ManageEngine
EventLog Analyzer MSSP

¡Gestionar varios clientes ahora es más fácil!

Una solución web de gestión de logs para escalar su compañía de MSSP más allá de las fronteras.

Tabla de contenido

El reto: la necesidad cambiante de mejores MSSP

Ya que la complejidad de los ataques cibernéticos aumenta, más compañías se dan cuenta ahora de la importancia de tener un equipo, ya sea interno o externo, para gestionar las operaciones de seguridad y garantizar la continuidad corporativa. Como resultado, podemos evidenciar que muchos servicios y proveedores de consultoría de TI tradicionales están ingresando al mercado de MSSP, ya sea mediante adquisiciones o sociedades. Ya que el espacio de MSSP se está llenando, he aquí cinco funciones que los clientes esperan de su socio de MSSP:

1. Capacidad de escalar con el cliente

Con la creciente adopción de la nube, más organizaciones alrededor del mundo están creciendo rápidamente. Como un MSSP, usted debe ser capaz de respaldar la compañía de su cliente durante esta etapa. Sus clientes necesitan que usted esté ahí para ellos y que implemente proactivamente las herramientas de seguridad que respalden su crecimiento anticipado.

No obstante, escalar no significa que siempre se va hacia arriba. Ya que el número de clientes que usted respalda varía, necesita herramientas de seguridad que puedan permitirle fácilmente aumentar o disminuir. Es mejor desarrollar un plan estratégico para la escalabilidad antes de que se genere el problema. Esto le permite adaptarse dinámicamente a los riesgos y escalar para proteger miles de dispositivos de sus clientes a la vez.

2. Capacidad de compartir inteligencia de fuentes contra amenazas

Una forma de mitigar los riesgos en este panorama de amenazas cambiante es tener una inteligencia compartida sobre las últimas amenazas. Esto se puede lograr utilizando fuentes contra amenazas STIX/TAXII para obtener inteligencia en tiempo real sobre URL, IP, archivos y más elementos maliciosos. La inteligencia de amenazas le permite detener intentos de ataques prontamente, así como evaluar alertas de seguridad y reducir falsos positivos.

Una ventaja significativa es que usted puede aprovechar la inteligencia de amenazas adquirida de un cliente para verificar patrones similares en entornos de otros clientes. Esto proporciona una ventaja competitiva sobre otros proveedores de servicios de seguridad que no ofrecen dicho servicio. Una herramienta de seguridad que pueda integrarse con fuentes contra amenazas de código abierto y comerciales puede ahorrar el tiempo que se invierte en prácticas preliminares de cacería de amenazas.

3. Capacidad de responder rápidamente ante incidentes de seguridad

Muchas empresas están optando por MSSP para detectar proactivamente y responder ante incidentes de seguridad a diario. Para combatir las amenazas cambiantes y los incidentes complejos, necesita ser capaz de coordinar con sus clientes durante las actividades de respuesta ante incidentes.

Cada minuto de inactividad durante un incidente le da al hacker una ventaja para infligir daño. Una vez se identifica la amenaza, los MSSP necesitan escalar el evento a la organización y desarrollar contramedidas. Integrarse con los procesos del cliente y automatizar alertas y medidas de respuesta puede reducir los falsos positivos durante un ataque a gran escala.

4. Capacidad de dar una gran experiencia de compatibilidad

La seguridad informática se ha vuelto uno de los más altos costos para las organizaciones, atizados por la latente crisis de la industria. Adquirir el mejor talento y desarrollar un robusto equipo interno se está volviendo cada vez más difícil. Ahí es donde entran los MSSP.

Las compañías se convierten en proveedores de servicios de seguridad por la experiencia en seguridad y el respaldo 24x7x365 que pueden dar. Se espera que los MSSP también tengan:

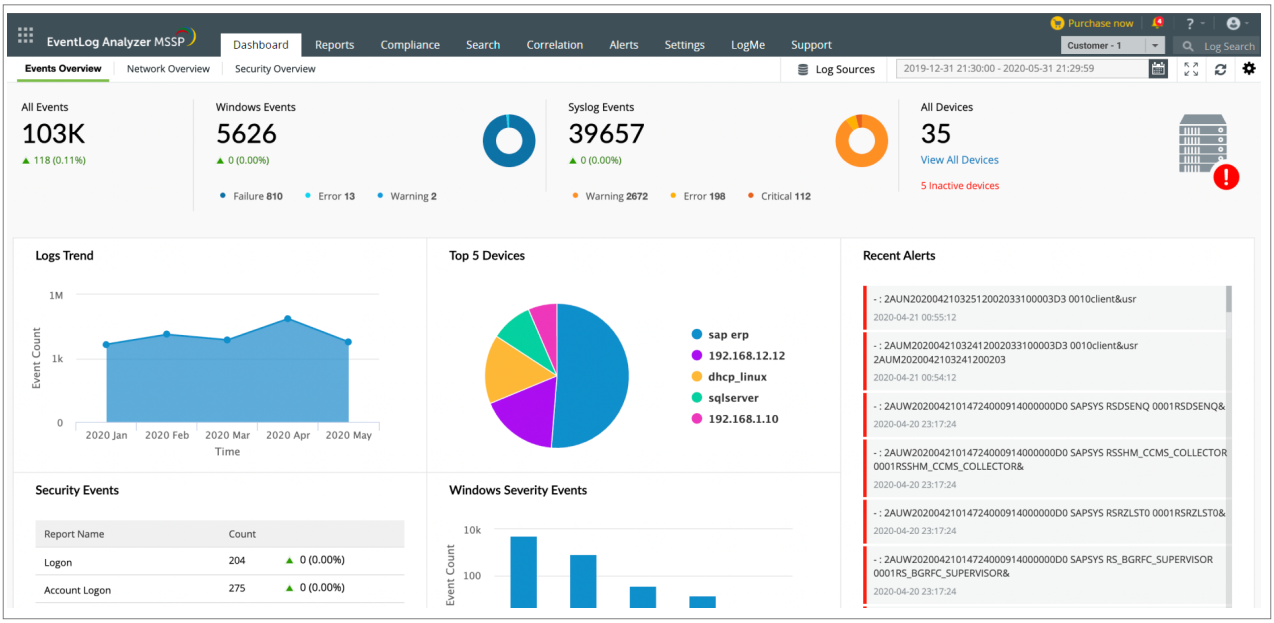
- Personal de seguridad capacitado y certificado que pueda proporcionar planes de respuesta y hojas de ruta de seguridad personalizados con base en las necesidades únicas del cliente
- Técnicos de TI locales que puedan llegar al lugar para resolver problemas
- Una buena relación con proveedores de software, de forma que las herramientas se puedan personalizar para resolver rápidamente problemas de seguridad

5. Capacidad de demostrar una sólida infraestructura de seguridad interna

Ya que más organizaciones comienzan a depender de MSSP para controlar sus operaciones de seguridad, puede que necesite fortalecer también su seguridad interna. Esto es esencial, ya que los MSSP se están volviendo el objetivo primario de los ataques de ransomware, y los hackers se esfuerzan por encontrar una vulnerabilidad que puedan explotar y usar para obtener acceso a la red de su cliente.

Implementar mejores prácticas de seguridad protegerá sus datos y los de su cliente. Esto incluye restringir el acceso determinando qué analistas de SOC pueden ver qué datos del cliente, almacenar de manera segura todos los datos de sus clientes, satisfacer las regulaciones de cumplimiento sobre privacidad y seguridad de su cliente e implementar la autenticación multi factor.

Solución: una herramienta centralizada para la gestión de logs multi cliente



Ya que las expectativas sobre los servicios de seguridad de las organizaciones crecen, los MSSP también necesitan fortalecer su arsenal de seguridad con las mejores herramientas con el fin de ayudar a satisfacer las necesidades de sus clientes. Esta es la razón por la que ManageEngine EventLog Analyzer MSSP es una solución obligatoria en su estrategia de seguridad.

EventLog Analyzer MSSP es la plataforma ideal para que los proveedores de servicios de seguridad suministren la visibilidad de lo que está sucediendo en el entorno de cada cliente. La solución es especialmente útil para monitorear grandes redes de clientes con miles de fuentes de logs esparcidas en varias regiones. Sigue una arquitectura distribuida con varios servidores gestionados, controlados por un solo servidor administrador central.

Usted puede usar la herramienta para obtener información de eventos de seguridad detectados y defenderse ante posibles ataques utilizando sofisticadas técnicas de respuesta ante amenazas. La integración con Webroot BrightCloud® Threat Intelligence Services da fuentes contra amenazas en tiempo real y exactas sobre URL, IP, archivos y más elementos maliciosos. Con esta solución usted puede monitorear el tráfico saliente y enviar alertas en tiempo real cuando se dé cualquier comunicación con IP maliciosas o en listas de bloqueo.

Ventajas de EventLog Analyzer

Recopilación integral de logs

Descubra automáticamente fuentes de logs y añádalas para su monitoreo. Utilice la recopilación centralizada y segura de logs con métodos con o sin agentes.

