیرساخت‌های حیاتی

پشتیبانی از محیط‌های حساس

- استقرار آفلاین
- مناسب شبکه‌های تفکیک‌شده
- مدیریت متمرکز شعب

افزایش کنترل و شفافیت

- ثبت کامل فرآیندها
- قابلیت ممیزی و گزارش‌گیری

خدمات جامع لایسنسینگ

معرفی خدمات جامع لایسنسینگ و آپدیت محصولات Fortinet

مقدمه و معرفی راهکار

با توجه به چالش‌های موجود در تامین لایسنس‌های اورجینال تجهیزات امنیتی و همچنین محدودیت‌های ناشی از تحریم‌ها، دسترسی به آپدیت‌های مداوم و پایدار برای سازمان‌ها به یک دغدغه اساسی تبدیل شده است .مجموعه ما با تکیه بر دانش فنی تخصصی، موفق به پیاده‌سازی راهکاری جامع و بومی جهت **فعال‌سازی (لایسنسینگ)و دریافت بی‌وقفه آپدیت‌های تجهیزات امنیتی Fortinet**شده است.
این سند به منظور معرفی ابعاد فنی این راهکار نرم‌افزاری و خدماتی تهیه شده است تا همکاران و مشتریان گرامی با اطمینان خاطر از این سرویس بهره‌مند شوند.

محصولات تحت پوشش

- **راهکار ما تمامی تجهیزات پر کابرد شرکت فورتینت را در هر دو بستر سخت افزار و ماشین مجازی (Applince) به طور کامل پشتیبانی می کند (VM)**
- **فایروال های پیشرفته نسل جدید FortiGate (NGFW)**
- **فایروال های برنامه های کاربردی وب FortiWeb (WAF)**
- **راهکار های امنیت ایمیل سازمانی FortiMail**

ویژگی ها و مزایای کلیدی خدمات ما

- **عملکرد ۱۰۰٪ مشابه لایسنس اورجینال**

روش پیاده سازی ما به گونه‌ای است که دستگاه از نظر کارکرد، پایداری و اعمال پالیسی‌ها، هیچ‌گونه تفاوتی با زمانی که لایسنس مستقیم از خود شرکت Fortinetخریداری شده باشد، ندارد.

- **دریافت کامل و منظم آپدیت‌ها**

تمامی دیتابیس‌های امنیتی به صورت منظم و پایدار آپدیت می‌شوند، از جملهAntivirus & Anti-Malware :، سامانه جلوگیری از نفوذ (IPS)، Web Filtering & Application Control، Anti-Spamو سایر ماژول‌های فعال.

- **مقرون‌به‌صرفه و اقتصادی**

هزینه این راهکار در مقایسه با خرید لایسنس‌های دلاری اورجینال بسیار پایین‌تر بوده و توجیه اقتصادی بسیار بالایی برای سازمان‌ها و شرکت‌های همکار دارد.

- **پایداری و عدم وابستگی به تحریم‌ها**

خطر مسدود شدن دستگاه‌ها (Blockشدن) یا قطع شدن آپدیت‌ها به دلیل تحریم‌های بین‌المللی کاملا از بین رفته و آپتایم بالایی برای شبکه شما تضمین می‌گردد.

خدمات ویژه و منحصربه فرد

🔓 لایسنس‌گذاری دستگاه‌های بلاک‌شده (Blocked Devices)

یکی از بزرگ‌ترین مشکلاتی که سازمان‌ها با آن مواجه هستند، بلاک شدن سریال دستگاه توسط Fortinet است .دستگاه‌هایی که به هر دلیلی توسط شرکت سازنده بلاک شده‌اند، از طریق کانال‌های رسمی امکان دریافت لایسنس مجدد را ندارند و عملا از چرخه به‌روزرسانی خارج می‌شوند.

راهکار اختصاصی:

ما این محدودیت را برطرف کرده‌ایم .با استفاده از راهکار اختصاصی ما، دستگاه‌های بلاک‌شده نیز قابل لایسنس‌گذاری مجدد بوده و تمامی سرویس‌های امنیتی آن‌ها بدون هیچ محدودیتی فعال خواهد شد.

🔄 حذف پنالتی دستگاه‌های منقضی‌شده (Penalty Removal)

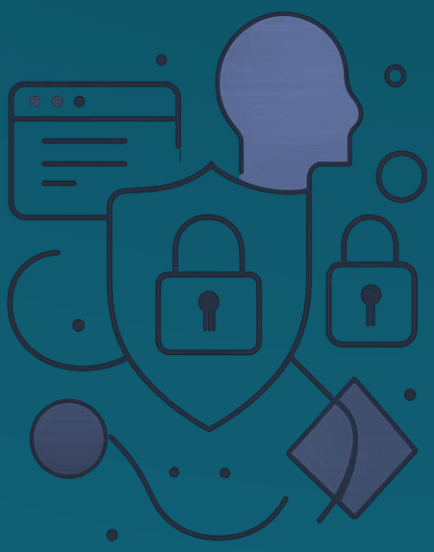
دستگاه‌هایی که پیش‌تر دارای لایسنس فعال بوده‌اند اما به دلیل عدم تمدید به‌موقع، لایسنس آن‌ها منقضی شده و مشمول پنالتی)جریمه (گردیده‌اند، معمولاً برای بازگشت به وضعیت عادی باید هزینه‌های سنگین پنالتی پرداخت کنند.

تضمین خدمات:

ما این پنالتی‌ها را کاملاً حذف می‌کنیم .دستگاه شما بدون نیاز به پرداخت هیچ‌گونه جریمه‌ای، با لایسنس کامل و بدون محدودیت به چرخه آپدیت و سرویس‌دهی بازمی‌گردد؛ درست مانند روز اول.

اینترنت امن، بدون ریسک

راهکاری مدرن برای دسترسی ایمن به اینترنت در سازمان‌هایی است که امنیت، پایداری و کنترل برای آن‌ها اولویت دارد.



برای درخواست دمو و PoC، با شرکت راد پژوهان ماندگار تماس بگیرید.

شرکت راد پژوهان ماندگار

۰۹۰۲۲۷۱۹۴۹۴

wwww.RPM-Power.ir