Cuatro factores críticos para el diseño de la arquitectura de seguridad

Presentación del Fortinet Security Fabric para una seguridad amplia, integrada y automatizada

Contenido

Resumen ejecutivo

Las organizaciones están adoptando rápidamente iniciativas de innovación digital (DI) para acelerar sus negocios, reducir costos, mejorar la eficiencia y ofrecer mejores experiencias al cliente. Para obtener resultados de DI mientras se minimiza la complejidad y gestionan los riesgos de manera efectiva, las organizaciones deben adoptar una plataforma de ciberseguridad que proporcione visibilidad en su entorno y los medios para administrar fácilmente las operaciones de seguridad y de red.

El Fortinet Security Fabric resuelve estos retos con soluciones amplias, integradas y automatizadas que habilitan redes basadas en seguridad, acceso a la red de confianza cero, seguridad dinámica en la nube y operaciones de seguridad basadas en inteligencia artificial (IA). Las ofertas de Fortinet se mejoran con un ecosistema de productos de terceros perfectamente integrados que minimizan las brechas en las arquitecturas de seguridad empresarial, mientras maximizan el retorno de la inversión (ROI) en seguridad.

El 84 % de los ejecutivos de seguridad cree que aumentará el riesgo de ciberataques.[1]

La innovación digital está transformando todas las industrias

En todos los sectores económicos alrededor del mundo, la DI se considera de gran importancia para el crecimiento empresarial y para mejorar la experiencia del cliente.[2]

Desde la perspectiva de los líderes de TI y ciberseguridad del proveedor de servicios en la nube, la DI se traduce en una diversidad de cambios en sus entornos de red. Los usuarios son cada vez más móviles y acceden a la red desde ubicaciones y terminales que no siempre están bajo el control corporativo de TI. También se conectan directamente a nubes públicas para utilizar aplicaciones comerciales clave, como Office 365. Superando en número a las terminales bajo el control humano, están los dispositivos de Internet de las cosas (IoT), los cuales están ampliamente distribuidos, por lo general, en lugares remotos y sin supervisión. Finalmente, la presencia comercial de los proveedores de servicios en la nube se está difundiendo en numerosas y remotas sucursales, la mayoría de las cuales se conectan directamente a servicios en la nube y celulares, evitando pasar por los centros de datos corporativos.

Con todos estos cambios el concepto de un perímetro de red defendible se vuelve obsoleto, obligando a los proveedores de servicios en la nube a adoptar una nueva estrategia de defensa profunda multicapa.

El 77 % de los profesionales de seguridad indican que su organización trasladó aplicaciones o infraestructura a la nube a pesar de las preocupaciones de seguridad conocidas.[3]

Migración de aplicaciones y cargas de trabajo a la nube

Casi todas las empresas han comenzado a trasladar algunas cargas de trabajo y aplicaciones a la nube o al menos planean hacerlo. Estas decisiones a menudo se basan en el deseo de reducir costos y mejorar la eficiencia operativa y la escalabilidad aprovechando la flexibilidad que ofrece la nube.

Los proveedores de servicios en la nube ofrecen una amplia variedad de posibles modelos de implementación, desde Software como servicio (SaaS) hasta Plataforma como servicio (PaaS).

Siendo cautelosas con la garantía del proveedor de servicios en la nube y con el objetivo de implementar cada aplicación y carga de trabajo en la nube más adecuada, muchas organizaciones han adoptado una infraestructura de múltiples nubes. La desventaja de esa libertad de elección es la necesidad de aprender las idiosincrasias de cada entorno de nube. Además, las organizaciones deben utilizar diferentes herramientas para administrar el entorno y sus disposiciones de seguridad, lo que desafía la visibilidad y obliga al uso de múltiples consolas de administración para la gestión de políticas e informes, entre otros.

