

Cumplir las directrices del NIST para una seguridad Zero Trust



Índice

- 3 Introducción**
- 3 Zero Trust: Más allá del enfoque "castillo y foso"**
- 4 ¿Un nuevo modelo para el Zero Trust?**
- 5 Enfoques del NIST para las arquitecturas Zero Trust**
 - 5 Centrado en la identidad
 - 6 Centrado en la red
 - 7 Combinación en la nube
- 7 Implementar el modelo Zero Trust con SafeNet Trusted Access de Thales**
- 8 Ventajas de utilizar SafeNet Trusted Access de Thales para implementar el modelo Zero Trust**
 - 8 Enfoque de arquitectura lógica
 - 8 Flexible y ágil
 - 8 Facilidad de implementación, gestión y escalabilidad
 - 9 Experiencia de usuario fluida y conocida
- 9 Conclusión**
- 9 Acerca de Thales**

Introducción

La transformación digital, la proliferación de las tecnologías disruptivas y las nuevas tendencias como el "teletrabajo" han acabado con los límites digitales de las empresas. Con la disminución de estos límites, las soluciones tradicionales de seguridad perimetral se han vuelto inadecuadas para responder a las crecientes demandas de acceso que provienen de todas partes.

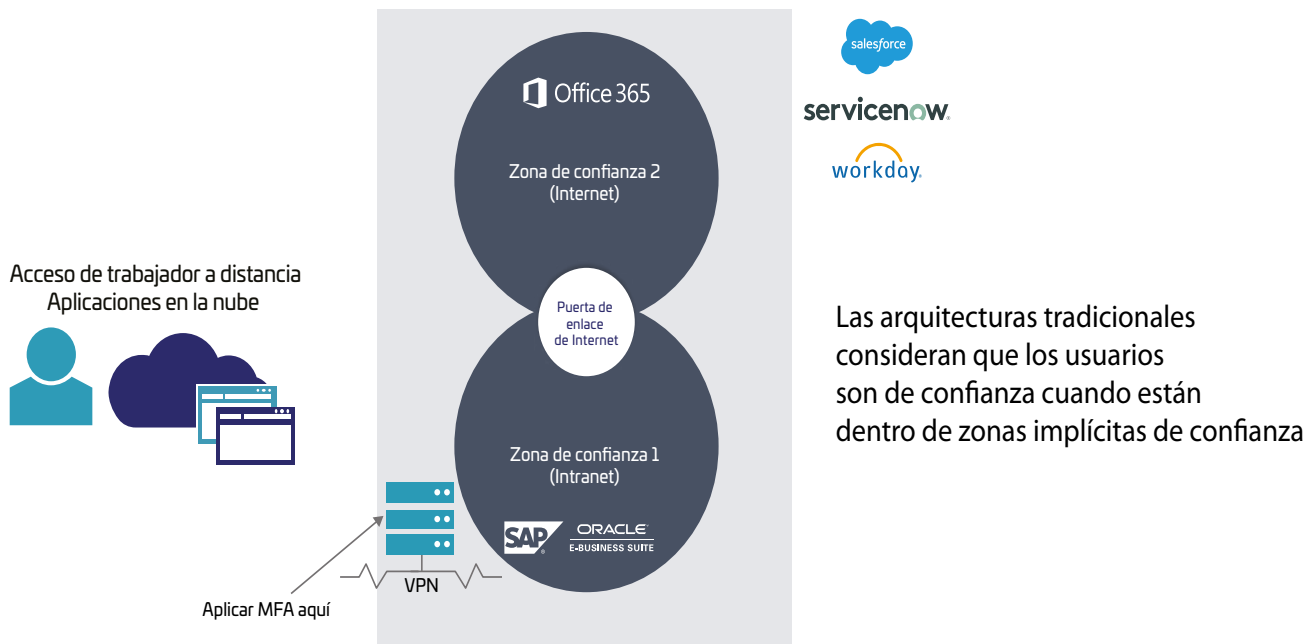
Estos avances, junto con el alarmante aumento de las brechas de datos e incidentes de seguridad, han hecho que el concepto de la confianza haya desaparecido. Por lo tanto, el enfoque de seguridad Zero Trust se basa en el principio "Nunca confíe, siempre verifique" y considera que la confianza es una vulnerabilidad. La seguridad Zero Trust requiere una verificación de la identidad estricta y continua para minimizar las zonas de confianza implícitas. Recientemente, el NIST ha publicado un modelo de seguridad Zero Trust que ofrece asesoramiento sobre cómo crear arquitecturas de seguridad Zero Trust.

