

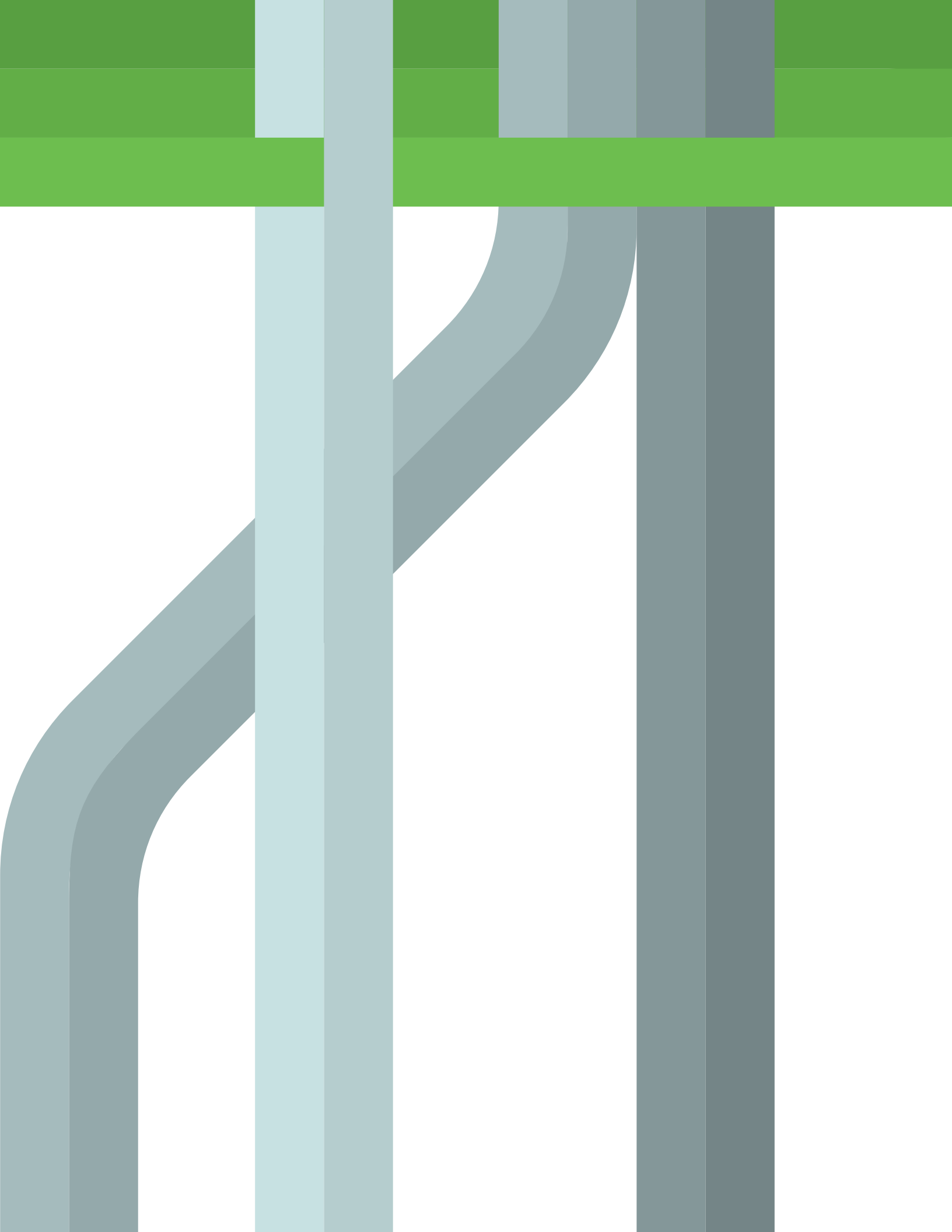
Guía de evaluación de Zero Trust

Para la fuerza laboral



Duo Security ahora
forma parte de Cisco





CONTENIDO

¿POR QUÉ ZERO TRUST?	1
ZERO TRUST: PARA LA FUERZA LABORAL	5
GENERAR CONFIANZA EN EL USUARIO	7
OBTENER VISIBILIDAD DE LOS DISPOSITIVOS	9
GENERAR CONFIANZA EN EL DISPOSITIVO	12
APLICACIÓN DE POLÍTICAS ADAPTATIVAS	15
HABILITAR EL ACCESO SEGURO A TODAS LAS APLICACIONES	18
ZERO TRUST DE DUO PARA LA FUERZA LABORAL	21
DUO BEYOND Y ACCESO CONFIABLE DE CISCO	27

Hoy en día, el aumento de una fuerza laboral remota, móvil y conectada a la nube ha puesto la visibilidad y el control de los usuarios y dispositivos fuera de la empresa.

¿Por qué
Zero Trust?



**PROVEEDORES Y
CONTRATISTAS**



**DISPOSITIVOS
MÓVILES Y
PERSONALES**



PERÍMETRO ORIGINAL

- TERMINALES
- USUARIOS EN EL SITIO
- SERVIDORES
- APLICACIONES
- CENTROS DE DATOS

NUEVO PERÍMETRO DE IDENTIDAD



**EMPLEADOS
REMOTOS**



**APLICACIONES E
INFRAESTRUCTURA
EN LA NUBE**

El perímetro se ha extendido más allá de los muros de la empresa, lo que dificulta a los equipos de seguridad y de TI verificar las identidades de los usuarios y la confianza de sus dispositivos, antes de otorgar acceso a las aplicaciones y los datos de la empresa.

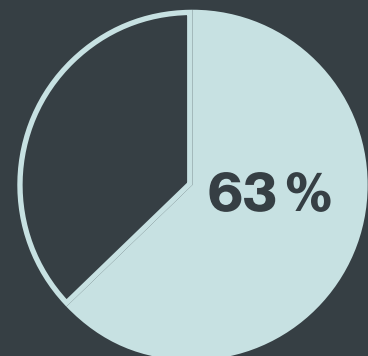
El nuevo modelo de fuerza laboral hoy en día requiere un modelo de seguridad igualmente extendido. **El perímetro extendido ahora se centra en la identidad del usuario y sus dispositivos.** El modelo de seguridad de la fuerza laboral extendida debe poder generar confianza en el usuario y en el dispositivo, sin importar dónde se encuentre físicamente el usuario y sin importar desde qué tipo de red se conecte.

Zero Trust trata cada intento de acceso como si se originara en una red no confiable. **Un modelo centrado en la confianza se centra en la autenticación de cada usuario y dispositivo antes de otorgar acceso a cualquier aplicación.**

Un enfoque Zero Trust no requiere una reinversión completa de su infraestructura. Las soluciones más exitosas deben superponer y admitir un entorno híbrido sin reemplazar por completo las inversiones existentes.

RIESGO DEL NUEVO PERÍMETRO DE IDENTIDAD

Las credenciales comprometidas son un objetivo principal de los atacantes, ya que permiten un acceso fácil y sin protección debido a la suplantación de identidad (phishing), los ataques de fuerza bruta y otros ataques con contraseña. En un análisis de campañas simuladas de suplantación de identidad (phishing), el **Informe de acceso confiable de Duo de 2018** descubrió que más de la mitad (63 %) captó correctamente las credenciales de usuario.



Los diferentes modelos de Zero Trust

El concepto de Zero Trust puede verse en el modelo **CARTA de Gartner**: evaluación adaptativa continua de riesgo y confianza. Esto requiere un cambio de las decisiones de acceso binario por única vez hacia decisiones contextuales, basadas en el riesgo y en la confianza. Este modelo consiste en brindar suficiente confianza a los usuarios, incluso después de la autenticación, para completar la acción solicitada.