Los entornos en la nube son dinámicos: el 74 % de las compañías trasladaron una aplicación a la nube y luego la regresaron a sus instalaciones locales.[4]

Profusión de terminales en múltiples entornos

Las terminales son posiblemente los nodos más vulnerables en la red del proveedor de servicios en la nube. Los proveedores más grandes tienen miles de empleados, cada uno de los cuales utiliza múltiples dispositivos personales y de trabajo para acceder a los recursos de la red. Garantizar una buena ciberhigiene y una seguridad de terminal actualizada en todos estos dispositivos es una tarea tremenda. Aún más intimidante es la proliferación de dispositivos del IoT. A finales de 2019, el número de dispositivos activos superó los 26.66 mil millones, y durante 2020, los expertos estiman que este número alcanzará los 31 mil millones.[5]

Los dispositivos del IoT están presentes en muchos contextos comerciales. Brindan experiencias personalizadas a clientes minoristas y de la industria hotelera, hacen un seguimiento del inventario en la manufactura y la logística y monitorean los dispositivos en las plantas de las fábricas o en plantas de energía.

Por lo general, los dispositivos del IoT, resistentes y de bajo consumo de energía, se enfocan en el rendimiento, muchas veces, a expensas de características de seguridad y protocolos de comunicación seguros. Además, a diferencia de la mayoría de los dispositivos conectados a la red, el equipo de IoT se por lo general se implementa en lugares remotos, al aire libre o en instalaciones sin personal o con poca afluencia de personal (como las estaciones eléctricas). Desde estas ubicaciones no seguras, el equipo con frecuencia transmite datos críticos y confidenciales a los centros de datos locales y a los servicios en la nube.

El 84 % de las empresas tienen una estrategia de múltiples nubes. El 81 % señala la seguridad como un gran reto para la nube.[6]

Presencia comercial expandida a través de geografías y mercados distribuidos

A medida que las empresas expanden su superficie global mediante la apertura de nuevas instalaciones, sucursales y otras ubicaciones satelitales, experimentan limitaciones cada vez mayores en el ancho de banda de la red de área amplia (WAN). Aunque las aplicaciones de SaaS, video y de Voz sobre IP (VoIP) aumentan la productividad y habilitan nuevos servicios, también contribuyen a un crecimiento exponencial del volumen del tráfico en la WAN.

El switching de etiquetas multiprotocolo (Multiprotocol label switching; MPLS) es sumamente confiable y ha sido la tecnología de conectividad de WAN predilecta durante muchos años. Sin embargo, con el MPLS es difícil optimizar el uso del ancho de banda de la WAN y variar los niveles de calidad de servicio en función de las diferentes aplicaciones. En consecuencia, la expansión de sucursales y las mejoras del servicio pueden conducir rápidamente al aumento vertiginoso de los costos de la WAN.

Por lo tanto, las organizaciones están recurriendo a la WAN definida por software (SD-WAN), que hace un uso eficiente del MPLS, de las conexiones a Internet e incluso de enlaces de telecomunicaciones. Además, la SD-WAN enruta cada tipo de tráfico de manera dinámica a través del enlace óptimo. La adopción de SD-WAN aumenta aún más la necesidad de una SD-WAN segura, que se presenta mejor como una combinación de funciones de red y seguridad en una plataforma integrada.

De 2017 a 2019, hubo un aumento del 73 % en el número de organizaciones que experimentaron violación a sus datos debido a aplicaciones y dispositivos del IoT no seguros.[7]

La SD-WAN ofrece un mejor rendimiento y seguridad a un costo menor que el MPLS.[8]

Cuatro factores críticos para el diseño de la arquitectura de seguridad

Conforme las organizaciones avanzan con entusiasmo con las iniciativas de DI, las implicaciones para la seguridad de la red a menudo se pasan por alto o se minimizan. De hecho, casi el 80 % de las organizaciones están agregando nuevas innovaciones digitales más rápido de lo que pueden protegerlas contra las ciberamenazas.[9]

Los líderes de TI deben priorizar cuatro factores sobre todo al diseñar arquitecturas seguras para sus actividades comerciales digitalmente innovadoras:

