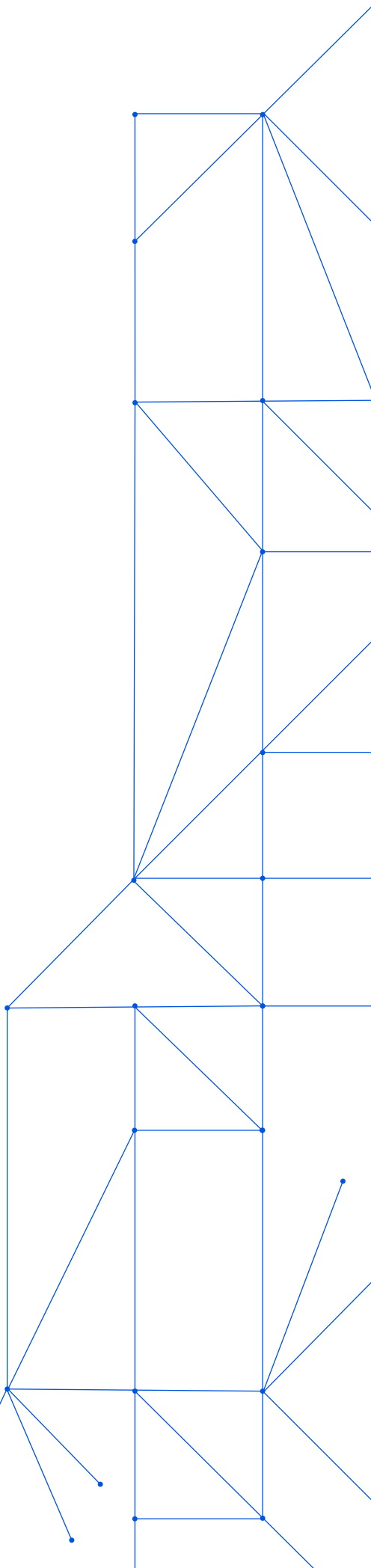
CLOUDFLARE

DOCUMENTO TÉCNICO

Guía de implementación de la arquitectura Zero Trust

Descubre los pasos, las herramientas y los equipos de trabajo necesarios para transformar tu red y modernizar tu seguridad

Contenido



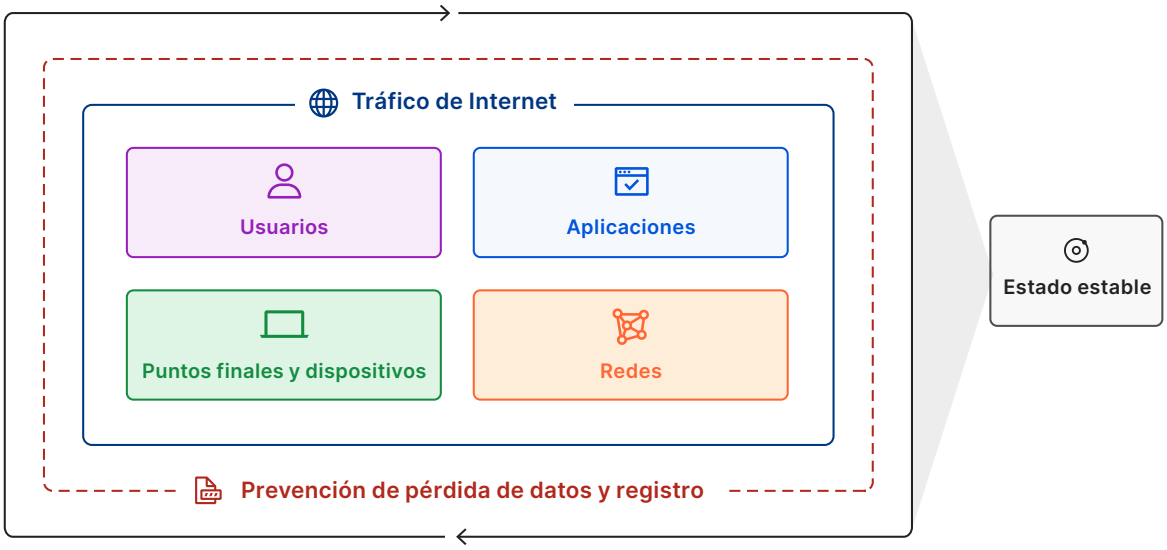
Introducción

La arquitectura de red tradicional se desarrolló sobre el principio de una red perimetral que otorgaba un nivel de confianza implícito a todo aquel que estaba en la red. El cambio hacia el alojamiento en la nube, el teletrabajo y otras innovaciones han planteado desafíos a la arquitectura de red perimetral tradicional.

Estos problemas se pueden abordar mediante la implementación de una arquitectura Zero Trust, que garantiza la verificación y la autorización de todo el tráfico que entra y sale de una empresa. La implementación de una arquitectura Zero Trust se puede hacer por etapas sin interrumpir la productividad y la conectividad de los usuarios.

Esta guía ha sido elaborada por expertos en seguridad para ofrecer una arquitectura Zero Trust multiproveedor y un ejemplo de cronograma de implementación. El cronograma parte de la base de que una organización está empezando su recorrido Zero Trust, pero pretende ser útil para todas las organizaciones.

