CYBERFENCE

Container Based Desktop Infrustracture

درباره ما

شرکت فنی و مهندسی توسعه امن آسا با حضور جمعی از متخصصان و نخبگان حوزه فناوری اطلاعات، به منظور ارائه راهکارهای جامع، حرفه‌ای و یکپارچه در زمینه امنیت فضای تبادل اطلاعات و پاسخ به نیازهای روزافزون کشور در حوزه تأمین امنیت سایبری تأسیس گردیده و در پردیس علم و فناوری دانشگاه یزد مستقر می‌باشد. این شرکت با تکیه بر عنایات الهی و دانش جوانان متخصص خود، گام‌های محکمی در زمینه طراحی و تولید محصولات بومی در حوزه امنیت سایبری برداشته است.

دنیای امروز . . .

دنیای اطلاعات است و امروزه زندگی افراد به گونه‌ای شکل گرفته است که در تمامی عرصه‌ها، چه در محیط‌های شخصی و چه در محیط‌های کاری در حال تبادل حجم بالایی از اطلاعات می‌باشند. مدیریت و راهبری سازمان‌های دولتی، تجاری و تولیدی در جهان امروز، منوط به مدیریت امن شبکه و دسترسی سریع و تبادل امن اطلاعات بین مشتریان و ذینفعان است، مدیریت موثر امور و رقابت با رقبا بدون دردسترس بودن آخرین اطلاعات امری بسیار مشکل و بعضا غیرممکن است. از این رو دسترسی به شبکه جهانی اینترنت، امری بدیهی و از نیازهای اساسی سازمان‌های امروزی است اما از طرفی استفاده بلاواسطه و توأمان از شبکه جهانی اینترنت و شبکه‌های داخلی و اختصاصی سازمان‌ها، امنیت تبادل اطلاعات را به مخاطره می‌اندازد و از اینروست که هر از گاهی اخبار گوناگونی مبنی بر سرقت یا از دست رفتن اطلاعات و داده‌های سازمان‌های مختلف از طریق اینترنت شنیده می‌شود.

از مهمترین چالش‌های پیش رو در رابطه با استفاده از اینترنت در سازمان‌ها می‌توان به مبحث تامین امنیت داده‌های سازمان، کاربران و ذینفعان سازمانی اشاره نمود که در این مستند قصد داریم به طور مختصر، جنبه‌های مختلف از محصولی را معرفی کنیم که توانسته است به کمک تکنولوژی‌های نوین، بستری امن برای استفاده از اینترنت در سازمان‌ها با حداقل ریسک، فراهم سازد، برای تیم فنی و مدیریتی توسعه امن آسا باعث افتخار است که در سایه‌ی عنایات الهی و به لطف تلاش‌های بی وقفه‌ی متخصصان دغدغه‌مند خود، موفق به ساخت محصولی کارا و بومی در این حوزه گردیده‌است.

راه‌کارهای دسترسی امن به اینترنت در سازمان

به طور کلی روش‌های پایش و مدیریت دسترسی به اینترنت در دو سطح قابل بررسی هستند :

- دسترسی مستقیم سیستم کاربر به اینترنت با استفاده از VPN
- جداسازی اینترنت از شبکه داخلی

در سطح اول سیستم کاربر قابلیت دسترسی مستقیم به اینترنت خواهد داشت و در صورت بروز آلودگی، انتقال و توزیع آن در سطح کلان در سازمان محتمل است.
این سطح بعلت فقدان حداقل لایه‌های حفاظتی، از کارایی لازم برای دستیابی به اینترنت امن برخودار نیست.

استراتژی کلی به منظور فراهم‌سازی بستر اینترنت امن در مجموعه‌ها، جداسازی اینترنت از اینترانت می‌باشد.

روش‌های جداسازی اینترنت از اینترانت به طور کلی به دو دسته فیزیکی و منطقی تقسیم بندی می‌شوند.

جداسازی فیزیکی اینترنت از اینترانت

در روش جداسازی فیزیکی، یک شبکه‌ی کاملا تفکیک شده صرفا به منظور دسترسی به اینترنت در نظر گرفته می‌شود. سازمان باید به منظور دسترسی کاربرانش به اینترنت بسته به طراحی شبکه و سایر ویژگی‌های فیزیکی ساختمانی که در آن مستقر شده، تعدادی سیستم مجزا به صورت متمرکز و صرفا به منظور دسترسی به اینترنت در بخشی از مجموعه‌ی خود قرار بدهد، یا اینکه در صورت امکان برای کاربرانی که نیاز به اینترنت دارند یک سیستم مجزا مختص دسترسی به اینترنت، تهیه، راه‌اندازی و در محدوده‌ی کاری هر فرد جایگذاری کند.

