

Network Traffic Security Analytics

Detección en tiempo real de las brechas de seguridad y visibilidad total de las amenazas

Bitdefender Network Traffic Security Analytics es una solución de seguridad empresarial que detecta con precisión las brechas de seguridad y proporciona información sobre los ataques avanzados mediante el análisis del tráfico de red. Permite a las organizaciones detectar y combatir con rapidez las amenazas sofisticadas complementando la arquitectura de seguridad preexistente (red y endpoints) con una defensa especializada basada en la red.

Al utilizar el tráfico de red como fuente fiable de información, Bitdefender NTSA detecta inmediatamente las vulneraciones debido a que el comportamiento del endpoint cambia en cuanto se infecta. Esta detección es eficaz contra las amenazas persistentes (APTs) tanto genéricas como dirigidas, conocidas o nunca vistas. Se generarán alertas para informar al equipo de operaciones de seguridad respecto a los cambios en el comportamiento de los endpoints que indiquen que se está produciendo un ataque avanzado o que hay endpoints que se han visto comprometidos.

"Bitdefender Network Traffic Security Analytics otorga al departamento TI una visibilidad total y pone de manifiesto que en la red suceden cosas muy poco deseables"

Leading Automotive & Manufacturing Company

Líderes en inteligencia sobre ciberamenazas e inteligencia artificial

NTSA aprovecha la excelente inteligencia sobre ciberamenazas de Bitdefender, recopilada de 500 Millones de puntos terminales de todo el mundo, y la combina con el aprendizaje automático avanzado y la heurística para analizar los metadatos de la red en tiempo real y revelar así con precisión la actividad de las amenazas y los patrones de tráfico sospechosos. Gracias a los análisis de seguridad automáticos y a su enfoque en el tráfico de red saliente, reduce el ruido y proporciona alertas útiles para el equipo de operaciones de seguridad.

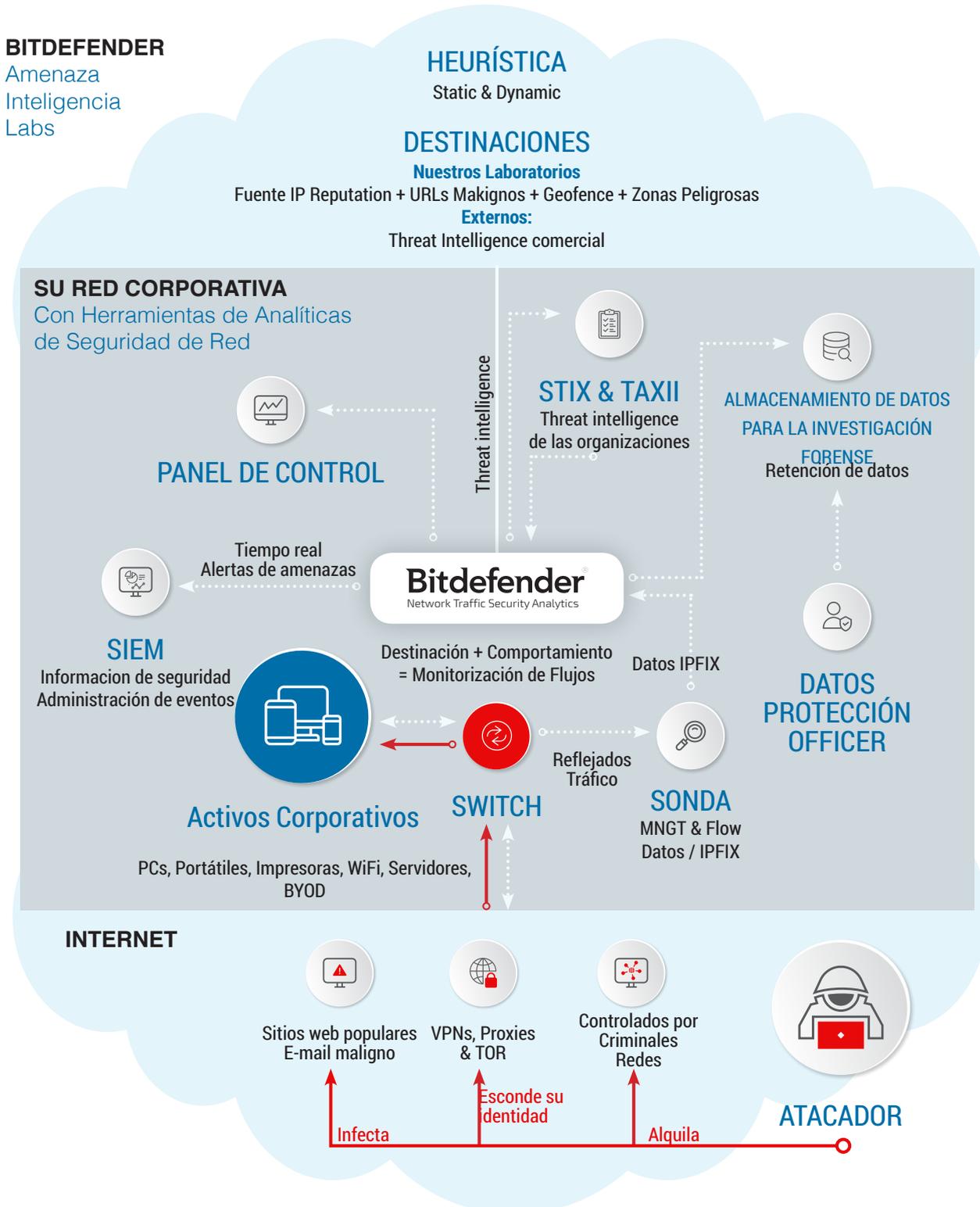
Protección del Internet de las Cosas (IoT) y BYOD en su entorno

