Administración de registro y seguridad basada en el análisis de Fortinet

FortiAnalyzer mide los riesgos, simplifica el cumplimiento y automatiza las respuestas

Contenido

FORTINET

Resumen ejecutivo

La rápida adopción empresarial de innovaciones digitales como los servicios en la nube y una mayor movilidad han provocado que la superficie de ataque de la red se expanda y aumente la complejidad de la infraestructura. Adicionalmente de estas vulnerabilidades, las amenazas avanzadas continúan creciendo tanto en número como en sofisticación. Como parte del Fortinet Security Fabric, FortiAnalyzer proporciona funciones de seguridad basadas en el análisis, así como capacidades de administración de registro para reducir riesgos y mejorar la postura de seguridad general de la organización.

El costo promedio de una violación a la seguridad de los datos (USD 3.92 millones) se incrementa por la complejidad del sistema (más de USD 290,000). Utilizar el uso compartido de inteligencia frente a amenazas (menos de USD 240,000) y el análisis de seguridad (menos de USD 200,000) disminuyen ese costo.[1]

Resolución de vulnerabilidad con visibilidad

La superficie de ataque digital se está expandiendo a un ritmo cada vez más rápido, lo que dificulta la protección contra amenazas avanzadas. Casi el 80 % de las organizaciones introducen la innovación impulsada digitalmente más rápido que su capacidad de protegerla contra ciberataques.[2] Además, los desafíos de las infraestructuras complejas y fragmentadas continúan permitiendo un aumento en los cibereventos y las violaciones de datos. El número de violaciones a la seguridad de los datos confirmadas ha aumentado en un 67 % en los últimos 5 años.[3]

Los distintos productos de seguridad de punto que se utilizan en algunas empresas generalmente operan en silos aislados. Esto impide que los equipos de operaciones de red tengan una visión clara y consistente de lo que sucede en toda la organización.

Los errores humanos y las fallas del sistema son la causa raíz de casi la mitad (49 %) de todas las violaciones de datos.[4]

Una arquitectura de seguridad integrada con análisis en tiempo real de toda la organización puede abordar esta falta de visibilidad. Como parte del Fortinet Security Fabric, FortiAnalyzer admite casos de uso basados en el análisis para proporcionar una mejor detección contra violaciones a la seguridad. Estos casos de uso incluyen:

- Medición del riesgo
- Simplificación de informes de cumplimiento
- Automatización de respuesta

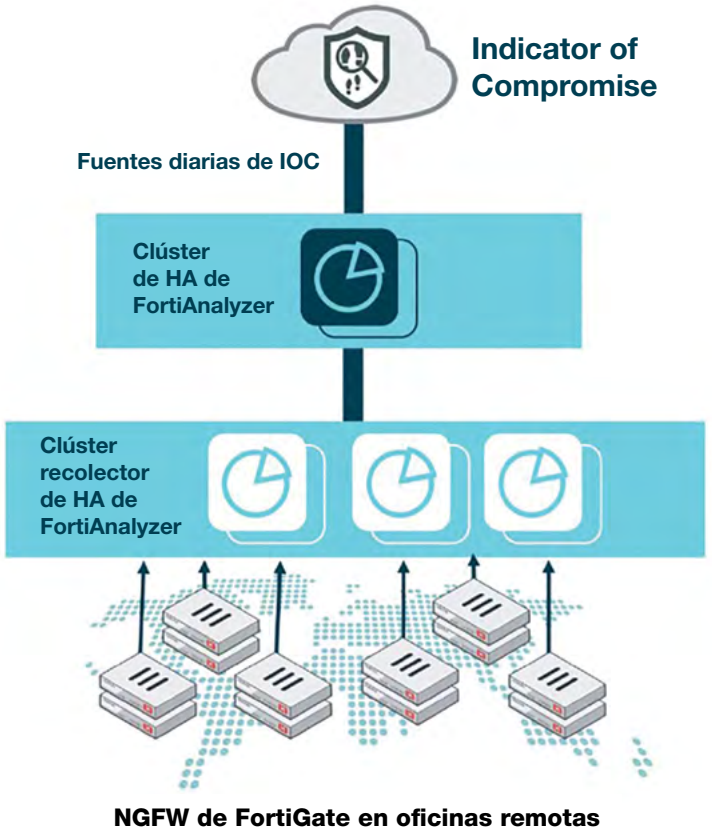

Figura 1: Appliances de administración de registro y seguridad basados en el análisis.