La finalidad de este libro blanco es evaluar las directrices Zero Trust del NIST y ofrecer directrices concretas sobre cómo implementar una arquitectura Zero Trust eficaz y centrada en la identidad con el objetivo de alcanzar la seguridad en un entorno posperimetral.

Zero Trust: Más allá del enfoque "castillo y foso"

En la década de los ochenta, cuando el presidente de EE. UU. Ronald Reagan se refería a la URSS, utilizaba el término "confíe pero verifique". Avancemos ahora hasta 2020, momento en el que la transformación digital de las empresas a través de la adopción y proliferación de tecnologías como el Internet de las cosas, la aparición de la nube y la adopción móvil han llevado a la desaparición del perímetro de seguridad tradicional de TI. En este contexto, donde las aplicaciones se proporcionan desde la nube hacia la nube, donde los usuarios se encuentran por todas partes y donde se utilizan varios dispositivos, la capacidad de depender de un único punto de confianza es insostenible. Todas las interacciones conllevan riesgos inherentes y necesitan un enfoque "nunca confíe, siempre verifique".

El Zero Trust es una iniciativa estratégica y un principio que ayuda a las organizaciones a evitar brechas de datos y proteger sus activos asumiendo que no se puede confiar en ninguna entidad. El National Institute of Standards and Technology (NIST) define el Zero Trust como "un conjunto de conceptos e ideas diseñados para minimizar la incertidumbre a la hora de tomar decisiones exactas de acceso por solicitud con un menor nivel de privilegios en sistemas de información y servicios frente a una red que se considera peligrosa".



El modelo Zero Trust va más allá del concepto del "castillo y el foso" que ha dominado la seguridad perimetral tradicional, reconociendo que, en cuestiones de seguridad, la confianza es una vulnerabilidad. Los conceptos tradicionales de seguridad consideraban que todos los usuarios que estaban dentro de una red corporativa eran de confianza, lo que también incluía a actores amenazantes e intrusos maliciosos. La confianza les daba el derecho de moverse de forma lateral y de acceder o extraer libremente cualquier dato al que no estuvieran limitados.

Zero Trust es un modelo de seguridad que requiere una verificación estricta de la identidad y acerca hacia el mismo recurso la decisión de autenticar y autorizar. La definición de Zero Trust se centra en la autenticación, autorización y minimización de las zonas de confianza implícitas, al tiempo que mantiene la disponibilidad y ofrece unos mecanismos de autenticación impecables. Las normas de acceso son lo más granulares posible para aplicar el menor número de privilegios necesarios para realizar la acción solicitada.

Para alcanzar su objetivo, el modelo Zero Trust se rige por los siguientes principios básicos:

- El acceso a recursos corporativos está determinado por una política dinámica, aplicada en cada sesión y actualizada en base a la información recogida sobre el estado actual de la identidad del cliente, de la aplicación/servicio, y del activo solicitado, además de otros atributos conductuales y contextuales
- Todas las comunicaciones a los recursos deben autenticarse, autorizarse y cifrarse
- La autenticación y autorización son independientes de la red subyacente
- La empresa supervisa y mide la postura de integridad y seguridad de todos los activos poseídos y asociados

¿Un nuevo modelo para el Zero Trust?

En un entorno moderno y digital, donde la movilidad de los empleados y los hábitos omnipresentes de los clientes exigen acceso a recursos en cualquier momento y desde cualquier lugar, el perímetro de seguridad tradicional parece inadecuado para proteger frente a los sofisticados ciberataques.