1. Conocer la superficie de ataque en expansión

Los datos confidenciales pueden residir potencialmente en cualquier lugar y pueden viajar a través de muchas conexiones fuera del control de la empresa. Las aplicaciones en la nube están expuestas al Internet de tal manera que cada nueva instancia en la nube aumenta la superficie de ataque de la empresa. Los dispositivos del IoT extienden la superficie de ataque a ubicaciones remotas y sin personal. En estas partes oscuras de la superficie de ataque, las intrusiones pueden pasar desapercibidas durante semanas y meses, causando estragos en el resto de la empresa. Los dispositivos móviles y las terminales de propiedad del usuario aportan imprevisibilidad a la superficie de ataque, ya que los usuarios deambulan

El 61 % de los CISOs afirman que ya tienen operaciones significativas en la nube, IoT y móviles.[11]

Hasta el 40 % del nuevo malware que se detecta en un día determinado es de día cero o previamente desconocido.[12]

entre ubicaciones corporativas, en espacios públicos y a través de fronteras internacionales. De hecho, la extensa migración a la nube, el extenso uso de plataformas móviles y el extenso uso de dispositivos del IoT son factores que amplifican el costo por registro de una violación a los datos por cientos de miles de dólares.[10]

Esta superficie expandida y dinámica de ataque disuelve el perímetro de la red, una vez bien definido, y las protecciones de seguridad asociadas con él. Es mucho más fácil para los atacantes infiltrarse en la red, y una vez dentro, por lo general, encuentran pocos obstáculos para moverse libremente hacia sus objetivos sin ser detectados. Por lo tanto, la seguridad en las empresas de DI debe ser multicapa, con controles en cada segmento de la red, basándose en el supuesto de que el perímetro será traspasado tarde o temprano. Además, el acceso a los recursos de la red debe basarse en el mínimo privilegio y la continua verificación de la confianza.

Las iniciativas de DI implican que los equipos de seguridad de la empresa deban implementar protecciones para 17 tipos diferentes de terminales.[13]

2. Atender la evolución de las ciberamenazas

El panorama de las ciberamenazas está creciendo rápidamente a medida que los malos actores intentan eludir y derrotar las defensas tradicionales de ciberseguridad. Hasta el 40 % del nuevo malware que se detecta en un día determinado es de día cero o previamente desconocido.[14] Ya sea que esto se deba a un mayor uso de malware polimórfico o a la disponibilidad de kits de herramientas de malware, el crecimiento del malware de día cero hace menos efectivos los algoritmos de detección de malware tradicional basado en firmas. Además, los malos actores continúan utilizando la ingeniería social vulnerando la seguridad de los métodos de confianza estáticos que se utilizan en los enfoques de seguridad tradicionales. Los estudios revelan que el 85 % de las organizaciones experimentaron ataques de suplantación de identidad o ingeniería social el año pasado.[15]

Una tercera parte de las empresas sufrió una violación a los datos críticos de la empresa en el último año, lo que podría conducir a sanciones normativas.[18]

A medida que las ciberamenazas se vuelven más sofisticadas, los incidentes y las violaciones a los datos son más difíciles de detectar y corregir. Entre 2018 y 2019, el tiempo para identificar y contener una violación a los datos aumentó de 266 a 279 días.[16] Más allá de la capacidad de detectar y prevenir un intento de ataque, las organizaciones también deben ser capaces de identificar y corregir rápidamente un ataque exitoso. Más del 88 % de las organizaciones informaron haber experimentado al menos un incidente en los 12 meses anteriores, lo que demuestra que todas las organizaciones están en riesgo de un ataque y que la ciberresiliencia es crucial.[17]

3. Simplificar un ecosistema de TI cada vez más complejo mediante la automatización

De acuerdo con casi la mitad de los CIOs, el aumento de la complejidad es el mayor desafío de una superficie de ataque en expansión.[19] Esta mayor complejidad se debe al hecho de que muchas organizaciones confían en una serie de productos puntuales no integrados para cuidar su seguridad. La empresa promedio utiliza más de 75 soluciones de seguridad distintas.[20]

Esta falta de integración de seguridad implica que estas organizaciones no puedan aprovechar la automatización en su implementación de seguridad. De hecho, el 30 % de los CIOs señalan la cantidad de procesos manuales como uno de los problemas principales de seguridad en su organización.[21] Sin la automatización de la seguridad, los CIOs necesitan profesionales de ciberseguridad más calificados para monitorear y proteger su red.

