AUTENTICACION BASADA EN RIESGO

Un elemento crítico para cualquier implementación de confianza cero

Abril 2021

Cyber-T

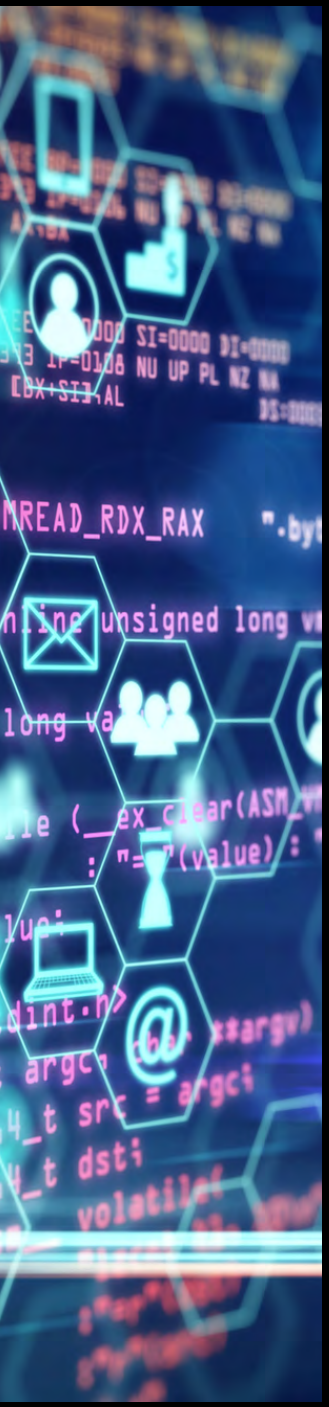
CONTENIDO

Forrester Research Inc. acuñó por primera vez el término "confianza cero" en 2010. Una década y una pandemia más tarde, con las empresas que implementan entornos híbridos de múltiples nubes, la gestión de identidad y acceso ya no puede considerarse opcional. Extender la protección VPN no es suficiente.

La autenticación basada en riesgos mejora tanto la seguridad como la experiencia del usuario al permitirle clasificar los recursos que desea proteger según el nivel de riesgo y el tipo de usuario. Esto le da el poder de crear reglas que son únicas para la estructura de seguridad de su organización, lo que permite una mayor flexibilidad y una mayor protección solo cuando es necesario.

En este libro electrónico, discutimos la poderosa conexión entre la adopción de confianza cero y las políticas de riesgo, y cómo la autenticación multifactor se encuentra en el centro de estos enfoques al brindar la tecnología tan necesaria hoy en día para proteger las identidades de los usuarios y las aplicaciones en la nube.

Cyber-T



¿Porque Autenticación basada en riesgo?

Autenticación de Usuario

- Algo que sabe (contraseña, PIN)
- Algo que tienes (ficha, teléfono móvil)
- Algo que eres (huella dactilar, cara)

La autenticación de usuario es una forma estática de verificar la identidad de un usuario cuando intenta acceder a un recurso protegido. Puede autenticarse usando un solo factor (débil) o múltiples factores (muy recomendado).

En un mundo dinámico, donde la movilidad de los usuarios afecta la seguridad casi el 100% del tiempo, la autenticación multifactor se ha vuelto imperativa y clave para implementar una red de confianza cero. ¿Por qué?

- Los usuarios se están conectando a los recursos de la empresa desde diferentes redes desprotegidas.
- Las horas de trabajo se han vuelto más flexibles, por lo que podrían trabajar desde las primeras horas hasta las últimas horas de la noche.
- Los dispositivos podrían haberse compartido con otros miembros de la familia.
- Y todo esto significa que los atacantes intentarán explotar este nuevo mundo de posibilidades.

Autenticación de Usuario

Factores de riesgo

- ¿A qué red está conectado?
- ¿Está segura su computadora?
- ¿Son seguros sus dispositivos móviles?
- ¿Cuál es su ubicación actual?
- ¿Están su dispositivo y su computadora ubicados en el mismo lugar?

Cyber-T

Cyber-T

La autenticación basada en riesgos tiene en cuenta los factores de riesgo al tomar una decisión de autenticación. Va más allá de una autenticación estática, permitiendo que los administradores creen reglas que puedan modificar el comportamiento de autenticación, lo que a veces lo hace más fácil si el riesgo es bajo; o solicitar pasos adicionales para asegurarse de que este es el usuario correcto y bloquear el acceso si el riesgo es demasiado alto, incluso si el usuario proporcionó una contraseña de un solo uso (OTP) correcta.

