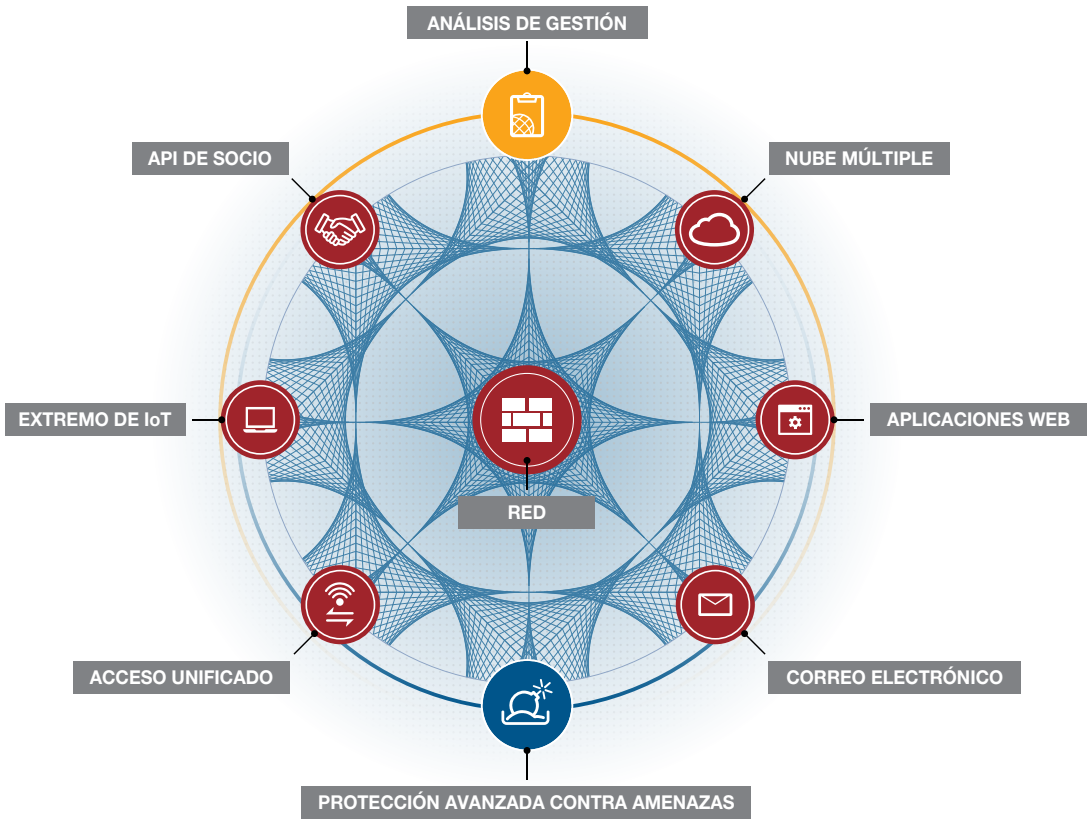
LA TRANSFORMACIÓN DE LA SEGURIDAD REQUIERE UN TEJIDO DE SEGURIDAD

El crecimiento y la adopción de la tecnología durante los últimos años han transformado los negocios, los gobiernos e incluso la economía. Esto afecta a la manera en que las personas interactúan socialmente, gestionan sus finanzas, realizan compras o transacciones, reciben noticias y entretenimiento, e incluso navegan por su entorno. También ha cambiado de manera radical sus expectativas y actitudes cuando interactúan con negocios y servicios, tanto como clientes como con empleados.

Para seguir siendo competitivos, las organizaciones han tenido que responder redefiniendo la manera en que participan en el nuevo mercado digital y satisfacen las demandas de cambio de los usuarios expertos en tecnología. Para la mayoría de las organizaciones, la transformación digital implica la integración de la tecnología digital en todas las áreas de un negocio, lo que da lugar a cambios fundamentales en la manera en que generan valor a sus clientes.

Para lograrlo, las empresas están entrelazando una variedad de dispositivos, tecnologías y servicios en una red integrada y única que se puede ampliar y adaptar dinámicamente conforme evolucionen las demandas de usuario y mercado. Esto significa luchar a la vez con asuntos como IoT, SDN, OT y entornos de nube múltiple, la proliferación de aplicaciones orientadas al cliente e internas, el crecimiento sin procedentes tanto en la velocidad como en el volumen de los datos que se generan y se consumen, la expansión de las cargas de trabajo más allá de los confines del centro de datos, y las expectativas de la próxima generación de empleados para combinar sus vidas profesionales y personas en cualquier dispositivo móvil que elijan en combinación con acceso instantáneo a cualquier dato en cualquier momento desde cualquier ubicación.



