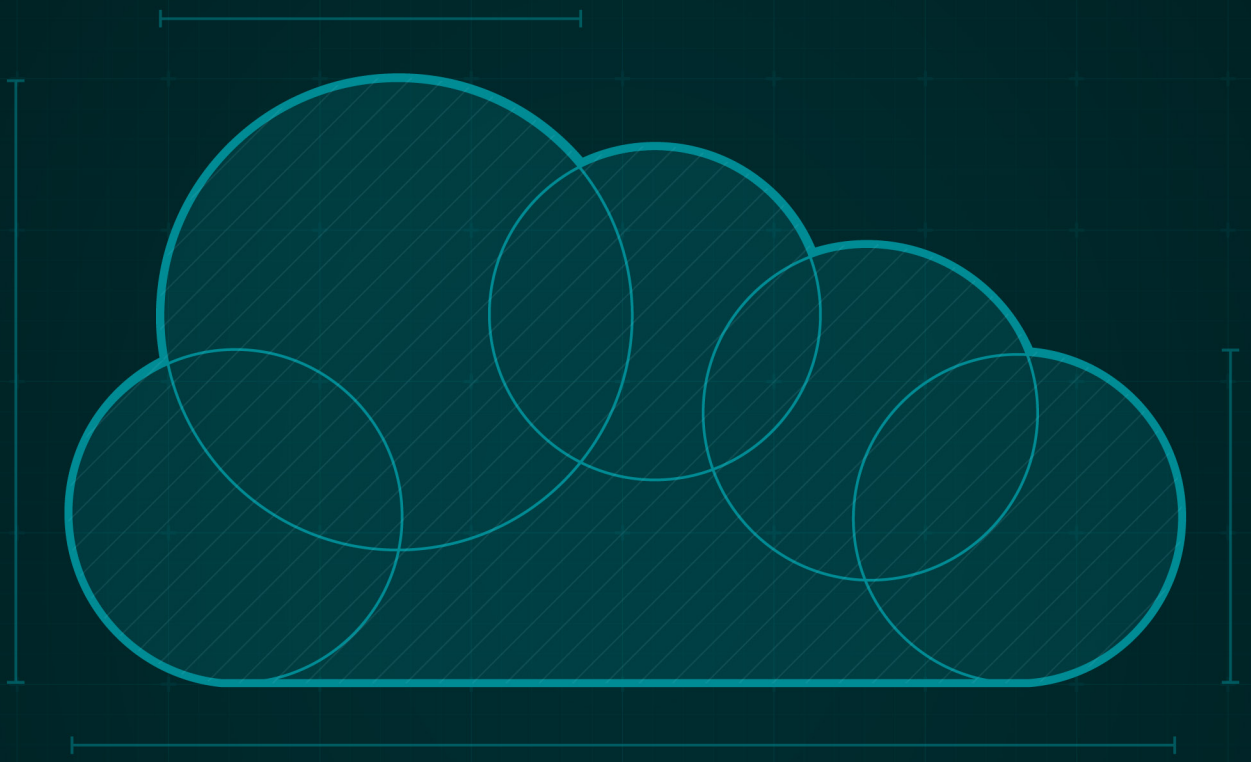
netskope

INFORME TÉCNICO



Plan de acción para zero trust en una arquitectura SASE

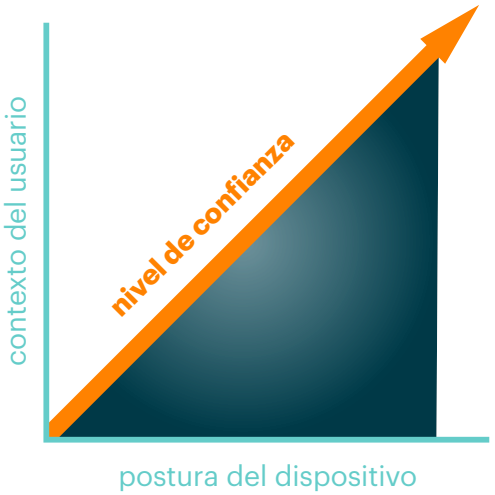
Confianza adaptativa continua: la clave para adoptar zero trust y SASE y los pasos a seguir

A pesar de ser un concepto que representa *nada*, «zero trust» (confianza cero) está en *todas partes*. Sin embargo, entre todo el ruido se esconde una descripción contundente de los objetivos de un enfoque zero trust y los resultados que dicho enfoque busca lograr. Las empresas que han explorado cómo embarcarse en proyectos zero trust se encuentran con enormes desafíos: definiciones contradictorias, antigua TI compleja e incompatible y falta de determinación en los signos de culminación. El traspaso hacia la nube, la transición hacia el teletrabajo y la transformación digital crean una oportunidad de darle un marco a la importancia de los principios zero trust particulares de las arquitecturas multinube bajo Secure Access Service Edge (SASE). En Netskope, creemos que zero trust en un entorno SASE o uno híbrido implica la capacidad de establecer confianza adaptativa continua entre usuarios, dispositivos, redes, aplicaciones y datos para sentir mayor seguridad en la ejecución de políticas en todas partes.

El objetivo principal de un enfoque zero trust es pasar de *confiar pero verificar* a *verificar y luego confiar*. Los recursos ya no confían de modo implícito (dirección IP, por ejemplo) en una entidad que quiere conectarse. Mediante la evaluación de varios elementos contextuales —identidad del usuario, postura de seguridad e identidad del dispositivo, momento del día, geolocalización, rol comercial, nivel de confidencialidad de los datos, entre otros— el mismo recurso puede determinar *un nivel de confianza adecuado* específicamente para esa interacción y para ese recurso. Como ejemplo, es probable que el nivel de confianza de un usuario en un dispositivo con un agente capaz de informar abundante telemetría que refleja su entorno sea mayor que el de un usuario cuyo dispositivo no informa nada más que una dirección MAC previamente identificada. Mayor integridad se traduce en mayor confianza.