Autenticación multifactorial e inteligencia de riesgos: gestión de usuarios optimizada

La autenticación basada en riesgos mejora tanto la seguridad como la experiencia del usuario al permitirle clasificar los recursos que desea proteger según el nivel de riesgo y el tipo de usuario. Esto le da el poder de crear reglas que son únicas para la estructura de seguridad de su organización, lo que permite una mayor flexibilidad y una mayor protección solo cuando es necesario.

Por ejemplo, puede decidir permitir que los usuarios se autentiquen solo con el nombre de usuario y la contraseña cuando están conectados directamente a una red corporativa local, pero usar MFA si trabajan desde una red separada. Y esta es la definición de gestión avanzada de usuarios.

Cyber-T

Factores de riesgo comunes que podrían agregarse potencialmente a las políticas de autenticación

UBICACION DE LA RED

Una red corporativa puede tener todas las medidas de seguridad del perímetro, como firewall, Wi-Fi seguro, detección de amenazas, etc. Por lo tanto, alguien conectado físicamente a esa red presentaría menos riesgo que alguien en una oficina remota con menos medidas de seguridad o alguien conectado a través de la oficina en casa.

RIESGO DE DISPOSITIVOS MOVILES

El dispositivo de un usuario que se ha visto comprometido representa un riesgo de seguridad para la empresa. Una forma en que un dispositivo puede verse comprometido fácilmente es cuando un usuario hace jailbreak a un dispositivo iOS o arraiga un sistema operativo Android, eludiendo las medidas de seguridad del sistema operativo. Un dispositivo vulnerable aumenta el riesgo general y debe bloquearse la mayor parte del tiempo.

ENDPOINT / COMPUTADORA EN RIESGO

Al igual que el riesgo de los dispositivos móviles, el riesgo del Endpoint o de la computadora también se puede utilizar para evaluar qué medidas deben tomarse. Un usuario con su propia computadora portátil, con todas las protecciones, supondría un riesgo bajo. El mismo usuario intenta conectarse más tarde en el día, con una computadora desconocida, tal vez una máquina Linux con un navegador Tor, y el riesgo aumentaría enormemente.

POLITICAS DE TIEMPO

La fecha y la hora se pueden utilizar para diferentes propósitos. Supongamos que una aplicación corporativa generalmente pasa por una copia de seguridad y mantenimiento todos los días, desde la 1 a.m. hasta las 3 a.m. Las políticas de tiempo podrían usarse para bloquear el acceso a esa aplicación durante este período de tiempo. En términos de riesgo, si un usuario intenta acceder a una aplicación un fin de semana, o quizás en medio de la noche, esto podría aumentar el riesgo drásticamente, ya que podría tratarse de un hacker realizando un ataque mientras el equipo de TI está descansando. por lo que se podrían tomar medidas adicionales.

Factores de riesgo comunes que podrían agregarse potencialmente a las políticas de autenticación

GEOCERCADO / GEOLOCALIZACION

La ubicación física podría usarse para evitar el acceso desde países específicos o geolocalizaciones, mitigando así las posibilidades de ataques. Una empresa con oficinas y actividades solo en los EE. UU. Podría bloquear potencialmente cualquier acceso fuera del país. El acceso a una aplicación específica también podría limitarse a un área alrededor de la oficina de la empresa.

