RESUMEN DE LA SOLUCIÓN

Simplificación de las operaciones de seguridad con FortiAnalyzer

Resumen ejecutivo

Los equipos de seguridad de todo el mundo luchan con la creciente complejidad de las operaciones de seguridad. A medida que las redes se expanden y evolucionan, y las ciberamenazas se vuelven más sofisticadas, los equipos de seguridad tienen el desafío de mantener el ritmo.

FortiAnalyzer, combinado con el Fortinet Security Fabric, proporciona una solución. FortiAnalyzer ofrece capacidades avanzadas de registro y generación de informes, análisis de seguridad centralizado a través del Fortinet Security Fabric y automatización de seguridad a través de los conectores del Fabric e Interfaces de programación de aplicaciones (API). Estos casos de uso permiten a los equipos de seguridad aumentar la eficiencia, reducir el riesgo y mejorar el costo total de propiedad (CTP).

FortiAnalyzer simplifica las operaciones basadas en la madurez del SOC, que incluyen:

- Registro y generación de informes avanzados
- Análisis del Security Fabric
- Automatización del Security Fabric

Security Fabric para simplificar la complejidad de las operaciones de seguridad

Los equipos de seguridad de todo el mundo luchan con la complejidad de las operaciones. Los problemas comunes incluyen:

- Demasiadas consolas
- Demasiada alertas
- Respuesta manual y lenta
- Escasez de personal de ciberseguridad

Fortinet Security Fabric ofrece una solución a estos desafíos de seguridad. La amplia visibilidad y control de toda la superficie de ataque digital de una organización minimiza el riesgo. Una solución integrada que reduce la complejidad de soportar múltiples productos de punto. La automatización de los flujos de trabajo de seguridad aumenta la velocidad de operación. Todas estas características permiten a una organización maximizar el impacto y la eficacia de un equipo de seguridad optimizado.

FortiAnalyzer, es una parte fundamental del Security Fabric, permite a los equipos simplificar las operaciones de seguridad, permitiendo a las empresas en cualquier etapa de la madurez del Centro de operaciones de seguridad (SOC) integrar sin problemas la visibilidad y la automatización de la seguridad.

Registro y generación de informes avanzados

Cualquier organización, ya sea que haya implementado solo unos pocos FortiGates o cientos de estos, necesita registrar actividad de la red y generar informes. El Fortinet Security Fabric permite a los clientes darse cuenta de la importancia de consolidar los proveedores para casos de uso comunes, como el Next-Generation Firewall (NGFW), redes de área amplia definidas por software (SD-WAN), sistemas de prevención de intrusiones (IPS) y otros. FortiAnalyzer proporciona una solución unificada de registro e informes para todos estos proyectos en toda la empresa.

Las organizaciones también requieren informes y herramientas personalizables que ayuden a demostrar el cumplimiento a los auditores. La admisión de informes de cumplimiento de Fortinet a través de FortiAnalyzer incluye informes predefinidos para estándares como el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS), Informe de actividad sospechosa (SAR), Centro de seguridad de Internet (CIS) e Instituto nacional de estándares y tecnología (NIST). FortiAnalyzer también proporciona registro de auditoría y Control de acceso basado en funciones (RBAC) para garantizar que los empleados solo puedan acceder a la información que necesitan para realizar sus tareas.