Zero Trust eXtended (ZTX) de Forrester se refiere a la división de los “perímetros monolíticos” en una serie de microperímetros o segmentos de red para aplicar controles de seguridad granulares a su alrededor. Pero también reconocen que es mucho más que una simple segmentación de la red: es un enfoque integral para proteger los datos, la red, los dispositivos, las cargas de trabajo y las fuerzas laborales.

Google BeyondCorp es la implementación de una arquitectura Zero Trust que requiere la identificación segura del usuario y el dispositivo, la eliminación de la confianza de la red, la externalización de aplicaciones y el flujo de trabajo y la implementación de control de acceso basado en el inventario.

Todos estos modelos requieren más controles en torno a la identidad como el nuevo perímetro: los usuarios y sus dispositivos a medida que acceden a las aplicaciones y los servicios. Hay muchos componentes diferentes de un modelo Zero Trust que requieren proteger diferentes flujos de trabajo:

Fuerza laboral

Asegúrese de que solo los usuarios correctos y los dispositivos seguros puedan acceder a las aplicaciones

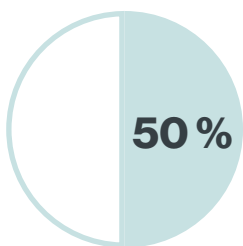
Carga de trabajo

Proteja todas las conexiones dentro de sus aplicaciones, en varias nubes.


Lugar de trabajo

Proteja todas las conexiones de usuarios y dispositivos en toda la red, incluida la IoT.

Un enfoque es comenzar garantizando que solo los usuarios correctos y los dispositivos de usuarios seguros accedan a las aplicaciones; su fuerza laboral: la base de un modelo Zero Trust. Esta guía se centra en evaluar los criterios necesarios para adoptar un enfoque de seguridad centrado en la confianza para la fuerza laboral.



Gartner predice que la seguridad como servicio representará al menos el 50 % de la entrega de software de seguridad para el año 2020.



El alcance de esta guía se centrará en Zero Trust en relación con la protección de la **fuerza laboral**, es decir, los usuarios y los dispositivos que utilizan para acceder a las aplicaciones de trabajo. Los usuarios pueden incluir empleados, partners, proveedores, contratistas y muchos otros, lo que dificulta el mantenimiento del control sobre sus dispositivos y el acceso.

Un enfoque Zero Trust para la fuerza laboral debe proporcionar a la organización las herramientas para poder evaluar y tomar decisiones de acceso basadas en un contexto específico basado en riesgos.

Por ejemplo:

- + **¿El usuario es quien dice ser?**
- + **¿Tienen acceso a las aplicaciones adecuadas?**
- + **¿El dispositivo es seguro?**
- + **¿Su dispositivo es confiable?**

Los equipos de seguridad deben poder responder estas preguntas para establecer confianza en los usuarios y dispositivos que acceden a los recursos de una organización. También deben hacerlo mediante un enfoque que equilibre la seguridad con la facilidad de uso.

Este enfoque de seguridad centrado en la confianza para el perímetro extendido hace que sea mucho más difícil para los atacantes o usuarios no autorizados obtener acceso a aplicaciones sin cumplir con ciertos criterios basados en la identidad, el dispositivo y la aplicación.

Zero Trust: para la fuerza laboral

Considere los siguientes pasos para emprender su recorrido de Zero Trust hacia la protección de su fuerza laboral:

Generar confianza en el usuario

¿Puede verificar que sus usuarios sean quienes dicen ser? ¿Está utilizando una solución de MFA escalable y sin complicaciones?

Usar MFA y generar confianza en el usuario es el primer paso para desarrollar un modelo Zero Trust y protegerse contra credenciales comprometidas, suplantación de identidad (phishing) y otros ataques basados en contraseñas.

Obtener visibilidad de los dispositivos del usuario

¿Tiene una perspectiva detallada de cada tipo de dispositivo que accede a sus aplicaciones en todas las plataformas?

La transparencia en cada terminal le permite ver cuál de ellos podría presentar un riesgo para su entorno: el software desactualizado puede contener fallas de seguridad que los atacantes pueden aprovechar.

Generar confianza en el dispositivo

¿Puede verificar el estado de seguridad y la confianza de todos los dispositivos de los usuarios que acceden a sus aplicaciones?

¿Puede admitir de manera segura todos los dispositivos y BYOD (traiga su propio dispositivo), tanto los dispositivos corporativos como los personales?

En el momento del inicio de sesión, verifique la confiabilidad de los dispositivos de los usuarios para determinar su estado de seguridad, independientemente de quién administre o tenga control sobre el dispositivo.

Aplicar políticas adaptativas

¿Puede aplicar políticas contextuales granulares basadas en el usuario, el dispositivo y la ubicación para proteger el acceso a aplicaciones específicas?

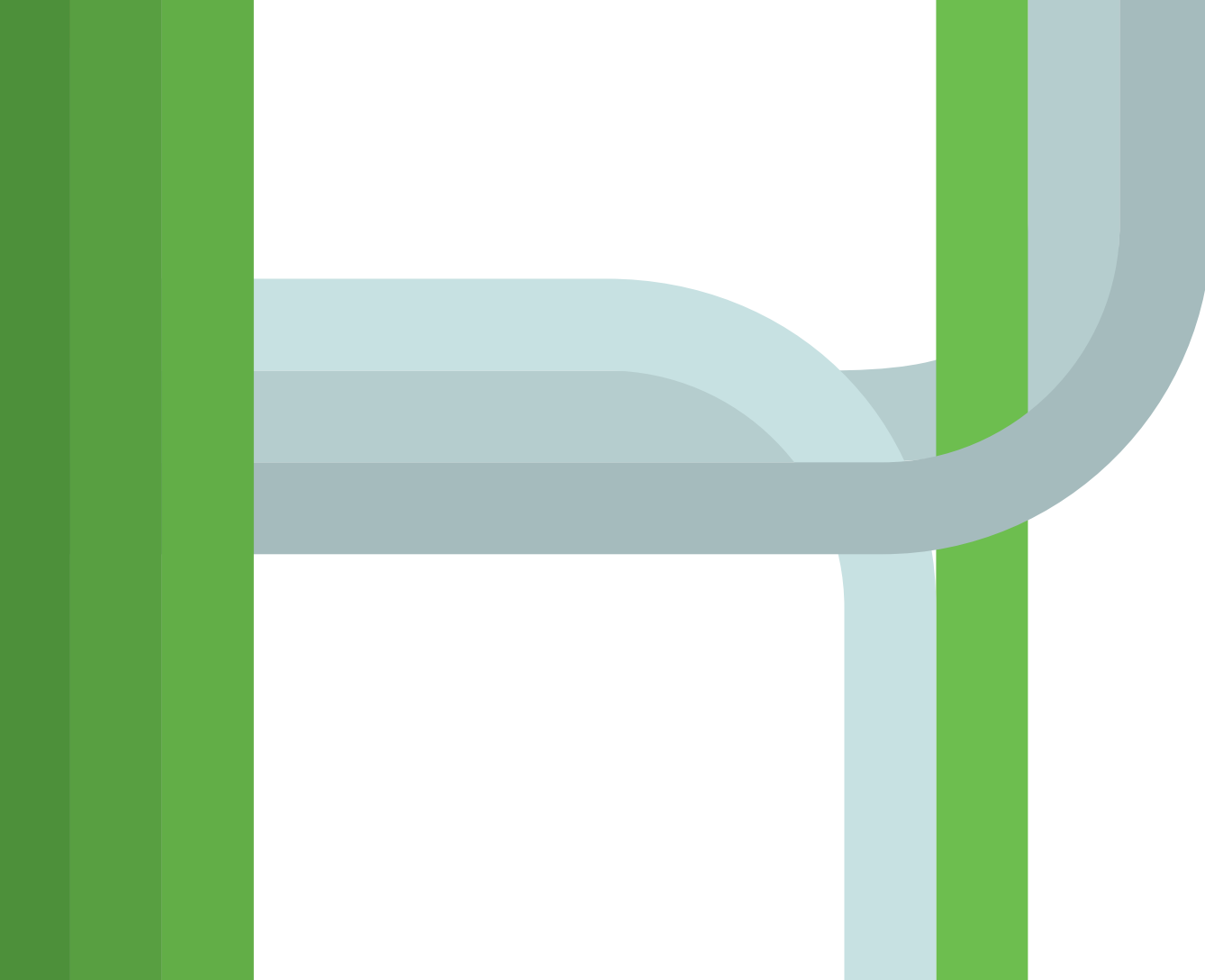
Al aplicar políticas de acceso contextual que evalúan el riesgo en función de atributos como la ubicación, el rol del usuario, el tipo de dispositivo, etc., puede tener un control más dinámico sobre quién y qué puede acceder a ciertas aplicaciones, lo que permite solo la cantidad mínima de acceso requerida para que un usuario haga su trabajo.