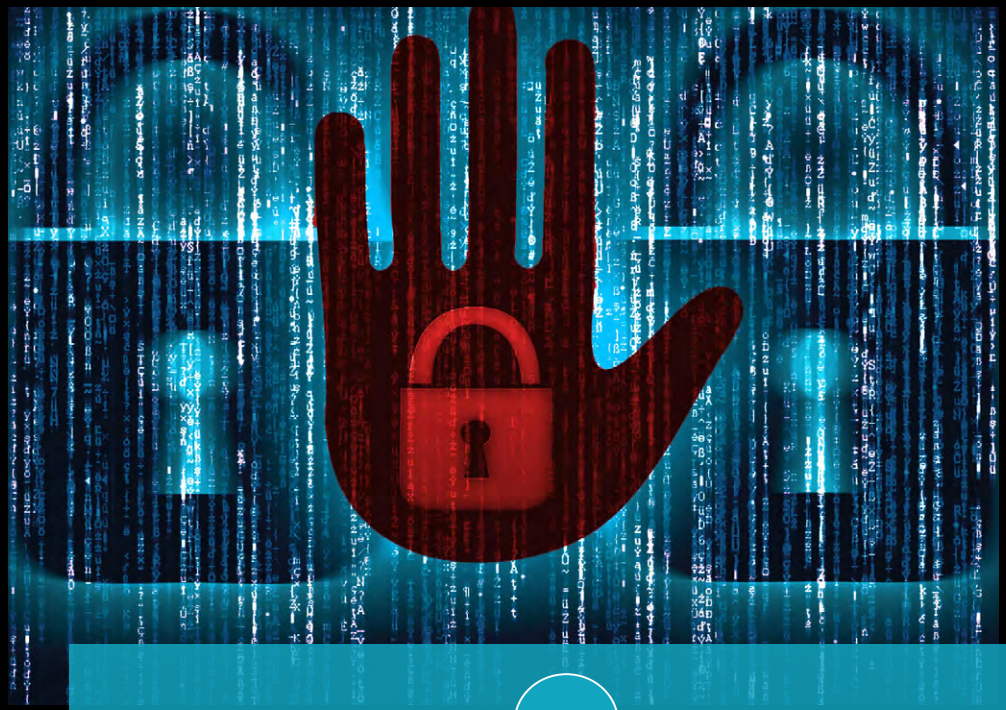
GEO-CORRELACION

Se espera que un usuario que se conecte a un servicio de la empresa tenga un teléfono móvil en sus manos. Una conexión iniciada desde una computadora ubicada en Sao Paulo, Brasil, con el teléfono móvil registrando su ubicación actual en Virginia, EE. UU., Podría mostrar que un pirata informático está tratando de conectarse a un servicio, mientras utiliza ingeniería social para convencer a un usuario de que apruebe la autenticación MFA.

Si bien algunas geolocalizaciones no son muy precisas (algunos operadores enrutarán la conexión a una ubicación diferente y algunos dispositivos Android pueden manipular su ubicación GPS), esta puede ser otra forma de descartar posibles ataques.

GEO CINETICA

Otra forma de utilizar GPS o factores de geolocalización para una decisión de riesgo es la geocinética o la velocidad de autenticación. Un usuario que se autentica desde Seattle a las 9:05 a.m. no puede autenticarse 25 minutos después desde San Diego, a 1.300 millas de distancia. Lo más probable es que el segundo intento de autenticación esté intentando reutilizar la primera autenticación.



Las Políticas de riesgos evitan infracciones

Cyber-T

Sin políticas de riesgo implementadas, su empresa necesitaría habilitar el método de autenticación más seguro en todo momento, para todos los usuarios, lo que podría causar fricciones entre los usuarios para algunos segmentos.

La autenticación de riesgos es una forma de modernizar su estrategia mediante el uso de la cantidad precisa de seguridad con protección de riesgos personalizada que mejora su capacidad para detectar y responder a amenazas.

Los siguientes escenarios muestran casos de posibles violaciones de datos que se pueden prevenir si se habilitan las políticas de riesgo.

A

USO DE CREDENCIALES ROBADAS

El usuario se autentica regularmente con nombre de usuario, contraseña y una OTP. Un atacante pudo obtener las credenciales de usuario a través de la web oscura o un ataque de phishing, pero el token no pudo ser pirateado ni clonado.

- Ataque:

  utilizando la ingeniería social, el atacante llama al usuario y lo convence de que entregue una OTP. El atacante ingresa las credenciales y los tipos en la OTP basada en el tiempo, obteniendo acceso al recurso protegido.

- Política de prevención de riesgo:

  las políticas de riesgo informático podrían mostrar que la computadora que se está utilizando no es la personal del usuario.

  Las políticas de geocinética posiblemente mostrarían que el usuario está intentando autenticarse desde una ubicación donde la transición entre dos autenticaciones es imposible.

B

RUPTURA iOS - JAILBREAKING

El usuario se autentica con nombre de usuario, contraseña y push. El usuario hizo jailbreak al iPhone y un atacante instaló malware, lo que les dio el control total. Push no está protegido por un PIN o biométrico.

