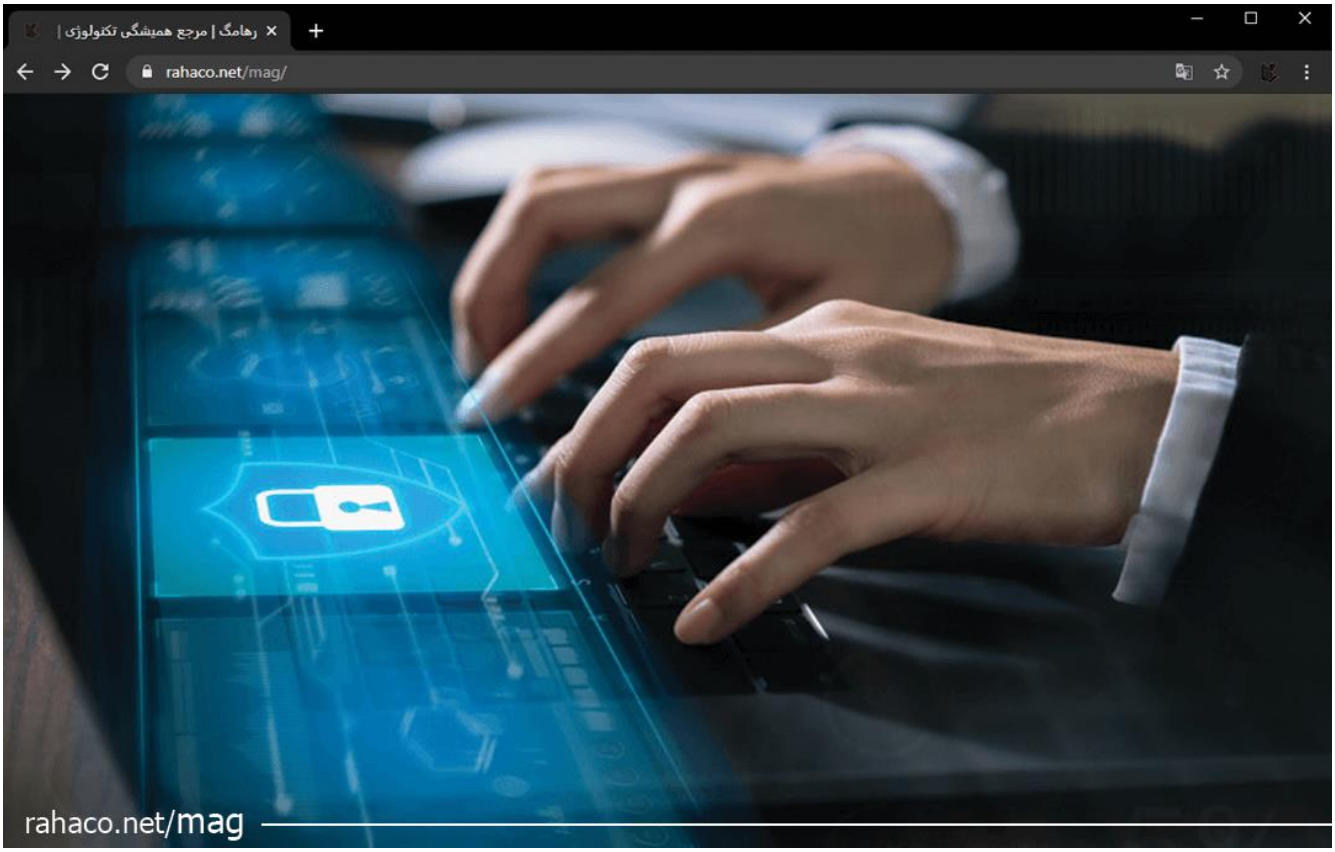
اطلاع از ویژگی های امنیتی سامانه دورکاری رها!

مجموعه شرکت‌های دانش بنیان رها

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



فهرست:

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

طیف گسترده ای از محصولات سیتریکس

محصولات سیتریکس طیف گسترده ای از ویژگی های امنیتی دورکاری و قابلیت ها را برای تامین و تضمین امنیت اپلیکیشن ها و داده ها در زیرساخت های Citrix Virtual Apps and Desktops ارائه می‌دهند.

این قابلیت ها به طور ویژه زمانی اهمیت پیدا می‌کنند.

که زیرساخت Citrix Virtual Apps and Desktops در سازمان ها و واحدهای دولتی، مالی و درمانی پیاده سازی شوند.

به عبارتی در جایی که امنیت به طور اساسی مورد توجه قرار دارد و یک الزام برای سازمان در نظر گرفته می‌شود.

این داکیومنت در واقع یک بررسی اجمالی و راهنمایی در رابطه با پیکربندی محیط های سیتریکسی برای کاهش تهدیدات امنیتی و تطابق یافتن با استانداردهای امنیتی، ارائه می‌دهد.