Habilitar el acceso seguro a todas las aplicaciones

¿Puede brindar a sus usuarios una experiencia de inicio de sesión segura y consistente para las aplicaciones en la instalación y la nube?

Implemente MFA y la información del dispositivo para permitir el acceso seguro a todos los diferentes tipos de aplicaciones, servicios y plataformas. La combinación de un usuario confiable y un dispositivo confiable hace que sea más difícil para un usuario no autorizado hacerse pasar por legítimo que inicia sesión en sus aplicaciones.

Esta guía profundizará en cada paso y lo ayudará a dar forma a sus criterios y requisitos de la tecnología y las soluciones para proporcionar acceso seguro y confiable de los usuarios y sus dispositivos a las aplicaciones laborales.



01.

Generar confianza en el usuario

El primer paso para crear una arquitectura Zero Trust para la fuerza laboral es verificar las identidades de los usuarios al inician sesión en sus aplicaciones, servicios y plataformas laborales en la nube y en las instalaciones.

¿Puede confiar en que sus usuarios son quienes dicen ser? ¿Y cómo reduce la amenaza de credenciales y dispositivos comprometidos provocada por la suplantación de identidad (phishing), malware y otros vectores, al tiempo que cumple con los requisitos de cumplimiento normativo de seguridad de acceso?

Autenticación multifactor

Verifique las identidades de sus usuarios con una solución de autenticación multifactor (MFA) escalable y sin complicaciones.

Admitir a cada usuario

¿Su solución MFA ofrece opciones flexibles de autenticación para adaptarse a una amplia gama de usuarios, perfiles de seguridad y antecedentes técnicos? Asegúrese de que su solución sea compatible con empleados, viajeros frecuentes, contratistas, proveedores, clientes, partners, etc.

Debe poder personalizar y aplicar qué métodos de MFA pueden utilizarse. Para un acceso más seguro a las aplicaciones de alto riesgo, se requiere el uso de:



Notificaciones push móviles fuera de banda y fáciles de usar



Claves de seguridad **universales DE SEGUNDO factor (U2F)** a prueba de suplantación de identidad (phishing)



WebAuthn biométrica

Fácil administración

¿Su solución de MFA es fácil de implementar para los administradores? Elija una solución basada en la nube que requiera una infraestructura y un personal mínimos para implementar la reducción de la carga de trabajo de su equipo.

¿Proporciona opciones de inscripción de usuarios y aprovisionamiento para escalar a medida que crece su organización? Por ejemplo:



Autoinscripción



API administrativas para aprovisionamiento escalable de usuarios



Opción para sincronizar usuarios de directorios existentes, como Active Directory y Azure AD

Ahorre en capacitación, soporte y casos continuos del centro de asistencia con la autoinscripción de usuarios y el autoservicio; permita que los usuarios se inscriban en MFA y administren sus propios dispositivos de autenticación sin asistencia administrativa.

Reduzca el riesgo con una solución de autenticación multifactor flexible, fácil de usar y fácil de implementar.



02.

Obtener visibilidad de los dispositivos

A continuación, evalúe si su solución puede brindarle información sobre los dispositivos que se conectan a sus aplicaciones y datos que puede aprovechar para controlar el acceso en función del estado de seguridad del dispositivo.

¿Tiene visibilidad de cada tipo de dispositivo de usuario final: móvil, de escritorio y portátil? ¿Existe una herramienta que centralice la autenticación y los datos de terminales en diferentes plataformas de dispositivos? ¿Puede obtener fácilmente una descripción general de los usuarios, los terminales y la actividad de autenticación?

Visibilidad de dispositivos

Obtenga información detallada sobre el estado de la seguridad de cada tipo de dispositivo (ya sea administrado por la empresa o personal) que accede a sus aplicaciones.

En todas las plataformas

Algunas soluciones de visibilidad de dispositivos solo ofrecen información limitada sobre ciertas plataformas y sistemas operativos, como solo aquellos que ejecutan Windows o equipos de escritorio. Reduzca la necesidad de acceder a diferentes sistemas de datos con un tablero centralizado que permite a los administradores supervisar:



TODOS LOS EQUIPOS DE ESCRITORIO, PORTÁTILES Y DISPOSITIVOS MÓVILES

Ya sea corporativo o de propiedad personal



NAVEGADORES

Chrome, Firefox, Edge, Internet Explorer, etc. (versiones, cantidad de dispositivos desactualizados)



SISTEMAS OPERATIVOS

Windows, Mac, iOS, Android, etc. (versiones, cantidad de dispositivos desactualizados)



COMPLEMENTOS

Java y Flash (versiones, cantidad de dispositivos desactualizados, habilitados, desactivados o desinstalados)

“Zero Trust exige que los equipos de seguridad conserven visibilidad y control en todo el ecosistema empresarial digital, independientemente de la ubicación, el dispositivo, la población de usuarios o el modelo de alojamiento”.

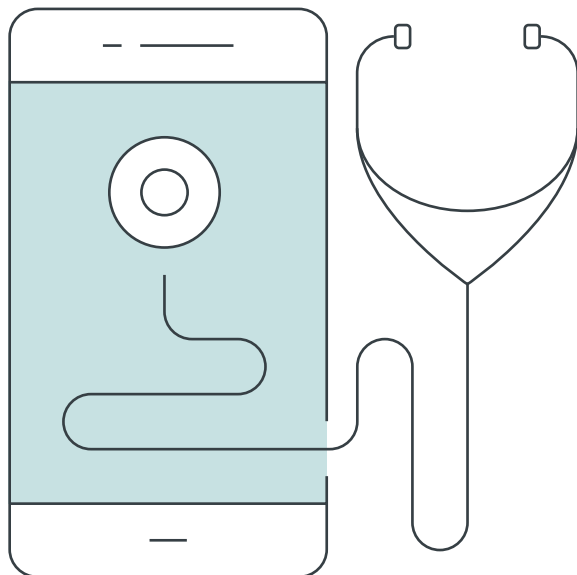
—Forrester Zero Trust eXtended (ZTX)

Admite BYOD y dispositivos móviles

El perímetro extendido presenta nuevos desafíos en torno a la protección de BYOD (traiga su propio dispositivo). Un modelo de confianza cero debe funcionar bien con la infraestructura existente sin causar problemas y admitir cualquier tipo de dispositivo.