Hay siete componentes principales que se deben tener en cuenta en la seguridad de una organización cuando se trata de implementar una arquitectura integral Zero Trust. El orden de implementación no tiene por qué coincidir con la enumeración de las secciones de los componentes y la arquitectura de referencia que aparecen a continuación.



Componentes de una arquitectura Zero Trust

	Componente	Objetivo	Nivel de esfuerzo	Página
Fase 1	Tráfico de Internet	Implementar el filtrado de DNS global	▮	9
	Aplicaciones	Supervisar los correos electrónicos entrantes y filtrar los intentos de phishing	▮	13
	Prevención de pérdida de datos y registros	Identificar configuraciones erróneas y datos compartidos públicamente en las herramientas SaaS	▮	20
Fase 2	Usuarios	Establecer una identidad corporativa	▮▮	5
	Usuarios	Aplicar la autenticación multifactor básica para todas las aplicaciones	▮	6
	Aplicaciones	Aplicar HTTPS y DNSSEC	▮	17
	Tráfico de Internet	Bloquear o aislar las amenazas detrás de SSL	▮▮	9-10
	Aplicaciones	Aplicar políticas ZT para aplicaciones de acceso público	▮	14-16
	Aplicaciones	Proteger las aplicaciones de los ataques a la capa 7	▮	16
	Redes	Cerrar todos los puertos de entrada abiertos a Internet para la entrega de aplicaciones	▮	12
Fase 3	Aplicaciones	Realizar un inventario de todas las aplicaciones corporativas	▮▮	13-14
	Aplicaciones	Aplicar políticas ZT para aplicaciones SaaS	▮▮	14-16
	Redes	Segmentar el acceso de los usuarios a la red	▮▮▮	11
	Aplicaciones	ZTNA para aplicaciones críticas de acceso privado	▮	14-16
	Dispositivos	Implementar soluciones MDM/UEM para controlar los dispositivos corporativos	▮▮	7
	Prevención de pérdida de datos y registros	Definir qué datos son confidenciales y dónde se alojan	▮▮	18-19
	Usuarios	Emitir tokens de autenticación basados en hardware	▮▮	6
	Prevención de pérdida de datos y registros	Familiarizarse con los ciberdelincuentes conocidos	▮	21
Fase 4	Usuarios	Aplicar la autenticación multifactor basada en tokens de hardware	▮▮	6
	Aplicaciones	Aplicar políticas ZT y de acceso a la red para todas las aplicaciones	▮▮▮	14-16
	Prevención de pérdida de datos y registros	Establecer un SOC para la revisión de registros, la actualización de políticas y la mitigación	▮▮	20
	Dispositivos	Implementar la protección de puntos finales	▮▮	7
	Dispositivos	Realizar un inventario de todos los dispositivos, API y servicios corporativos	▮	8
	Redes	Utilizar Internet de banda ancha para la conectividad entre filiales	▮▮▮	11-12
	Prevención de pérdida de datos y registros	Registrar y revisar la actividad de los usuarios en las aplicaciones confidenciales	▮▮	18
	Prevención de pérdida de datos y registros	Impedir que los datos confidenciales salgan de tus aplicaciones	▮▮▮	19
	Estado estable	Enfoque DevOps para la aplicación de políticas de nuevos recursos	▮▮	22
	Estado estable	Implementar el escalado automático para los recursos de acceso directo	▮▮▮	22-23

Definimos los diferentes niveles de esfuerzo necesarios para cada paso de la siguiente manera:

- ▮ - **Esfuerzo mínimo:** se necesita un único usuario o un pequeño equipo de trabajo.
- ▮▮ - **Esfuerzo medio:** se necesita un equipo de trabajo y una preparación avanzada.
- ▮▮▮ - **Esfuerzo importante:** se necesitan varios equipos de trabajo y un plan de proyecto.

Guía de implementación de Zero Trust

Usuarios

Este grupo incluye a empleados, proveedores y clientes. Para implementar una arquitectura Zero Trust, una organización tiene que saber con exactitud en quién debe confiar realmente y con qué, lo que se conoce como identidad. A continuación, debe establecer un método de autenticar de forma segura la identidad de sus usuarios.

Establecer una identidad corporativa

Nivel de esfuerzo	- **Esfuerzo medio**
Equipo(s) involucrado(s)	• Equipo responsable de tu proveedor de identidad (normalmente equipo de informática o seguridad) • Administradores que gestionan las aplicaciones internas que utilizan los empleados y socios
Producto(s)	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
Resumen	Se necesita una identidad corporativa unificada para autenticar y autorizar con precisión el acceso de los usuarios a las aplicaciones corporativas. Una identidad corporativa coherente simplificará la aplicación de políticas granulares para tus aplicaciones. **Otros puntos a tener en cuenta:** • ¿Está tu empresa inmersa en algún proceso de fusión o adquisición? ¿Cómo vas a consolidar los almacenes de identidades? • ¿Estás usando algún protocolo de autenticación no basado en la web (p. ej. directorio activo, ntlm, kerberos)?
Pasos	1. Añade todos los usuarios corporativos al proveedor de identidad. a. Estos valores se pueden sincronizar a menudo desde un sistema de RR.HH. como Workday, ADP, etc. 2. Verifica que la información de cada usuario es correcta. 3. Envía la información de registro de los nuevos usuarios para configurar las credenciales de acceso.