حوزه و موارد کاربرد(Scopes and Use Cases)

سیتریکس راهکارها و مدل های گوناگون لایسنس، مرتبط با زیرساخت هایی که در محل مشتری پیاده سازی شده اند.

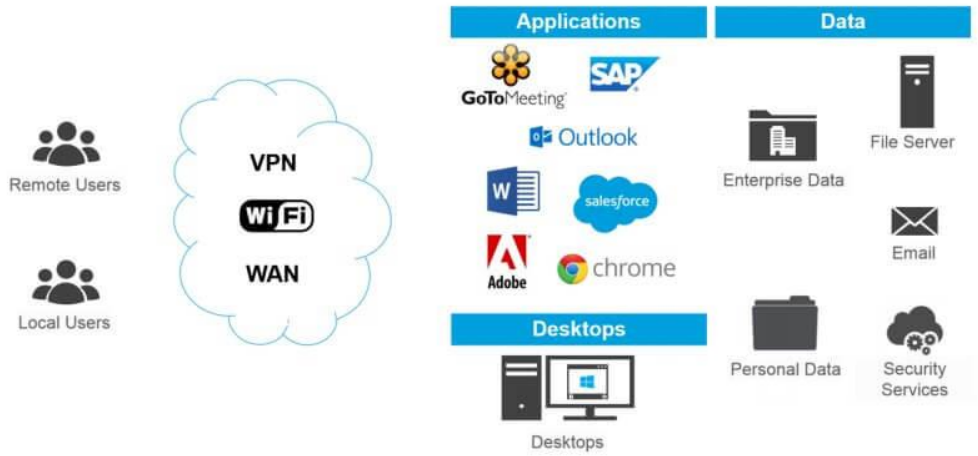
یا زیرساخت هایی که در Cloud مدیریت می‌شوند، ارائه می‌دهد.

این داکیومنت راهنمایی های امنیتی برای راهکارهای سیتریکسی که در محل مشتری پیاده سازی شده اند را ارائه می‌دهد. و نه راهکار ابری سیتریکس!

کاربرد اصلی این داکیومنت در واقع زیرساختی است.

که به کاربران لوکال و همچنین کاربران از راه دور امکان دسترسی به منابع منتشر شده (دسکتاپ ها و اپلیکیشن ها) را که در محل مشتری میزبانی و مدیریت می‌شوند ،می‌دهد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



مخاطبین

این داکیومنت به منظور پاسخ‌گویی به نیازهای متخصصین امنیتی، مدیران سیستم و مشاورینی که مسئول طراحی، پیاده سازی و تامین امنیت زیرساخت های سیتریکسی هستند، طراحی شده است.

چالش ها و روندهای امنیتی در دورکاری

در سال های اخیر موارد بسیار زیادی از نقض امنیت و حملات امنیتی رخ داده است.

بنابراین تأکید بر لزوم درنظر گرفتن امنیت در مرحله طراحی به منظور نظارت مداوم و پاسخ‌گویی به تهدیدات امنیتی و سازگاری و قوی تر کردن محیط بر این اساس می‌باشد.

به طور قطع، محافظت از داده های حساس و دارایی های فکری امری ضروری است.

امنیت، با افزایش کار از راه دور و محیط کار متحرک و موبایل، از جمله ورود سبک های کاری آوردن دستگاه خود به محیط کار(BOYD) ، روز به روز به مبحثی پیچیده‌تر تبدیل می‌شود.

نتیجه دستگاه های غیرقابل کنترل و یا ناشناخته است که به منابع دسترسی دارند.

با ظهور و استفاده از انواع بیشتری از دستگاه ها (از جمله دستگاه های تلفن همراه، تبلت ها و دستگاه های متصل به اینترنت) و انواع شبکه های دیگر(

مانند ۳ G / 4G، Wi Fi و (Bluetooth پیچیدگی امنیتی افزایش می‌یابد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

نظارت، شناسایی و پاسخ‌گویی به رخنه های امنیتی یک چالش مهم و اساسی برای اطمینان از تداوم تجارت‌ها و امنیت منابع است.

علاوه بر این، بسیاری از بخش‌های سازمانی بر برخی اعتبارسنجی یا انطباق امنیتی اصرار دارند.

به عنوان مثال، برای پیاده سازی محصولات Citrix در محیط های فدرال ایالات متحده، پیاده سازی باید مطابق با FIPS باشد.

محصولات Citrix ویژگی های امنیتی دورکاری

و گزینه های امنیتی قابل توجهی برای کمک به محافظت از داده های حساس و دارایی های فکری، اطمینان از استمرار تجارت و کمک به سازمان‌ها در رعایت استانداردهای امنیتی ارائه می دهد.