La empresa promedio implementa 47 soluciones y tecnologías de seguridad diferentes, muchas de las cuales solo abordan un solo vector de ataque o requerimiento de cumplimiento.[5]

Medición del riesgo

Los ataques contra empresas son cada vez más sofisticados y más difíciles de detectar. Para empeorar las cosas, la práctica generalizada de implementar productos de seguridad dispares y desconectados inhibe el intercambio de inteligencia frente a amenazas. Esto significa que las defensas de la red no pueden detectar ni coordinar rápidamente respuestas oportunas frente amenazas multivectoriales o polimórficas en las infraestructuras de red cada vez más dispersas.

Los líderes de ingeniería y operaciones de redes deben combatir las amenazas avanzadas mediante la identificación de riesgos de redes y seguridad en tiempo real. De esta manera, Fortinet ayuda a las organizaciones a reducir el tiempo de detección de amenazas. Al respecto, FortiAnalyzer ofrece administración de registro y seguridad basada en análisis para obtener una visibilidad completa de las anomalías en la expandida empresa digital, lo que permite a los equipos monitorear el movimiento de datos e identificar actividades anómalas. FortiAnalyzer también funciona bien con las implementaciones de las operaciones de seguridad (SecOps) existentes, lo que permite a los equipos de seguridad administrar informes de registro y alertas, además de otras tareas de manera más eficiente.

Tres formas en que FortiAnalyzer mide los riesgos

Visibilidad

- Ofrece informes y paneles avanzados para operaciones y seguridad
- Proporciona herramientas para permitir la programación de informes

Indicadores de Compromiso (IOC)

- Hace referencia a 4.4 millones de sensores en todo el mundo, así como asociaciones con más de 200 organizaciones.
- Los investigadores de FortiGuard Labs utilizan tecnologías como el aprendizaje automático (ML) para detectar anomalías y permitir la identificación de IOC de clase empresarial

Correlación avanzada del Security Fabric

- Compara todos los eventos asociados con un incidente en las soluciones integradas del Security Fabric

Actualmente toma un promedio de 279 días identificar y contener una sola violación a la seguridad.[6]

Simplificación de informes de cumplimiento

La administración del cumplimiento suele ser un proceso muy manual. A menudo involucra múltiple personal de tiempo completo y puede requerir meses de trabajo realizarlo correctamente. Los datos se deben agregar a partir de varios productos de seguridad de punto y luego normalizarse para garantizar que los controles reglamentarios se informen con precisión. Para hacer esto, el personal de redes y seguridad debe monitorear los controles de seguridad mediante herramientas de auditoría distintas para cada proveedor y luego correlacionar esa información para demostrar el cumplimiento. Este complejo y difícil proceso de auditoría es ineficiente y, a menudo, ineficaz.

FortiAnalyzer automatiza el seguimiento del cumplimiento y los informes de las regulaciones de la industria y los estándares de seguridad para tener una mayor eficiencia del flujo de trabajo en el Security Fabric. Esta integración se encuentra en la capa de operaciones de red, lo que proporciona a los equipos de ingeniería y operaciones de red transparencia de inteligencia frente a amenazas. Además, FortiAnalyzer proporciona de forma nativa la capacidad de evaluar el entorno de la red contra las mejores prácticas, midiendo así los riesgos de cumplimiento. Los equipos de operaciones de la red posteriormente aplican y ejecutan controles en la red para protegerse contra las ciberamenazas. FortiAnalyzer ofrece un análisis exhaustivo de las operaciones de red para determinar el alcance del riesgo en la superficie de ataque y luego identifica dónde se requiere una respuesta inmediata.

Tres formas en que FortiAnalyzer simplifica el cumplimiento

Fácil demostración del cumplimiento

- Proporciona informes en tiempo real sobre los estándares de la industria, como el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)
- Es compatible con estándares de seguridad como el del Instituto Nacional de Estándares y Tecnología (NIST) y Centro de Seguridad de Internet (CIS)

Visibilidad basada en funciones

- Permite procesos de aprobación del flujo de trabajo para ofrecer recomendaciones de políticas y configuración entre los equipos de seguridad y de red para una implementación colaborativa
- Ofrece paneles específicos para las principales partes implicadas en la empresa (por ejemplo, CIO, CISO, arquitecto de red, arquitecto de seguridad)