Pero evaluar el nivel de confianza al comienzo de cualquier interacción no es suficiente. Durante la interacción, debe evaluarse el contexto *continuamente*. Las alteraciones del contexto pueden provocar una *adaptación* (un aumento o una reducción) en el nivel de confianza, que a su vez podría alterar el tipo de acceso al recurso.

Las decisiones binarias —como acceso total o ningún acceso— carecen de la flexibilidad que demandan los estilos laborales actuales y emergentes; por ejemplo, una aplicación SaaS de alto riesgo necesaria para la productividad de los empleados, pero que no se puede usar porque en cuestión de acceso es «todo» o «nada». El acceso debe tener en cuenta el contexto, manteniendo el equilibrio entre confianza y riesgo. En situaciones de alto riesgo, el acceso



Aunque, sobre todo, un enfoque zero trust reduce el riesgo y aumenta la agilidad comercial al eliminar la confianza implícita y evaluar continuamente cuánto confiamos en dispositivos y usuarios en base a la identidad, el acceso adaptativo y el análisis exhaustivo.

70%

de los usuarios siguieron trabajando a distancia **durante el primer semestre de 2021.**

Más de la mitad del tráfico web está relacionado con la nube

53%

WEB

APLICACIONES Y SERVICIOS CLOUD

90 % del tráfico está cifrado con TLS*

90%

CIFRADO CON TLS

*Transparencia HTTPS de Google

está limitado, pero no bloqueado completamente, lo que permite iniciar con parte del trabajo. En situaciones de bajo riesgo, el acceso se amplía y ciertas obligaciones (como autenticación multifactor o un dispositivo gestionado) pueden reducirse. El modelo de confianza adaptativa continua aumenta los requisitos del nivel de confianza en paralelo con el valor del recurso al cual se accede. En base a señales como el riesgo de actividad o aplicación, riesgo de usuario, confidencialidad de datos, postura del dispositivo, ubicación del usuario y otros atributos, el acceso adaptativo proporciona la capacidad de tomar decisiones en tiempo real a fin de permitir, negar, restringir, redirigir e incluso orientar al usuario. El acceso adaptativo alinea las políticas con el apetito de riesgo, que podría incluir revocar el acceso, de ser necesario en un momento dado.

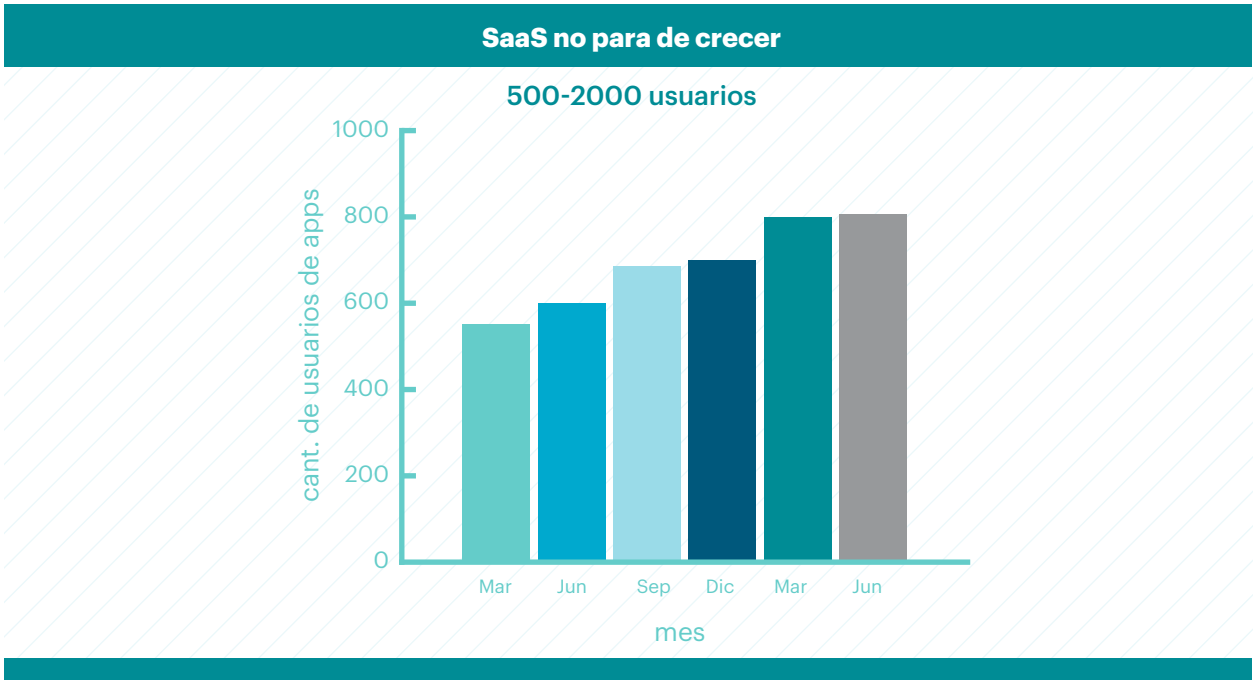
Un objetivo secundario del enfoque zero trust es asumir que el entorno puede vulnerarse en cualquier momento, o incluso que ya fue vulnerado, y diseñarlo partiendo de eso. Tal suposición, que es prácticamente una nueva mentalidad, facilita la implementación de patrones y prácticas que reducen las superficies expuestas a ataques, limitan los radios de explosión, restringen el movimiento lateral y responden ante amenazas con mayor velocidad y precisión.

