WHITE PAPER

Trabajar desde cualquier lugar no tiene por qué ser complicado

Proporcionar una seguridad robusta con independencia de la ubicación de los usuarios

Resumen ejecutivo

Durante la última década, la tecnología ha ido evolucionando sin cesar para ofrecer a los trabajadores más flexibilidad en los dispositivos que utilizan, los lugares desde los que pueden trabajar y los recursos a los que pueden acceder. BYOD (del inglés "Bring Your Own Device") y el acceso a las aplicaciones en la nube fueron los primeros pasos para permitir el trabajo flexible.

Aunque las organizaciones estaban en camino de adoptar una verdadera estrategia de trabajo desde cualquier lugar (WFA) en algún momento de los próximos años, la pandemia de la COVID-19 aceleró esta necesidad. Y ahora más trabajadores exigen que sus compañías ofrezcan una opción de WFA. El desafío radica en cómo ofrecer una experiencia laboral híbrida que mantenga a los trabajadores productivos y seguros.

Según el informe Global Threat Landscape Report, los incidentes de ransomware aumentaron casi un 1100 % de junio de 2020 a junio de 2021[1]

Proteger a los empleados híbridos

Cuando comenzó la pandemia, pocas organizaciones estaban preparadas para soportar el trabajo remoto. Los trabajadores se conectaron de repente a la oficina desde redes domésticas poco seguras. Los controles de acceso eran inadecuados y los dispositivos de endpoints eran vulnerables. No es de extrañar que los ciberdelincuentes se apresuraran a explotar estas debilidades. De hecho, Forrester observó recientemente que el 67 % de las organizaciones habían sufrido un ciberataque con impacto en el negocio atribuido a las vulnerabilidades del trabajo remoto.[2]

De cara al futuro, muchas organizaciones están planeando dejar que un número significativo de sus empleados siga trabajando a distancia al menos una parte del tiempo. Como ya han invertido en herramientas y soluciones para ayudar a sus empleados a seguir siendo productivos, no hay razón para negar a los empleados que prefieren el trabajo remoto la posibilidad de seguir haciéndolo.

Los trabajadores híbridos pueden estar en la oficina unos días a la semana y trabajar desde casa o desde cualquier otro lugar el resto del tiempo. Estos trabajadores y sus dispositivos necesitan moverse sin problemas entre esos entornos. Con independencia de dónde se encuentren, necesitan poder acceder de forma segura a las aplicaciones y recursos de la nube o del centro de datos.

Para apoyar el trabajo desde cualquier lugar, las organizaciones deben pensar en la seguridad e implementar soluciones que sean capaces de seguir, habilitar y proteger a los usuarios sin importar dónde se encuentren. Necesitan seguridad en el endpoint combinada con acceso de confianza cero (ZTA) y acceso a redes de confianza cero (ZTNA). También necesitan redes de área extensa definida por software (SD-WAN) y un Secure Access Service Edge (SASE) para una conectividad segura. Los motores de políticas de acceso deben proporcionar un acceso adecuado basado en la identidad del usuario y del dispositivo, la ubicación, el tipo de dispositivo y la postura para establecer un acceso seguro.

El desafío al que se enfrentan la mayoría de las organizaciones es intentar dar soporte al WFA empleando productos de una docena o más de proveedores independientes. Un proveedor puede ofrecer protección de endpoints (EPP), otro proporcionar detección y respuesta de endpoints (EDR), otro encargarse de la identidad, etc. Incluso puede haber diferentes proveedores de firewall implementados en el centro de datos, en las delegaciones y en las diversas plataformas en la nube que se utilizan. La creación de una solución cohesiva y fiable con tantos proveedores es casi imposible. En última instancia, las organizaciones acaban creando complejos métodos alternativos para conseguir que las soluciones funcionen de manera conjunta. Y el mantenimiento de esos sistemas requiere una cantidad considerable de gastos generales de TI.

Un enfoque mejor es implementar soluciones como parte de una arquitectura de ciberseguridad totalmente integrada. Este enfoque de plataforma proporciona una seguridad más sólida, una gestión y orquestación más sencillas, y un mejor coste total de propiedad que las soluciones que funcionan de manera aislada.