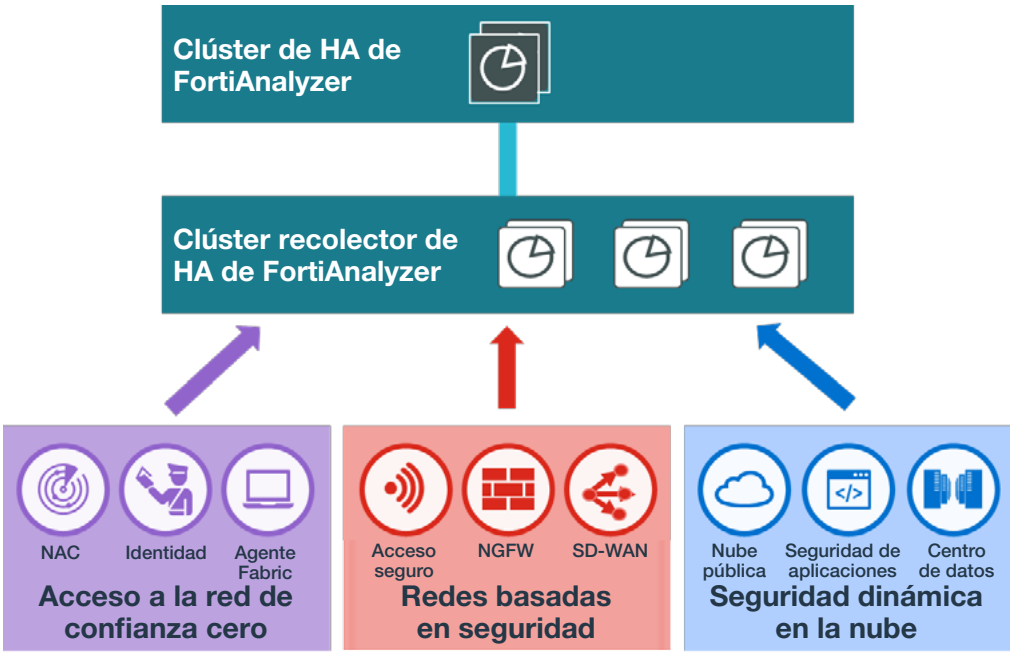

Figura 1: FortiAnalyzer proporciona agregación de registros e informes avanzados.

Análisis del Security Fabric

FortiAnalyzer permite a las organizaciones aprovechar la inteligencia frente a amenazas de FortiGuard Labs para identificar anomalías en su red, en tiempo real. FortiAnalyzer utiliza un motor de análisis integrado para correlacionar los datos de amenazas que se recopilan en el Security Fabric. La calificación de riesgos se utiliza para priorizar las anomalías que se identifican y compartir esta inteligencia frente a amenazas en el Security Fabric.

El motor de análisis de Security Fabric también potencia la visualización del Security Fabric en tiempo real. Estas visualizaciones permiten a los miembros de los equipos de TI, seguridad y SOC identificar e investigar posibles amenazas para la red de inmediato.

FortiAnalyzer viene con paneles e informes integrados fácilmente personalizables. En FortiAnalyzer se incluyen más de 720 conjuntos de datos que permiten una inducción fácil a los informes y paneles. Estos incluyen consultas avanzadas que se optimizan para obtener tiempos de respuesta rápidos en tiempo real.

Figura 2: FortiAnalyzer proporciona información de red específica en tiempo real.

Automatización del Security Fabric

FortiAnalyzer incluye automatización integrada a través del módulo FortiSOC. Este módulo viene con manuales de estrategias y conectores para el Security Fabric, lo que permite a los equipos de seguridad aprovechar la automatización de la seguridad en de todo el modelo de madurez del SOC.

La automatización puede originarse en FortiOS a través de puntos de automatización, que aprovechan FortiAnalyzer como un motor de correlación avanzado. Este proceso define controladores de eventos detallados y se conecta a la tecnología IF-THIS-THEN-THIS de FortiOS para optimizar los tiempos de respuesta. La automatización también se puede activar a través de FortiAnalyzer, que proporciona integración con soluciones de terceros, como la Administración de servicios de TI (ITSM), la Administración de eventos e información de seguridad (SIEM) y el webhook o mediante el Security Fabric utilizando conectores nativos.