این داکیومنت راهنمایی و توصیه هایی را برای کمک به طراحی و مدیریت زیرساخت Citrix به شما ارائه می‌دهد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

Product	TLS 1.2 support
NetScaler - version 11.0	Yes *
NetScaler - version 11.1	Yes
StoreFront - version 3.5	Yes
Windows Virtual Desktop Agent - version 7.6	Yes
Linux Virtual Desktop Agent	No
Receiver for Windows	Yes
Receiver for Linux - ARM - version 13.2	Yes
Receiver for Linux - x86 - version 13.2	Yes
Receiver for Mac	Yes
Receiver for iOS	Yes
Receiver for Android - version 3.7	Yes
Receiver for Chrome	Yes
Receiver for HTML5	Yes
Receiver for Windows 10 Mobile	No

ملاحظات امنیتی دورکاری در زیرساختCitrix Virtual Apps and Desktops

ویژگی امنیتی دورکاری زیادی در هنگام طراحی و پیاده سازی Citrix Virtual Apps and Desktops وجود دارد.

این نمودار حوزه های امنیتی اصلی در زیرساخت مورد نظر را نشان می‌دهد

که به حصول اطمینان از محرمانه بودن، یکپارچگی و در دسترس بودن منابع کمک می کند.

برای اطمینان از امنیت، یکپارچگی و تداوم تجارت، باید نوع مدیریت و کنترل فناوری اطلاعات، مدیریت ریسک و استراتژی انطباق خود را تعیین کنید.

استراتژی شما باید شامل ارزیابی ریسک های امنیتی، رویه ها، روندها، آموزش و آگاهی باشد.

جامعیت و محرمانه بودن اطلاعات ضروری است.

رمزنگاری مناسب، تقسیم بندی کاربران (User Segmentation) و دسترسی به منابع و مدیریت مکان داده ها، به فراهم آوردن سازگاری و تطابق بیشتر، قابلیت اجرایی بیشتر و نیز اعتبار بیشتر کمک می‌کند.

با محدود کردن دسترسی به داده ها و انتقال ها به دستگاه های کاربران، می‌توانید در مقابل از دست رفتن داده ها در خارج از شبکه سازمان محافظت کنید.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

به عنوان مثال، کارمندانی که به مسافرتی کاری رفته اند ممکن است لپ تاپ خود را گم کنند

(به عنوان مثال در یک تاکسی)، یا اینکه دستگاه آنها در مرز توقیف شود

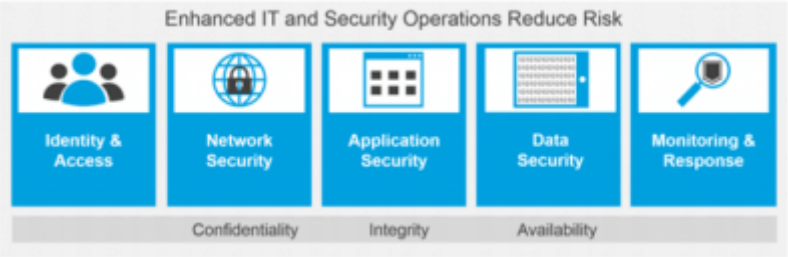
بنابراین شما می‌توانید داده های این دستگاه ها را محدود و از آنها محافظت کنید.

شما می توانید حریم خصوصی را کنترل و پیکربندی کنید تا هم سازمان و هم کاربران سیستم سود ببرند.

حوزه های کلیدی، که در نمودار نشان داده شده است

به شما کمک می کند، پیاده سازی زیرساخت خود را بهینه کرده، خطرات امنیتی را کاهش داده

و به استراتژی امنیتی و مطابقت مورد نظر خود دست یابید.



هویت و دسترسی(Identity and Access)

مدیریت هویت و کنترل دسترسی ای که به خوبی طراحی شده باشد

مشخص می‌کند که چه کسی می تواند به منابع دسترسی داشته باشد،

احراز هویت آنها چگونه انجام می‌شود

و پس انجام احراز هویت، منابع موجود و سطح دسترسی که به هر کاربر اعطا می شود را تعیین می‌کند.

هویت و دسترسی یک اصل مهم از ویژگی امنیتی دورکاری، برای همه انواع حساب‌ها از جمله کاربران عادی،

مدیران سیستم و حساب های مربوط به سرویس دهندگان است.

مزایای استفاده از یک استراتژی Identity and Access صحیح شامل دسترسی ایمن و کنترل شده به منابع به

وسیله دستگاه های شخصی است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

به عنوان مثال، هنگامی که کارمندان از راه دور کار می‌کنند.

و یا کارمندان دستگاه های خود را به سازمان می‌آورند) و یا زمانی که با غیر کارمندان سر و کار داریم.به عنوان مثال پیمانکاران، شرکا، تأمین کنندگان و دانشجویان!

احراز هویت در زیرساخت هایی با مقیاس وسیع با فراهم آوردن یک URL مشترک برای ورود به سیستم و دسترسی به منابع مورد نیاز و مرتبط ،بسیار ساده شده است.

امنیت شبکه(Network Security)

به جهت اطمینان از اینکه ترافیک شبکه درطول پیاده سازی زیرساخت، امن و رمزنگاری شده باشد.