Protección en todas partes

El apoyo al WFA requiere una seguridad que funcione tanto si el usuario trabaja desde la oficina corporativa, como si lo hace desde su oficina en casa o mientras se desplaza y no se encuentra ni en la oficina corporativa ni en su oficina en casa. Cada una de estas ubicaciones plantea desafíos y requiere cierta tecnología de seguridad para una protección completa.

En la Encuesta Global de Ransomware de Fortinet, el 67 % de las organizaciones informan haber sido objetivo de ransomware.[3]

Trabajar desde la oficina

Dado que las organizaciones dependen de aplicaciones para llevar a cabo sus negocios, la protección del acceso a esas aplicaciones, de las redes para conectarse a esas aplicaciones y de los dispositivos que las ejecutan sigue siendo un componente esencial de una defensa por capas, incluso cuando un empleado trabaja desde una oficina corporativa tradicional. En la mayoría de las oficinas corporativas se encuentran los datos de los clientes, los servidores, las aplicaciones, la información de identidad, las credenciales de los usuarios y el código fuente al que los hackers quieren acceder. La protección de los usuarios, los dispositivos y los servidores en la oficina comienza con los firewalls de nueva generación (NGFW) como la primera de las múltiples defensas para este repositorio crítico de información. Las organizaciones necesitan complementar esos NGFW con una combinación integrada de seguridad de endpoints, confianza cero y gestión de identidades:

- Los NGFW protegen el acceso externo al demostrar una seguridad avanzada y coherente en entornos de campus, centros de datos, sucursales y nubes.
- Los agentes y servicios de identidad de ZTNA controlan y protegen el acceso a las aplicaciones y otros recursos. ZTNA ofrece control interno mediante el control del acceso a las aplicaciones, túneles cifrados en la oficina y verificaciones de los usuarios.
- Seguridad de endpoints, como EDR, para la seguridad de los usuarios y de los dispositivos. EDR proporciona los medios para proteger los dispositivos de los usuarios e interactúa con los datos críticos.

Los entornos de oficina también deben incluir soluciones de seguridad y redes, como Secure SD-WAN, que ofrecen herramientas de redes avanzadas diseñadas para operar desde una plataforma de seguridad unificada que optimiza la conectividad WAN entre centros de datos, nubes, delegaciones y campus con inteligencia de reconocimiento de aplicaciones.

Trabajar desde casa

Los empleados remotos e híbridos suelen conectarse desde un entorno de oficina en casa con un portátil, un monitor y una cámara web externa. Sin embargo, esas redes domésticas suelen estar mal protegidas con routers inalámbricos y pueden contener dispositivos vulnerables del Internet de las Cosas (IoT) que pueden servir de vía de acceso para los hackers. Los empleados que utilizan las redes domésticas también se enfrentan a desafíos cuando se trata de videoconferencias y otras actividades que requieren un gran ancho de banda. La productividad de los trabajadores puede verse afectada si otros miembros de la casa, como miembros de la familia o compañeros de piso, consumen ancho de banda con actividades de videostreaming o juegos on line. Los usuarios domésticos necesitan:

- Seguridad de los endpointsz como EDR, para proteger al trabajador y a los dispositivos
- Agentes de ZTNA y servicios de identidad para controlar y proteger el acceso a las aplicaciones y otros recursos
- Seguridad de clase empresarial para que las redes domésticas garanticen un acceso seguro a la red corporativa, así como a las aplicaciones en la nube y al centro de datos. Debe incluir la gestión del tráfico para priorizar el tráfico empresarial sobre el videostreaming o los juegos.

Una solución para la oficina en casa debe extender las protecciones del firewall corporativo a toda la red doméstica. También debe segmentar la red doméstica para proporcionar al departamento de TI de la empresa visibilidad del tráfico corporativo y optimizar el ancho de banda para las aplicaciones empresariales, al tiempo que se garantiza la privacidad de los empleados para la sección que no es de trabajo de la red.