Integraciones de la empresa

- Programa y comparte informes por correo electrónico, webhooks, etc.
- Interoperable con las soluciones existentes de Administración de eventos e información de seguridad (SIEM) y otras herramientas

66 %

de los profesionales de seguridad indican que los mandatos de cumplimiento son un factor determinante del gasto en seguridad.[7]

Automatización de respuestas

Con un estimado de 4.07 millones de puestos de ciberseguridad sin cubrir en todo el mundo, casi dos tercios (65 %) de las empresas actualmente carecen del personal calificado que necesitan para mantener operaciones de seguridad efectivas.[8] Como resultado, la mayoría de las empresas no tienen los recursos para contratar personal para la detección y respuesta de amenazas avanzadas. Esto intensifica los problemas de complejidad de seguridad y falta de visibilidad. Esto, a su vez, ralentiza significativamente el proceso de detección y corrección de un evento de violación a la seguridad. El año pasado, las violaciones con un ciclo de vida de menos de 200 días fueron en promedio USD 1.22 millones menos costosas que las violaciones a la seguridad con un ciclo de vida de más de 200 días (USD 3.34 millones frente a USD 4.56 millones respectivamente), una diferencia del 37 %[9]

FortiAnalyzer ayuda a disminuir el tiempo de corrección de amenazas de meses a minutos mediante la coordinación de acciones de respuesta automatizadas basadas en políticas en toda la arquitectura integrada del Security Fabric. Los incidentes detectados, combinados con pruebas y análisis detallados, permiten a los especialistas en redes y seguridad automatizar y orquestar las respuestas de seguridad. Los eventos también pueden desencadenar cambios automáticos en las configuraciones del dispositivo para cerrar el ciclo de mitigación de ataques. Las capacidades de administración de registro en FortiAnalyzer reducen aún más la carga del flujo de trabajo sobre un personal humano limitado, lo que permite a los equipos enfocarse en decisiones críticas de seguridad.

Solo el 38 % de las organizaciones utilizan la automatización, la inteligencia artificial y el aprendizaje automático, lo que representa una oportunidad perdida para muchos.[10]

Tres formas en que FortiAnalyzer mejora la detección y respuesta a las amenazas

Adopción del Centro de Operaciones de Seguridad (SOC)

- Proporciona controladores de eventos programables para la corrección personalizada de los riesgos
- Incluye paneles, informes del SOC y una vista cronológica del incidente para una mejor investigación de los incidentes

Integraciones

- Los conectores del Fabric de Fortinet proporcionan integración con herramientas externas como la SIEM, Administración de servicios de tecnología de la información (ITSM) y muchas otras

Flujo de trabajo y orquestación

- Permite respuestas rápidas o automatizadas dentro de la interfaz nativa
- Proporciona interoperabilidad con las herramientas de análisis y administración existentes

Reducción de la exposición mientras mejora la protección

Como parte del Fortinet Security Fabric, FortiAnalyzer reduce el riesgo a través de análisis e información en tiempo real, admite informes de cumplimiento optimizados y permite respuestas de seguridad automatizadas en entornos locales, en la nube e híbridos.

Las capacidades de administración de registro y seguridad basadas en el análisis en FortiAnalyzer ayudan a los líderes de ingeniería y operaciones de redes a detectar rápidamente las ciberviolaciones. Al reducir las ventanas de detección y corrección, las organizaciones pueden controlar rápidamente la exposición de datos confidenciales, prevenir interrupciones operativas y reducir drásticamente los costos de corrección.

[1] "2019 Cost of a Data Breach Report", Ponemon Institute and IBM Security, julio de 2019.

[2] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security and Ponemon Institute, 6 de marzo de 2019.

[3] Ibid.

[4] Ibid.

[5] "53 % of enterprises have no idea if their security tools are working", Help Net Security, 31 de julio de 2019.

[6] "2019 Cost of a Data Breach Report", Ponemon Institute and IBM Security, julio de 2019.

[7] Michael Nadeau, "Compliance mandates, cybersecurity best practices dominate 2019 security priorities", CSO, 23 de octubre de 2019.

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

[9] "2019 Cost of a Data Breach Report", Ponemon Institute and IBM Security, julio de 2019.

[10] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study", Accenture Security and Ponemon Institute, 6 de marzo de 2019.

www.fortinet.com

589703-A-0-ES

julio 23, 2020 2:05 p.m.

eb-fortianalyzer_es-MX