Aplicar la autenticación multifactor para todas las aplicaciones

Nivel de esfuerzo	 - **Esfuerzo mínimo** (si se aplica la autenticación multifactor básica)  - **Esfuerzo medio** (si se usan claves de seguridad)
Equipo(s) involucrado(s)	• Equipo responsable de tu proveedor de identidad (normalmente equipo de informática o seguridad) • Administradores que gestionan las aplicaciones internas que utilizan los empleados y socios
Producto(s)	**Proveedores de identidad:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **Proxies inversos para aplicaciones:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Claves de seguridad:** Yubico
Resumen	La autenticación multifactor (MFA) es el método que garantiza la mejor protección contra el robo de credenciales de usuarios a través de la suplantación de identidad o la fuga de datos. La mayoría de los métodos de autenticación multifactor se pueden habilitar directamente en un proveedor de identidad. Para las aplicaciones no integradas directamente con tu proveedor de identidad, contempla el uso de un proxy inverso delante de las aplicaciones para implementar la autenticación multifactor.
Pasos	1. Alerta a los usuarios internos de la próxima aplicación de la autenticación multifactor. Ofrece opciones de inicio de sesión que incluyan autenticadores por SMS o aplicaciones. 2. Activa la autenticación multifactor en tu proveedor de identidad. 3. Activa el proxy inverso delante de las aplicaciones no integradas con tu proveedor de identidad. 4. (Extra) Distribuye las claves del hardware a los empleados por correo electrónico o en persona. 5. (Extra) Aplica la autenticación multifactor solo con clave de hardware para tus aplicaciones confidenciales.

Puntos finales y dispositivos

Se incluye cualquier dispositivo, API o servicio de software dentro de una organización o con acceso a los datos de la organización. Las organizaciones deben conocer primero el conjunto de dispositivos, API y servicios que tienen. A continuación, se pueden aplicar políticas Zero Trust basadas en el contexto del dispositivo, la API y el servicio.

Implementar la gestión de dispositivos móviles

Nivel de esfuerzo	**- Esfuerzo medio**
Equipo(s) involucrado(s)	• Equipo informático
Producto(s)	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
Resumen	La mayoría de las arquitecturas Zero Trust requieren la instalación de software en al menos un subconjunto de equipos de usuario. La gestión de dispositivos móviles (MDM) es la forma en que la mayoría de las organizaciones gestionan el software y la configuración en su inventario de dispositivos de usuario.
Pasos	Consulta el sitio del proveedor de MDM para más información.

Implementar la protección de puntos finales

Nivel de esfuerzo	**- Esfuerzo medio**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo informático
Producto(s)	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
Resumen	El software de protección de puntos finales se instala en los equipos de los usuarios y analiza las amenazas conocidas que afectan a los dispositivos. También se puede utilizar para garantizar la conformidad de las revisiones y las actualizaciones del sistema operativo. La señal de tu software de protección de puntos finales se puede y se debe utilizar en tus políticas de control de acceso a aplicaciones.
Pasos	1. Instala el software de protección de puntos finales en los equipos de los usuarios usando la MDM. 2. Habilita la protección contra amenazas y el control de conformidad en la plataforma de protección de puntos finales.

Realizar inventario de los dispositivos, API y servicios

Nivel de esfuerzo	**- Esfuerzo mínimo**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo informático
Producto(s)	**Inventario de dispositivos:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **Inventario de API/servicios:** conector de aplicaciones de Cloudflare, Zscaler Private Access (ZPA)
Resumen	El software de protección de puntos finales y el software de gestión de activos se pueden utilizar para monitorear todos los dispositivos que se han distribuido a los usuarios. Se debe mantener una lista detallada de dispositivos para rastrear cuál de ellos son válidos y deben tener acceso a aplicaciones específicas. También hay que detectar y mantener las API y los servicios en un inventario. Se puede aprovechar el análisis de la red para identificar las API y los servicios de software recién vistos que se pueden comunicar a través de una red interna o externa.
Pasos	1. Instala el software de protección de puntos finales en los equipos de los usuarios usando la MDM. 2. Instala el escáner de API/servicios en tu red.

Tráfico de Internet

Incluye todo el tráfico de usuarios destinado a sitios web fuera del control de una organización. Puede abarcar desde tareas relacionadas con la empresa hasta el uso personal de sitios web. Todo el tráfico saliente es susceptible de ser objeto de malware y sitios peligrosos. Una organización debe establecer visibilidad y control sobre el tráfico de usuarios destinado a Internet.

Bloquear las solicitudes de DNS hacia amenazas conocidas o destinos peligrosos

Nivel de esfuerzo	**- Esfuerzo mínimo**
Equipo(s) involucrado(s)	• Equipo informático con acceso a la configuración del enrutador o dispositivo • Equipo de seguridad
Producto(s)	**Filtrado de DNS:** Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
Resumen	El filtrado de DNS se puede aplicar a través de la configuración del enrutador o directamente en el equipo del usuario. Es una de las formas más rápidas de proteger a los usuarios de sitios web maliciosos conocidos.
Pasos	**Filtrado de DNS:** actualiza la configuración de la resolución DNS en el wifi de tu oficina para que apunte al servicio de resolución DNS apropiado. Esta práctica se puede utilizar para bloquear sitios maliciosos conocidos.