یعنی از امنیت دستگاه های کاربر گرفته تا سرورهای میزبان منابع و داده ها، امنیت مناسب شبکه الزامی است.

همچنین ممکن است نیاز باشد که نوع و سطح امنیت شبکه مورد نیاز، مطابق با استانداردهای خاص باشد.

برای مثال باید اطمینان حاصل کنید که رمزنگاری end-to-end TLS و نیز لیست های کنترل دسترسی ویژه شبکه (Access Control Lists (ACLs))را دارید.

امنیت اپلیکیشن‌ها(Application Security)

تهیه، میزبانی و نظارت بر برنامه ها باید به گونه ای طراحی شود که برنامه ها فقط در صورت نیاز برای کاربران مناسب در دسترس باشند.

و در صورت نیاز در بین چندین سرور میزبانی شوند تا خطرات امنیتی به حداقل برسد.

امنیت برنامه های کاربردی ازدیگر ویژگی امنیتی دورکاری، می تواند با استفاده ازApplication Policy ها فعال شود.

به جهت اطمینان از اینکه برنامه ها فقط به منابع مورد نیاز در شرایط بخصوص دسترسی داشته باشند.

شما می توانید برنامه ها را در سیلوهای مناسب میزبانی کنید و از ابزارهای شخص ثالث برای جلوگیری از رخنه امنیتی بین برنامه ای استفاده کنید.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

امنیت اطلاعات(Data Security)

محافظت از داده ها از برتری ها و ویژگی های مهم Citrix Virtual Apps and Desktops است.

بطوری که داده ها در دیتاسنتر محافظت می‌شوند.

امنیت داده ها را می توان از طریق پیکربندی کانال های مجازی سیتریکس (Citrix virtual channels) ،

Windows Policiesو ابزارهای شخص ثالث تقویت کرد.

سیاست های امنیتی داده ها اطمینان می‌دهند که داده های حساس در مراکز داده نگهداری می‌شوند.

و نه بر روی دستگاه های شخصی کاربران و نیز دسترسی به منابع و داده های حساس را به ازای هر برنامه محدود می‌کنند.به عنوان مثال، Policyها فقط به بعضی از کاربران و دستگاه ها امکان دسترسی به داده ها و برنامه های حساس مانند داده های حقوق و دستمزد را می‌دهند.

شما می توانید سیاست های مربوط به اعتبارسنجی و کنترل دستگاه کاربران endpoint validation and)

(controlرا فعال و پیکربندی کنید.تا از دسترسی ای که صحت و امنیت آن توسطPolicy ها تایید شده است.

و نیز از امکان مدیریت داده های باقیمانده اطمینان حاصل کنید.و سطح دسترسی به درایوهای دستگاه های کاربران و لوازم جانبی دیوایس های آنان را تعریف، محدود و کنترل کنید.

نظارت و پاسخگویی(Monitoring and Response)

نظارت اصلی مهم و اساسی از ویژگی های امنیتی دورکاری، برای شناسایی ریسک های امنیتی و استراتژی ارزیابی شما است.

نظارت به شما این امکان را می دهد که کاربرد، سازگاری، بهینه سازی و امنیت برنامه ها را تعیین کنید.

بر اساس گزارش ها وlog ها، رویدادها و هشدارها، می توانید به صورت پیش‌گیرانه و فعال، خطرات امنیتی را شناسایی کرده و به آنها پاسخ دهید.

نظارت بر مسائل مربوط به امنیت، شما را قادر می سازد.

وضعیت زیرساخت خود را بررسی کنید و رویدادها یا مسائل غیرمعمول را شناسایی کنید.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

دسترسی Access -	هویت Identity -	نوع حساب کاربری
کاربران قادر به دسترسی به منابع منتشر شده مناسب ، براساس امتیازات خود هستند.	احراز هویت، همانطور که توسط مدیر سیستم تعریف شده است. احراز هویت مورد نیاز متناسب با محیط شما تنظیم شده است) به عنوان مثال، ممکن است two-factor authentication لازم باشد(	کاربر معمولی User
سرپرستان معمولاً از داخل شبکه، دسترسی مستقیم به ابزارهای مدیریتی و کنسول‌ها دارند. همراه با دسترسی به منابع و داده های حساس امنیتی.	احراز هویت برای ایجاد دسترسی به ابزارهای مدیریتی و کنسول‌ها.	مدیر سیستم Administrator
امتیازات ویژه جهت دسترسی به برنامه ها، منابع و اسکریپت ها	حساب کاربری اتوماتیک سرویس دهندگان که توسط برنامه ها یا فرآیندهای خاص استفاده می شود. احراز هویت مختص هر برنامه.	Service Account

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

قابلیت‌ها و توصیه‌های امنیتی درCitrix Virtual Apps and Desktops

محصولات Citrix بسیاری از ویژگی‌های امنیتی دورکاری را ارائه می‌دهند.