El uso de las soluciones de seguridad tradicionales, que dependen de enrutamientos en las instalaciones locales, para hacer cumplir la autenticación y la autorización a la nube reduce la productividad, la escalabilidad y la experiencia de usuario, mientras que aumenta los costes operativos. Depender de soluciones tradicionales se traduce en complejidad, sobrecarga administrativa y crea incertidumbre y tensiones para los usuarios.

La proliferación del Internet de las cosas, las plataformas multinube y los contenedores requiere la creación y gestión de numerosas identidades para autenticarlas. Como resultado, las empresas dependen mucho más de las identidades y credenciales. No resulta sorprendente que estas credenciales sean objetivos atractivos para los ciberdelincuentes. Las credenciales amenazadas y la suplantación de identidad son las principales causas de incidentes de seguridad y brechas de datos.

Debido a la ampliación de la superficie de ataques, algunos reglamentos como el RGPD, la CCPA, el PCI DSS y la HIPAA se basan en el principio de responsabilidad y exigen una fuerte autenticación y autorización de cada comunicación y proceso de datos.

Además, el entorno laboral a nivel mundial está cambiando. Las tendencias de teletrabajo, motivadas por la pandemia de la COVID-19, aceleran la adopción de plataformas en la nube y aumentan la necesidad de autenticar de forma eficaz y conceder acceso a recursos corporativos basados en decisiones contextuales, adaptables y dinámicas en el punto de acceso.

Estos avances han llevado al NIST a estandarizar las arquitecturas Zero Trust. La arquitectura Zero Trust del NIST SP 800-207 sirve como modelo para Zero Trust y "ofrece unos modelos de implementación general y casos prácticos donde la confianza cero podría mejorar la postura general de seguridad de tecnología de la información de una empresa". El lanzamiento de esta publicación conducirá a una mayor adopción del modelo de seguridad Zero Trust.

"El uso de las soluciones de seguridad tradicionales, que dependen de enrutamientos en las instalaciones locales, para hacer cumplir la autenticación y la autorización a la nube reduce la productividad, la escalabilidad y la experiencia de usuario."

Enfoques del NIST para las arquitecturas Zero Trust

El NIST describe tres enfoques para construir una arquitectura Zero Trust efectiva.

Centrado en la identidad

El enfoque centrado en la identidad de la arquitectura Zero Trust sitúa la identidad de los usuarios, servicios y dispositivos en el centro de la creación de políticas. Las políticas de acceso a recursos empresariales se basan en la identidad y atributos asignados. El requisito principal para acceder a los recursos corporativos se basa en los privilegios de acceso concedidos a un usuario, servicio o dispositivo determinado. Para proporcionar una autenticación más adaptable, la aplicación de la política también puede considerar otros factores, como el dispositivo utilizado, el estado del activo y los factores contextuales.

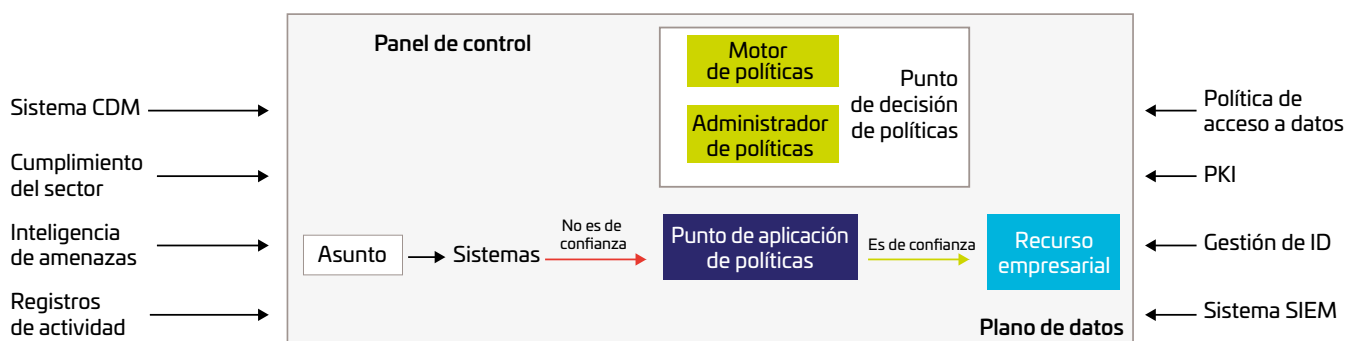


Figura 1: Enfoque de la arquitectura Zero Trust centrada en la identidad del NIST. Fuente: NIST SP 800-207