Bloquear o aislar las amenazas detrás de SSL/TLS

Nivel de esfuerzo	**- Esfuerzo medio**
Equipo(s) involucrado(s)	• Equipo informático con acceso a la configuración del enrutador o dispositivo • Equipo de seguridad
Producto(s)	**Descifrado TLS:** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Aislamiento de navegador:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

Bloquear o aislar las amenazas detrás de SSL/TLS (continuación)

Resumen	Algunas amenazas se ocultan detrás de SSL y no se pueden bloquear solo con la inspección HTTPS. Se debe aprovechar el descifrado TLS para ofrecer mayor protección a los usuarios de las amenazas detrás de SSL.

Pasos	**Descifrado TLS:**
	1. Asegúrate de que el equipo del usuario tiene instalado el software de cliente correcto.
	  a. Comprueba si hay alguna VPN u otro software que pueda interferir con el tráfico web saliente en el dispositivo.
	2. Configura el certificado raíz en el dispositivo para el descifrado TLS.
	3. Activa políticas que establezcan cuándo evitar el descifrado del tráfico del usuario.
	  a. Se debe hacer para los sitios que utilizan asignación de certificados.
	  b. Algunas empresas también omiten el descifrado para el tráfico personal del usuario (p. ej. operaciones bancarias, redes sociales, etc.).
	
	Aislamiento del navegador:
	1. El aislamiento del navegador se puede implementar a través del software cliente en el dispositivo o a través de un enlace de aislamiento. Ambos enfoques se deben tener en cuenta.

Redes

Abarca todas las redes públicas, privadas y virtuales de una organización. Las organizaciones deben conocer primero el conjunto de redes que tienen y segmentarlas para evitar el movimiento lateral. A continuación, se pueden crear políticas Zero Trust que controlen de forma granular a qué segmentos de una red pueden acceder los usuarios, los puntos finales y los dispositivos.

Segmentar el acceso de los usuarios a la red

Nivel de esfuerzo	 **- Esfuerzo importante**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo informático
Producto(s)	**Acceso a la red Zero Trust (ZTNA):** Cloudflare Zero Trust (Access y Gateway juntos), Netskope Private Access, Zscaler Private Access (ZPA)
Resumen	Por lo general, los usuarios pueden acceder a toda una red privada utilizando una VPN o mientras están en la red de la oficina. Un marco Zero Trust requiere que los usuarios solo tengan acceso a los segmentos específicos de la red necesarios para completar una tarea determinada. Las soluciones de red Zero Trust permiten a los usuarios acceder a una red local de forma remota, pero con políticas granulares basadas en el usuario, el dispositivo y otros factores.
Pasos	1. Permite que tu red privada disponga de ZTNA a. Normalmente, un conector de aplicaciones, un túnel GRE o IPSec 2. Instala el cliente ZTNA en los dispositivos de los usuarios usando soluciones MDM. 3. Configura políticas para segmentar el acceso de los usuarios a través de la red privada.

Utilizar Internet de banda ancha para la conectividad entre filiales

Nivel de esfuerzo	 **- Esfuerzo importante**
Equipo(s) involucrado(s)	• Equipo de ingeniería de redes • Equipo informático
Producto(s)	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore

Utilizar Internet con banda ancha para la conectividad entre filiales (continuación)

Resumen	La conectividad entre las ubicaciones de la red privada (p. ej. los centros de datos y las filiales) se ha establecido generalmente utilizando líneas de conmutación de etiquetas multiprotocolo (MPLS) u otras formas de conexiones privadas que ofrecen los proveedores de telecomunicaciones. Estas conexiones MPLS suelen ser caras, y como la red pública de consumo es ahora de mayor calidad, las organizaciones pueden proporcionar el mismo nivel de acceso seguro enrutando el tráfico a través de Internet mediante túneles seguros a precio inferior.
Pasos	1. Elige dos ubicaciones conectadas por MPLS para empezar. Estas ubicaciones necesitarán algún tipo de conectividad a Internet. 2. Crea un par de túneles redundantes GRE Anycast o IPsec sobre tus circuitos de Internet a la red perimetral de tu proveedor de WAN en la nube. 3. Verifica el estado y la conectividad entre esos túneles. Comprueba que el rendimiento (capacidad de proceso, latencia, pérdida de paquetes, vibración) de las cargas de trabajo de tráfico sea lo más igual posible al tráfico de producción. 4. Cambia las políticas de enrutamiento para migrar el tráfico de producción de MPLS a los túneles de Internet. 5. Repite en la siguiente ubicación conectada a MPLS 6. Elimina los circuitos MPLS.

Cerrar todos los puertos de entrada abiertos a Internet para la entrega de aplicaciones

Nivel de esfuerzo	**- Esfuerzo mínimo**
Equipo(s) involucrado(s)	• Equipo de ingeniería de redes
Producto(s)	**Proxies inversos Zero Trust:** Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Resumen	Se pueden encontrar puertos de red entrantes abiertos utilizando tecnología de análisis y son un vector de ataque común. Los proxies inversos Zero Trust te permiten exponer de forma segura una aplicación web sin abrir ningún puerto de entrada. El registro DNS de la aplicación es el único registro de la aplicación visible públicamente, y está protegido con políticas Zero Trust. Como capa de seguridad adicional, se puede aprovechar el DNS interno/privado utilizando un servicio de acceso a la red Zero Trust (más detalles a continuación).
Pasos	1. Instala el conector de la aplicación de proxy inverso - normalmente un daemon o máquina virtual en algún lugar de la misma red. 2. Conecta la aplicación de proxy inverso al conector de aplicaciones. 3. Cierra todos los puertos de entrada en la red privada con una regla de firewall.