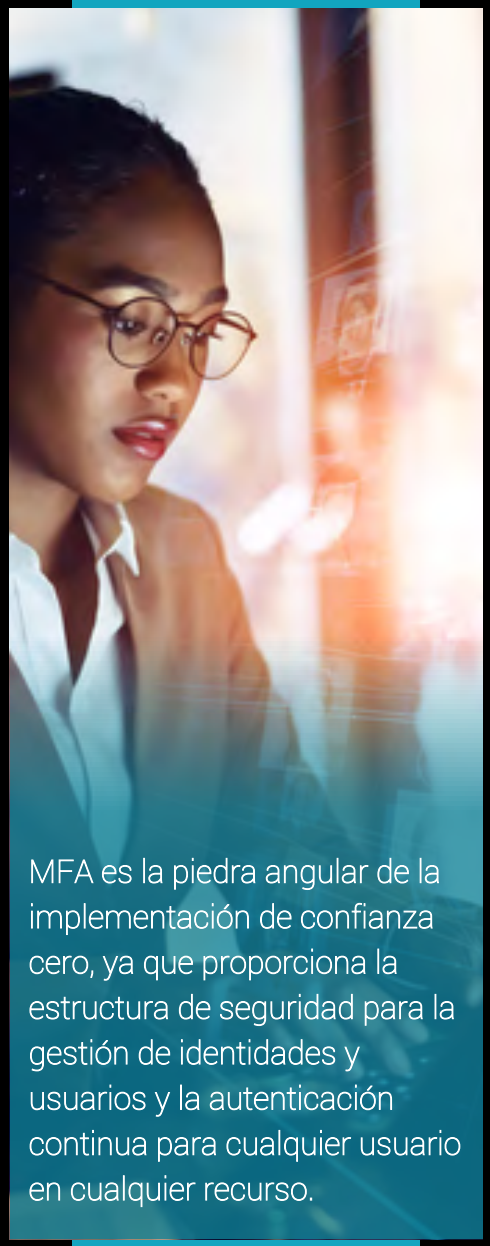
- Ataque:

  el atacante, de un país diferente, usaría credenciales robadas para autenticarse, mientras monitoreaba el teléfono del usuario. Cuando la inserción llega al teléfono del usuario, el atacante utilizará la Herramienta de acceso remoto (RAT) para aprobar la inserción y obtener acceso al recurso.

- Política de prevención de riesgo:

  las políticas de riesgo de dispositivo detectarían que el dispositivo móvil del usuario no es confiable y negarían las autenticaciones de este.

  Las políticas de correlación geográfica verificarían que la computadora esté ubicada en una ubicación diferente a la del dispositivo móvil, bloqueando también la conexión.



MFA es la piedra angular de la implementación de confianza cero, ya que proporciona la estructura de seguridad para la gestión de identidades y usuarios y la autenticación continua para cualquier usuario en cualquier recurso.

No puede haber confianza cero sin MFA

Cyber-T

La gestión de identidades y accesos ya no puede considerarse opcional. Las empresas deben centrarse en una sólida estrategia de gestión y protección del usuario, que son áreas centrales que rigen la autenticación de riesgos y MFA. Esto le dará la oportunidad de adoptar verdaderamente el enfoque de "no confiar en nadie" para la red de su empresa, los puntos finales y las aplicaciones en la nube sin comprometer la experiencia del usuario.

Mientras que una red tradicional se basa en la idea de la confianza inherente, un marco de confianza cero supone que cada dispositivo y usuario, dentro o fuera de la red, representa un riesgo de seguridad. El enfoque de "nunca confiar, verificar siempre" utiliza varios niveles de protección para prevenir amenazas, bloquear el movimiento lateral y hacer cumplir controles granulares de acceso de los usuarios.

Bajo la premisa de que no se puede confiar completamente en nada, el enfoque de confianza cero se centra en tres principios:

Identificación de Usuarios y Dispositivos

Siempre sepa quién y qué se conecta a la red empresarial. A medida que las empresas luchan por que el predominio de su fuerza laboral trabaje de forma remota, a las herramientas internas presenta un gran desafío. Los Servicios de Autenticación multifactor basada en la nube (MFA) ofrecen mitigación contra el robo de credenciales, el fraude y los ataques de phishing.