Correlación de logs de eventos en tiempo real

Descubra incidentes de seguridad al correlacionar eventos a lo largo de su red. Incluya más de 30 reglas de correlación predefinidas y un generador de reglas personalizadas de correlación.

Almacenamiento seguro de logs

Retenga los datos de logs de la red tanto como lo necesite. Los archivos están protegidos utilizando un fechado y técnicas de hashing.

Análisis forense de logs eficiente

Realice búsquedas de logs de alta velocidad utilizando opciones flexibles de búsqueda. Descubra la causa raíz de los ataques y realice investigaciones forenses.

Gestión de incidentes optimizada

Use el sistema de tickets integrado para asignar incidentes como tickets, supervisar su estado y acelere el proceso de resolución de incidentes.

Implementación de EventLog Analyzer MSSP: reglas prácticas sencillas

EventLog Analyzer MSSP es una aplicación on premise que se debe instalar en los servidores de su cliente. Sin embargo, cuando necesite monitorear infraestructuras en la nube, puede usar agentes para tomar los datos de logs necesarios para su análisis.

Algunos modelos de MSSP involucran tomar datos de clientes de su fuente para almacenarlos y procesarlos en el entorno del MSSP.

Mientras que esto puede garantizar que tienen el control de todos los datos, supone muchos riesgos cuando enfrentan un ataque, lo que facilita a los atacantes obtener acceso a los datos de varios clientes. Para minimizar el riesgo, EventLog Analyzer MSSP permite gestionar los datos de forma discreta al almacenarlos en entornos separados de clientes, mientras que da a los SOC la visibilidad de toda la red.

¿Cómo se implementa EventLog Analyzer?

La edición MSSP de EventLog Analyzer involucra la implementación de un servidor administrador y varios servidores gestionados. Los servidores gestionados se pueden instalar en las ubicaciones de distintos clientes (uno por entorno LAN) y conectarse al servidor administrador central.

Servidor gestionado

El servidor gestionado es la instalación de EventLog Analyzer que recopila logs de fuentes presentes en la ubicación de su cliente. Esta información se transmite al único servidor administrador central.

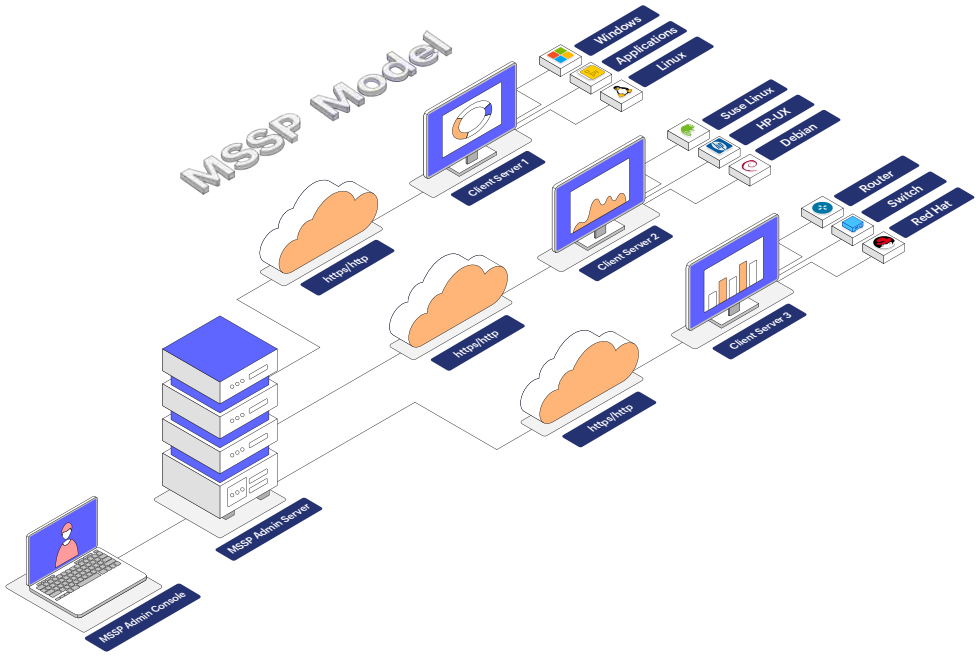
Servidor administrador

El servidor administrador es la instalación de EventLog Analyzer que agrega información de todos los servidores gestionados instalados alrededor del mundo. El servidor administrador actúa como una consola única central y muestra informes, alertas y otra información de logs de todos los servidores gestionados.