از چالش‌های جداسازی فیزیکی می‌توان به موارد زیر اشاره نمود:

- تحمیل هزینه‌های هنگفت برای سازمان
- عدم امکان پیاده‌سازی در بسیاری از سازمان‌ها به دلیل نبود زیر ساخت لازم
- چالش جابه‌جایی فایل از اینترنت به شبکه داخلی و مخاطرات امنیتی مرتبط با این امر
- امکان گسترش آلودگی سیستم‌های متصل به شبکه با آلودگی حداقل یک سیستم

جداسازی منطقی اینترنت از اینترانت

روش‌های جداسازی منطقی عموما شامل: Vlaning, MS-Virtual App, Terminal Service, Container می‌شوند.
در صورت بررسی روش‌های نامبرده با معیارهای امنیتی، ناکارآمدی اکثر این روش‌ها بیش از پیش مشخص می‌شود، چرا که در صورت استفاده از این روش‌ها با چالش‌های امنیتی اساسی نظیر: آسیب‌پذیری‌های پروتکل RDP، وجود ارتباط میان سیستم اتصال یافته به اینترنت با شبکه داخلی سازمان، امکان بروز آلودگی گسترده در سازمان و موارد دیگر مواجه خواهیم شد.

جداسازی بر مبنای Container

براساس مستندات ابلاغ شده از سوی مرکز مدیریت راهبردی افتا، صرفا روش‌های مبتنی بر Container، مورد تایید می‌باشند زیرا نحوه کار به گونه‌ای است که برنامه در محیطی ایزوله خارج از شبکه داخلی سازمان اجرا می‌شود و با هر بار اتمام نشست کاربر، Session به طور کامل حذف می‌گردد از این رو در صورت آلوده‌شدن نشست، سازمان در معرض خطر قرار نخواهد گرفت و صرفا تصاویر رندر شده از پردازش برنامه، به شبکه داخلی سازمان راه پیدا خواهند کرد.

معماری RBDI

استفاده از تکنولوژی RBI (Remote Browser Isolation) و RDI (Remote Desktop Isolation) به منظور جلوگیری از حملات سایبری و تقویت امنیت اطلاعات بسیار حائز اهمیت است. این تکنولوژی بر اساس فناوری‌های مبتنی بر Container، فعالیت‌های مرور کاربران را در محیطی ایزوله (Sandbox) و خارج از شبکه داخلی سازمان، قرار می‌دهد.

CYBERFENCE RBDI

سامانه اینترنت امن CYBERFENCE RBDI به عنوان راهکار مورد تأیید افتا به منظور جداسازی شبکه‌های ناهمگون شناخته می‌شود، یک اقدام امنیتی است که اجرای تمام فعالیت‌های روزمره کاربران را در یک کانتینر ایزوله، محدود می‌کند. این عمل sandboxing، مرور اینترنت داده‌ها، دستگاه‌ها و شبکه‌ها را در برابر انواع تهدیدات ناشی از اینترنت و سایت‌های آلوده محافظت می‌کند.

این سامانه با وجود مصرف حداقلی منابع، کارایی مطلوب و ایمنی را برای سازمان به ارمغان می‌آورد.

CYBERFENCE
ASA GROUP

مزایای سامانه CYBERFENCE-RBDI

محافظت از داده های سازمان

در بسیاری از حملات مخرب، نفوذ به سیستم عامل، به‌واسطه‌ی نشست‌های کاربری رخ می‌دهد. تکنولوژی RDI و RBI سبب می‌شوند تا کاربران در محیطی ایزوله و خارج از شبکه داخلی سازمان به نشست‌ها دسترسی داشته باشند، از این رو سازمان در برابر بخش عمده‌ای از حملات مخرب مانند: حملات Phishing، اسکریپت‌های مخرب، باج‌افزارها و ... ایمن می‌ماند.

