jamf

ZTNA y acceso de confianza:

Mejores prácticas para el acceso a la identidad y el cumplimiento de la seguridad

Zero Trust ha arrasado en el mundo de la ciberseguridad. Según el informe **The State of Zero Trust Security 2022 de Okta** (La situación de la seguridad de confianza cero 2022 de Okta), el porcentaje de empresas que desarrollaron o implementaron Zero Trust en los siguientes 12-18 meses de esa fecha, aumentaron del 16% en 2019 al 97% en 2022. La eliminación del perímetro de la red que provino del aumento del trabajo a distancia como consecuencia de la pandemia hizo que la arquitectura de confianza cero se convirtiera en una necesidad, no solo en una moda agradable de tener.

El Zero Trust Network Access, (Acceso a la Red de Confianza Cero, o ZTNA), es un pilar de la implementación de la confianza cero. Piense en la arquitectura de confianza cero como en un castillo cerrado con varios aposentos que alberga su red: ZTNA es la guardia que verifica la identidad de cualquier invitado, le abre la puerta y le acompaña a los aposentos a los que tenga permiso de acceder. Si las intenciones del huésped resultan sospechosas en algún momento, se le expulsará inmediatamente de sus habitaciones y se le revocará el permiso.

Dejando a un lado las analogías medievales, comprender la ZTNA es fundamental para avanzar en la ciberseguridad.

En este documento abordamos:

- Concesión de acceso con privilegios mínimos
- Verificación de la identidad con autenticación multifactor (MFA) y proveedores de identidad en la nube (IdP)
- Cumplimiento de normatividad y seguridad
- Apoyo al usuario final

Acceso con privilegios mínimos

El principio del privilegio mínimo es sencillo: los usuarios y sus dispositivos solo tienen acceso a lo que sea necesario para su función laboral y nada más. Por un lado, esto conlleva cierta tarea de contabilidad, ya que hay que llevar un registro de quién necesita acceso a qué, y quién lo tiene actualmente. Por otro lado, usted no gastará dinero en un número excesivo de licencias. Pero el verdadero poder reside en la reducción de la superficie de ataque: si usted limita el número de usuarios con permisos, limitará el número de cuentas que puedan poner en peligro su red a través de un determinado recurso. Esto también reduce el riesgo de movimiento lateral si un actor malicioso entra en su red, ya que los usuarios no tienen acceso a su red en su conjunto.

ZTNA aplica el principio del privilegio mínimo creando un perímetro definido por software (SDP). Un SDP no separa las conexiones de red mediante una VLAN o una dirección de red; por medio de la tunelización dividida, concede acceso solo al subconjunto de recursos al que el usuario tiene permiso de acceso, independientemente de su ubicación en la red de la empresa. Los recursos a los que el usuario no tiene permiso de acceso se mantienen invisibles e inaccesibles para el usuario.

Identidad: autenticación y autorización

El fundamento del ZTNA es la identidad. "Nunca confíes, siempre verifica", es el mantra de Zero Trust, y significa obligar siempre a los usuarios y dispositivos a demostrar su identidad al iniciar sesión en los recursos, independientemente de la frecuencia o recurrencia de un inicio de sesión con éxito.

Establecer la identidad en un entorno remoto tiene sus dificultades. Las organizaciones no pueden confiar en las configuraciones locales de Active Directory (AD) o LDAP, especialmente en los dispositivos Apple para los que AD no fue creado. Ahí es donde entran en juego los proveedores de identidad en la nube (IdP), como Okta, G Suite y Microsoft Entra ID.

Los IdP en la nube proporcionan el servicio de directorio dondequiera que se encuentren sus usuarios. Su IdP realiza un rastreo de la información de un usuario: quién es, cuál es su puesto y a qué aplicaciones tiene permiso de acceder. En otras palabras, autentica al usuario y determina su autorización a los recursos de la empresa.

Microtúneles basados en aplicaciones

Cuando hablamos de ZTNA, a menudo mencionamos la identidad del usuario, pero otro aspecto relevante es la identidad de la aplicación. Las políticas de microtunelización basadas en aplicaciones trabajan tras bambalinas para hacer realidad la ZTNA. Al asignar a las aplicaciones una identidad independiente de la red, se consigue una segmentación más precisa de la red, al mismo tiempo que se permite que las directivas sigan siendo válidas sin importar la ubicación de la aplicación en un servidor local o en la nube. Esto facilita la aplicación de las políticas de seguridad de norte a sur y de este a oeste al ofrecerle una visibilidad clara del tráfico de la aplicación.

El uso de IdP en la nube con este tipo de microtunelización le permite aprovechar las ventajas de una implementación basada en la nube. No tiene que administrar la identidad ni alojar las aplicaciones únicamente en sus servidores: su proveedor de ZTNA puede redirigir el tráfico según sea necesario. De este modo, no tendrá que mantener o supervisar servidores o hardware que no desee, al tiempo que ofrece a los usuarios el acceso seguro y cómodo que necesitan.