Aplicaciones

Incluyen cualquier recurso en el que existan datos de la organización o se realicen procesos empresariales. Las organizaciones deben conocer primero las aplicaciones que tienen y luego crear políticas Zero Trust para cada una de ellas o, en algunos casos, bloquear las aplicaciones no autorizadas.

Supervisar las aplicaciones de correo electrónico y filtrar los intentos de phishing

Nivel de esfuerzo	**- Esfuerzo mínimo**
Equipo(s) involucrado(s)	• Equipo responsable de la configuración de tu proveedor de correo electrónico (normalmente el equipo informático)
Producto(s)	**Seguridad del correo electrónico en la nube:** Seguridad del correo electrónico de Cloudflare Area 1, Mimecast, TitanHQ **Aislamiento de navegador:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
Resumen	El correo electrónico es uno de los pocos canales de comunicación a los que los atacantes acceden a tus usuarios sin restricciones. La implementación de una puerta de enlace segura de correo electrónico es un paso fundamental para garantizar que los correos electrónicos maliciosos o que no son de confianza no lleguen a tus usuarios. Además, los equipos de seguridad deben contemplar la opción de poner en cuarentena en un navegador aislado aquellos enlaces que no sean lo suficientemente sospechosos como para bloquearlos completamente.
Pasos	1. Configura los registros MX de tu dominio para que apunten al servicio de puerta de enlace de correo electrónico seguro 2. Supervisa los falsos positivos en las primeras semanas 3. (Extra) Implementa un enfoque de aislamiento del navegador para casos probables de enlaces de correo electrónico sospechosos

Realizar un inventario de todas las aplicaciones corporativas

Nivel de esfuerzo	**- Esfuerzo medio**
Equipo(s) involucrado(s)	• Equipo de seguridad
Producto(s)	**Puerta de enlace web segura y agente de seguridad de acceso a la nube (CASB) con detección de elementos de Shadow IT:** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)

Realizar un inventario de todas las aplicaciones corporativas (continuación)

Resumen	Es fundamental que el equipo de seguridad conozca el inventario completo de las aplicaciones utilizadas en la empresa. Los equipos de seguridad de elementos de Shadow IT descubren a menudo aplicaciones no autorizadas o desconocidas que se utilizan en la empresa. Se puede utilizar una puerta de enlace web segura con descifrado TLS para identificar las aplicaciones. La puerta de enlace web segura también se puede utilizar para bloquear aplicaciones o inquilinos de aplicaciones no autorizados (p. ej. cuentas personales de Dropbox).
Pasos	1. Activa el análisis de Shadow IT en la puerta de enlace web segura. 2. Asegúrate de que los dispositivos de los usuarios tienen instalado el cliente de puerta de enlace web segura. 3. Permite 2-3 semanas de tráfico de los usuarios. 4. Revisa la lista de aplicaciones identificadas. 5. Cualquier aplicación no autorizada se debe bloquear con las políticas de puerta de enlace web segura. 6. Las aplicaciones autorizadas se deben proteger con políticas de Zero Trust.

Aplicar políticas Zero Trust para aplicaciones

Nivel de esfuerzo	**- Esfuerzo mínimo (para aplicaciones esenciales)** **- Esfuerzo importante (para todas las aplicaciones)**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo de desarrollo de aplicaciones • Equipo informático
Producto(s)	**Proxies inversos Zero Trust:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Acceso a la red Zero Trust (ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB **Aislamiento remoto del navegador:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

Aplicar políticas Zero Trust para aplicaciones (continuación)

Resumen	Las aplicaciones se deben proteger con políticas Zero Trust que tengan en cuenta la identidad del usuario, el dispositivo y el contexto de la red antes de autenticar y autorizar el acceso. Las aplicaciones deben tener políticas granulares que apliquen privilegios mínimos, sobre todo en aplicaciones que contienen datos confidenciales. Hay tres tipos principales de aplicaciones y el modelo de seguridad Zero Trust varía para cada uno de ellos. Los principales tipos de aplicaciones son: 1. Aplicaciones privadas autoalojadas (accesibles solo en la red corporativa). 2. Aplicaciones públicas autoalojadas (accesibles a través de Internet) 3. Aplicaciones SaaS. **Nota:** si el contexto del dispositivo o el estado de cumplimiento es una política de seguridad requerida, normalmente se requiere un software cliente en dispositivo.
Pasos	**Aplicaciones privadas autoalojadas** 1. Crea un túnel encriptado entre la aplicación y la capa de política Zero Trust. Normalmente será un "conector de aplicaciones", un túnel GRE o IPSec. 2. Permite que los usuarios del cliente en dispositivo ZTNA puedan acceder al solucionador DNS privado. 3. Crea políticas basadas en el usuario, el dispositivo y el contexto de la red para establecer quién puede acceder a la aplicación. **Aplicaciones públicas autoalojadas** 1. Traslada el DNS autoritativo o un registro CNAME al proxy inverso de la aplicación. 2. Asegúrate de que todos los puertos de entrada están cerrados para la red de la aplicación. 3. Crea políticas basadas en el contexto del usuario, el dispositivo y la red para establecer quién puede acceder a la aplicación. **Aplicaciones SaaS** Existen varias opciones para aplicar políticas Zero Trust a las aplicaciones SaaS. **Proxy de identidad** Cloudflare, Netskope y Zscaler ofrecen proxies de identidad que permiten la misma aplicación de políticas que una aplicación autoalojada de proxy inverso. Este caso requiere que el proxy de identidad se configure como el proveedor de inicio se sesión único (SSO) de la aplicación SaaS. 1. Elimina la integración SSO existente en la aplicación SaaS, si hay. 2. Integra el proxy de identidad con la aplicación SaaS. 3. Asegúrate de que se envían los atributos SAML correctos para la creación y actualización de usuarios. 4. Crear políticas basadas en el usuario, el dispositivo y el contexto de red.