Centrado en la red

El enfoque centrado en la red de la arquitectura Zero Trust se basa en la microsegmentación de la red de recursos corporativos protegidos mediante un componente de seguridad de la puerta de enlace. Para implementar este enfoque, la empresa debería utilizar dispositivos de infraestructura como interruptores inteligentes (o rúteres), cortafuegos de última generación (NGFW) o redes definidas por software (SDN) para que actúen como un mecanismo de aplicación de políticas que proteja cada recurso o grupo de recursos relacionados.

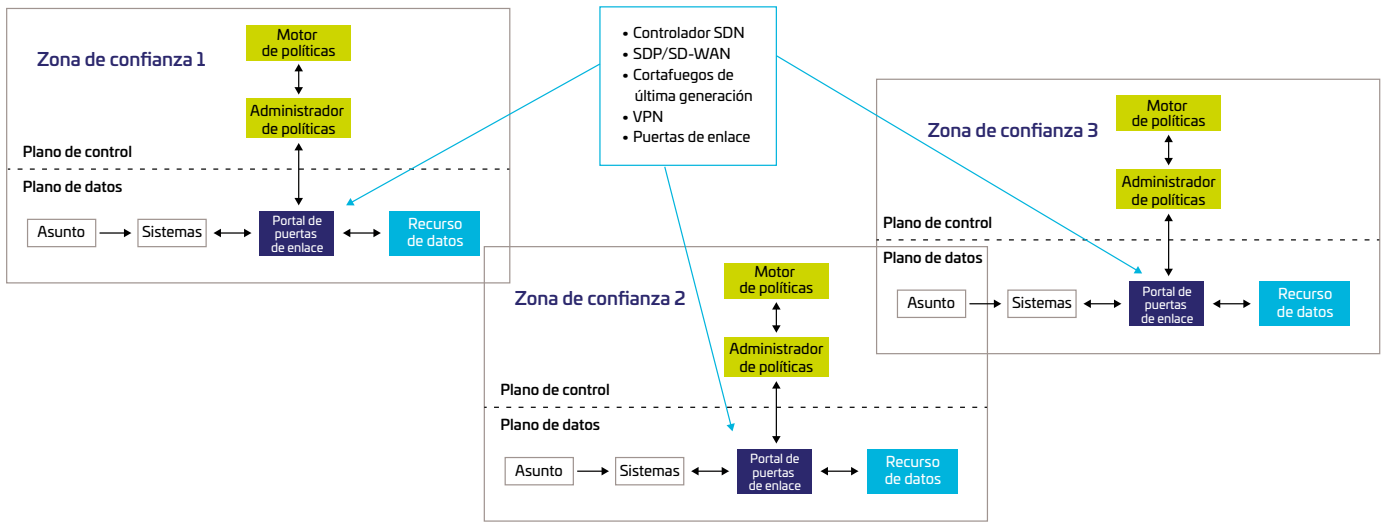


Figura 2: Enfoque de la arquitectura Zero Trust centrado en la red del NIST. Adaptada de NIST SP 800-207.

Un enfoque centrado en la red busca segmentar el perímetro tradicional en subzonas. Los usuarios se consideran de confianza una vez que están dentro de una zona. Aunque se reduce el riesgo en cierta medida, el enfoque centrado en la red no está libre de riesgos ya que asume que una entidad es de confianza una vez que está dentro de la zona. Por este motivo, este enfoque requeriría unas medidas de seguridad adicionales y una sólida gestión de identidades.