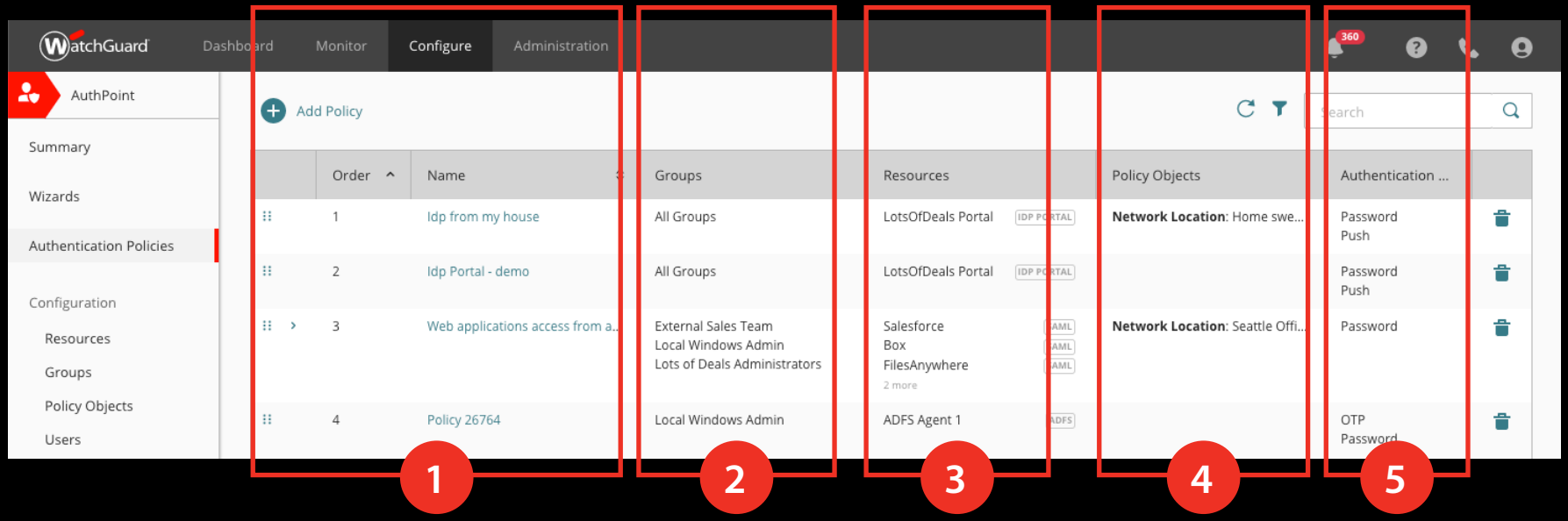
Provisión de Acceso Seguro

Limite acceso a aplicaciones y sistemas críticos solo a los dispositivos con permiso explícito para accederlos. En el marco de confianza cero, el objetivo de la gestión de acceso es proporcionar un medio para gestionar centralmente el acceso a los sistemas de TI, al tiempo que se limita ese acceso solo a usuarios, dispositivos o aplicaciones específicos. Inicio de sesión único (SSO), combinadas con MFA, pueden mejorar la seguridad del acceso y minimizar la carga de las contraseñas para los usuarios.

Monitoreo Continuo

Supervise la situación de salud y seguridad de la red y todos los puntos finales administrados. Las amenazas de malware y ransomware solo se han acelerado como resultado del coronavirus. Mantener a los usuarios seguros mientras navegan por Internet es más difícil cuando se conectan desde fuera de su red. Mantenerse al tanto de las amenazas requiere una seguridad avanzada y persistente que va más allá del antivirus del Endpoint.