FortiAnalyzer y el Fortinet Security Fabric ofrecen:

- Aumento de eficiencia
- Reducción de riesgo
- CTP mejorado

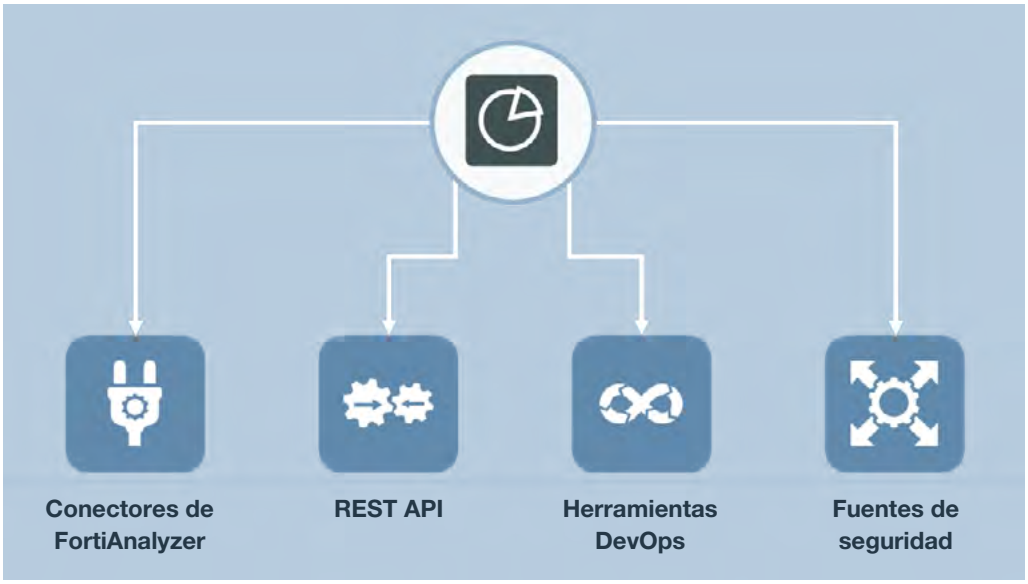

Figura 3: FortiAnalyzer permite la automatización centralizada de la infraestructura de seguridad a través del Security Fabric.

Producción de ROI, simplicidad y seguridad

La combinación del Fortinet Security Fabric y FortiAnalyzer ofrece capacidades de seguridad de clase empresarial con beneficios líderes en la industria, que incluyen:

Aumento de eficiencia. Fortinet instituye una infraestructura simplificada que reduce la complejidad operativa en toda la organización. A medida que las empresas avanzan a través del Modelo de madurez del SOC, siempre necesitarán una forma fácil y automatizada de responder a las anomalías que se descubren dentro de la red. FortiAnalyzer y FortiSOC (el módulo adicional en FortiAnalyzer) la habilitan con manuales de estrategias y conectores dentro del Security Fabric que mejoran la eficiencia de los equipos de TI y seguridad.

Reducción de riesgo. Las funciones de seguimiento e informes de Fortinet ayudan a las organizaciones a garantizar el cumplimiento de las leyes de privacidad, los estándares de seguridad y las regulaciones de la industria mientras reducen los riesgos asociados con multas y costos legales en caso de incumplimiento. FortiAnalyzer rastrea la actividad de las amenazas en tiempo real, facilita la evaluación de riesgos, detecta problemas potenciales y ayuda a mitigarlos.

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). Ambos, 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]

CTP mejorado. El Fortinet Security Fabric y la integración de casos de uso común, como NGFW y SD-WAN, en el NGFW de FortiGate mejoran el CTP al eliminar productos de punto. Además, con FortiAnalyzer, el cual se integra con otras ofertas de Fortinet a través de Security Fabric, las organizaciones pueden aprovechar el análisis y la automatización de seguridad sin requerir soluciones de terceros adicionales.

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

julio 22, 2020 5:06 p.m.

618026-0-0-ES

Z:_argostranslations\158\03_DTP\sb-simplifying-security-operations-with-fortianalyzer_es-MX\sb-simplifying-security-operations-with-fortianalyzer_es-MX