Centrado en la identidad	Centrado en la red
Utilizar un modelo de confianza de identidad sólido permite la adopción rápida de nuevas tecnologías	Complejo de configurar, resolver problemas y gestionar dada la multitud de zonas de seguridad de red
La confianza en la identidad es un modelo que se autorrefuerza: cuando más evalúe/controla las identidades en los sistemas, más conocimiento obtiene y más se refuerza la confianza	Único punto de vulnerabilidad: una vez que los usuarios están en la zona, son libres de merodear con un control limitado y con visibilidad sobre lo que hacen
La evaluación de confianza-identidad se generaliza y puede ser utilizada por los nuevos servicios para tomar decisiones de seguridad sencillas	Puede que no sea compatible con aplicaciones en la nube en una zona de confianza
	Dejar que personas que no son empleadas entren en estas zonas es una mala práctica, pero es difícil de evitar (p. ej., contratistas)

Tabla 1: Comparación de los enfoques Zero Trust centrados en la identidad y centrados en la red

Combinación en la nube

Un enfoque de arquitectura Zero Trust combinado en la nube saca provecho del Access Management en la nube y del SASE (Software at the Service Edge). La solución de Access Management en la nube protege e impone las identidades de las aplicaciones y servicios en la nube, mientras que los componentes SASE, como las redes definidas por software (SDN) o los cortafuegos de última generación (NGFW) protegen los recursos en las instalaciones locales y controlan el tráfico de red.

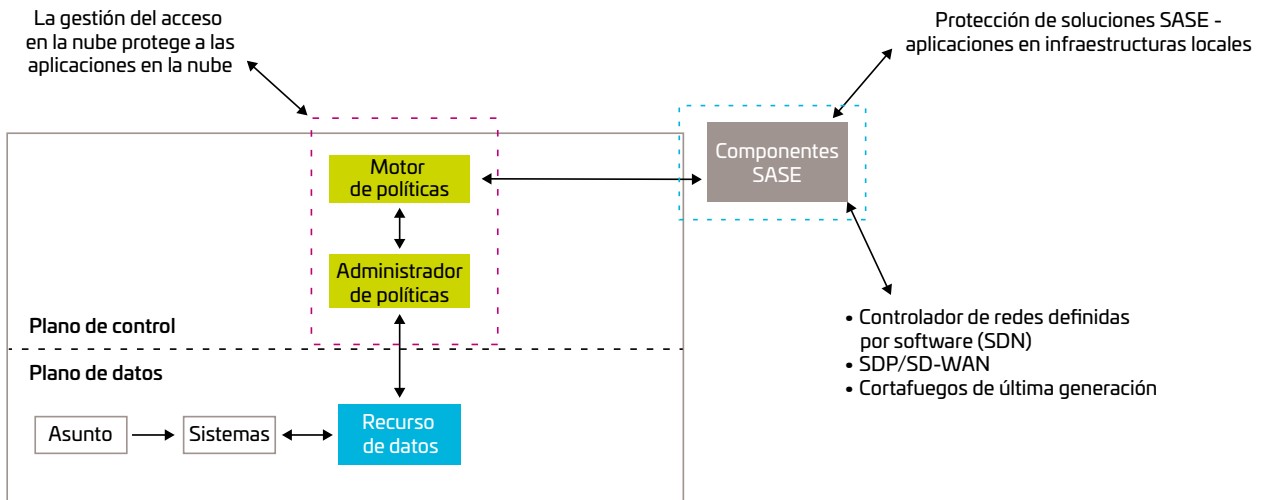


Figura 3: Enfoque de arquitectura Zero Trust combinado y en la nube.

Implementar el modelo Zero Trust con SafeNet Trusted Access de Thales

El perímetro de seguridad empresarial moderno ya no es una ubicación física: es un conjunto de puntos de acceso dispersos y accesibles en la nube. Las identidades son ahora el nuevo perímetro y deberían ser la prioridad a la hora de tomar decisiones de acceso. La identidad de cualquier recurso, usuario, dispositivo o servicio ofrece el contexto clave para la aplicación de las políticas de acceso.

La identidad es la piedra angular de la seguridad Zero Trust para las aplicaciones y activos de datos que una empresa quiere proteger. El mayor desafío es emplear una solución de seguridad Zero Trust integral que abarque identidades y datos de forma completa. Con sus soluciones de autenticación y gestión de acceso en la nube, Thales da respuesta a las necesidades esenciales de seguridad Zero Trust de las empresas de forma holística.