En esencia, zero trust es más que solo un replanteamiento de dos principios de seguridad comunes, pero importantes: acceso menos privilegiado y ocultamiento de recursos. Es cierto que un enfoque zero trust provoca que los usuarios autorizados reciban solo el acceso necesario a los recursos autorizados y que los recursos no autorizados no sean visibles ni accesibles para los usuarios no autorizados. Aunque, sobre todo, un enfoque zero trust reduce el riesgo y aumenta la agilidad comercial al eliminar la confianza implícita y evaluar continuamente cuánto confiamos en dispositivos y usuarios en base a la identidad, el acceso adaptativo y el análisis exhaustivo.

LA IMPORTANCIA DE ZERO TRUST EN LA ACTUALIDAD

El tradicional modelo de redes se originó en la era en la que los trabajadores accedían a aplicaciones corporativas que se ejecutaban desde centros de datos in situ. Las empresas inicialmente desarrollaron la seguridad de sus redes de un modo similar a la seguridad física, es decir, suponiendo que «los malos» estaban afuera y solo «los buenos» estaban adentro. Con un nivel decente de protección contra las amenazas entrantes, la mayoría de las empresas consideró este nuevo concepto de redes zero trust como algo curioso, y nada más. El perímetro era suficiente por el momento; los responsables de seguridad y de TI tenían otras preocupaciones.

Y entonces, el mundo cambió: las aplicaciones, los usuarios y los datos migraron fuera del perímetro. Atraídas por una amplia variedad de opciones y su facilidad de adquisición, las empresas empezaron a recurrir cada vez más a las aplicaciones de Software-as-a-Service (SaaS) para sus procesos de negocios. De hecho, la empresa promedio de entre 500 y 2000 usuarios actualmente se suscribe a 805 *aplicaciones SaaS diferentes*.

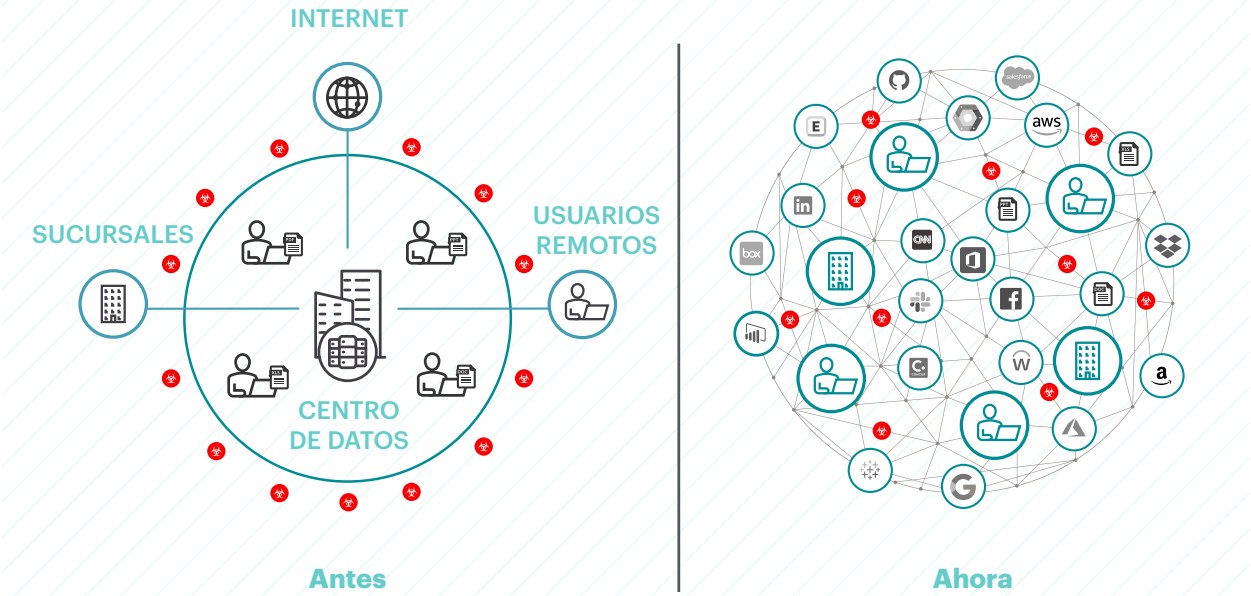


Fuente: Netskope Cloud and Threat Report, julio de 2021

Claro que algunos procesos de negocios siguen requiriendo aplicaciones personalizadas. Las empresas descubrieron que las nubes públicas de Infrastructure-as-a-Service (IaaS) y Platform-as-a-Service (PaaS) ofrecían mayor agilidad que los centros de datos tradicionales, por lo cual se convirtieron en el objetivo por defecto para la mayoría de las aplicaciones nuevas. Y así es que ahora la mayoría de las empresas adoptan una estrategia multinube, eligiendo entre varios proveedores a hiperescala en base a los requisitos de las aplicaciones y la habilidad de los desarrolladores. (Lift-and-shift, el proceso de migrar aplicaciones existentes a la nube pública, ha tenido menos éxito, en particular debido a que la nube amplifica los problemas de las arquitecturas deficientes y las malas decisiones de seguridad).

2020 demostró que las empresas pueden adaptarse a un cambio gigante, en el cual gran parte de la fuerza laboral mundial de repente pasó a trabajar de forma remota. Al principio, el cambio fue disruptivo y no todas las industrias pueden, ni deben, sostener un estilo de trabajo mayormente a distancia. Pero para muchas empresas, el teletrabajo ya es la nueva normalidad. Los empleados y sus socios comerciales necesitan acceder a las aplicaciones donde sea que estén (in situ, SaaS, nube pública) desde cualquier tipo de dispositivo (gestionado o no).