که می توانند متناسب با محیط، الزامات، ارزیابی ریسک‌ها و سازگاری محیط شما پیکربندی شوند.

شما باید شرایط و نیازمندی‌های امنیتی خود را مرور کرده

و محصولات و ویژگی‌های سیتریکسی را مطابق با آنها پیکربندی کنید.

امنیت باید در فاز برنامه‌ریزی یک مورد اساسی باشد.

پیکربندی، آزمایش و تصحیح کردن زیرساخت و نحوه پیاده سازی در یک محیط و برنامه‌ریزی

و پیش‌بینی برای هر فاز، قبل از اجرای پروژه و پیاده‌سازی زیرساخت، بسیار توصیه می‌شود.

برای اطمینان از کاهش تهدیدات امنیتی، نظارت مستمر، بازرسی و ارزیابی زیرساخت شما نیز ضروری است.

سیتریکس موارد زیر را برای طراحی و پیاده سازی امنیت جهت مقابله با چالش‌ها و تهدیدات امنیتی توصیه می‌کند.

هویت و دسترسی(Identity and access)

برای تعیین هویت و نیازهای دسترسی، در مورد نیازمندی های هر نوع حساب کاربری، تعریف هویت، احراز هویت و حق دسترسی و امتیازات را در نظر گرفته و تأیید کنید.

هر نوع حساب کاربری چالش های متفاوتی را ارائه می‌دهد و بنابراین به پیکربندی دسترسی Identity و Accessخاص نیاز دارد.

زیرساخت نماینده(Representative deployment)

ساختار زیر، نمونه ای از یک ساختار سیتریکسی است که برای مطابقت با دستور العمل های مفصل در این داکیومنت طراحی شده است.

این ساختار شامل(Citrix Workspace App) Citrix Receiver ، Citrix Gateway، StoreFront، Citrix Virtual Apps and Desktops (Delivery Controller and VDA)می‌شود.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

برای سادگی، تنها یک Delivery Controller و VDA نمایش داده شده است.

این ساختار بر اساس خدمات بلند مدت XenApp و7.6 XenDesktop منتشر شده است.

با این حال، این ساختار شامل StoreFront 3.5 می شود؛ زیرا این امر، امکان رمزگذاری ترافیک شبکه را با استفاده از TLS 1.2 امکان پذیر می کند.

NetScaler Gateway MPX 11.0 (با استفاده از سخت افزار (Cavium 2.2 شامل ساختار هایی می شود که از TLS 1.2پشتیبانی می‌کند.

کاربران با استفاده ازNetScaler Gateway ، احراز هویت شده و وارد سیستم می شوند.

NetScaler Gateway

NetScaler Gateway، در DMZ پیاده سازی شده و امن می شود. در این قسمت، احراز هویت دو عاملی انجام شده است.

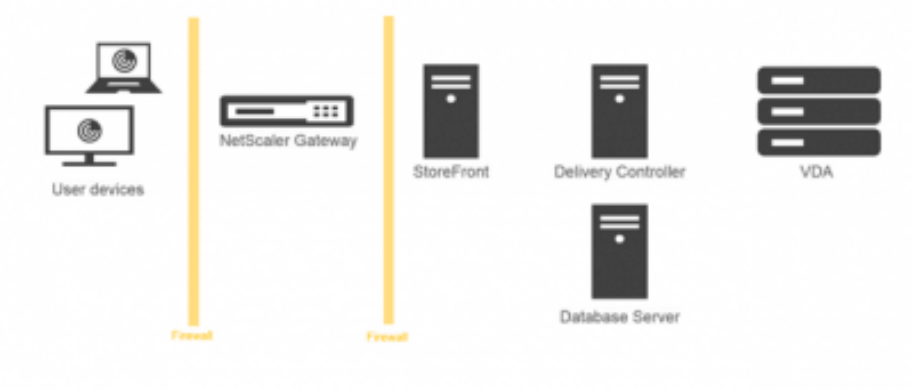
بر اساس credential کاربران، منابع و برنامه های مربوطه در اختیار کاربران قرار می گیرد.

نرم افزار ها و داده ها، بر روی سرور های مناسب قرار دارند (در نمودار نشان داده نشده است) به همراه سرور های جداگانه برای تامین امنیت نرم افزار ها و داده های حساس است.

این ساختار، شامل ابزارهای نظارتی برای بررسی میزان مصرف منابع، خطرات و مشکلات امنیتی است.

مراحلی که طی می شود، برای بررسی و پاسخ به خطرات امنیتی می باشد.