Esta transformación digital ha estirado al límite de manera simultánea los equipos de IT a la vez que ha ampliado de manera exponencial la superficie de ataque que se debe proteger. Por ejemplo, los entornos de nube múltiple implican que las organizaciones se deben preocupar por una superficie de ataque que no siempre es visible para IT, y la convergencia de entornos de IT y OT ha expuesto ahora cuestiones como las plantas de fabricación, los sistemas de control industriales y las infraestructuras críticas a nuevos riesgos. La proliferación de dispositivos de IoT en estos entornos que dependen de manera exclusiva de la red de acceso para seguridad ha agravado estos desafíos.

Al mismo tiempo que los datos empresariales de propiedad y críticos se están pasando a la nube o se están gestionando a través de servicios y aplicaciones basadas en la nube, el crecimiento del IT oculto ha dado lugar a que las organizaciones simplemente pierdan la pista de dónde se encuentran los datos o de qué medidas de seguridad están implementadas para protegerlos. BYOD complica los problemas de la gobernanza de datos aún más, ya que los usuarios pueden acceder a datos críticos de las ubicaciones públicas y guardarlos en dispositivos personales que mezclan sus perfiles profesionales y personales.

TRANSFORMACIÓN DE SEGURIDAD

Conforme las fuerzas económicas y empresariales impulsan rápidamente la evolución de la red, los equipos de seguridad de IT han estado esforzándose por mantenerla. Una parte importante del problema es que la transformación digital no se está produciendo como una actividad única e integrada. En su lugar, tiende a producirse de manera orgánica a través de proyectos independientes que realizan pequeñas transformaciones cada vez. La tendencia es proteger cada segmento de red nuevo conforme se desarrolla mediante las herramientas de red tradicionales que están más disponibles. Finalmente, esto da lugar a una compleja infraestructura de seguridad muy accidental integrada en torno a soluciones almacenadas en silos de proveedores independientes.

Lamentablemente, la complejidad suele ser el enemigo de la seguridad. Dado que los diferentes entornos requieren diferentes factores de diseño de solución, puede resultar difícil estandarizar en un único proveedor, ya que puede haber grandes variaciones entre una versión física, virtual o basada en nube del mismo producto si están incluso disponibles. Como resultado, las empresas han implementado ahora una medida de más de 30 soluciones de seguridad diferentes en sus redes distribuidas. Las soluciones de seguridad aisladas con interfaces de gestión independientes y sin manera importante de recopilar o compartir información de amenazas con otros dispositivos de la red pueden obstruir la visibilidad y limitar el control.

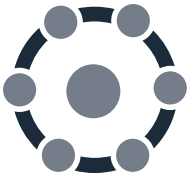
La mejor respuesta ante los entornos en red cada vez más complicados es la sencillez. Eso requiere una transformación de seguridad que pueda mantener el ritmo de la transformación digital. La transformación de seguridad implica la integración de la seguridad en todas las áreas de la tecnología digital, lo que da lugar a una arquitectura de seguridad integral y coherente que permite un ciclo de vida de seguridad eficaz que abarca todo el ecosistema distribuido de las redes. Esto incluye la identificación de la superficie de ataque, la protección frente a amenazas conocidas, la detección de amenazas desconocidas, la respuesta rápida a eventos cibernéticos de una manera coordinada y el suministro de evaluaciones continuas de amenazas.

Una estrategia de transformación de seguridad eficaz debe incluir inteligencia de colaboración e integración del sistema para que se pueda compartir la inteligencia de amenazas local y global entre dispositivos y se puedan coordinar las respuestas entre soluciones; la orquestación de las políticas de seguridad unificadas y la aplicación; la segmentación inteligente en todos los entornos físicos y virtuales para una visibilidad profunda del tráfico que se desplaza lateralmente en toda la red, incluso entre entornos de nube múltiple, e identificar dispositivos infectados y ponerlos en cuarentena; y la automatización de cribar el creciente ruido de red, correlacionar información de amenazas y responder en tiempo real a las amenazas que se encuentren en cualquier lugar de la superficie de ataque ampliada.