El antes versus el ahora



El modelo zero trust es especialmente apto para dar lugar a tal necesidad. A grandes rasgos, han surgido dos categorías de productos que implementan este modelo: Zero Trust Network Access (ZTNA) y la segmentación basada en identidad (microsegmentación).

Los productos en el mercado de ZTNA aplican principios zero trust al proceso de poner las aplicaciones a disposición de los usuarios. Un enfoque basado en zero trust para aplicaciones privadas, ya sea in situ o en la nube pública, y para aplicaciones SaaS puede otorgarse a usuarios específicos independientemente de a qué red se conecten. El grado de acceso se adapta al contexto de la interacción, que a su vez proporciona un determinado nivel de confianza. Por ejemplo, los usuarios en dispositivos no gestionados pueden recibir acceso total a las aplicaciones gestionadas que procesan información pública, acceso de solo lectura a las aplicaciones gestionadas que procesan información delicada, y no tener acceso a las aplicaciones que procesan información confidencial. Además, los análisis que combinan el comportamiento histórico de los usuarios con un entendimiento de la funcionalidad específica de las aplicaciones pueden detectar y mitigar las amenazas antes de que causen estragos.

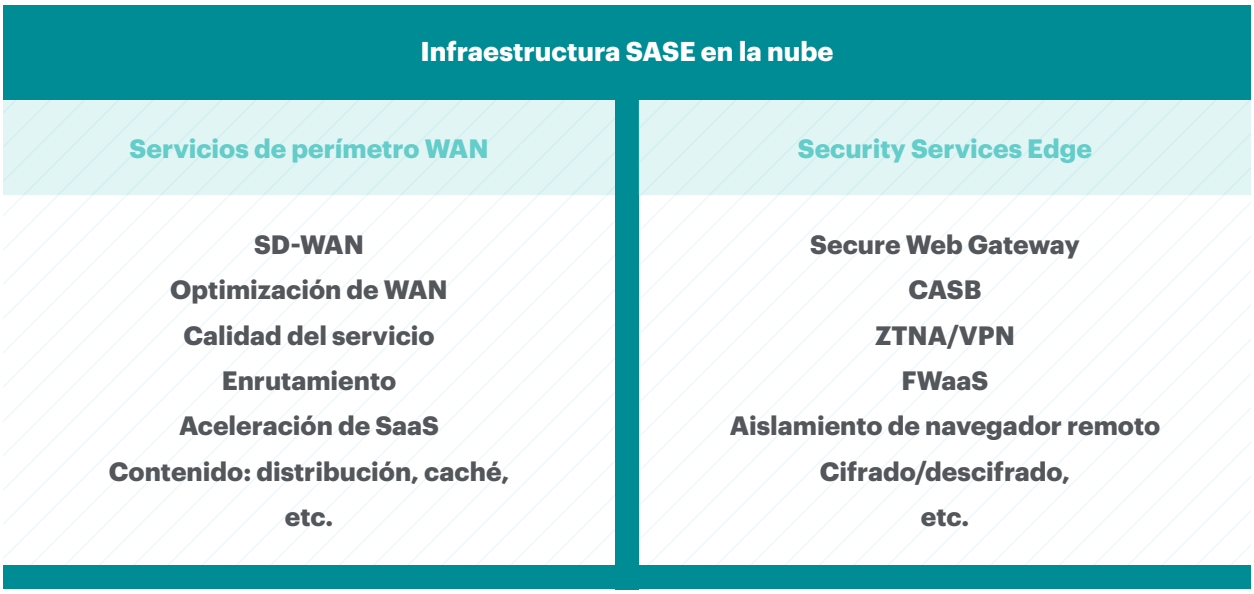
La segmentación basada en identidad (según la define Gartner) es una reinterpretación de la microsegmentación. La microsegmentación es una forma de aislamiento impuesta por un conjunto de reglas estáticas que definen qué recursos (por ejemplo un dispositivo, una carga de trabajo o un contenedor) pueden comunicarse entre sí. La segmentación basada en identidad amplía este concepto, añadiendo reglas dinámicas que evalúan la identidad y otros atributos como factores para determinar si permitir o no el acceso. Las identidades de los recursos son portátiles e independientes de la red subyacente. La suma de la segmentación basada en la identidad y el contexto adicional medido en tiempo real permite una mayor flexibilidad, agilidad y amplitud del control y las políticas de segmentación.

Claro que hay que reconocer que los modelos zero trust necesariamente añaden un grado de esfuerzo de gestión. Aquellos a cargo de los recursos deben asumir la responsabilidad de evaluar con cuidado y ajustar continuamente las listas de usuarios permitidos en sus recursos, lo que se conoce como administración de privilegios. Este proceso puede ser mayormente manual, pero las tecnologías emergentes buscan brindar una automatización (muy beneficiosa y bienvenida) que puede reducir los errores que suelen acarrear los procesos manuales. Además, un enfoque zero trust no solo exige que se administren los privilegios, sino también que se definan los atributos y los elementos contextuales que, en conjunto, determinan el nivel de confianza necesario para interactuar con los recursos. De hecho, en entornos en los que los modelos de autorización y acceso tradicionales no pueden definirse bien, incorporar el contexto posibilita una evaluación más precisa de la confianza.