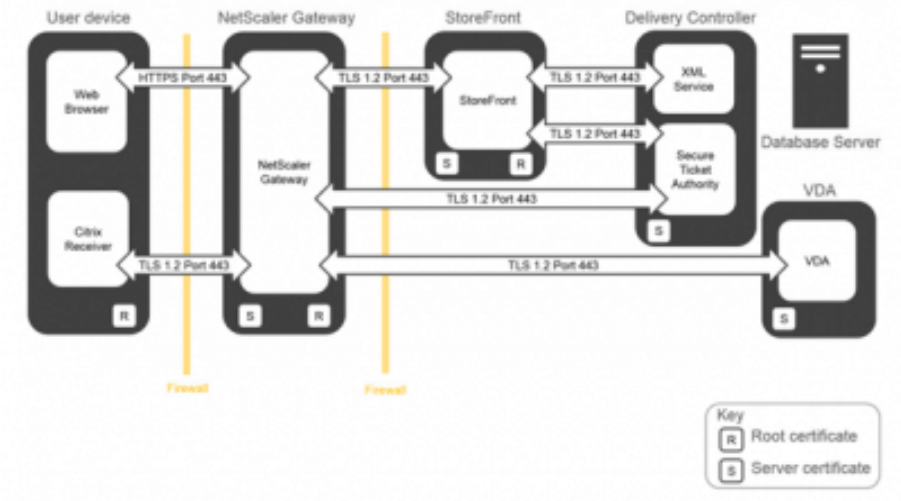
آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



نحوه تعامل اجزای مختلف

نمودار زیر، جزئیاتی از زیرساخت را نمایش می‌دهد. که شامل اجزای مختلف و گواهی‌نامه‌های (certificate) هر سرور می‌شود.

به علاوه‌ی نمایش تنظیمات ارتباطات آن‌ها و پورت‌هایشان!



Citrix Gateway

Citrix Gatewayموجود درDMZ ، یک راه ارتباطی ایمن برای دسترسی داشتن به محیط Virtual Apps and Desktopsارائه می‌کند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

ترافیک بین مرورگر دستگاه کاربر وCitrix Gateway ، از طریق پروتکل HTTPS ایمن شده است.

تمامی ترافیک‌های دیگر نیز از طریق TLS 1.2 امن شده است.

Citrix Gatewayاتصالات TLS / HTTPS را از دستگاه کاربر) مرورگر و (Citrix Receiver خاتمه می‌دهد.

ترافیکی که به طور مستقیم از Citrix Gateway به StoreFron ، Delivery Controllerو VDA ارسال و از آن دریافت می‌شود. از طریق TLS 1.2 امن شده است.

ترافیک شبکه از ابتدا تا انتها(end-to-end) ، با استفاده از TLS 1.2 رمزنگاری می‌شود.

همان‌طور که اشاره شد، داشتن یک StoreFront 3.5 برای این رمزنگاری، ضروری می‌باشد) پشتیبانی از1.2 TLS ، اولین بار در StoreFront 3.5 معرفی شد.

استانداردهای امنیتی

گذشته از ویژگی امنیتی دورکاری که گفته شد رعایت استانداردهای امنیتی امری بسیار مهم است.

در این بخش، جزئیاتی درباره استاندارد های امنیتی ارائه شده است.

که ممکن است با بالاترین سطح از زیرساخت شما ارتباط داشته باشد. بسته به نوع استفاده و محیط شما، ممکن است اعمال برخی از استاندارد ها الزامی باشد.

معیار های متداول

صدور گواهی نامه معیار های متداول، یک استاندارد شناخته شده بین المللی برای ارزیابی امنیت محصولات و سیستم های فناوری اطلاعات است.

گواهینامه معیارهای متداول(Common Criteria) ، تضمین می کند که محصولات کاملاً معتبر می باشند.

و به طور مستقل در برابر مجموعه ای از الزامات ایجاد شده توسط سازمان جهانی استاندارد بین المللی برای اطمینان از امنیت فناوری اطلاعات آزمایش و تأیید شده اند.

برای مشتریان، به ویژه آژانس های دولتی فدرال و بین المللی ایالات متحده، صدور گواهینامه معیار های متداول، در تهیه محصولات و سیستم های فناوری اطلاعات، یک نیاز مهم است.

گواهینامه معیارهای متداول برای صنایع بخش خصوصی مانند مراقبت های بهداشتی و مالی نیز کاربرد دارد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

FIPS 140-2 به همراه Citrix Virtual Apps and Desktops

FIPS 140-2 یک استاندارد دولت فدرال ایالات متحده است که معیار پیاده سازی نرم افزار رمزنگاری را شرح می دهد.

جامعه امنیتی در محصولات با ارزش از دستورالعمل های مفصل در FIPS 140-2 و استفاده از ماژول های رمزنگاری معتبر FIPS 140-2 پیروی می کنند.

برای تسهیل در پیاده سازی دسترسی application server امن و برآورده کردن نیازهای FIPS ، محصولات Citrix می توانند از ماژول های رمزنگاری شده استفاده کنند.

که از لحاظ FIPS 140-2 معتبر بوده و برای پیاده سازی اتصالات امن TLS / SSL هستند.

ابزار Citrix Gateway MPX-FIPS appliance که FIPS فعال دارد کاملاً سازگار است.