Ejemplo de políticas de autenticación basadas en riesgos habilitadas que cumplen con el enfoque de confianza cero:



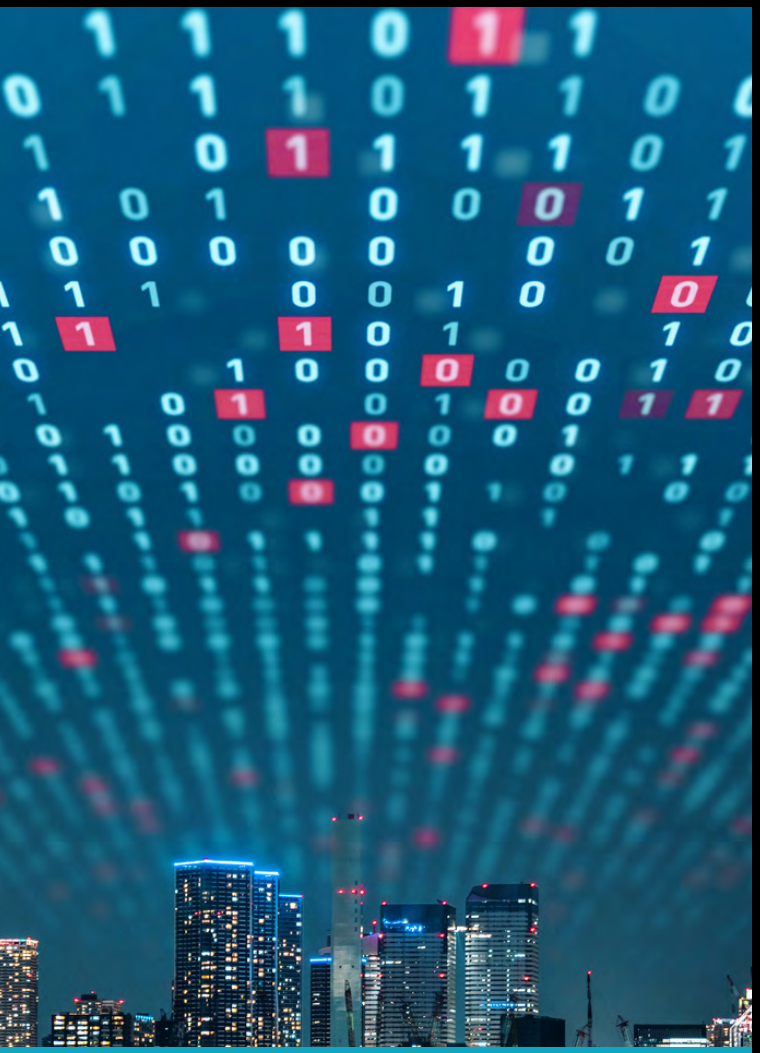
1. El nombre de la política representaría un microsegmento de confianza cero y se puede organizar en orden de prioridad y / o importancia.

2. Los grupos de usuarios, sincronizados o no con Active Directory, representan a aquellos a quienes se les debe permitir, y solo a ellos, el recurso protegido.

3. La (s) aplicación (es) del microsegmento. Podría ser una sola aplicación, podría ser múltiple, en caso de que las aplicaciones tengan exactamente la misma política.

4. Objetos de política, o políticas de riesgo, que pueden determinar restricciones específicas, basadas en red, tiempo, geolocalización, etc.

5. Se refiere a los métodos de autenticación que deben permitirse, si corresponde, o simplemente denegar la autenticación, en función de un factor de riesgo.



Las políticas de riesgo se pueden utilizar para definir reglas más granulares basadas en situaciones dinámicas, que se ajusta mejor a las tendencias actuales de acceso remoto y los modelos de trabajo híbridos que están experimentando las empresas.

Uso de políticas de riesgo y MFA para una implementación de confianza cero

Como sabemos, la implementación de confianza cero comienza con el supuesto de que no se puede confiar en nada. Al definir microsegmentos y aplicar políticas que se adapten a las necesidades de seguridad de su organización, está creando un entorno confiable. Esto comienza identificando al usuario que accederá a esas aplicaciones y servicios.

Un microsegmento podría ser una aplicación de gestión de relaciones con el cliente (CRM) basada en la nube. Por ejemplo, los equipos de ventas y soporte técnico pueden necesitar acceso a ese CRM. ¿Ingenieria? Posiblemente no para que no se incluyan. En el caso del equipo de soporte técnico, todos los empleados se encuentran en la misma ciudad y trabajan solo en horario comercial, lo que significa que tal vez el acceso para este grupo debe ser limitado geográficamente y en el tiempo.