SE ABRE PASO LA ARQUITECTURA SASE

La seguridad nació de la red. Con el paso del tiempo, muchas herramientas maniobraron para posicionarse en los centros de datos y compitieron por la atención de los administradores. En general, fueron eficaces mientras las aplicaciones y los datos permanecieran in situ y los usuarios trabajaran desde oficinas convencionales. Algunas de las herramientas ofrecían mecanismos para comunicarse entre sí. Pero a medida que los usuarios empezaron a salir de las oficinas y los datos y las aplicaciones migraron a la nube, las antiguas herramientas se quedaron ciegas. Todas funcionaban bajo un supuesto predominante: las aplicaciones, los datos y los usuarios son estáticos. Dado que este supuesto ya no es válido, esas herramientas perdieron mucha de su idoneidad. No funcionan las unas con las otras, no adaptan su escala adecuadamente, carecen de una administración unificada y, sobre todo, no pueden desempeñar sus funciones cuando los datos se almacenan y procesan en una infraestructura ajena.

SASE, una arquitectura definida por Gartner en 2019, promete superar las limitaciones de lidiar con demasiadas herramientas y demasiada consolas. SASE combina funciones de red comunes (SD-WAN, optimización de WAN, QoS, enrutamiento, CDN, etc.) con funciones de seguridad comunes (SWG, CASB, ZTNA, VPN, FWaaS, RBI, etc.) en una arquitectura consolidada con administración unificada. Las políticas aplican control de acceso a cualquier aplicación o servicio para monitorear y controlar el movimiento de la información delicada, desde y hacia todos los usuarios y recursos. SASE brinda funciones de red y de seguridad desde la nube para garantizar una experiencia de usuario uniforme, donde sea que estén los usuarios y las aplicaciones.



Fuente: Gartner, «2021 Strategic Roadmap for SASE Convergence», G00741491, https://www.gartner.com/document/3999828

Las buenas arquitecturas SASE implementan principios zero trust. SASE consolida todas las formas en las que los usuarios acceden a los recursos, a la vez que permanece neutral respecto a cómo se evalúa la confianza y se otorga acceso. Los principios zero trust remarcan que se otorgue el acceso y se monitoree la confianza en base a grupos de condiciones, a la vez que permanecen neutrales ante cualquier arquitectura técnica dada. Combinados, SASE y zero trust representan un cambio fundamental en cómo las empresas protegen sus recursos digitales. De hecho, SASE puede ser un buen punto de partida para desarrollar un programa zero trust eficaz que abarque entornos totalmente híbridos en los que no importe dónde se encuentren los usuarios, las aplicaciones y los datos.

En un nivel alto, y según las aptitudes de los proveedores, las empresas que adoptan una arquitectura SASE con principios zero trust pueden esperar:

- Comprender mejor los riesgos de usuarios y de aplicaciones para determinar un nivel de confianza en el acceso otorgado bajo diferentes condiciones y adaptar el acceso en base a cuánta confianza se tiene.
- Extender los principios zero trust más allá de las aplicaciones privadas y hacia las aplicaciones SaaS y web en base a información sobre riesgos mediante posturas y políticas adaptativas.
- Aplicar información sobre riesgos a las aplicaciones para controlar el acceso a actividades específicas (por ejemplo, una situación de poca confianza que permita ver y comentar, pero prohíba compartir y eliminar).
- Activar servicios de seguridad adicionales, como aislamiento de navegador remoto y prevención de pérdida de datos avanzada, en base al nivel de riesgo o de confianza evaluado.
- Monitorear continuamente los cambios en el contexto que requieran reevaluar la confianza (por ejemplo, reautenticación, autenticación por pasos, alteración de permisos o aumento/reducción de acceso).
- Reducir la superficie expuesta a ataques al eliminar la exposición de protocolos y servicios ante el internet público.

RESULTADOS PARA LOS NEGOCIOS Y LOS USUARIOS

Los negocios digitales modernos no esperan a que les den permiso. En simultáneo, se valen cada vez más de que las aplicaciones y los datos se ofrezcan en internet (algo que, en realidad, no fue diseñado pensando en la seguridad). Las empresas pueden lograr sus objetivos comerciales sin sacrificar la seguridad si integran principios de confianza adaptativos continuos en sus programas de riesgos y seguridad, y en sus planes de transformación digital, desde el primer momento.

Agilidad en los negocios

La agilidad en los negocios requiere de elasticidad en la infraestructura y los servicios, tanto en la escala de volumen y ubicación como en la amplitud de nuevos servicios y aplicaciones. Los resultados que deben lograrse en base a principios zero trust en una arquitectura híbrida y SASE incluyen:

- Experiencia de usuario armónica: el acceso es el mismo, al margen de dónde se encuentre el usuario; el acceso es predecible, al margen del tipo de dispositivo del usuario.
- Independencia de ubicación: el acceso a las aplicaciones está separado del diseño de red subyacente; las aplicaciones se pueden mover (por ejemplo, de in situ a la nube pública) sin forzar a los usuarios a cambiar sus hábitos.
- Más oportunidades de brindar algo de acceso: para reorientar la mayoría de las decisiones de seguridad de «no» a «sí, con condiciones».
- Mayor colaboración con proveedores y partners sin aprovisionarles cuentas de usuarios locales y sin imponer demandas en sus entornos informáticos.
- Operaciones de seguridad proactivas desarrolladas para apoyar el crecimiento de las aplicaciones y para eliminar los simulacros de perseguir y garantizar el acceso retroactivamente a las aplicaciones que ya fueron implementadas.