Debe poder obtener información sobre los dispositivos personales y corporativos, incluidos los dispositivos móviles. Los dispositivos BYO pueden no cumplir con los requisitos de seguridad o pueden estar ejecutando versiones de software antiguas propensas a vulnerabilidades.

Una solución integral de visibilidad de dispositivos debe permitirle identificar dispositivos móviles con ciertas funciones de seguridad activadas o desactivadas, así como su estado de seguridad:



SISTEMA OPERATIVO

Versión de iOS o Android



CIFRADO DE DISCO



BLOQUEO DE PANTALLA



BIOMETRÍA

Huella digital, identificación táctil o facial



ESTADO DEL DISPOSITIVO

Liberado, descifrado o manipulado

Informes y registros de dispositivos

Muchas auditorías y regulaciones de cumplimiento requieren actividad del usuario y registros e informes de seguridad de los dispositivos. ¿Su solución de visibilidad de dispositivos puede brindarle acceso a informes detallados sobre el comportamiento del usuario y los dispositivos riesgosos, todo en un tablero? ¿Se integra bien con cualquier software SIEM (información de seguridad y administración de eventos) existente?

Asegúrese de que sus administradores tengan informes fácilmente accesibles y exportables para los auditores, con información sobre autenticaciones, usuarios, administradores, políticas y más.



03.

Generar confianza en el dispositivo

Al iniciar sesión, verifique el estado de seguridad de todos los dispositivos de usuarios que intentan acceder a sus aplicaciones. Generar confianza va más allá de administrar el estado del dispositivo e incluye la inspección y el control del acceso basado en dispositivos móviles y personales.

¿Puede aplicar controles de terminales para dispositivos riesgosos o de propiedad corporativa? ¿Cómo genera confianza en los dispositivos móviles? ¿Puede notificar automáticamente a los usuarios sobre software desactualizado para reducir los casos del centro de asistencia?

Aplicación de controles de terminales

Al aprovechar la visibilidad de los dispositivos que se conectan a sus aplicaciones (como se mencionó anteriormente), debe poder establecer políticas de acceso basadas en dispositivos para evitar que cualquier dispositivo riesgoso o no confiable acceda a sus aplicaciones.

Acceso a dispositivos basado en riesgos

Para tener acceso a aplicaciones de alto riesgo, puede requerir que un dispositivo sea propiedad de la empresa o esté administrado por el equipo de TI de su organización. Las aplicaciones de alto riesgo pueden incluir sistemas de historias clínicas electrónicas (EHR) como Epic que contienen información de salud del paciente; infraestructura de la nube como Microsoft Azure y Google Cloud Platform; y muchos otros.

¿Puede aplicar políticas de acceso basadas en el riesgo de la aplicación o si el dispositivo es corporativo o personal?
¿Y puede hacerlo sin requerir certificados de terminales?

Además, puede requerir MFA para acceder a aplicaciones más confidenciales a fin de garantizar un mayor nivel de identidad de los usuarios. ¿Puede exigir a sus usuarios que utilicen notificaciones push, claves de seguridad de U2F o WebAuthn biométrico antes de otorgarles acceso a ciertas aplicaciones?

Generar confianza en los dispositivos móviles

Asegúrese de que su solución le permita establecer confianza en los dispositivos móviles con o sin el uso de software de administración de dispositivos móviles (MDM).

Los usuarios pueden oponerse a la instalación de MDM en sus dispositivos personales por cuestiones de privacidad, lo que da como resultado una menor adopción general y una menor comprensión de la seguridad de sus dispositivos. Y, a veces, está fuera del control de su equipo de TI instalar un agente en los dispositivos personales de proveedores externos que puedan necesitar acceso a sus aplicaciones.

Ya sea que tenga una solución de MDM o no, debe poder bloquear el acceso de los dispositivos a las aplicaciones por:

- + Versiones del SO, navegador y complementos y cuánto tiempo han estado desactualizadas
- + Estado de las funciones de seguridad activadas (configuradas o desactivadas)
- + Cifrado completo del disco
- + Identificación biométrica de dispositivos móviles (Face ID/Touch ID)
- + Bloqueo de pantalla
- + Manipulación (liberado, descifrado o no aprobó SafetyNet de Google)

Notificar a los usuarios para actualizar los dispositivos riesgosos

¿Su solución permite a los usuarios administrar sus propios dispositivos? Elija una solución que pueda detectar versiones de software anteriores y luego notifique a los usuarios cuando el software de su dispositivo esté desactualizado.

Para aliviar la carga del equipo de soporte del centro de asistencia, solicite a los usuarios que actualicen el software en sus propios dispositivos al iniciar sesión. Un portal de autoservicio también les permite administrar fácilmente sus propios dispositivos de autenticación sin enviar un caso al centro de asistencia.



Aplique controles y políticas para evitar que los terminales riesgosos accedan a sus aplicaciones.



04.

Aplique políticas adaptativas

Aplique políticas de acceso contextual que permitan el acceso a sus aplicaciones con controles basados en el usuario, el dispositivo y la ubicación. El contexto incluye diferentes aspectos de su intento de inicio de sesión: dónde se encuentran, qué rol tienen en su organización, qué tipo de dispositivo utilizan, etc.

Limite el acceso solo a lo que los usuarios necesitan para hacer su trabajo y agregue controles más estrictos para acceder a aplicaciones más sensibles, sin afectar negativamente los flujos de trabajo de los usuarios. ¿Puede personalizar las políticas según los usuarios, los grupos de usuarios o la ubicación del usuario? ¿O desafiar a los usuarios con un método de MFA más seguro, según la aplicación a la que acceden?

Políticas de acceso contextual

Personalice las políticas para permitir, denegar o exigir una seguridad más estricta basada en roles y responsabilidades específicos del usuario, dispositivos y aplicaciones, todo mientras se equilibra la seguridad con la facilidad de uso.

Políticas de acceso basadas en roles

No todos los usuarios necesitan acceso a todas las aplicaciones. ¿Puede personalizar el acceso según el tipo de grupo de usuarios? Brinde a los contratistas o proveedores de terceros acceso temporal y restringido a aplicaciones o sistemas no confidenciales.

Debe poder aplicar políticas para otorgar un mayor nivel de acceso a los administradores y usuarios con privilegios, al tiempo que garantiza que solo los desarrolladores tengan acceso a sus entornos de producción y a la infraestructura de la nube.