Y debido a la sensibilidad de los datos dentro del CRM, siempre se debe usar MFA.
Si lo ponemos en el contexto de la autenticación y los factores de riesgo, hay dos reglas que definirán la política de riesgo asociada con este microsegmento:

NOMBRE DE REGLA #1

CRM PARA VENTAS

Quién puede acceder: Ventas

Aplicación: Cloud CRM

Restricciones de riesgo: bajo riesgo de dispositivos móviles, bajo riesgo de correlación geográfica

Autenticación: contraseña + autenticación basada en push

NOMBRE DE REGLA #2

CRM PARA SOPORTE TECNICO

Quién puede acceder: Soporte técnico

Aplicación: Cloud CRM

Restricciones de riesgo: riesgo bajo de dispositivos móviles, horario comercial, solo en CDMX., Riesgo bajo de correlación geográfica

Autenticación: contraseña + autenticación basada en push

Guía de evaluación de riesgos comerciales

Cyber-T

Evaluar el riesgo en su organización al observar sus posibles escenarios de riesgo puede mejorar enormemente esas implementaciones al agregar hechos y análisis dinámicos a la decisión.

CREAR UN CUESTIONARIO DE RIESGO

Casos de uso empresarial común que pueden ayudar a identificar las políticas de riesgo adecuadas para usted:

- En el sitio: ¿sus empleados acceden a los datos y plataformas de la empresa desde la oficina?
- Oficina en casa remota: ¿Tiene muchos empleados trabajando desde casa?
- Cafetería remota, oficina compartida: ¿Espera que sus empleados remotos accedan a las redes de la empresa desde ubicaciones como cafeterías?
- Usuarios que viajan: ¿Tiene empleados que viajan y pueden acceder a las plataformas de trabajo mientras están en movimiento?
- Vertical: ¿El servicio que ofrece su empresa está asociado con un horario comercial específico? Por ejemplo, oficinas de salud
- Proveedores externos: ¿Proporciona la empresa acceso a contratistas o proveedores externos?
- Dispositivo: ¿Espera que los empleados accedan a la información del trabajo utilizando sus propios dispositivos?

PRUEBA LA MICRO-SEGMENTACIÓN

Un ejercicio de microsegmentación también le dará una mejor visibilidad sobre sus activos y usuarios. A continuación, una plantilla de tabla simple que podría usarse para este ejercicio, al menos la primera parte, que trata sobre la identidad.

Ejemplo de microsegmento: utilice esta plantilla como punto de partida para crear sus microsegmentos y expandirla según sus propias necesidades de seguridad para crear políticas de acceso más específicas.

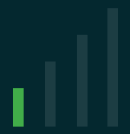
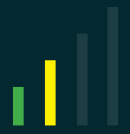
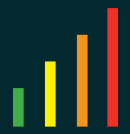
Microsegmento de confianza cero

CRM Cloud

Grupo de Usuarios	Escenario	Ubicación de Red	Geolocalización	Restricción de Tiempo	Riesgo del dispositivo	Riesgo de computadora	Autenticación
Ventas	Trabajo desde casa	Red de Oficina			Bajo riesgo	Portatil empresa	Password
Soporte Tecnico Finanzas	Viaje de trabajo	Cualquiera			Bajo riesgo	Portatil empresa	Push MFA QR code MFA
Grupo de Soporte Externo	Trabajo solo en oficina	Red de Oficina		Horario Oficina	Bajo riesgo	Desktop empresa	Password
	Trabajo por VPN	VPN de Empresa		Horario Oficina	Bajo riesgo	Desktop empresa	Push MFA
CRM de TI	Consultor de CRM	Cualquiera	Solo CDMX	Horario Oficina			Push MFA
	Soporte de CRM	Cualquiera	Solo GDL		Bajo riesgo		Push MFA

Continuación de la Guía de evaluación de riesgos comerciales

Cyber-T

GUÍA DE EVALUACIÓN DE RIESGOS	Factor de riesgo		MFA	Atributos de riesgo		
	Nombre de usuario	Password	OTP, QR Code or Push	Ubicación de red	Resultado de Autenticación	Nivel de riesgo
ESCENARIO #1 El empleado de la empresa se conecta desde su casa a un recurso corporativo	✓	✓	✓	✗	Permitido	 Pasa
ESCENARIO #2 El empleado de la empresa se conecta desde la ubicación de la oficina de CDMX a un recurso corporativo	✓	✓	MFA no Requerido	✓	Permitido	 Pasa
ESCENARIO #3 El usuario intenta iniciar sesión para acceder a los datos corporativos desde una ubicación desconocida	✓	✓	✗ MFA no Permitido	✗	Denegado	 Denegado