Reducción de riesgos

Los riesgos informáticos son una prioridad para la mayoría de las juntas directivas. Cada empresa debe determinar su propia inclinación y tolerancia al riesgo; esto suele ser más o menos similar en la mayoría de las empresas de cualquier sector. Gestionar los riesgos se dificulta ante la dependencia en las cadenas de suministro que cada vez son más largas y menos transparentes, la proliferación de aplicaciones y servicios en la nube, y un entorno normativo ambiguo. La reducción de riesgos en este nuevo entorno implicará un enfoque zero trust en el cual:

- Los recursos se trasladan del acceso público al privado y, por ende, quedan protegidos de internet y son invisibles para quienes carecen de credenciales de acceso seguras o la habilidad de demostrar confianza.
- El acceso inapropiado queda limitado, lo que reduce el radio de explosión de las cuentas comprometidas.
- La visibilidad de las ubicaciones, los movimientos y los tipos de datos de índole confidencial es mejor y constante.
- El análisis ofrece el panorama completo de las conductas y las políticas aceptables, y expone más rápido los riesgos y las amenazas (actividad tanto anómala como malintencionada) para contenerlos y neutralizarlos en el acto.
- Se mejora la estrategia de seguridad haciendo que las empresas sean menos atractivas para los ciberdelincuentes.

Proceso optimizado de implementación de producto y mantenimiento

La agilidad de negocios y la reducción de riesgos requieren de la arquitectura adecuada, que incluye:

- Un servicio de seguridad cloud-native que adapta su escala según lo demande el negocio, eliminando las complejidades de la implementación y las limitaciones de capacidad que se suelen asociar con el hardware de seguridad.
- Una plataforma única en la nube, con inspección de un solo paso y un punto de ejecución de políticas, impulsados por una única consola y motor de políticas que se aplica para garantizar una política de seguridad congruente en todos los canales.
- Una relación con un solo proveedor que elimina las demoras que suelen venir con la resolución de problemas y la reparación de productos con características de interoperabilidad desconocidas o no comprobadas.

LAS CINCO FASES DE LA CONFIANZA ADAPTATIVA CONTINUA CON NETSKOPE

Netskope ayuda a las empresas a lograr sus objetivos de confianza adaptativa continua. Puede que el trayecto no sea el mismo para cada empresa. De hecho, su industria, su grado de adopción de la nube y sus sistemas existentes seguramente influirán, no solo en el punto de partida de su trayecto, sino también en el esfuerzo que será necesario.

Unos sencillos pasos pueden ayudar a todas las empresas a prepararse. Comience con estas tareas:

- Imagine un conjunto de tipos de usuarios que reflejen los roles comerciales típicos. Elabore una lista con los requisitos de acceso para cada tipo de usuario. Comience desde cero, no se valga de definiciones establecidas de acceso basado en roles.
- Haga un inventario de todas las aplicaciones privadas y las de SaaS. Trace un mapa que ilustre cómo interactúan las aplicaciones y sus componentes entre sí y con los recursos ajenos a la empresa.
- Identifique todos los recursos de datos: sus ubicaciones, sus niveles de confidencialidad, sus funciones comerciales y sus vidas útiles.

Todo proyecto exitoso de confianza adaptativa continua exige un robusto programa de gestión de acceso e identidades. Si no se cuenta con un sistema de registro de identidad fiable y preciso, no puede determinarse ni inferirse un nivel de confianza elevado. Cada entidad —ya sea una persona, un dispositivo o un objeto— debe presentar una identidad que todas las demás entidades puedan validar. Por suerte, la mayoría de las empresas ya tienen establecido algún tipo de sistema de gestión de identidad. Es de vital importancia para zero trust que el sistema sea compatible con estándares comunes como SAML, OIDC y OAuth, dado que la mayoría de las organizaciones lo esperan. La federación de identidad establece un grado de confianza entre ámbitos de identidad dispares, lo que permite que los usuarios de un ámbito accedan a recursos autorizados en otros ámbitos sin procesar identidades separadas.

Con esta información, usted puede empezar a planificar y llevar a cabo las cinco fases que encontrará en la próxima página.

FASE 0 — Antes de comenzar

- Imaginar tipos y asignar requisitos de acceso
- Inventario de las aplicaciones privadas y SaaS
- Inventario de recursos de datos

FASE 1 — Acceso Zero Trust

- Diseñar fuentes veraces por identidad
- Mapear los usuarios con las aplicaciones
- Eliminar privilegios obsoletos o sin usar
- Direccionar todo el acceso por un punto de ejecución de políticas para eliminar riesgos de acceso directo

Establecer este estándar de acceso zero trust

FASE 2 — Acceso adaptativo

- Aportar contexto a las políticas de acceso
- Permitir que el contexto indique si hace falta una autenticación segura
- Incorporar contexto a la orientación de usuarios
- Ajustar continuamente las políticas de acceso

Fortalecer el estándar de confianza de autorización dentro de actividades en aplicaciones

FASE 3 — Aislamiento bajo demanda

- Insertar aislamiento de navegador remoto para el acceso a sitios web riesgosos o de mala reputación
- Vigilar intentos de mando y control y otros comportamientos anómalos

Aplicar controles de confianza explícita a los destinos

FASE 4 — Protección de datos continua

- Separar el acceso en gestionado y no gestionado
- Adaptar las políticas de acceso según el contexto
- Garantizar la correcta configuración de los recursos cloud
- Identificar información delicada y controlar su difusión
- Evaluar constantemente los permisos de intercambio y las integraciones entre aplicaciones

Investigar y eliminar la confianza excesiva de forma constante. Adoptar e imponer un modelo de menor privilegio en todas partes

FASE 5 — Informar y optimizar con análisis en tiempo real

- No perder visibilidad de aplicaciones y riesgos
- Inspeccionar la actividad en la web y la nube para evaluar y ajustar mejor las políticas
- Crear visualizaciones especiales para distintas partes interesadas
- Implementar perfeccionamiento de políticas de ciclo cerrado

Fortalecer la postura de confianza y seguridad mediante un perfeccionamiento de ciclo cerrado de las políticas

FASE 1

Acceso zero trust: no permita acceso anónimo a nada

Comience a construir el contexto desde el punto de acceso inicial. Empiece apuntalando la gestión de acceso e identidad (incluidos los roles y la pertenencia de rol), el descubrimiento de aplicaciones privadas y una lista de categorías de sitios web y aplicaciones SaaS aprobadas. Reduzca las oportunidades de movimiento lateral y oculte las aplicaciones para protegerlas del fingerprinting, el escaneo de puertos o el sondeo de vulnerabilidades. Exija el inicio de sesión único (SSO) con autenticación multifactor (MFA).