Sin embargo, muchas organizaciones no pueden adquirir el talento de ciberseguridad que requieren. Las estimaciones indican que más de 4 millones de puestos de ciberseguridad se quedan actualmente sin cubrir y la cifra aumenta constantemente.[22] Esta falta de acceso al talento necesario está poniendo en riesgo a las organizaciones, según el 67 % de los CIOs que manifiestan que la escasez de habilidades de ciberseguridad inhibe su capacidad para mantener el ritmo del cambio.[23]

Los atacantes conocen bien estos problemas y los utilizan como ventaja.

4. Mantenerse por delante del aumento de los requerimientos normativos

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea (UE) y la Ley de Privacidad del Consumidor de California (CCPA) son dos de los reglamentos de protección de datos más conocidos. Sin embargo, están lejos de ser los únicos. Actualmente, todos los estados de EE. UU. tienen una ley de notificación de violación de datos y muchos de ellos están promulgando protecciones adicionales de privacidad del consumidor. Con el impulso de la presión política y social, se espera que las regulaciones se expandan en los próximos años y que las sanciones por incumplimiento se vuelvan más grandes, más punitivas y más comunes.

Las organizaciones también deben cumplir con los estándares de la industria y muchas se esfuerzan por hacerlo. Por ejemplo, menos del 37 % de las organizaciones aprueban su auditoría de cumplimiento del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).[24] Dado que el Marco de Seguridad de Software PCI (PCI SSF) reemplaza el PCI DSS, es probable que estas organizaciones se enfrenten a más obstáculos para continuar con su cumplimiento.

La necesidad de alcanzar y mantener el cumplimiento normativo tiene un impacto significativo en la capacidad de una organización para lograr los objetivos de transformación de la seguridad y además informa cómo invierten las organizaciones en soluciones tecnológicas. Por ejemplo, del 71 % de las organizaciones que han movido las aplicaciones basadas en la nube de regreso a centros de datos locales, el 21 % lo hizo para mantener el cumplimiento normativo.[25]

El Fortinet Security Fabric

El Fortinet Security Fabric aborda los cuatro desafíos de seguridad mencionados con anterioridad ya que ofrece amplia visibilidad y control de toda la superficie de ataque digital de una organización para minimizar el riesgo. El Security Fabric es una solución integrada que reduce la complejidad que se crea al admitir múltiples productos puntuales y automatizar el flujo de trabajo para aumentar la velocidad de operación, todo mientras las operaciones de la empresa siguen siendo productivas y resilientes.

Con el Fortinet Security Fabric, los equipos pueden obtener:

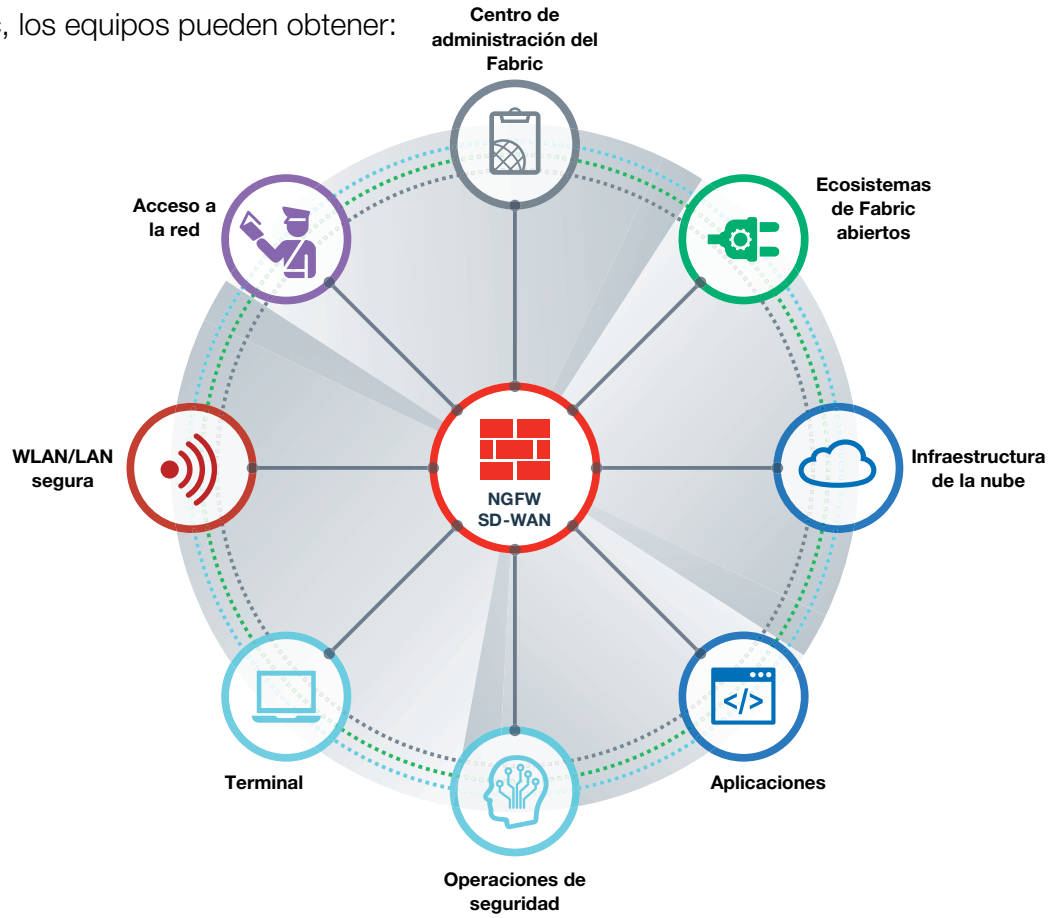

Figura 1: El Fortinet Security Fabric permite que múltiples tecnologías de seguridad trabajen juntas sin problema, en todos los entornos y con el respaldo de una única fuente de inteligencia de amenazas en una sola consola. Esto elimina las brechas de seguridad en la red y acelera las respuestas a ataques e infracciones.

Casi la mitad de los CISOs señalan que la integración de seguridad y la mejora de la analítica son una prioridad importante para su estrategia de tecnología de ciberseguridad.[26]

Visibilidad amplia y profunda de la superficie de ataque

Con la diversidad más amplia de soluciones basadas en seguridad de red de alto rendimiento para centros de datos, sucursales y pequeñas empresas y todos los principales proveedores de la nube, el Fortinet Security Fabric se adapta para proteger cada segmento de la red. Todos los componentes se configuran, administran y monitorean desde un único sistema de administración centralizado. Además de eliminar los silos asociados con las infraestructuras de seguridad de productos puntuales, la interfaz única para todos los componentes de seguridad reduce la carga de tener que entrenar al escaso personal. El sistema de administración también facilita la implementación sin intervención de componentes remotos, ahorrando en el envío de técnicos y reduciendo aún más los costos operativos.

Una arquitectura de seguridad verdaderamente integrada

Con todos los componentes controlados por el mismo sistema operativo de red FortiOS, el Fortinet Security Fabric permite una configuración uniforme y una administración de políticas y comunicación en tiempo real sin esfuerzo a través de la infraestructura de seguridad. Esto minimiza los tiempos de detección y mitigación de amenazas, reduce los riesgos de seguridad resultantes de los errores de configuración y de la compilación manual de datos y facilita una respuesta de auditoría de cumplimiento precisa y oportuna. Además de integrar los productos y soluciones de Fortinet, el Security Fabric incluye conexiones de interfaz de programación de aplicaciones (APIs) previamente desarrolladas para más de 70 socios Fabric-Ready que garantizan la integración profunda en todos los elementos del Security Fabric.