Compruebe que los administradores puedan:

- + Personalizar las políticas según el usuario, el grupo o sus roles y responsabilidades específicos
- + Establecer políticas personalizadas basadas en el método de autenticación
- + Solo permite que los usuarios se autenticuen mediante ciertos métodos
- + Use fácilmente grupos de usuarios de Active Directory o Azure AD para aplicar políticas

Políticas de aplicaciones específicas

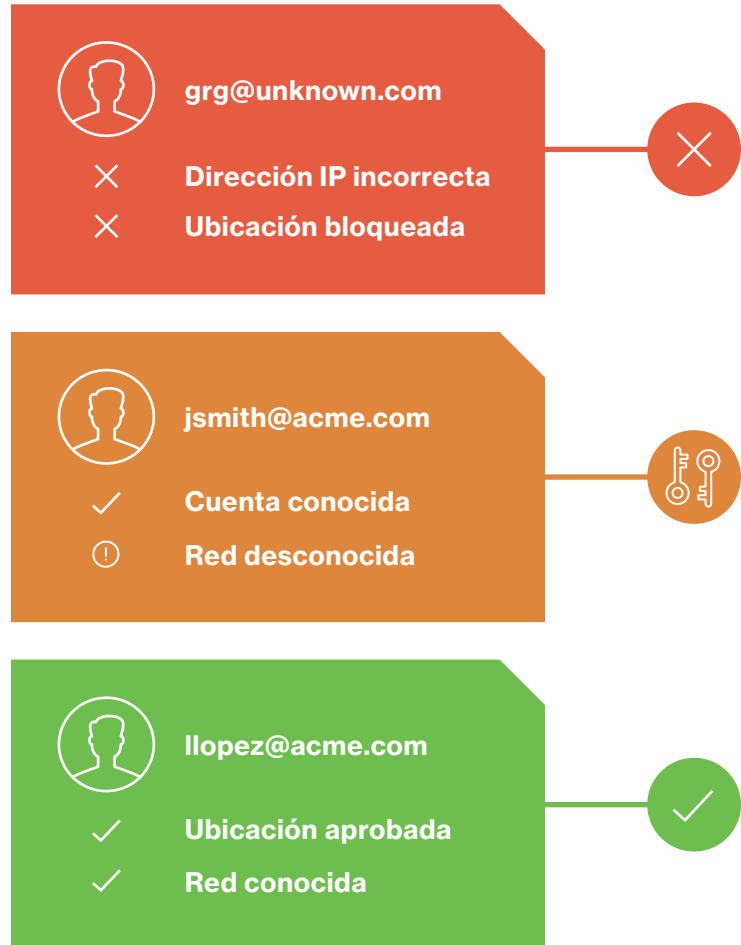
Aplique el uso de métodos MFA más seguros para el acceso a aplicaciones y servicios cruciales para el negocio a fin de reducir el riesgo de acceso no autorizado.

Sus administradores deben poder configurar políticas específicas de la aplicación para requerir solo el uso de claves de seguridad U2F basadas en inserción para verificar las identidades de los usuarios antes de otorgar acceso a estas aplicaciones. El uso de métodos más seguros requiere un mayor nivel de aseguramiento de la identidad del usuario; fortaleciendo el control de acceso a sus aplicaciones y datos más confidenciales.

Ubicación del usuario

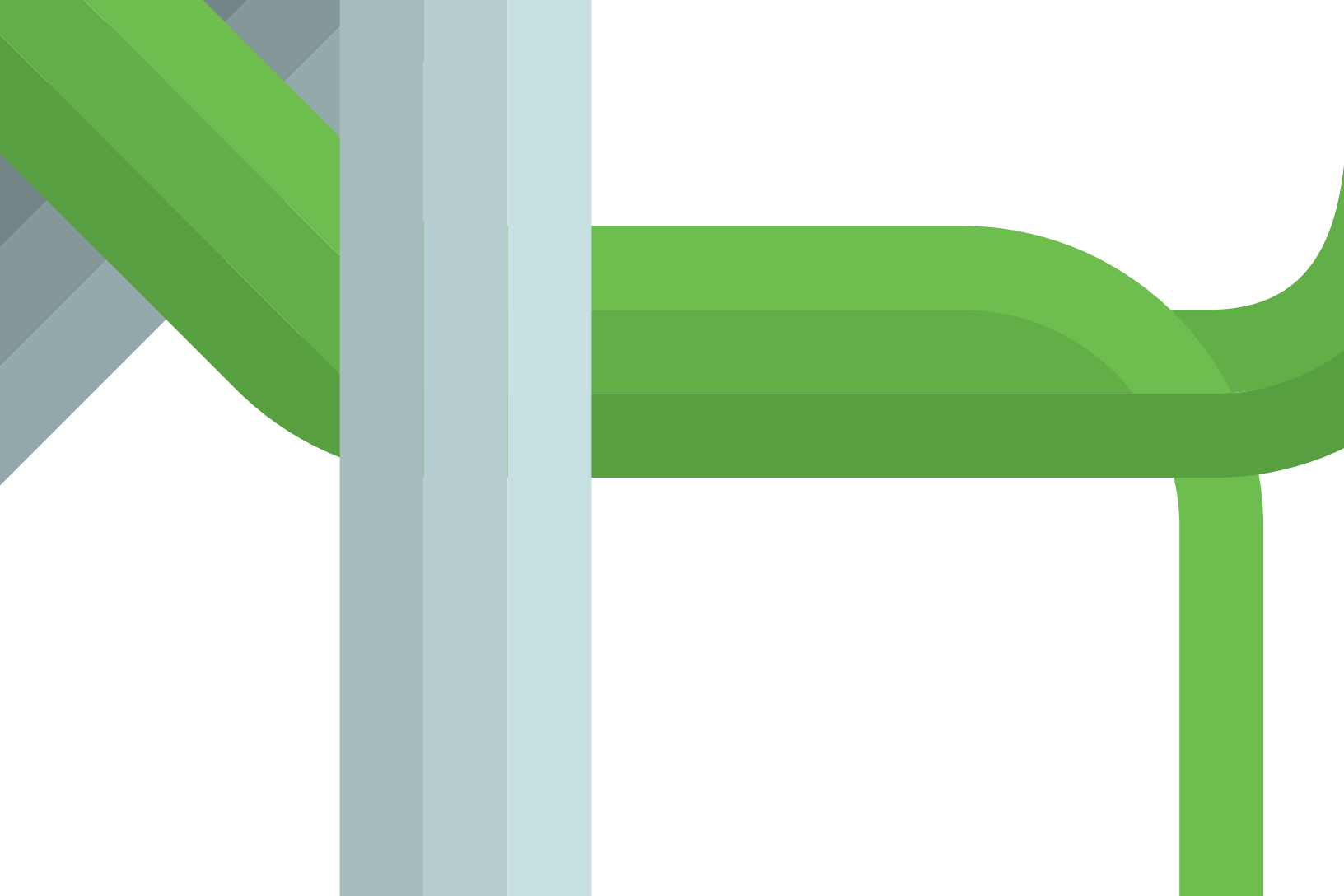
Evite el acceso no autorizado desde cualquier ubicación geográfica con políticas de acceso basadas en el usuario. Si no realiza negocios en ciertos países, debe poder bloquear los intentos de acceso que se originan en esas regiones.

Los administradores también deben poder bloquear los intentos de autenticación basados en un conjunto de rangos de direcciones IP o aquellos que provienen de redes anónimas como Tor o proxies. Sin embargo, las direcciones IP no bloqueadas no implican que se permita el acceso; este es solo un atributo a tener en cuenta en el contexto más amplio de una solicitud de acceso.



“Pasar de las macrodecisiones 'buenas' a las 'malas' hacia un conjunto de decisiones más pequeñas basadas en el contexto. Otorgue suficiente confianza a entidades como los usuarios, incluso una vez que hayan sido autenticados, para completar la acción solicitada”.

—Evaluación adaptativa continua de riesgo y confianza de Gartner (CARTA)



05.

Habilitar el acceso seguro a todas las aplicaciones

Brinde a los usuarios acceso seguro y uniforme a todas las aplicaciones, servicios y plataformas, sin importar dónde estén alojados.