SafeNet Trusted Access es el punto de inicio de las implementaciones efectivas de seguridad Zero Trust, que cumplen los principios Zero Trust:

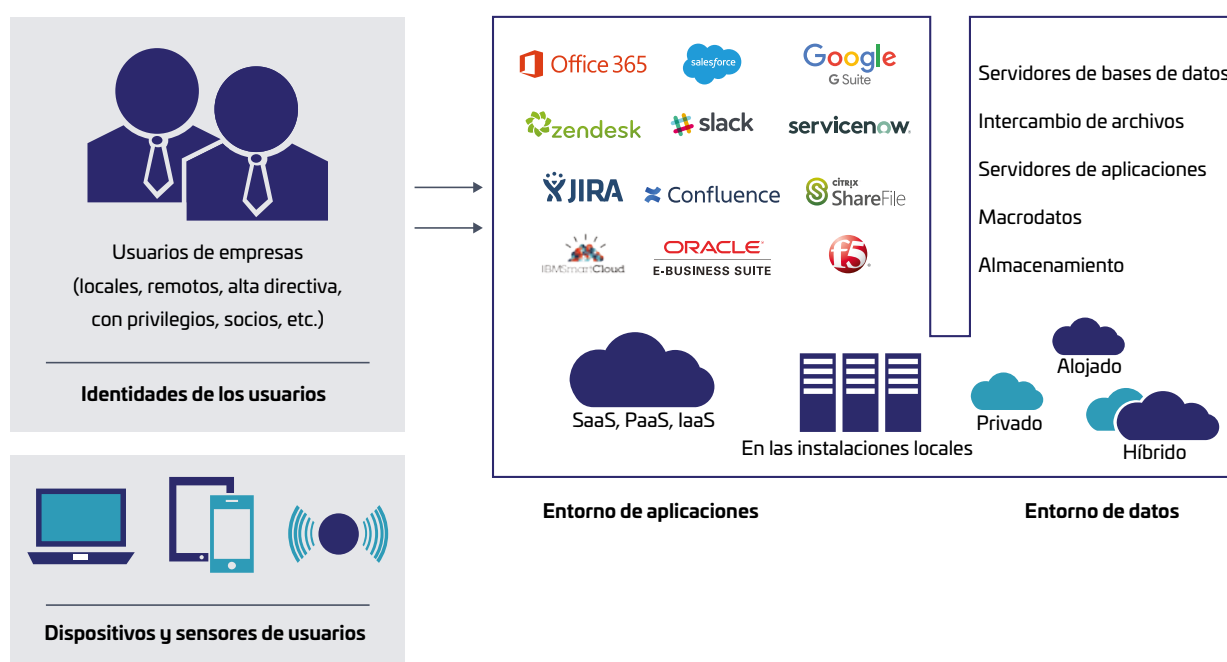
- Las decisiones de acceso se aplican de forma dinámica en el punto de acceso de la aplicación, independientemente de dónde se encuentre la aplicación, de dónde se encuentren los usuarios, de qué dispositivos utilicen los usuarios y del enrutamiento de red
- Las decisiones se fundamentan en las aportaciones actualizadas de las tecnologías de los proveedores externos de seguridad de redes como VPN, WAM, WAF, SASE, etc.
- Las decisiones de acceso que se adhieren a una estancia de "rechazo predeterminado" se reevalúan continuamente incluso si las funciones de inicio de sesión único (SSO) están habilitadas.