Los NGFW de FortiGate ofrecen la relación precio-rendimiento más alta en evaluaciones de terceros mientras analizan el tráfico cifrado. Alcanzan un rendimiento SSL de 5.7 Gbps mientras bloquean el 100 % de las evasiones.[27]

Reducir el tiempo de detección y respuesta a violaciones puede generar una reducción del 25 % en los costos generales de una violación a los datos.[28]

Respuesta y operaciones automatizadas

Además de una integración perfecta, el Fortinet Security Fabric lidera la industria en la aplicación de tecnologías de aprendizaje automático (ML) para mantenerse actualizado con el panorama de ciberamenazas en rápida evolución. El Fortinet Security Fabric incluye funcionalidad avanzada de orquestación, automatización y respuesta de seguridad (SOAR), así como la detección proactiva de amenazas, correlación de amenazas, alertas de intercambio de inteligencia e investigación y análisis de amenazas.

Para las operaciones de red, el Security Fabric ofrece flujos de trabajo y operaciones automatizados para ayudar a reducir las complejidades en toda la organización y en las implementaciones, independientemente de si son locales, en la nube o en las sucursales.

Gestione los riesgos y busque las oportunidades

La DI permite a las organizaciones alcanzar nuevos niveles de eficiencia y ahorro para sí mismas y mejores experiencias para sus clientes. Sin embargo, las iniciativas de DI también expanden y cambian la superficie de ataque de las organizaciones, abriendo nuevos vectores de ataque para que las ciberamenazas aprovechen las vulnerabilidades de seguridad.

Para las organizaciones que lideran la carga en la DI, es de primordial importancia reconocer, aceptar y gestionar adecuadamente los riesgos. El Fortinet Security Fabric es la base para esto. Unifica las soluciones de seguridad detrás de un único panel de control, hace visible la creciente superficie de ataque digital, integra la prevención de violaciones basada en la inteligencia artificial y automatiza las operaciones, la orquestación y la respuesta. En resumen, permite a las organizaciones crear un nuevo valor con DI sin comprometer la seguridad para la agilidad, el rendimiento y la simplicidad del negocio.

[1] Nick Lansing, "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources", Forbes y Fortinet, 2019.

[2] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 de mayo de 2019.

[3] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments", IHS Markit, 2019.

[4] Ibid.

[5] Gilad David Maayan, "The IoT Rundown For 2020: Stats, Risks, and Solutions", Security Today, 13 de enero de 2020.

[6] "Rightscale 2019 State of the Cloud Report", Flexera, 2019.

[7] Larry Ponemon, "Third-party IoT risk: companies don't know what they don't know", ponemonsullivanreport.com, consultado el 4 de febrero de 2020.

[8] Nirav Shah, "SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019", Fortinet, 9 de septiembre de 2019.

[9] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security y Ponemon Institute, 2019.

[10] "2019 Cost of a Data Breach Report", IBM Security y Ponemon Institute, 2019.

[11] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 de mayo de 2019.

[12] Según datos internos de FortiGuard Labs.

[13] "6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders", Fortinet, 8 de septiembre de 2019.

[14] Según datos internos de FortiGuard Labs.

[15] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security y Ponemon Institute, 2019.

[16] "2019 Cost of a Data Breach Report", IBM Security y Ponemon Institute, 2019.

[17] Basado en la investigación interna de Fortinet.

[18] Según datos de la investigación interna de Fortinet.

[19] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 de mayo de 2019.

[20] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating", CSO, 14 de marzo de 2016.

[21] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges", Fortinet, 23 de mayo de 2019.

[22] "Strategies for Building and Growing Strong Cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study, 2019", $(ISC)^2$, 2019.

[23] "CIO Survey 2019: A Changing Perspective", Harvey Nash and KPMG, 2019.

[24] "2019 Payment Security Report", Verizon, 2019.

[25] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments", IHS Markit, 2019.

[26] "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources", Forbes y Fortinet, 2019.

[27] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests", Fortinet, Enero de 2020.

[28] "2019 Cost of a Data Breach Report", IBM Security y Ponemon Institute, 2019.

www.fortinet.com

664959-0-0-MX

agosto 14, 2020 9:21 a. m.

ebook-considerations-security-architect