Trabajar mientras se viaja

Los usuarios que viajan o trabajan fuera de la oficina corporativa o de su espacio remoto principal suelen estar expuestos a entornos de amenazas únicos. Cuando los usuarios móviles se conectan a las aplicaciones y recursos que necesitan para realizar su trabajo, pueden utilizar redes y puntos de acceso desconocidos y no seguros, que pueden utilizarse potencialmente para poner en peligro la red. Los usuarios móviles necesitan:

- Seguridad de los endpoints, como EDR, para proteger al usuario y a los dispositivos
- Agentes de ZTNA y servicios de identidad para controlar y proteger el acceso a las aplicaciones y otros recursos
- Soluciones SASE de seguridad de red remota para capacidades de firewall basadas en la nube para proteger a los empleados que están fuera de la oficina o de la red doméstica

Una solución de red móvil debe incluir la autenticación multifactor, una puerta en enlace web segura basada en la nube (SWG) y un agente de seguridad de acceso a la nube (CASB).

Seguridad integrada de la WFA mejorada con inteligencia sobre amenazas

Para apoyar el WFA, las organizaciones deben identificar una plataforma de ciberseguridad con soluciones que estén diseñadas para trabajar como un sistema integrado, con inteligencia de amenazas procesable para mantener los productos de seguridad informados y preparados con información de identificación y protección de amenazas en todos los tipos de ubicaciones. Este tipo de enfoque de plataforma significa que la seguridad de red, endpoints y confianza cero pueden unificarse mediante un conjunto común de interfaces de programación de aplicaciones (API) y puntos de integración para garantizar que los usuarios puedan pasar sin problemas de una ubicación a otra con una experiencia coherente y segura. Y en el lado de TI, la malla de ciberseguridad simplifica la creación y aplicación de políticas, garantiza configuraciones uniformes, centraliza la gestión, y permite supervisar y controlar a los usuarios, los dispositivos, los datos, las aplicaciones y los flujos de trabajo.

El trabajo desde cualquier lugar ha cobrado importancia debido a la reciente pandemia, pero esta no ha hecho más que acelerar una tendencia que ya estaba en marcha. El entorno de trabajo híbrido ha llegado para quedarse y las organizaciones deben asegurarse de que están preparadas para utilizar con seguridad ese modelo de trabajo.

[1] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs", Fortinet, agosto de 2021.

[2] "Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work", Forrester, 2021

[3] "The 2021 Ransomware Survey Report", Fortinet, 3 de noviembre del 2021.

FORTINET

www.fortinet.com

Copyright © 2021 Fortinet, Inc. Todos los derechos reservados. Fortinet®, FortiGate®, FortiCare®, FortiGuard® y otras marcas son marcas comerciales registradas de Fortinet, Inc., y otros nombres de Fortinet contenidos en este documento también pueden ser nombres registrados y/o marcas comerciales de Fortinet conforme a la ley. El resto de nombres de productos o de empresas pueden ser marcas registradas de sus propietarios respectivos. Los datos de rendimiento y otras métricas contenidas en este documento se han registrado en pruebas internas de laboratorio bajo condiciones ideales, de forma que el rendimiento real y otros resultados pueden variar. Variables propias de la red, entornos de red diferentes y otras condiciones pueden afectar a los resultados del rendimiento. Nada de lo contenido en este documento representa un compromiso vinculante de Fortinet, y Fortinet renuncia a cualquier garantía, expresa o implícita, salvo en los casos en los que Fortinet celebre un contrato vinculante por escrito, firmado por el Director del Departamento Jurídico de Fortinet, con un comprador, en el que se garantice expresamente que el producto identificado cumplirá una determinada métrica de rendimiento expresamente identificada y, en tal caso, solamente la métrica de rendimiento especificada en dicho contrato por escrito será vinculante para Fortinet. Para dejarlo absolutamente claro, cualquier garantía de este tipo se verá limitada al rendimiento en las mismas condiciones ideales que las de las pruebas de laboratorio internas de Fortinet. Fortinet no se hace en absoluto responsable de ningún pacto, declaración y garantía en virtud de este documento, expresos o implícitos. Fortinet se reserva el derecho de cambiar, modificar, transferir o revisar de cualquier otro modo esta publicación sin previo aviso, siendo aplicable la versión más actual de la misma.

mayo 14, 2022 10:43 a.m.
1400814-0-0-ES