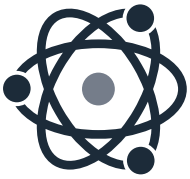
FORTINET SECURITY FABRIC

Fortinet Security Fabric es un enfoque de arquitectura que unifica las tecnologías de seguridad implementadas en toda la red digital, incluida la nube múltiple, los extremos, las aplicaciones web y de escritorio, y los puntos de acceso en un sistema de seguridad integrado a través de una combinación de estándares abiertos y un sistema operativo común. A continuación, estas soluciones se mejoran a través de la integración de tecnologías de Advanced Threat Protection y de una correlación, gestión, orquestación y sistema de análisis unificados.

Este enfoque de seguridad basado en tejido se desarrolla en torno a tres bases:



Amplitud. La visibilidad y la protección deben ampliarse en toda la superficie de ataque digital. Con el cruce de datos y las cargas de trabajo entre una variedad de factores de diseño de dispositivo y ecosistemas de red, los equipos de IT necesitan una vista integral de los dispositivos, del tráfico, de las aplicaciones, y de los eventos y de la capacidad de detener una amenaza en cualquier lugar de su cadena de ataque. Este enfoque necesita abarcar y unificar las redes físicas, los dispositivos móviles y los usuarios, y los entornos de nube múltiple cada vez más complejos tanto para soluciones IaaS como SaaS.



Integración. La integración de los dispositivos que usan estándares abiertos, sistemas operativos comunes y plataformas de gestión unificada, permite el uso compartido y la correlación de la inteligencia de amenazas en tiempo real. Este marco común también admite la detección coordinada de las amenazas avanzadas a través de análisis sofisticados y centralizados que son difíciles o imposibles de lograr con las implementaciones de seguridad tradicionalmente aisladas.

Automatización. Como en la empresa digital actual, el cibercrimen se produce a velocidades digitales. El tiempo transcurrido entre una fuga de red y la puesta en peligro de los datos o sistema pronto se medirá en microsegundos. Los sistemas de seguridad deben proporcionar automáticamente evaluación de confianza continua y una respuesta inmediata y coordinada para las amenazas detectadas. Y, dado que los entornos de red actuales son muy elásticos, las necesidades de seguridad también se deben adaptar de manera dinámica a medida que cambian los requisitos de red y las configuraciones.

Para ofrecer estas funcionalidades, Fortinet Security Fabric se crea en torno a varios elementos clave:

- *Seguridad de red*. A medida que las redes siguen evolucionando más allá de sus límites tradicionales, los ataques cibernéticos sofisticados se lanzan en la superficie de ataque ampliada, buscando debilidades. La familia de firewalls de alto rendimiento de Fortinet, creada en torno a un conjunto integrado y consolidado de soluciones de seguridad avanzada, es la primera línea esencial de defensa de cualquier organización.
- *Seguridad de nube múltiple*. La mayoría de las organizaciones han adoptado una estrategia de nube múltiple, incluidos varios proveedores de IaaS y más de una docena de proveedores de SaaS diferentes. La expansión de los datos y las cargas de trabajo en un entorno de nube distribuido dificulta la detección y la prevención de seguridad consolidada. Las soluciones de nube física y virtual integradas de Fortinet, con tecnología de Fortinet Security Fabric, amplían la seguridad sin fisuras en toda la implementación de nube distribuida, incluyendo ser la primera en proporcionar soluciones de seguridad avanzada para los cinco proveedores de servicio de nube principales.
- *Web Application Security*. Las aplicaciones web vulnerables o no protegidas son puntos de entrada comunes a la red. El Web Application Firewall de FortiWeb usa la inteligencia avanzada y las tecnologías de protección y detección más recientes para proteger las aplicaciones web de los ataques sofisticados.
- *Seguridad de correo electrónico*. El correo electrónico sigue siendo el punto de entrada principal para que el malware infecte su red. Los spammers y los phishers de correo electrónico usan datos adjuntos infectados, vínculos malintencionados y timos sofisticados para engañar a los usuarios para que hagan clic en malware o lo ejecuten. De hecho, el correo electrónico fue el vector principal de ransomware en 2017. Secure Email Gateway de FortiMail inspecciona el correo electrónico entrante y saliente, bloquea los mensajes malintencionados y los datos adjuntos, y evita que se filtre información confidencial o se produzca una fuga de la misma.
- *Acceso unificado seguro*. La mayor parte de los puntos de acceso inalámbricos proporcionan conectividad, pero poca de la manera de la seguridad real. Pero a medida que cada vez más dispositivos necesitan acceso a red inalámbrica, la protección de las comunicaciones empresariales, la información de identificación personal (IIP), dispositivos móviles y una variedad de usuarios, requiere mucho más que un control de acceso sencillo. Las soluciones de acceso seguro de Fortinet ofrecen un acceso de alto rendimiento con control de aplicaciones y seguridad completos para Wi-Fi seguro que está totalmente integrado con sus políticas y protocolos de seguridad de red.