Proteger sus inversiones

Puede ser una organización hacia la nube o una gran empresa con una combinación compleja de aplicaciones y de infraestructura en las instalaciones heredadas y en la nube. Sea lo que sea, asegúrese de proteger el acceso a todo esto con MFA, políticas de acceso contextual y controles y visibilidad del dispositivo.

Acceso remoto

El cambio a la infraestructura de la nube ha dificultado que las organizaciones apliquen controles de acceso más sólidos en entornos híbridos y multinube.

Su solución debe simplificar y mantener la uniformidad de la experiencia de inicio de sesión del usuario, sin importar dónde se encuentren, cuando se conecten a diversos sistemas y aplicaciones alojados en diferentes entornos de nube.

Asegúrese de poder garantizar el acceso a:



Entornos multinube, como Azure, AWS y Google Cloud Platform



Infraestructura, entornos de desarrollo/ DevOps y servidores internos de Linux



Aplicaciones web HTTPS y servidores SSH



Red privada virtual (VPN) y aplicaciones de acceso remoto

Aplique controles de seguridad más sólidos para permitir solo el acceso de los dispositivos administrados y actualizados a la infraestructura y los entornos de desarrollador.

Acceso a la nube/a la identidad

Acceso seguro a todas sus aplicaciones en la nube, como Office 365, Google, Box, Dropbox, Slack y más, así como acceso a cualquier inicio de sesión único (SSO) existente, proveedores de identidad y servicios de federación. Asegúrese de que su solución proporcione acceso seguro a cualquier aplicación en la nube habilitada para SAML 2.0.

Las mejores prácticas recomiendan proteger el acceso a estas aplicaciones separando el método de autenticación principal del secundario (mediante MFA). Deje de depender únicamente de un proveedor de autenticación principal para evitar una infracción basada en el proveedor que pueda exponer la autenticación primaria y secundaria.

Inicio de sesión único (SSO) seguro

Para una experiencia de inicio de sesión uniforme, permita que los usuarios inicien sesión una vez para acceder a todas sus aplicaciones laborales internas y en la nube con una solución segura de inicio de sesión único (SSO).

Proteja su SSO con MFA y políticas de acceso contextual y verifique la seguridad de los dispositivos de los usuarios cada vez antes de otorgar acceso.



Acceso seguro a todas las aplicaciones, servicios y plataformas, ya sea multinube, en las instalaciones, personalizado, acceso remoto o VPN.



Zero Trust de Duo para la fuerza laboral

Duo le ofrece los cimientos para un modelo de seguridad Zero Trust al generar confianza con los usuarios y dispositivos antes de otorgarles acceso a las aplicaciones, lo cual garantiza un acceso seguro desde cualquier lugar para todos los usuarios y dispositivos que se conectan con alguna aplicación.

Cada vez que un usuario inicia sesión en una aplicación, Duo verifica la confianza de su identidad y la seguridad de su dispositivo, antes de otorgar acceso solo a las aplicaciones que necesita. Duo le ofrece controles y políticas adaptativas para tomar decisiones de acceso en función del riesgo de los usuarios, los dispositivos y las aplicaciones.

Generar confianza en el usuario

Verifique la identidad de sus usuarios con una autenticación multifactor (MFA) sólida que proporcione una cobertura flexible y amplia para cada tipo de usuario.

Autenticación multifactor

Elimine la amenaza de ataques que provienen de credenciales comprometidas con la **autenticación multifactor** fácil y eficaz de Duo. El MFA intuitivo de Duo facilita la inscripción y los inicios de sesión seguros para los usuarios, lo que reduce la fricción en su flujo de trabajo. Los usuarios pueden tocar rápidamente un botón en una notificación de **Duo Push** enviada a su teléfono inteligente a través de la aplicación de autenticación de **Duo Mobile** para verificar su identidad.

Para todo tipo de usuarios

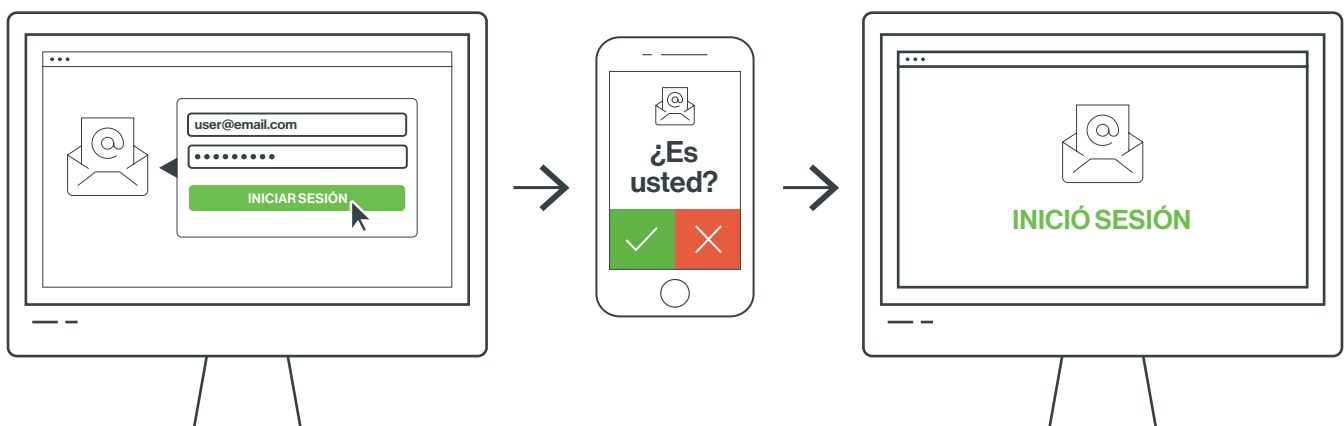
El MFA de Duo funciona bien para todos los grupos de usuarios de la empresa, incluidos empleados, contratistas, proveedores, clientes, partners, etc., que admiten políticas de acceso específicas para grupos de usuarios.

Diseñado para admitir todos los escenarios de inicio de sesión de usuarios, desde fuera de línea a servicios celular limitados y conectividad a Internet, Duo ofrece muchos **métodos diferentes de MFA**, incluidas aplicaciones móviles, notificaciones push, opciones sin conexión, **WebAuthn biométrico**, claves de seguridad y más.

Además, con las políticas de acceso de Duo, los administradores pueden requerir el uso de ciertos métodos para acceder a aplicaciones más confidenciales a fin de garantizar más la identidad de los usuarios.

Fácil de implementar

Los administradores se benefician de las integraciones nativas de Duo, la fácil configuración basada en la nube y la solución de bajo mantenimiento. Las opciones de registro automatizado de Duo, como la **inscripción automática de usuarios** y las opciones de sincronización de Active Directory, permiten el aprovisionamiento escalable de usuarios. Para reducir la administración y los casos del centro de asistencia, el **portal de autoservicio** de Duo permite a los usuarios administrar rápida y fácilmente sus propios dispositivos de autenticación.



Obtener visibilidad de los dispositivos del usuario

Obtenga una descripción detallada de los dispositivos de sus usuarios con la **visibilidad de los terminales** de Duo y una **vista única** del estado de seguridad general con Duo Admin Panel que indica los dispositivos riesgosos.

En todas las plataformas

Obtenga **visibilidad completa** de dispositivos móviles, portátiles, de escritorio y de PC en todas las plataformas (Windows, Mac, iOS, Android y Chrome). Identifique y supervise los dispositivos corporativos y personales para obtener información sobre su estado de seguridad.