Los MSSP necesitan instalar las versiones premium de EventLog Analyzer en su propio entorno y en el de los clientes. Una vez se establecen las alertas, las medidas de respuesta ante incidentes y las funciones de inteligencia de amenazas en las instancias de cada cliente, serán capaces de obtener una visibilidad completa de la consola centralizada del servidor administrador.

Nota:

Un solo servidor administrador está diseñado para gestionar hasta 50 servidores gestionados.



Cada nodo en el lado del cliente representa una implementación independiente completa con sus propias alertas, alta disponibilidad, respuesta ante incidentes y funciones de protección de datos. Los logs recopilados por el servidor gestionado se almacenan solo en la base de datos del servidor gestionado. No puede almacenar los logs en el servidor administrador. No obstante, usted puede redirigir los logs al servidor administrador para almacenarlos. Como MSSP, diseñar el software de esta forma cumplirá las siguientes metas por usted:

1. Garantizar que los datos del cliente estén protegidos al mantenerlos en sus respectivos entornos.
2. Personalizar el producto y las estrategias de seguridad específicamente para la industria de cada cliente o caso de uso.
3. Obtener una vista central de lo que está sucediendo en la red de cada cliente y responder ante amenazas inmediatamente.
4. Evitar problema de rendimiento al dar a cada cliente implementaciones separadamente sin afectar a los otros.
   Cada industria o compañía necesita seguir una legislación de cumplimiento específica.
5. Usted puede establecer alertas para el respectivo informe de cumplimiento y notificar a sus clientes cuando haya una violación.

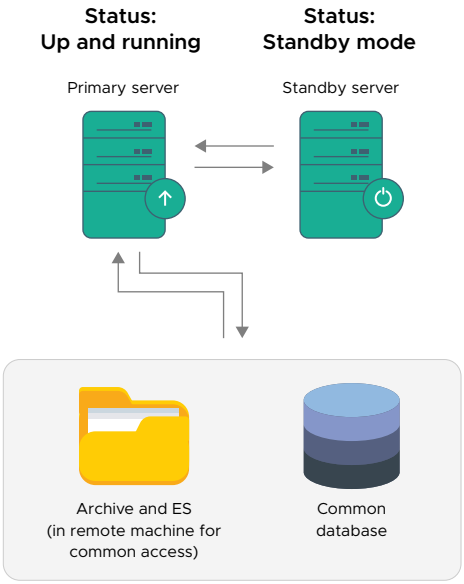
Arquitectura de alta disponibilidad y medidas para la recuperación ante desastres

El servidor de EventLog Analyzer MSSP es un componente crítico desde la perspectiva de la seguridad de la red en una organización. En el evento improbable de que ocurra un fallo importante en su entorno que cause que el servidor de EventLog Analyzer MSSP se apague, el procesamiento y análisis de logs se detendrá. Esta interrupción podría volverse la entrada a brechas de seguridad. Dichas brechas pueden causar no solo enormes pérdidas financieras y multas por incumplimiento, sino también la pérdida de la credibilidad y la reputación. Para evitar dichos desastres, EventLog Analyzer MSSP tiene un mecanismo de respaldo.

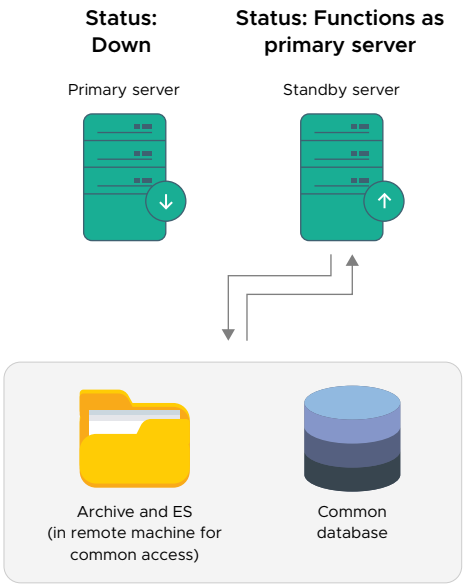
Como una medida de recuperación ante desastres, EventLog Analyzer MSSP ofrece una función de alta disponibilidad. Permite configurar cada servidor de EventLog Analyzer, administrador y gestionado, con un servidor esclavo. Este servidor esclavo monitorea continuamente el servidor primario. En el caso de que el servidor primario falle, el servidor esclavo toma el mando inmediatamente y empezará a realizar todas las funciones del primario sin retraso.

Cómo actúa la función de alta disponibilidad

El entorno de alta disponibilidad en EventLog Analyzer incluye dos instalaciones separadas. Una de ellas actúa como el servidor primario, mientras que la otra como el servidor esclavo. Ambas instalaciones apuntan a la misma base de datos. Y los datos de logs archivados y de Elasticsearch estarán disponibles en el recurso de red común.