و امکان تنظیم کامل TLS را در کارهایی که شامل Citrix Gateway است فراهم می کند.

لوازم Citrix Gateway MPX FIPS Appliance سازگار با FIPS 140-2 سطح ۲ هستند.

هنگامی که برای FIP 140-2 ، Citrix Virtual Apps and Desktops ، StoreFront و Receiver پیکربندی شده اند.

از ماژول های رمزنگاری شده ارائه شده توسط سیستم عامل Microsoft Windows استفاده کنید.

Citrix Gateway از ماژول رمزنگاری شده معتبر Cavium FIPS 140-2 استفاده می کند.

قسمت زیرساخت نماینده (Representative deployment) در این راهنما با اتصالات TLS با ماژول های رمزنگاری شده معتبر FIPS 140-2 فعال شده است.

TSL/SSL

Transport Layer Security (TLS) یک پروتکل باز و غیر اختصاصی است.

که رمزگذاری داده ها، احراز هویت سرور، یکپارچگی پیام و احراز هویت مشتری به صورت اختیاری را برای اتصال TCP / IP فراهم می کند.

در ساختار Citrix ، می توانید ارتباطات امن TLS را بین دستگاه های کاربر و سرورهای Citrx Virtual Apps and Desktops پیکربندی کنید.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

تا اطمینان حاصل کنید از اینکه ترافیک موجود در شبکه به صورت رمزنگاری شده باشد.

Secure Socket Layer (SSL)استاندارد پیشین است که توسط TLS جایگزین شده است.

شما می توانید هم TLS و هم SSL را در یک ساختار سیتریکسی پیکربندی کنید؛ زیرا گواهینامه های سرور در زیرساخت سیتریکسی شما از TLS و SSL پشتیبانی می کنند.

محصولات سیتریکس- پشتیبانی ازTLS 1.2

این جدول محصولات و مؤلفه های Citrix را نشان می دهد که از TLS 1.2 پشتیبانی می‌کنند و می توانند برای) TLS 1.2آخرین نسخه توصیه شده TLS پیکربندی شوند.(

NetScaler 11.0به Cavium با سطح ۲.۲ نیاز دارد.

IP Security

IP Security (IPsec)مجموعه ای از استاندارد ها است که پروتکل اینترنت (IP) را گسترش می‌دهد.

که ارتباطات معتبر و رمزگذاری شده را با یکپارچگی داده ها و محافظت مجدد از آن ارائه می دهد IPsec . یک مجموعه پروتکل تحت لایه های شبکه است.

بنابراین پروتکل های سطح بالاتر مانند Citrix ICA می توانند از آن بدون نیاز به ایجاد تغییر استفاده کنند.

نسخه های فعلی و اخیر Citrix Virtual Apps and Desktops از رمزگذاری) TLS که به صورت end-to-end عمل می کند (پشتیبانی می کنند.بنابراین هیچ نیازی به IPsec وجود ندارد.

با این حال، برای نسخه های اولیه XenApp و XenDesktop ، استفاده از IPsec برای رمزگذاری کامل ترافیک شبکه در یک شبکه خصوصی مجازی (VPN) ضروری بود.

IPsecدر " Internet RFC 2401 " شرح داده شده است. کلیه نسخه های فعلی Microsoft Windows ازIPsec ، پشتیبانی داخلی دارند

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

از ویژگی امنیتی دورکاری استفاده از کارت های هوشمند

برای دسترسی امن به منابع و داده های منتشر شده می توانید. از کارت‌های هوشمند برای ارتباط با Citrix Virtual Apps and Desktopsاستفاده کنید.

استفاده از کارت‌های هوشمند فرآیند ویژگی امنیتی دورکاری دیگری است. که احراز هویت را در عین افزایش امنیت ورود به سیستم ساده می کند.

Citrix Virtual Apps and Desktopsاز احراز هویت با کارت هوشمند برای برنامه های منتشر شده پشتیبانی می کند.

از جمله برنامه هایی که امکان فعالیت با کارت هوشمند را دارند مانند Microsoft Outlook در یک شبکه تجاری و سازمانی

کارتهای هوشمند یک پیاده سازی مؤثر از فناوری "کلیدهای عمومی" است و می توان از آنها برای موارد استفاده کرد:

- **احراز هویت کاربران به شبکه ها و رایانه ها**
- **ارتباطات کانال های موجود در شبکه را ایمن می کند.**
- **از امضاهای دیجیتالی برای تأمین امنیت محتوا استفاده کنید.**

اگر برای احراز هویت امن شبکه از کارتهای هوشمند استفاده می کنید.

کاربران می توانند از طریق برنامه ها و محتوای منتشر شده در Citrix Virtual Apps and Desktops احراز هویت بشوند.

علاوه بر این، عملکرد کارت هوشمند در این برنامه های منتشر شده نیز پشتیبانی می شود.

به عنوان مثال، یک برنامه منتشر شده مانند مایکروسافت Outlook را می توان طوری پیکربندی کرد که نیاز داشته باشد.