Admite BYOD y dispositivos móviles

Obtenga mayor información y control de BYOD con la plataforma de Duo que detecta y rastrea cada dispositivo que tiene acceso a aplicaciones protegidas, incluidas computadoras de escritorio, computadoras portátiles y dispositivos móviles, sin utilizar un agente.

Identifique tanto los dispositivos corporativos administrados por TI como los de propiedad personal con **Trusted Endpoints** de Duo. Utilice la infraestructura de administración de dispositivos existente para generar y reforzar la confianza en los dispositivos con las integraciones de Duo con Active Directory, AirWatch, Google, Jamf, Landesk, MobileIron y Sophos sin la necesidad de implementar y administrar una infraestructura de certificados de PKI compleja.

Tablero centralizado

Los administradores obtienen una interfaz centralizada e intuitiva para administrar fácilmente usuarios, dispositivos y políticas a nivel global, así como informes y registros de seguridad para las auditorías de cumplimiento.

Los **informes detallados** de Duo proporcionan a los administradores datos sobre el comportamiento de los usuarios y los dispositivos riesgosos, así como datos de usuarios, administradores y telefonía, todo fácilmente integrable con los sistemas de administración de eventos e información de seguridad (SIEM).



Generar confianza en el dispositivo

Duo ofrece a los administradores visibilidad de los riesgos de usuarios y dispositivos y la capacidad de aplicar controles que eviten que las amenazas y los dispositivos riesgosos obtengan acceso a aplicaciones y datos confidenciales.

Acceso a dispositivos basado en riesgos

Los administradores pueden admitir políticas de BYOD marcando los terminales como **confiables o no confiables**, a la vez que aplican políticas que requieren mayor seguridad o limitan el acceso de los dispositivos no confiables.

Generar confianza en los dispositivos móviles

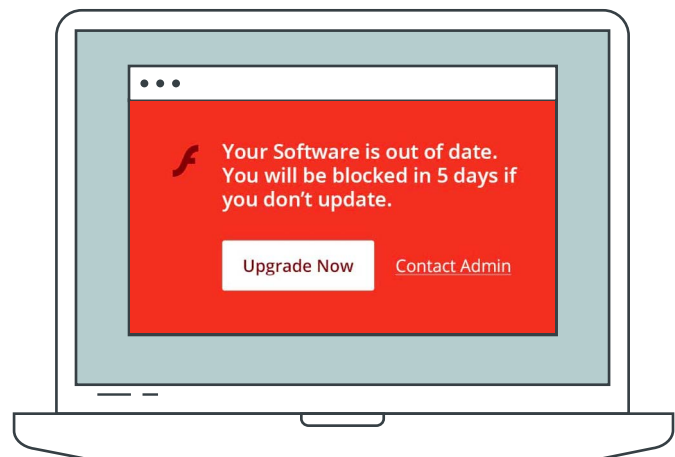
Con **Duo Mobile para Trusted Endpoints**, puede bloquear el acceso de los dispositivos a las aplicaciones basándose en lo siguiente:

- + Versiones del SO, navegador y complementos y cuánto tiempo han estado desactualizadas
- + Estado de las funciones de seguridad habilitadas (configuradas o deshabilitadas):
 - + Cifrado completo del disco
 - + Identificación biométrica de dispositivos móviles (Face ID/Touch ID)
 - + Bloqueo de pantalla
 - + Manipulación (liberado, descifrado o no aprobó SafetyNet de Google)

La aplicación Duo Mobile instalada en los teléfonos de los usuarios puede servir como herramienta de verificación de dispositivos administrados con Android/iOS.

Notificar a los usuarios para actualizar los dispositivos riesgosos

Para aliviar la carga de su equipo de soporte y reducir los casos de soporte, la **corrección automática** de Duo notifica y ayuda a los usuarios a actualizar los dispositivos desactualizados. Informe a los usuarios que se les negará el acceso por una cantidad determinada de días salvo que realicen una actualización y proporcione un enlace directo para actualizar su software para cerrar brechas de seguridad más rápidamente.



Aplique políticas adaptativas

Duo le ofrece los controles para limitar el acceso de los usuarios y terminales riesgosos a las aplicaciones según el riesgo condicional (autenticación adaptable).

Políticas de acceso basadas en roles

El principio de privilegios mínimos implica limitar el acceso a los datos y las aplicaciones solo a las personas que necesitan acceso para hacer su trabajo. Duo le permite establecer controles de acceso basados en roles y restringir el acceso a las aplicaciones según los roles de los usuarios y las responsabilidades laborales.

Por ejemplo, puede usar el marco de políticas de Duo para garantizar que solo los desarrolladores tengan acceso a la infraestructura crítica alojada en AWS, y que solo puedan acceder a ella mediante dispositivos emitidos por la empresa que ejecutan el último sistema operativo, mediante el método seguro de MFA Duo Push.

Políticas de aplicaciones específicas

Aplique el uso de métodos de MFA más seguros (Duo Push, U2F, etc.) para el acceso a aplicaciones y servicios de alto riesgo (como aquellos con datos financieros, de salud, RR. HH. u otros datos confidenciales) para un mayor nivel de garantía de las identidades de los usuarios. Requieren que los usuarios se autenticuen para cada sesión nueva, lo que solicita a los usuarios que pasen un tiempo determinado.

Ubicación del usuario

Para cumplir con las leyes regionales de privacidad de datos, es posible que deba aplicar políticas de acceso según la ubicación. Para permitirle hacerlo, Duo le permite establecer políticas para otorgar o denegar acceso a sus aplicaciones en función de dónde proviene el usuario/dispositivo (un conjunto de rangos de direcciones IP).

También puede solicitar MFA para ciertas ubicaciones. Además, Duo le permite bloquear los intentos de autenticación de sus aplicaciones desde redes anónimas como Tor y proxies.

Habilitar el acceso seguro a todas las aplicaciones

Duo ofrece una **amplia cobertura en cada aplicación** con integraciones listas para usar para configurar fácilmente todo tipo de aplicaciones, desde herramientas antiguas hasta herramientas modernas. Para las aplicaciones personalizadas, Duo también ofrece API, WebSDK y soporte para otros protocolos que le permiten ampliar la plataforma de seguridad de Duo para proteger los servicios patentados.

Duo brinda acceso flexible y sin complicaciones a entornos híbridos y multinube, lo que le permite aplicar un enfoque de seguridad de confianza cero para el acceso remoto a la infraestructura de la nube y las aplicaciones corporativas.

Acceso remoto

Protéjase contra credenciales comprometidas y proteja el acceso a sus proveedores de gateway de acceso remoto con la integración de Duo para redes privadas virtuales (VPN), infraestructura de escritorio virtual (VDI) y proxies como Cisco AnyConnect, Juniper, F5, Citrix y más.

Acceso a la nube/a la identidad

A medida que las organizaciones migran sus aplicaciones e infraestructura a la nube, Duo puede proteger completamente un entorno híbrido y multinube. Duo ofrece a los usuarios acceso remoto uniforme a entornos multinube e híbridos, incluidos los proveedores de infraestructura de nube, así como las aplicaciones en las instalaciones y en la nube.

Duo admite casos de uso de acceso a la nube, como desarrolladores que acceden a Amazon Web Services (AWS) y contratistas que necesitan acceso remoto a aplicaciones internas. El MFA de Duo también se integra con otras ofertas de SSO como Ping, Azure, Okta, Oracle y Shibboleth, lo que ofrece integración de identidad con AD y SAML.