Ventajas de utilizar SafeNet Trusted Access de Thales para implementar el modelo Zero Trust

Hay varias ventajas al utilizar SafeNet Trusted Access para implementar una arquitectura Zero Trust centrada en la identidad:

Enfoque de arquitectura lógica

Las soluciones perimetrales tradicionales controlan el tráfico a través de un punto central en las instalaciones locales que no es efectivo para el tráfico generado o enrutado a la nube y podrían crear un cuello de botella y un fallo de punto único de acceso. SafeNet Trusted Access se diseñó para la nube y se implementa en la nube. Por lo tanto, no depende de la infraestructura en las instalaciones locales y puede controlar el acceso en la nube evitando cuellos de botella. Además, ya que todas las decisiones relacionadas con la autenticación y el acceso se aplican continuamente en cada punto de acceso, SafeNet Trusted Access permite la seguridad en todos los entornos de red dispersos, permitiendo la implementación de el enfoque Zero Trust.



Flexible y ágil

Uno de los principales puntos fuertes de SafeNet Trusted Access es su motor de políticas, que permite establecer políticas de acceso que son sumamente flexibles. Las políticas de seguridad permiten la creación de normas muy granulares y específicas para reevaluar constantemente a los usuarios durante una sesión abierta, en vez de solo para ciertos eventos como los tiempos de espera de autenticación. Si el nivel de riesgo cambia, SafeNet Trusted Access obliga al usuario a reautenticar o a proporcionar una forma de autenticación más segura. Las políticas se pueden establecer por aplicación, aplicarse a rangos de red, sistemas operativos, colecciones de usuarios y geolocalizaciones. Las normas de autenticación se pueden establecer de forma tan dinámica y específica por contexto como sea necesario, adaptándose a los cambios en un entorno en la nube dinámico.

Facilidad de implementación, gestión y escalabilidad

SafeNet Trusted Access ofrece una forma sencilla y escalable de facilitar el teletrabajo o el trabajo a distancia desde cualquier punto. Mientras que las soluciones SASE todavía están evolucionando y las soluciones tradicionales no son adecuadas para cumplir los requisitos modernos Zero Trust, la plataforma SafeNet Trusted Access ya está disponible, establecida y probada. Dado que todas las tecnologías y servicios están utilizando el enfoque Zero Trust centrado en la identidad, SafeNet Trusted Access ofrece una solución preparada para el futuro y adaptable para proteger los recursos corporativos estén donde estén.

Experiencia de usuario fluida y conocida

La capacidad de integrar perfectamente una amplia gama de aplicaciones y servicios es clave para garantizar un marco de acceso unificado y estandarizado, así como una experiencia de autenticación coherente para los usuarios finales. SafeNet Trusted Access ofrece un acceso coherente a las aplicaciones en todos los escenarios de inicio de sesión y aplica rutas de red unificadas para todas las aplicaciones, independientemente de que estén en la nube, o protegidas por VPN o proxies de Internet. Por último, para hacer frente a los requisitos del teletrabajo, SafeNet Trusted Access puede facilitar la implementación de programas "traiga sus propios dispositivos" (o BYOD) sin poner en riesgo la seguridad.

Conclusión

En el concepto de seguridad tradicional de "castillo y foso", se confiaba en los actores con malas intenciones una vez que estos estaban dentro de las redes corporativas y tenían libertad para merodear sin trabas. Los conceptos de seguridad Zero Trust permiten a las organizaciones desarrollarse de forma segura en la nube y adaptarse a entornos sin fronteras y dispersos. SafeNet Trusted Access da respuesta a estas necesidades garantizando una actitud "no confíe en nadie, verifíquelo todo" gracias a su capacidad de proteger continuamente aplicaciones y servicios en el punto de acceso, independientemente de la red subyacente implementada, la ubicación de la aplicación, la ubicación del usuario o el dispositivo final que se esté utilizando.

Acercas de Thales

Las personas a las que confía la protección de su privacidad confían en Thales para proteger sus datos. Las empresas se enfrentan a un número cada vez mayor de momentos decisivos relacionados con la seguridad de los datos. Tanto si se trata de elaborar una estrategia de cifrado, como de migrar a la nube o de cumplir los requisitos normativos, puede confiar en Thales para proteger su proceso de transformación digital.

Tecnología decisiva para momentos decisivos.

THALES

Póngase en contacto con nosotros

Para conocer la ubicación de las oficinas y nuestros datos de contacto, visite cpl.thalesgroup.com/es/contact-us

> cpl.thalesgroup.com/es <