Netskope Security Cloud permite un SSO federado con controles de acceso adaptativos para sitios web, aplicaciones privadas y miles de aplicaciones SaaS, incluido el shadow IT adoptado por diversas unidades de negocios. Netskope Private Access otorga funcionalidad ZTNA total, desde la detección de aplicaciones privadas hasta el acceso a nivel de la aplicación, para usuarios gestionados, proveedores externos o casos de uso de fusiones y adquisiciones. Netskope Next Generation Secure Web Gateway (NG SWG) como punto de control de acceso a la web y SaaS puede frustrar el phishing u otros ataques contra las credenciales del correo web SaaS y el almacenamiento en la nube, las principales amenazas para las empresas actuales.

Tareas específicas para esta fase:

- Defina la fuente de verdad de las identidades y otras fuentes de identidad con las que estas se pueden federar.
- Establezca cuándo es necesaria una autenticación segura.
- Arme y mantenga una base de datos que mapee a los usuarios (empleados y terceros) con las aplicaciones. Para esto es necesario hablar habitualmente con las unidades de negocios. Postule a un grupo específico de personas para que estén a cargo de esto.
- Racionalice el acceso a las aplicaciones eliminando los privilegios obsoletos (de empleados y de terceros) que ya no son necesarios debido a cambios de puestos, partidas, rescisiones contractuales, etc.
- Elimine la conectividad directa dirigiendo todo el acceso a través de un punto de ejecución de políticas para cada aplicación privada o interna (ZTNA) y para acceder a SaaS y la web (CASB, SWG).
- Mantenga visualizaciones y un panel de control de usuarios y aplicaciones en tiempo real. Controle qué usuarios deberían tener acceso a qué aplicaciones y servicios.

FASE 2

Acceso adaptativo: mantenga el modelo de confianza explícita

Añada más contexto para que el control de acceso se vuelva adaptativo a fin de mantener un modelo de confianza explícita. Evalúe las señales de análisis de riesgo de las aplicaciones, de los usuarios, verificaciones de postura de endpoints, y las ubicaciones de los usuarios, las aplicaciones y los datos. Implemente políticas adaptativas que invoquen autenticación por pasos, alerten al usuario para que indique si cancelar o proceder con la actividad de una aplicación, proporcione una justificación comercial para continuar, u orientación en tiempo real hacia aplicaciones aprobadas.

Netskope Security Cloud proporciona un contexto profundo entre el tráfico cloud y web inspeccionado y brinda información y calificaciones de riesgo de aplicación en tiempo real, evaluación de riesgo de usuarios e información sobre el comportamiento de los usuarios con el paso del tiempo. Las calificaciones activan medidas de política adaptativa en tiempo real, como la autenticación por pasos, la finalización de procesos y más, según las políticas deseadas para usuarios, datos o aplicaciones.

Tareas específicas para esta fase:

- Determine cómo identificar si un dispositivo está gestionado o no.
- Aporte contexto a las políticas de acceso (bloquear, solo lectura o permitir actividades específicas según diversas condiciones).
- Aumente el uso de autenticación segura cuando el riesgo del entorno sea elevado (por ejemplo, para que todo el acceso remoto a las apps privadas y SaaS elimine contenido) y disminuya su uso cuando el riesgo sea bajo (por ejemplo, cuando los dispositivos gestionados tienen acceso de solo lectura a aplicaciones locales).
- Evalúe el riesgo de los usuarios; oriente a clases de usuarios hacia categorías específicas de aplicaciones.
- Ajuste políticas de modo continuo para que reflejen los requisitos comerciales cambiantes a medida que las aplicaciones evolucionan, aparecen nuevas y las viejas se descontinúan.
- Establezca un estándar de confianza para la autorización dentro de actividades en la aplicación.

FASE 3

Aislamiento bajo demanda: contenga el radio de explosión

Desacople los navegadores de las aplicaciones y aplique controles al tráfico saliente. Implemente aislamiento de navegador remoto (RBI) para reducir la funcionalidad del navegador a la de un dispositivo visualizador. Habilite un firewall dentro del dispositivo para restringir los destinos con los cuales puede establecer conexiones.

El RBI de Netskope es nativo, de un único paso, y está integrado con las funcionalidades existentes de neutralización de amenazas y protección de datos. Además, ofrece un grado de rendimiento que no está disponible en productos de RBI ligados a proxies tradicionales o puertas de enlace de red. A tono con el tema de eliminar confianza implícita, el acceso directo a recursos web riesgosos debe minimizarse, en especial a medida que los usuarios interactúan en simultáneo con las aplicaciones gestionadas.

El aislamiento bajo demanda —es decir, aquel que se inserta automáticamente en condiciones de alto riesgo— restringe el radio de explosión de los usuarios comprometidos y de los sitios web peligrosos o riesgosos. Además, Netskope Cloud Firewall es un mecanismo altamente eficaz que frustra los intentos de comunicarse con nodos de mando y control que pertenecen a ciberdelincuentes.

Tareas específicas para esta fase:

- Inserte automáticamente el aislamiento de navegador remoto en la ruta de acceso a sitios web riesgosos con malas reputaciones.
- Configure el aislamiento de navegador remoto para acceder a aplicaciones privadas desde dispositivos no gestionados.
- Evalúe el aislamiento de navegador remoto como una alternativa al proxy inverso CASB para las aplicaciones SaaS que se comportan de manera errónea cuando se reescriben las URL.
- Vigile en los paneles de usuarios y amenazas en tiempo real si se detectan anomalías o intentos de mando y control.