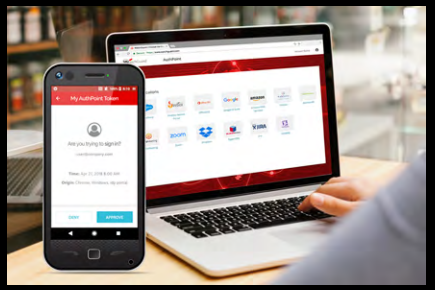
PLATAFORMA UNIFICADA DE SEGURIDAD WATCHGUARD

Seguridad de la red

Las soluciones WatchGuard de Network Security están diseñadas desde cero para ser fáciles de implementar, usar y administrar, además de brindar la mayor seguridad posible. Nuestro enfoque único para la seguridad de la red se enfoca en brindar la mejor seguridad de nivel empresarial a cualquier organización, independientemente de su tamaño o experiencia técnica.

Wi-Fi seguro

La solución Wi-Fi segura de WatchGuard, un verdadero cambio de juego en el mercado actual, está diseñado para proporcionar un espacio aéreo seguro y protegido para entornos Wi-Fi, al tiempo que elimina los dolores de cabeza administrativos y reduce en gran medida los costos. Con herramientas de participación expansivas y visibilidad de la analítica empresarial, ofrece la ventaja competitiva que las empresas necesitan para triunfar.



Autenticación multifactor

WatchGuard AuthPoint® es la solución adecuada para abordar la brecha de seguridad basada en contraseñas con autenticación multifactor en una plataforma en la nube fácil de usar. El enfoque único de WatchGuard agrega el "ADN del teléfono móvil" como factor de identificación para garantizar que solo la persona correcta tenga acceso a redes sensibles y aplicaciones en la nube.

Seguridad del Endpoint

WatchGuard Endpoint Security es una cartera de seguridad avanzada de endpoints nativa de la nube que protege a las empresas de cualquier tipo de ciberataques presentes y futuros. Su solución insignia, Panda Adaptive Defense 360, impulsada por inteligencia artificial, mejora inmediatamente la postura de seguridad de las organizaciones. Combina capacidades de protección de endpoints (EPP) y detección y respuesta (EDR) con aplicaciones de confianza cero y servicios de búsqueda de amenazas.

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es líder mundial en seguridad de redes, seguridad de terminales, Wi-Fi seguro, autenticación multifactor e inteligencia de redes. Más de 18.000 revendedores de seguridad y proveedores de servicios confían en los productos y servicios galardonados de la empresa en todo el mundo para proteger a más de 250.000 clientes. La misión de WatchGuard es hacer que la seguridad de nivel empresarial sea accesible para empresas de todos los tipos y tamaños a través de la simplicidad, lo que convierte a WatchGuard en una solución ideal para medianas empresas y empresas distribuidas. La compañía tiene su sede en Seattle, Washington, y oficinas en América del Norte, Europa, Asia Pacífico y América Latina.
Para obtener más información, visite WatchGuard.com.

Acerca de Cyber-T

Cyber-T IT Integration and Services, es una empresa mexicana dedicada a la Integración de Soluciones de T.I. con foco en ciberseguridad y respaldo de datos, adicionalmente cuenta con un SOC Tipo 3 y un Centro de Datos DRP, desde donde entregan servicios a Nivel Nacional.
Cyber-T es Partner GOLD de Watchguard, y esta enfocado a proveer soluciones de seguridad a sus clientes comercializando todas las lineas de negocio de Panda Security y Watchguard Technologies.
Cuenta con presencia y representación comercial en Merida, CDMX, Naucalpan, México, Guadalajara, Querétaro, Celaya, Monterrey, Guanajuato y Aguscalientes.
La misión de Cyber-T es hacer que la seguridad de nivel empresarial sea simple y rapida de incorporar para empresas de todos los tipos y tamaños a través del servicio, lo que convierte a Cyber-T en un buen aliado como proveedor de elección y confianza.

WEB www.watchguard.com

INTERNATIONAL SALES 1.206.613.0895

VENTAS MEXICO 55.2583.7474

WEB www.cybert.com.mx

Part No. WGCE67444_012821