Aplicar políticas Zero Trust para aplicaciones (continuación)

Pasos	**Puerta de enlace web segura y SSO** El otro enfoque es utilizar un proveedor de SSO existente para controlar qué usuarios pueden acceder a la aplicación SaaS y cuales no. A continuación, se puede utilizar la puerta de enlace web segura, con una dirección IP dedicada, para garantizar que solo los usuarios de dispositivos administrados con inspección de tráfico puedan acceder a la aplicación SaaS. 1. Añade la aplicación SaaS al proveedor SSO. 2. Crea políticas para determinar qué usuarios están autorizados. 3. Añade la dirección IP de la instancia de la puerta de enlace web segura a la lista de direcciones IP permitidas de la aplicación SaaS (la mayoría de las aplicaciones SaaS admiten listas de direcciones IP permitidas en sus configuraciones de seguridad básica). 4. Crea políticas de puerta de enlace web segura que controlen qué usuarios pueden acceder a la aplicación SaaS.

Proteger las aplicaciones de los ataques a la capa 7 (DDoS, inyección, bots, etc.)

Nivel de esfuerzo	**- Esfuerzo mínimo**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo de desarrollo de aplicaciones
Producto(s)	Akamai, AWS, Azure, Cloudflare, GCP
Resumen	Cualquier aplicación autoalojada es susceptible de sufrir ataques a la capa 7 como DDoS, inyección de código, bots y otros. Los equipos de seguridad deben implementar un firewall de aplicaciones web y medidas de protección contra DDoS delante de todas las aplicaciones autoalojadas y de acceso privado o público.
Pasos	1. Añade el registro DNS autoritativo de cualquier aplicación pública. 2. Activa el firewall de aplicaciones web y la protección contra DDoS.

Aplicar HTTPS y DNSSEC

Nivel de esfuerzo	**- Esfuerzo mínimo**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo de desarrollo de aplicaciones
Producto(s)	Akamai, AWS, Azure, Cloudflare, GCP
Resumen	Cualquier aplicación web autoalojada debe usar HTTPS y DNSSEC. De esta manera se evita cualquier posibilidad de rastreo de paquetes o secuestro de dominios.
Pasos	1. Añade el registro DNS autoritativo de cualquier aplicación pública. 2. Configura HTTPS como estricto y activa DNSSEC.

Prevención de pérdida de datos y registro

Una vez que hayas establecido todos los componentes Zero Trust de tu arquitectura que hemos mencionado hasta aquí, tu arquitectura generará grandes volúmenes de datos sobre lo que está ocurriendo dentro de tu red. Ahora es el momento de implementar la prevención de pérdida de datos y el registro. Se trata de un conjunto de procesos y herramientas que se centran en mantener los datos confidenciales dentro de la empresa y marcar cualquier fuga de datos posible. Las organizaciones deben saber primero dónde se encuentran sus datos confidenciales. A continuación, pueden establecer controles Zero Trust para bloquear el acceso a los datos confidenciales y su filtración.

Establecer un proceso para registrar y revisar el tráfico en las aplicaciones confidenciales

Nivel de esfuerzo	**- Esfuerzo medio**
Equipo(s) involucrado(s)	• Equipo de seguridad
Producto(s)	**Puerta de enlace web segura (SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Gestión de eventos e información de seguridad (SIEM):** DataDog, Splunk, SolarWinds
Resumen	Las soluciones de puerta de enlace web segura pueden trasladar los registros de tráfico de los usuarios a una herramienta SIEM. Un equipo de seguridad debería hacer periódicamente el ejercicio de revisar los registros de tráfico destinados a las aplicaciones confidenciales. Las alertas específicas para el tráfico anómalo o malicioso se pueden configurar y ajustar en el SIEM con el tiempo.
Pasos	1. Asegúrate de que todo el tráfico de los usuarios destinado a las aplicaciones confidenciales se redirecciona mediante proxy utilizando la puerta de enlace web segura. 2. Activa la función de envío o recepción de registros entre tu puerta de enlace web segura y el SIEM. 3. Configura un intervalo específico para que el equipo de seguridad revise los registros de tráfico. 4. Configura alertas en el SIEM basadas en los resultados a lo largo del tiempo.