- *Seguridad de extremos*. Las redes deben admitir una plantilla de gran movilidad y una gama creciente de dispositivos de extremos personales conectados a la red. No resulta extraño que estos dispositivos son otro punto de entrada común para las amenazas. El desafío es que las soluciones de extremo a menudo no comparten inteligencia de amenazas con el resto de la red, lo que impide determinar si un dispositivo está infectado y ralentiza la respuesta de amenazas si su comportamiento empieza a ser incorrecto. FortiClient permite a los equipos de IT la integración de una capa de seguridad de extremos automática en Security Fabric para lograr una protección de red más rápida y completa.
- *Protección avanzada contra amenazas*. Las amenazas avanzadas actuales están diseñadas para evadir la detección a través de ataques de etapa múltiple, vectores de ataque complejos y observando e imitando el tráfico y las aplicaciones legítimas. La inteligencia frente amenazas de FortiGuard ayuda a las empresas a combatir estas amenazas avanzadas ofreciendo de manera automática inteligencia en tiempo real acerca de las amenazas recientemente detectadas directamente en sus soluciones de seguridad, mientras que las soluciones de sandboxing de Fortinet detectan amenazas desconocidas y después aíslan e inspeccionan los archivos sospechosos detectados por los dispositivos de Security Fabric.
- *Gestión y análisis*. En una red grande y muy elástica, la visibilidad y el control adquieren mayor importancia que nunca. Los equipos de IT necesitan poder ver y comprender amenazas y eventos con independencia de dónde se producen en toda la red distribuida. Sin embargo, esto puede resultar un gran desafío para las empresas que han implementado productos de seguridad aislados. Las soluciones de Fortinet para registro e informes, SIEM y la gestión de seguridad centralizada recopilan y correlacionan datos de sus productos de seguridad preparados para Fabric y Fortinet, proporcionando la visibilidad crítica y el control granular necesarios para gestionar de manera eficaz procesos de seguridad y orquestar respuestas automáticas.

SOLUCIÓN DISEÑADA PARA LA EMPRESA DIGITAL ACTUAL

La transformación digital es el mayor desafío que los equipos de seguridad de IT han tenido que realizar nunca. Dado que la evolución de las redes y la informática continúan impulsando cambios en las infraestructuras empresariales críticas, las arquitecturas y las prácticas, las organizaciones requieren un enfoque de transformación de seguridad innovador que les permita adoptar dichos cambios.

Una vez que las soluciones de seguridad aisladas tradicionalmente se combinan en un marco de Security Fabric unificado, las organizaciones pueden ver dentro de la red distribuida para detectar amenazas avanzadas, adaptarse dinámicamente al panorama de amenazas y a la arquitectura de red en evolución, y aprovechar la evaluación de confianza continua que las empresas digitales actuales requieren, desde el núcleo hasta la nube.

Haga clic aquí para obtener más información sobre qué puede hacer Fortinet Security Fabric para su organización.

OFICINAS CENTRALES MUNDIALES
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Estados Unidos
Tel. +1.408.235.7700
www.fortinet.com/sales

OFICINA COMERCIAL EMEA
905 rue Albert Einstein
06560 Valbonne
Francia
Tel.: +33 4 8987 0500

OFICINA COMERCIAL APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel. +65.6513.3730

LATINOAMÉRICA SEDE CENTRAL
Sawgrass Lakes Center
13450 W. Sunrise Blvd.,
Suite 430
Sunrise, FL 33323
Tel. +1.954.368.9990

ESPAÑA
Avda. Europa, 24, Edif. B, 2B.
28108 Alcobendas,
Madrid – España
Ventas: +34 91 502 48 74

 171575-A-0-EN *julio 2, 2018 3:39 p.m.*
wp-fortinet-security-fabric-A4_ES