کنترل دقیق و حفظ محرمانگی

امکان کنترل دقیق تبادل اطلاعات، میان شبکه داخلی و محیط ایزوله توسط سامانه CYBERFENCE-RBDI فراهم می‌شود بدین صورت که امکان انتقال فایل‌های مهم تعیین شده مانند اسناد کاری و ... برای هیچ کاربری بدون اعطای دسترسی مربوطه امکان پذیر نخواهد بود.

طراحی استاندارد و مهندسی

سامانه بر اساس اصل (Zero Trust Network Architecture) ZTNA طراحی و تولید شده‌است از این رو به منظور پیشگیری از نشت اطلاعات و بروز حوادث نامطلوب، برای هر کاربر، حداقلِ دسترسی، صرفا به منظور انجام امور مجاز مربوطه، اعطا می‌شود.

سهولت در عین کارایی

هزینه هنگفت و ارتباط‌گیری سخت کاربران با روش‌های متداول جداسازی، سبب فدا شدن امنیت در سازمان‌ها شده است. سامانه CYBERFENCE-RBDI با ارائه یک رابط کاربری تحت وب، محیطی امن و آسان برای دسترسی به اینترنت فراهم می‌سازد.

کاهش هزینه‌ها

سامانه CYBERFENCE-RBDI برای اجرای برنامه‌های هدف نیازی به راه‌اندازی بسترهایی با مصرف منابع بالا ندارد و برنامه در بستر Container اجرا می‌شود ، از این رو نیاز به تامین منابع، کاهش یافته و در نتیجه هزینه‌های سازمان به منظور تامین و نگهداری سخت‌افزار کاهش می‌یابد.

ارتقاء سطح امنیت

صرفا مجموعه‌ای از پیکسل‌ها هستند که به منظور ساخت جلوه بصری برای کاربر به شبکه داخلی سازمان راه می‌یابند از این رو نگرانی‌ها از بابت تهدیدات Zero Day به حداقل می‌رسد چرا که برنامه‌های مورد نیاز کاربران بر روی محیطی ایزوله خارج از شبکه داخلی سازمان اجرا می‌شوند و Container مربوطه بلافاصله پس از اتمام استفاده از بین خواهد رفت، بنابرین آسیب‌پذیری‌های برنامه‌ها، نمی‌توانند یک تهدید برای سازمان محسوب شوند.

ویژگی‌های سامانه

- قابلیت اجرا Virtual APP و Full Desktop مبتنی بر لینوکس
- قابلیت اجرا Virtual APP و Full Desktop مبتنی بر ویندوز
- Full Media Support (WebCam, Microphone, Audio, ScreenShare)
- قابلیت اتصال به انواع سامانه احراز هویت مرکزی (ActiveDirectory)
- قابلیت اضافه کردن نرم‌افزارهای مورد نیاز سازمان به سامانه
- پشتیبانی از احراز هویت چند عاملی مبتنی بر توکن سخت‌افزاری
- قابلیت مشاهده و گزارش‌گیری از لاگ‌های سیستمی