FASE 4

Protección de datos continua: aplique políticas de datos en un único paso

Obtenga visibilidad sobre dónde se almacena y dónde se propaga la información confidencial. Monitoree y controle el movimiento de información confidencial mediante aplicaciones SaaS, sitios web, almacenamiento cloud público, aplicaciones personalizadas en nubes públicas y correo electrónico saliente, tanto autorizados como no autorizados. Aplique políticas de protección de datos en un único paso en el tráfico en la nube, el correo electrónico y la web para los datos en movimiento y a través de API para los datos en reposo.

Netskope Security Cloud brinda control sobre los movimientos de datos por error o no autorizados, además de análisis completos de toda la actividad de datos inspeccionada. Las defensas anticuadas no pueden decodificar el tráfico en la nube, por lo que no pueden aplicar la protección de datos necesaria, en especial en las instancias personales de aplicaciones autorizadas y no autorizadas. Netskope Cloud Firewall-as-a-Service (FWaaS) proporciona control de acceso de red saliente en todos los puertos y protocolos para los usuarios remotos y las sucursales, lo que mitiga los ataques de mando y control y la exfiltración de datos.

Tareas específicas para esta fase:

- Defina la diferenciación general del acceso de datos para dispositivos gestionados y no gestionados.
- Añada detalles de política adaptativa para acceder al contenido según el contexto (por ejemplo, acceso total a contenido público en dispositivos no gestionados, solo lectura para contenido delicado en dispositivos no gestionados, bloqueo de contenido confidencial en dispositivos no gestionados).
- Invoque la gestión de postura de seguridad en la nube (CSPM) para evaluar continuamente las configuraciones de servicios cloud públicos para proteger los datos y cumplir con las normativas.
- Evalúe el uso de políticas y reglas DLP inline para web, SaaS gestionado, shadow IT, servicios cloud públicos y correo electrónico para proteger los datos y cumplir con las normativas.
- Defina políticas y reglas de DLP de datos en reposo para entornos SaaS e IaaS gestionados, en especial permisos de intercambio de archivos para objetos de almacenamiento en la nube e integraciones de aplicación a aplicación que permiten que se compartan y muevan datos.
- Ajuste las políticas añadiendo atributos de usuarios o grupos cuando corresponda.
- Investigue y elimine la confianza excesiva de modo continuo. Adopte e imponga un modelo de menor privilegio en todas partes.

FASE 5

Informe y optimice con visualización y análisis en tiempo real: mantenga una postura robusta de confianza y seguridad.

Enriquezca y mejore las políticas en tiempo real. Evalúe la idoneidad de la eficacia de la política actual en base a tendencias de usuarios, anomalías de acceso, alteraciones a las aplicaciones y cambios en el nivel de confidencialidad de los datos. Ajuste las políticas en consecuencia para tolerar la exposición al riesgo sin salirse de los límites.

El análisis y la visualización en tiempo real de Netskope proporcionan información sobre las operaciones dentro de Netskope Security Cloud, identificando quién debe (y quién no) estar trabajando con los datos de la empresa en un conjunto de aplicaciones determinado. Estas funcionalidades colaboran con las operaciones de seguridad, las de redes y los equipos de búsqueda de amenazas, y explican los resultados del programa de seguridad al personal directivo y las partes interesadas en la aplicación. La información derivada del análisis ayuda a las organizaciones a planificar y prever el rumbo de su programa de seguridad y a determinar su próximo paso.

Tareas específicas para esta fase:

- No pierda la visibilidad de las aplicaciones y los servicios que usa la empresa, ni los niveles de riesgo asociados.
- Averigüe quién debe y quién no debe tener acceso a los recursos privados y regule el acceso a niveles mínimos para reducir la exposición.
- Obtenga mayor visibilidad y conozca a fondo la actividad en la web y la nube para realizar ajustes constantes y monitorear las políticas de amenazas y datos.
- Identifique a los principales responsables de su programa de gestión de riesgos y seguridad (CISO/CIO, legal, CFO, SecOps, etc.) y aplique visualizaciones a los datos que ellos pueden entender.
- Cree los paneles de mando para obtener visibilidad de estos componentes: sitio, aplicación, instancia, usuario, actividad, archivo, fuente/destino y más.
- Garantice la capacidad de importar y exportar paneles de mando para colaborar con otros equipos de seguridad.
- Refuerce la postura de confianza y seguridad mediante un perfeccionamiento de ciclo cerrado de las políticas.

La pandemia de 2020 aceleró la transformación digital, por lo que muchas empresas han tenido que evaluar la forma de rediseñar sus programas e infraestructuras de seguridad y de redes para abordar las necesidades actuales. Es evidente que se necesita un nuevo enfoque para permitir una experiencia ágil y fácil para los usuarios, con controles simples y eficaces de gestión de riesgos a lo largo de arquitecturas híbridas y multinube.

Netskope conecta a los usuarios de modo rápido y seguro directamente a internet, cualquier aplicación y su correspondiente infraestructura, desde cualquier dispositivo, dentro o fuera de la red. Con CASB, SWG y ZTNA integrados de modo nativo en una sola plataforma, Netskope Security Cloud brinda el contexto más granular, mediante tecnología patentada, para permitir acceso condicional y concientización de usuarios, a la vez que impone principios zero trust en la protección de datos y la prevención de amenazas, sea donde sea. La nube privada de seguridad a nivel mundial de Netskope proporciona funcionalidades computacionales completas para lograr una robusta seguridad, alto rendimiento y redes globales confiables.