تا کاربران، یک کارت هوشمند را در کارت خوان هوشمند متصل به دستگاه کاربر، درج کنند.

تا به یک سرور که دارای زیرساخت سیتریکسی است وصل شوند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

پس از احراز هویت کاربران به برنامه، آنها می توانند با استفاده از گواهینامه های ذخیره شده در کارت های هوشمند خود، وارد ایمیلشان شوند.

Citrix

Citrixاز کارت‌های هوشمند رایانه شخصی (PC / SC) مبتنی بر کارتهای هوشمند رمزنگاری شده پشتیبانی می کند.

این کارت ها شامل پشتیبانی از عملیاتی مانند امضاهای دیجیتال و رمزگذاری هستند. کارت‌های رمزنگاری به گونه ای طراحی شده اند.

که امکان ذخیره سازی ایمن کلیدهای خصوصی مانند آن‌هایی را که در سیستم های امنیتی کلید عمومی (PKI) استفاده می شوند را فراهم می کنند.

این کارت‌ها عملکردهای رمزنگاری واقعی را روی خود کارت هوشمند انجام می دهند.

به این معنی که کلید خصوصی و گواهینامه های دیجیتال هرگز کارت را ترک نمی کنند.

علاوه بر این، می توانید برای افزایش امنیت از تأیید هویت دو شاخصه استفاده کنید.

به جای ارائه تنها یک کارت هوشمند (یک عامل) برای انجام عملیات، از یک پین تعریف شده توسط کاربر (یک عامل دوم) که فقط برای کاربر شناخته شده است. هم استفاده می شود.

تا ثابت کند که دارنده کارت صاحب کارت هوشمند است.یعنی علاوه بر کارت هوشمند، کاربر باید یک پین کد مخصوص به خود را داشته باشد.

تا مشخص بشود کسی که کارت را وارد می کند، صاحب کارت هوشمند می باشد.

پشتیبانی کارت های هوشمند

Citrixبه طور مدارم تست کارت های هوشمند مختلف را برای رفع مشکلات کاربردی و سازگاری آنها با Citrix Virtual Apps and Desktopsادامه می‌دهد.

Citrix Virtual Apps and Desktopsبطور کامل از کارت های Common Access Card (CAC) و (PIV)

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

Personal Identity Verificationپشتیبانی می‌کنند.

به همراه نسخه های مناسبReceiver Citrix (Workspace App

انواع مختلفی از کارتهای هوشمند و فروشندگان کارت های هوشمند وجود دارند. در دولت ایالات متحده، از هر دوی این کارتها بطور گسترده استفاده می شود:

- **(Common Access Card (CAC):**

توسط کارمندان و سایر پرسنل در وزارت دفاع ایالات متحده (DoD) استفاده می شود.

CAC، شامل عکسی از کاربر، به علاوه نام آنها و جزئیات مربوطه می باشد.

CAC، برای دستیابی فیزیکی به ساختمانها و مناطق DoD استفاده می‌شود.

و همچنین برای ورود به سیستم های IT در شبکه NIPR استفاده می شود.

CACاز یک اپلیکیشن اختصاصی کارت استفاده می کند و به واسطه اختصاصی نیاز دارد.

PIV) Personal Identify Verification):

مشابه CAC است که توسط کارمندان و پیمانکاران شاغل در آژانس های فدرال ایالات متحده استفاده می شود.

شامل یک عکس و اطلاعات کاربر است و برای دستیابی فیزیکی به ساختمان های فدرال استفاده می شود.

و برای ورود به سیستم های IT از آن استفاده می شود.

با این حال، بر خلافCAC ، PIVکه به عنوان یک نتیجه از دستورالعمل ریاست جمهوری امنیت داخلی ۱۲ (HSPD-12)توسعه یافته است.

لزوماً نیازی به واسط اختصاصی ندارد و به طور پیش فرض در مایکروسافت ویندوز ۷ یا بالاتر پشتیبانی می شود.

برای اطلاعات بیشتر، سایت زیر را مشاهده فرماییدhttp://csrc.nist.gov/groups/SNS/piv/ .

برای راهنمایی در مورد پیکربندی کارت هوشمند در محیط های دولت ایالات متحده، به سایت زیر مراجعه کنید :

http://support.citrix.com/article/CTX200939

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

جان کلام در ویژگی امنیتی دورکاری

اگرچه ویژگی امنیتی دورکاری به گونه ای است که می توان به شیوه گروهی نیز آن را انجام داد.

لیکن شغل‌های مناسب کار از راه دور به شغل‌هایی اطلاق می‌گردد. که یک فرد توانایی انجام آن‌ها را به تنهایی داشته باشد.

هم اکنون **شرکت دانش بنیان رها**، اولین مرجع مجازی سازی ایران آماده هرگونه پیاده سازی دورکاری در هر گونه ارگان، سازمان و اداره است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net