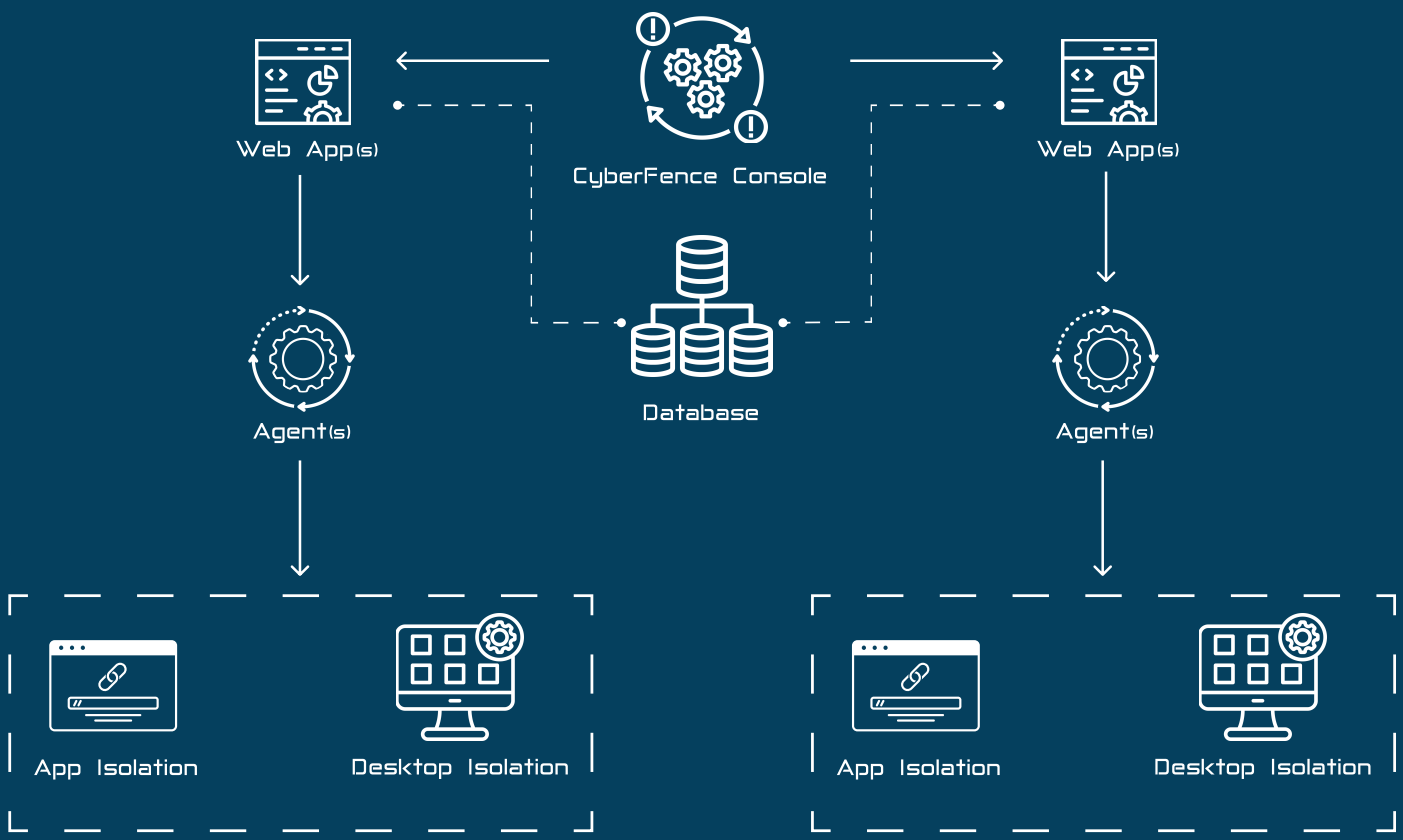
- ☑ قابلیت مشاهده و گزارش‌گیری از فعالیت مرور کاربران
- ☑ قابلیت زون‌بندی و تفکیک شبکه کاربران بر اساس پروفایل‌های کاربری به منظور اعمال سیاست‌های مبتنی بر ZTNA
- ☑ قابلیت ارسال لاگ سامانه به سرور مدیریت لاگ (Syslog Server | SIEM)
- ☑ قابلیت مدیریت پهنای باند ورودی و خروجی کاربران (Bandwidth Shapping)
- ☑ قابلیت مدیریت مدت زمان استفاده از سامانه براساس گروه‌های کاربری (Time Shapping):
  - پیاده سازی بدون وابستگی به نرم افزارهای جانبی
  - پشتیبانی از Suspended و Immediately Destroy
- ☑ قابلیت IP Restriction و Time Restriction براساس گروه‌های کاربری
- ☑ قابلیت بررسی فایل‌ها توسط چندین موتور ضد ویروس آفلاین و آنلاین (MAV Support):
  - KasperSky
  - ClamAV
  - ESET Server Security
  - AFTA Malicious DB
- ☑ قابلیت پیاده‌سازی به صورت توزیع‌شده:
  - ACTIVE / ACTIVE
  - ACTIVE / PASSIVE
- ☑ قابلیت شخصی‌سازی Image های سامانه (تعیین افزونه‌های مجاز و غیرمجاز و ...)
- ☑ قابلیت ذخیره اطلاعات نشست‌های کاربری بر اساس پروفایل‌های کاربری (تاریخچه جستجوها، Bookmark و سایر تنظیمات)
- ☑ قابلیت Printer Redirection

- قابلیت انتقال دیوایس‌های جانبی از سیستم کاربر به محیط ایزوله
- قابلیت AutoBackup و SyncBackup به صورت BuiltIn
- قابلیت کنترل و محدودسازی مرور کاربران در فضای اینترنت بر اساس:

  - MIME Filtering
  - URL Filtering
  - Regex Filtering
  - Content Size

- قابلیت اتصال خودکار به انواع سامانه‌های اکانتینگ:

  - Sophos
  - pfSense
  - KerioControl
  - Mikrotik
  - IBSNG
  - APKGate



Fence Policy Module

ماژول Fence Policy، یک ابزار قدرتمند است که امکان مدیریت و کنترل ترافیک وب را فراهم می‌سازد. این ماژول، با ارائه قابلیت‌های پیشرفته فیلترینگ و دسته‌بندی، به مدیران این امکان را می‌دهد تا بر اساس سیاست‌ها و محدودیت‌های تعیین شده در سازمان، محتوای مد نظر را مدیریت نمایند، همچنین الگوریتم‌های پیشرفته ماژول Fence Policy قادر هستند به طور دقیق، محتواهای غیرمجاز را شناسایی و مسدود نمایند، در نتیجه سطح امنیت و حریم خصوصی کاربران ارتقاء می‌یابد. با پیاده‌سازی این ماژول در سازمان، ریسک‌های مربوط به حملات سایبری و نفوذهای ناخواسته به سیستم‌های داخلی به شدت کاهش یافته و این امکان برای مدیران فراهم می‌شود تا به طور کامل و مؤثر، ترافیک وب را کنترل و مدیریت نمایند.

- URL Filtering (امکان ایجاد محدودیت بر اساس لیست دامنه‌های مخرب سازمان افتا و پروفایل‌های کاربری)
- MIME Filtering (ایجاد محدودیت بر اساس ماهیت فایل)
- Regex Filtering
- Content Filtering

SSO & SLO Module

Single SignOn (SSO) و Single LogOut (SLO) دو راهکار هوشمند در حوزه امنیت و مدیریت هویت می‌باشند.
SSO مکانیزمی است که به کاربران اجازه می‌دهد، تنها با یکبار ورود به سیستم، به صورت خودکار و بدون نیاز به وارد کردن مجدد اطلاعات کاربری، به سایر سامانه‌های اکانتینگ نیز دسترسی پیدا کنند. این رویکرد، علاوه بر فراهم ساختن امکان دسترسی سریع و آسان کاربران به منابع، در کاهش ریسک‌های امنیتی مانند فراموشی رمز عبور نیز نقش بسزایی دارد.
SLO به عنوان یک تکمیل‌کننده مهم برای SSO، به کاربران امکان می‌دهد تا با خروج از سیستم، همزمان از تمام سیستم‌های اکانتینگ مرتبط نیز خارج شوند. این عملیات خروج همزمان و یکپارچه، تضمین می‌کند که دسترسی غیرمجاز به منابع بعدی برای کاربران امکان پذیر نباشد .

Activity Ingestion Module

URL Ingestion و Malicious Tracking، دو عنصر کلیدی در زمینه امنیت و حفاظت از اطلاعات در فضای دیجیتال هستند.
URL Ingestion به عنوان یک فرایند خودکار، به سامانه اجازه می‌دهد تا URLها را به صورت خودکار دریافت کند و آنها را مورد بررسی و پردازش قرار دهد. این رویکرد نه تنها به سازمان‌ها امکان می‌دهد تا از مقصد کاربر مطلع گردند، بلکه همچنین در تحلیل و بررسی جریان ترافیک، شناسایی تهدیدات امنیتی و حفاظت از کاربران نقش حیاتی ایفا می‌کند.
Malicious Tracking به عنوان یک فرایند هوشمند، به سامانه اجازه می‌دهد تا مسیر فایل های مخرب را به صورت خودکار رهگیری نموده و آنها را مورد بررسی و پردازش قرار دهد. این رویکرد نه تنها به سازمان‌ها این امکان را می‌دهد تا از لینک دانلود فایل‌های مخرب مطلع گردند بلکه در ترکیب با Fence Policy از دانلود مجدد این فایل‌های مخرب جلوگیری می‌کند.

پازل امنیت را چیده‌ایم . . .

توسعه امن آسا

یزد، صفائیه، بلوار دانشگاه، دانشگاه یزد، مرکز فناوری و نوآوری ۲، واحد ۶۰۳

تلفن تماس: ۰۳۵-۳۸۳۰۹۳۷۰

کد پستی: ۸۹۱۵۸۱۳۱۸۰

info@asa-group.net

www.asa-group.net