Definir qué datos son confidenciales y dónde se alojan

Nivel de esfuerzo	**- Esfuerzo medio**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo de cumplimiento/jurídico
Producto(s)	**Gestión de eventos e información de seguridad (SIEM):** DataDog, Splunk, SolarWinds

Definir qué datos son confidenciales y dónde se alojan (continuación)

Resumen	Los datos confidenciales varían mucho en función del sector. Las empresas tecnológicas se preocupan por proteger el código fuente, mientras que los proveedores de servicios médicos se centran más en el cumplimiento de la ley HIPAA. Es importante establecer qué datos son confidenciales para tu empresa y dónde se alojan. Una definición y un inventario precisos de los datos confidenciales servirán de base para la aplicación de las herramientas de prevención de la pérdida de datos.
Pasos	1. Revisa los registros de tráfico en las herramientas SIEM o directamente en una puerta de enlace web segura para identificar las aplicaciones y los almacenes de datos objetivo. 2. Realiza un inventario de los datos confidenciales actuales.

Impedir que los datos confidenciales salgan de tus aplicaciones

Nivel de esfuerzo	 **- Esfuerzo importante**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo informático • Equipo de cumplimiento/jurídico
Producto(s)	**Prevención de pérdida de datos en línea (DLP):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
Resumen	Las soluciones de DLP en línea inspeccionan el tráfico de usuarios y las cargas/descargas de archivos en busca de datos confidenciales. Los datos confidenciales están disponibles en listas predefinidas bien conocidas (p. ej. PII, números de la seguridad social, tarjetas de crédito, etc.) o un administrador puede configurar manualmente patrones específicos. Se deben activar controles de DLP para las aplicaciones confidenciales y se pueden ampliar para todo el tráfico de usuarios.
Pasos	1. Instala el software cliente del proveedor de DLP. 2. Asegúrate de que no existe una VPN u otra herramienta que pueda interrumpir la conexión. 3. Asegúrate de que el descifrado TLS está activado y de que hay un certificado raíz en cada equipo de usuario. 4. Activa controles de DLP. 5. Supervisa los eventos de bloqueo de DLP y verifica si es legítimo o un falso positivo.

Identificar las configuraciones erróneas y los datos compartidos públicamente en las herramientas SaaS

Nivel de esfuerzo	**- Esfuerzo mínimo**
Equipo(s) involucrado(s)	• Equipo de seguridad
Producto(s)	**Agente de seguridad de acceso a la nube basado en la API (CASB):** Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
Resumen	Los CASB se integran con las principales aplicaciones SaaS a través de una integración API. A continuación, el CASB analizará la aplicación SaaS en busca de errores de configuración de seguridad conocidos y de datos que se hayan compartido públicamente. El equipo de seguridad debe establecer una cadencia regular para revisar los hallazgos del CASB.
Pasos	1. Conecta cada aplicación SaaS a través de las instrucciones de integración de la API del proveedor. 2. Ejecuta análisis para cada aplicación SaaS. 3. Revisa los resultados de los análisis y comienza la solución en cada aplicación SaaS cuando proceda.

Establecer un centro de operaciones de seguridad (SOC) para la revisión de registros, actualizaciones de políticas y mitigación

Nivel de esfuerzo	**- Esfuerzo medio**
Equipo(s) involucrado(s)	• Equipo de seguridad
Producto(s)	**Ninguno**
Resumen	Un SOC es una función crítica dentro de un equipo de seguridad en un marco Zero Trust. Se debe centrar en la revisión de la información de los registros y las alertas de seguridad, y en el ajuste de las políticas Zero Trust en todos los productos de seguridad esenciales.
Pasos	1. Revisa los registros en el SIEM o directamente en el producto de seguridad. 2. Identifica cualquier alerta o actividad anómala. 3. Actualiza las políticas Zero Trust en cada herramienta sobre la base de los resultados.

Familiarizarse con los ciberdelincuentes conocidos

Nivel de esfuerzo	**- Esfuerzo mínimo**
Equipo(s) involucrado(s)	• Equipo de seguridad
Producto(s)	**Proveedores de información sobre amenazas:** Cloudflare Radar, CISA, OWASP
Resumen	Existen varios proveedores dedicados a la recopilación de listas de ciberdelincuentes conocidos y sitios web maliciosos. Estas fuentes de amenazas se pueden cargar de manera automática en una puerta de enlace web segura para proteger a los usuarios de los ataques.
Pasos	1. Conecta la fuente de amenazas a la puerta de enlace web segura. 2. Activa la protección contra amenazas en el filtrado de DNS y HTTP.

Estado estable

Una vez que hayas desarrollado tu arquitectura Zero Trust para todos los demás componentes de tu organización, puedes adoptar varias medidas para garantizar el estado estable de Zero Trust en tu organización, garantizando la coherencia con la arquitectura en el futuro.

Usar un enfoque DevOps para garantizar la aplicación coherente de políticas para todos los nuevos recursos

Nivel de esfuerzo	 **- Esfuerzo importante**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo de desarrollo de aplicaciones
Producto(s)	**Automatización de la infraestructura:** Ansible, Puppet, Terraform
Resumen	Las herramientas de automatización de infraestructura permiten a los desarrolladores implementar de manera automática la seguridad Zero Trust como parte de su plan de desarrollo de aplicaciones. Define pruebas internas que se activen si una aplicación se implementa con la protección de proxy inverso Zero Trust.
Pasos	1. Define una política estándar para las nuevas aplicaciones. 2. Añade pruebas en el proceso de implementación de aplicaciones que requieran la protección de proxy inverso Zero Trust.