Inicio de sesión único (SSO) seguro

Los usuarios obtienen una experiencia de inicio de sesión uniforme con el inicio de sesión único de Duo, que ofrece acceso centralizado a las aplicaciones en las instalaciones y en la nube. Reduzca la fatiga de la contraseña y aumente la productividad del usuario, ya que permite que los usuarios inicien sesión solo una vez en el **inicio de sesión único (SSO)** de Duo para acceder a todas sus aplicaciones. El SSO seguro de Duo verifica la seguridad del dispositivo cada vez antes de otorgar acceso a cada aplicación.

Asociaciones de tecnología

El ecosistema de **asociación de tecnología y seguridad** de Duo facilita la eliminación de la complejidad y protege las inversiones de TI existentes. Nuestros partners tecnológicos (Microsoft, Cisco, Workday, Citrix, VMware y muchos otros) incluyen la administración de identidad y acceso; red y acceso remoto; administración y seguridad de terminales; detección y respuesta; y aplicaciones comerciales populares.

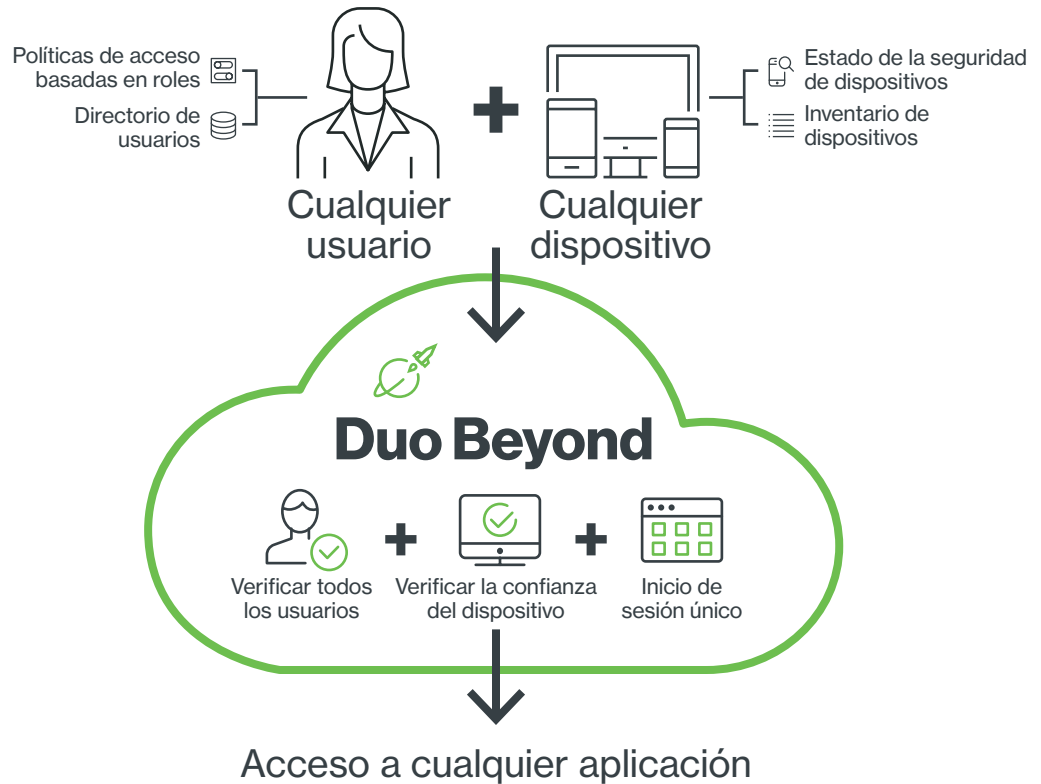
Comience su recorrido de Zero Trust con

Duo Beyond

En la **edición Duo Beyond**, recibirá:

Autenticación de dos factores con todas las funciones para cada organización:

- + Proteger los inicios de sesión con **MFA de Duo**
- + Información sobre una descripción general de la **higiene en materia de seguridad de los dispositivos**
- + Administrar la solución de Duo con **API de administrador**
- + El **inicio de sesión único seguro (SSO)** de Duo proporciona un flujo de trabajo de inicio de sesión de usuario uniforme en todas las aplicaciones
- + Proteger el acceso a las **aplicaciones en las instalaciones y en la nube**



Paquete de seguridad de acceso esencial para abordar los riesgos de la nube, BYOD y móviles:

- + Visibilidad completa de dispositivos móviles y equipos de escritorio, incluidos los dispositivos **administrados y no administrados por la empresa** (personales) para admitir políticas BYOD
- + Desglose de dispositivos móviles con visibilidad de las **funciones de seguridad activadas y los dispositivos alterados o sin cifrar**
- + Aplicar reglas sobre quién puede **acceder a qué aplicaciones y en qué condiciones** (autenticación adaptativa)
- + Aplicar una política para **permitir que solo los dispositivos administrados** tengan acceso a aplicaciones sensibles
- + Proporcionar **acceso remoto moderno a entornos multinube** (en las instalaciones, Azure, AWS, Google Cloud Platform) mientras aplica principios de seguridad Zero Trust
- + **Notificar a los usuarios** para actualizar sus dispositivos según las políticas de acceso de dispositivos
- + Identificar a los usuarios vulnerables a la suplantación de identidad (phishing) **a través de campañas de suplantación de identidad (phishing)**
- + Tableros completos e informes personalizados para **auditorías de cumplimiento** y facilidad de gestión administrativa

Obtenga más información sobre Duo Beyond en nuestra **documentación**.

Duo Security

Duo es una plataforma de seguridad basada en la nube que protege el acceso a todas las aplicaciones, para cualquier usuario y dispositivo, desde cualquier lugar. Está diseñada para ser fácil de usar e implementar, a la vez que otorga visibilidad y control completos de los terminales.

Duo verifica las identidades de los usuarios con una autenticación multifactor sólida. Junto con información detallada sobre los dispositivos de los usuarios, Duo le brinda las políticas y el control que necesita para limitar el acceso en función de los riesgos del terminal o del usuario. Los usuarios obtienen una experiencia de inicio de sesión uniforme con el inicio de sesión único de Duo, que ofrece acceso centralizado a las aplicaciones en las instalaciones y en la nube.

Con Duo, puede protegerse contra credenciales comprometidas y dispositivos riesgosos, así como contra el acceso no deseado a sus aplicaciones y datos. Esta combinación de confianza entre usuarios y dispositivos crea una base sólida para un modelo de seguridad Zero Trust.

Obtenga una **prueba gratuita** **durante 30 días** y proteja rápidamente a todos los usuarios, dispositivos y aplicaciones. O bien, **póngase en contacto con nosotros.**

Cisco Zero Trust

Duo Zero Trust ofrece un enfoque integral para asegurar el acceso en todos sus entornos y aplicaciones, desde cualquier usuario, dispositivo y ubicación. Protege su fuerza laboral, las cargas de trabajo y el lugar de trabajo.

- + Para proteger la fuerza de trabajo, Cisco garantiza que solo los usuarios correctos y dispositivos seguros accedan a las aplicaciones.
- + Para proteger las cargas de trabajo, Cisco protege todas las conexiones dentro de las aplicaciones, en varias nubes.
- + Para proteger el lugar de trabajo, Cisco protege todas las conexiones de usuarios y dispositivos en toda la red, incluida IoT.

Este modelo completo de seguridad Zero Trust le permite mitigar, detectar y responder a los riesgos en todo el entorno.

Obtenga más información sobre **Cisco Zero Trust**