Política de acceso unificada

Todo ello culmina en una política de acceso unificada. Esta política debe cubrir todos los hosts relevantes para su organización, ya sea en las instalaciones, en una nube privada o pública, dentro de una aplicación SaaS, en un sistema operativo moderno o en otro paradigma de administración. Una política efectiva incluye:

- Servicios de directorio y funciones de inicio de sesión único a través de un IdP en la nube
- Autenticación multifactor
- Control de acceso basado en funciones o cargos según los principios del privilegio mínimo
- Repositorio de SSO habilitado de aplicaciones permitidas
- Un sistema de control para dirigir el tráfico a las ubicaciones de red adecuadas (incluido el tráfico web local, en la nube, SaaS y no empresarial)

Cumplimiento de la normativa y seguridad

La identidad es la mitad de la batalla en la ZTNA, la otra mitad es el cumplimiento. A usted no le conviene permitir que los dispositivos comprometidos o en riesgo tengan acceso a los recursos de su empresa, ni siquiera con el resto de las medidas de protección establecidas.

¿Cómo puede asegurarse de que los dispositivos que se conecten a sus recursos cumplan con la normativa? Como lo implica la "confianza cero", no se puede confiar en que ningún dispositivo, servidor o aplicación estén libres de riesgos. Sus políticas de acceso deben incluir métodos para identificar dispositivos vulnerables y/o comprometidos.

Su software de cumplimiento puede comprobar:

- Las versiones de sistemas operativos o aplicaciones no parchadas/vulnerables
- El software de protección activa de endpoints
- La actividad sospechosa no característica del usuario
- Las amenazas en el dispositivo o sitios maliciosos a los que ha accedido el usuario

Si se cuestiona la conformidad de un dispositivo, puede suprimir su acceso a los recursos de la empresa. La aplicación de estos controles de conformidad tiene un aspecto diferente en función del tipo de dispositivo, ya sea si éste es propiedad de la empresa o personal. En cualquier caso, el dispositivo debe disponer de algún tipo de software de administración cuando se conecte a aplicaciones corporativas, aunque debe seguir respetándose la privacidad del usuario. Los dispositivos personales (BYO) deben dirigir el tráfico personal directamente, no a través del software de control de la empresa, y los datos personales y de la empresa deben mantenerse totalmente separados por motivos de seguridad y privacidad.

Verificación continua

La verificación del cumplimiento de normatividad de un dispositivo no solo tiene lugar en el momento del inicio de sesión. Forma parte del paradigma "nunca confíes, verifica siempre": el dispositivo podría ponerse en riesgo en cualquier momento. La verificación continua del estado de un dispositivo es primordial; incluso el usuario mejor intencionado puede ser víctima de un intento de phishing o de infiltración de malware.

Experiencia del usuario final

Un servicio ZTNA burdo, difícil de usar y poco confiable no augura nada bueno para su éxito. Si el servicio entorpece el uso a los usuarios, es más probable que intenten saltarse las medidas que usted ha puesto en marcha para proteger sus recursos.

Sin importar cómo se implemente el ZTNA, los usuarios apenas deben notarlo, al tiempo que se proporciona un acceso fluido y siempre disponible a las aplicaciones empresariales. La aplicación local del dispositivo que controla la conexión no debe afectar a la duración de la batería y automáticamente debe establecer túneles con las aplicaciones empresariales cuando se le solicite, reconectándose si se produce una interrupción. Esto no solo facilita la vida de sus usuarios (y tal vez también les haga más felices), sino que evita que la IT en la sombra introduzca vulnerabilidades ocultas en su infraestructura.

El uso del inicio de sesión único (SSO) con su IdP en la nube puede agilizar aún más el proceso al administrar la contraseña de un usuario para cualquier aplicación disponible y simplificar el proceso de autenticación. Al fin y al cabo, es mucho más sencillo recordar una contraseña y verificarla con datos biométricos u otro tipo de MFA que recordar las contraseñas de todas sus aplicaciones empresariales.

Debe tener un software ZTNA que:

- Utilice la potencia del SSO y los IdP en la nube para una autenticación sencilla
- Funcione dondequiera que se encuentren los recursos en redes internas o externas
- Cree microtúneles seguros a una aplicación sin proporcionar acceso total a las redes corporativas
- Facilite la disponibilidad de las aplicaciones cuando se verifica el estado del usuario y del dispositivo
- Proteja la privacidad de los usuarios al tiempo que mantiene a salvo los datos de la empresa
- Pase desapercibido para el usuario final, y esta es la receta para una implementación satisfactoria que mantenga contentos y productivos a los usuarios, los equipos informáticos y de seguridad

Implemente Trusted Access (Acceso de confianza)

Aunque no puede confiar ciegamente en los dispositivos de su red, sí puede confiar en que sus controles de acceso mantengan a salvo a sus usuarios y a su empresa. La solución ZTNA de Jamf es lo que su organización necesita para lograr el acceso de confianza. Obtenga más información sobre cómo el acceso de confianza une la administración de dispositivos, la identidad y el acceso, así como la seguridad de los endpoints. Y compruebe por qué la solución segura ZTNA de Jamf gusta tanto a los administradores como a los usuarios con una prueba gratuita.

Solicite una prueba

O comuníquese con su distribuidor favorito para empezar.

jamf

www.jamf.com/es/