Implementar el escalado automático para los recursos de acceso directo

Nivel de esfuerzo	 **- Esfuerzo importante**
Equipo(s) involucrado(s)	• Equipo de seguridad • Equipo de desarrollo de aplicaciones
Producto(s)	**Equilibradores de carga:** Akamai, Cloudflare **Automatización de la infraestructura:** Ansible, Puppet, Terraform

Implementar el escalado automático para los recursos de acceso directo (continuación)

Resumen	Los equilibradores de carga pueden ser herramientas eficaces para garantizar que la infraestructura de las aplicaciones individuales nunca se sobrecargue, así como para proporcionar un nivel de redundancia si un servidor de aplicaciones comenzara a fallar. Las herramientas de automatización de la infraestructura se pueden utilizar para poner en marcha nuevos recursos si se superan determinados umbrales de tráfico.
Pasos	1. Configura un equilibrador de carga frente al conector de aplicaciones de proxy inverso Zero Trust. 2. Activa reglas de equilibrio de carga basadas en los volúmenes de tráfico y/o la geolocalización de los usuarios. 3. Implementa políticas de automatización de la infraestructura que faciliten nuevos equipos virtuales si se genera suficiente carga para un conjunto específico de aplicaciones.

Ejemplo de cronograma de implementación

Cada implementación de arquitectura Zero Trust es única, pero la mayoría de los proyectos se adhieren a un conjunto de pasos comunes. A continuación, recomendamos el siguiente cronograma a cualquier empresa que esté iniciando su recorrido hacia la implementación de una arquitectura Zero Trust.

Cronograma		Objetivo	Productos relevantes
Fase 1	☐	Implementar el filtrado de DNS global	Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
	☐	Supervisar los correos electrónicos entrantes y filtrar los intentos de phishing	Seguridad del correo electrónico en la nube: Cloudflare Area 1 Email Security, Mimecast, TitanHQ Aislamiento de navegador: Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	Identificar configuraciones erróneas y datos compartidos públicamente en las herramientas SaaS	Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
Fase 2	☐	Establecer una identidad corporativa	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
	☐	Aplicar la autenticación multifactor básica para todas las aplicaciones	Proveedores de identidad: Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin Proxies inversos de aplicaciones: Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	Aplicar HTTPS y DNSSEC	Akamai, AWS, Azure, Cloudflare, GCP
	☐	Bloquear o aislar las amenazas detrás de SSL	Descifrado TLS: Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) Aislamiento de navegador: Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	Aplicar políticas ZT para aplicaciones de acceso público	Proxies inversos Zero Trust: Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	Proteger las aplicaciones de los ataques a la capa 7	Akamai, AWS, Azure, Cloudflare, GCP
	☐	Cerrar todos los puertos de entrada abiertos a Internet para la entrega de aplicaciones	Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Fase 3	☐	Realizar un inventario de todas las aplicaciones corporativas	Puerta de enlace web segura y agente de seguridad de acceso a la nube (CASB) con detección de elementos de Shadow IT: Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
	☐	Aplicar políticas ZT para aplicaciones SaaS	Acceso a la red Zero Trust (ZTNA): Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) CASB: Cloudflare CASB, Netskope CASB, Zscaler CASB

	☐ **Segmentar el acceso de los usuarios a la red**	**Acceso a la red Zero Trust (ZTNA):** Cloudflare Zero Trust (Access y Gateway juntos), Netskope Private Access, Zscaler Private Access (ZPA)
	☐ **ZTNA para aplicaciones críticas de acceso privado**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **Implementar soluciones MDM/UEM para controlar los dispositivos corporativos**	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
	☐ **Definir qué datos son confidenciales y dónde se alojan**	DataDog, Splunk, SolarWinds
	☐ **Emitir tokens de autenticación basados en hardware**	**Claves de seguridad:** Yubico
	☐ **Familiarizarse con los ciberdelincuentes conocidos**	Cloudflare Radar, CISA, OWASP
Fase 4	☐ **Aplicar la autenticación multifactor basada en tokens de hardware**	**Claves seguras:** Yubico
	☐ **Aplicar políticas ZT y acceso a la red para todas las aplicaciones**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **Establecer un SOC para la revisión de registros, la actualización de políticas y la mitigación**	n/a
	☐ **Implementar la protección de puntos finales**	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
	☐ **Realizar un inventario de todos los dispositivos, API y servicios corporativos**	**Inventario de dispositivos:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **Inventario de API/servicios:** conector de aplicaciones de Cloudflare, Zscaler Private Access (ZPA)
	☐ **Utilizar Internet de banda ancha para la conectividad entre filiales**	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore
	☐ **Establecer un proceso para registrar y revisar la actividad de los empleados en las aplicaciones confidenciales**	**Puerta de enlace web segura (SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Gestión de eventos e información de seguridad (SIEM):** DataDog, Splunk, SolarWinds
	☐ **Impedir que los datos confidenciales salgan de tus aplicaciones (p. ej. PII, tarjetas de crédito, números de la seguridad social, etc.)**	Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
	☐ **Usar un enfoque DevOps para garantizar la aplicación de políticas para todos los nuevos recursos**	Ansible, Puppet, Terraform
	☐ **Implementar el escalado automático para los recursos de acceso directo**	**Equilibradores de carga:** Akamai, Cloudflare **Automatización de la infraestructura:** Ansible, Puppet, Terraform

CLOUDFLARE

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-3584.09AGO2022