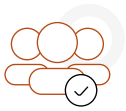


De forma predeterminada, el servidor primario prestará todos los servicios requeridos. El servidor esclavo también se iniciará, pero permanecerá en modo de reposo. Aunque permanecerá monitoreando continuamente el estado del servidor primario. Cuando el servidor primario falle, el servidor esclavo tomará el rol del servidor esclavo. Empezará a recopilar los logs para evitar cualquier pérdida de datos y continuar la realización de todas las funciones del servidor primario hasta que el servidor primario real vuelva a funcionar.



Otras funciones de seguridad de EventLog Analyzer MSSP

Proteger la comunicación web:
EventLog Analyzer MSSP es una solución web con un cliente web al que se puede acceder desde cualquier lugar de la red. Habilitar el protocolo HTTPS garantiza que toda la comunicación web está protegida.



Control de acceso basado en roles:
RBAC le permite compartimentalizar sus datos entre los técnicos del producto. Se dan tres niveles de acceso: administrador, operario e invitado, con el fin de limitar el acceso de los usuarios y controlar funciones específicas e información de dispositivos. De esta forma, puede garantizar que solo el personal autorizado accede a los datos-

Auditar las acciones de los técnicos de EventLog Analyzer:
La solución proporciona una opción integrada para generar la pista de auditoría de las acciones de todos los usuarios realizadas en el producto. Esto le permite garantizar la aprobación dentro de la solución misma.

Terminar la sesión después del tiempo de inactividad:
Usted puede establecer un tiempo de vencimiento de la sesión y si la sesión está inactiva por más de 30 minutos (que es el tiempo mínimo), la sesión se terminará. Los usuarios pueden cambiar el parámetro predeterminado de 30 minutos para el vencimiento de la sesión a 10 minutos.

Encriptación de archivos:
Los datos almacenados están protegidos utilizando el mecanismo de encriptación AES 256.

Detección de alteraciones en los datos almacenados:
EventLog Analyzer MSSP tiene una opción para detectar archivos de logs alterados. Cuando habilita la opción Integridad de archivos, la solución muestra el estado del archivo almacenado como Alterado si se ha manejado mal. Lo hace al utilizar técnicas de fechado.

La función para el monitoreo de la integridad de los archivos en EventLog Analyzer MSSP puede implementarse en los archivos de logs almacenados con el fin de obtener notificaciones instantáneas por cambios hechos a los datos de log almacenados.

Por qué debe tener EventLog Analyzer MSSP en el centro de sus servicios

ManageEngine EventLog Analyzer MSSP está comprometido con darle una solución fiable de gestión de logs para proveedores de servicios de seguridad alrededor del mundo. Con miles de clientes que confían en EventLog Analyzer para sus necesidades internas de seguridad, es la solución ideal para fortalecer su compañía.

Nuestra visión es facultar a cada organización con las herramientas correctas y así ayudarlas a obtener una visibilidad más detallada de los eventos de seguridad, acelerar la detección y respuesta ante amenazas y mejorar la postura de seguridad de su red.

Nuestra propuesta de valor

- Modelo de precio transparente para organizaciones de todos los tamaños —con base en el número de nodos y funciones de seguridad del add-on que escoja
- Experiencia excepcional de respaldo 24/7 y capacitación en el lugar y en línea para ayudarlo a hacer el mejor uso de la herramienta
- Compatibilidad con más de 750 fuentes de logs y un analizador de logs personalizados para satisfacer los requisitos de registro de sus clientes
- Funciones de mejora de la seguridad para fortalecer la seguridad interna de su organización —MFA, protección de transmisión de datos y más
- Análisis robusto de logs y funciones automatizada de respuesta ante incidentes para aprovechar por completo las inversiones en su fuerza laboral capacitada

Premios y testimonios

ManageEngine Log360 reconocido como ganador de la medalla de oro en los Premios a la excelencia en ciberseguridad 2022

ManageEngine reconocido como ganador en Gartner Peer Insights Customers' Choice 2021 para la categoría de SIEM

Reconocido en el Cuadrante Mágico de Gartner 2021 para SIEM por quinta vez

ManageEngine
EventLog Analyzer MSSP

EventLog Analyzer es una solución web para le gestión de logs y cumplimiento del TI en tiempo real que combate los ataques de seguridad de la red. También ofrece informes y alertas de cumplimiento out-of-the-box que ayudan a las organizaciones a satisfacer los estrictos requisitos de las normas regulatorias de TI con facilidad.

$ Cotizar Descargar