Los atacantes aprovechan que los empleados utilizan tabletas, móviles y otros dispositivos personales en entornos empresariales para hacerse con información de las compañías. Proteger el BYOD aumenta la productividad de los empleados y reduce el riesgo de exposición de la información corporativa. La tecnología de Bitdefender NTSA ayuda a proteger las organizaciones contra el robo de información, mediante la monitorización y el seguimiento constante del comportamiento de usuarios y dispositivos en tiempo real y gracias a la implementación de una excelente inteligencia sobre amenazas. Esa una solución sin agente, discreta e independiente del sistema operativo.

Los entornos empresariales se distribuyen cada vez más entre dispositivos operados por personas y por cosas inteligentes (IoT). Mientras que los endpoints tradicionales suelen quedar vigilados y bien protegidos, las cosas inteligentes actúan en una zona gris bajo protección limitada o, incluso, sin protección alguna. Con creciente frecuencia, los dispositivos en la red son un blanco preferente y se utilizan como puntos de entrada durante los ataques avanzados. La capacidad de detección de brechas de NTSA se extiende también a las cosas inteligentes en la red empresarial. Al centrarse en el comportamiento de los endpoints en la red, puede proteger dispositivos que adolezcan de una limitada capacidad de seguridad integrada, o carentes de ella, sin la necesidad de ejecutar algún agente de seguridad de endpoints (como suele pasar con la mayoría de los dispositivos IoT).

Arquitectura e implementación de Bitdefender NTSA

Bitdefender NTSA se puede implementar fácilmente (plug-and-play) y proporciona resultados inmediatos. El rendimiento de la red no se ve afectado en modo alguno, ya que el appliance actúa fuera de banda, analizando una copia duplicada del tráfico de la red.



Soporte de la conformidad

Muchas normativas, incluido el RGPD, exigen que las organizaciones proporcionen rápidamente información detallada sobre las actividades maliciosas en caso de que se produzcan violaciones de la seguridad. NTSA ayuda a las organizaciones a cumplir con esos requisitos de cumplimiento al registrar información sobre el tráfico de datos de la red durante hasta doce meses. Dicho registro solo contiene metadatos, sin información del contenido y, además, el acceso a él está reservado únicamente al Data Protection Officer, lo que elimina el riesgo de exposición de información confidencial.

Principales beneficios

Evitar la interrupción del negocio

- Detecta brechas y amenazas avanzadas que eludieran los mecanismos de prevención a nivel de endpoint o de red
- Proporciona visibilidad total e información sobre la actividad de red relacionada con las amenazas y anomalías de tráfico en cualquier punto terminal
- Combina inteligencia de amenazas en la nube, aprendizaje automático y análisis del comportamiento para detectar las amenazas más sofisticadas tipo ataques dirigidos avanzados - APT

Cumplir con los requisitos de conformidad

- Identifica comportamientos anormales de los usuarios o amenazas internas que puedan conducir a violaciones de la política corporativa
- Permite la búsqueda de amenazas y el análisis forense mediante el acceso a datos almacenados a largo plazo
- Proporciona acceso rápido y fácil a la información requerida por las autoridades en un período de 72 horas después de que se descubra una brecha (RGPD)

Facilidad de uso y rápido retorno de la inversión

- Solución complementaria, fácil de implementar y de mantener, que ofrece resultados inmediatos para un rápido retorno de la inversión
- Las integraciones con otros sistemas de monitorización permiten automatizar la seguridad y ofrecer una respuesta rápida
- Cubre todos los endpoints de la red, independientemente del tipo o de las soluciones de seguridad preexistentes (dispositivos corporativos o administrados por el usuario, elementos de red, BYOD, IoT)

Características de Bitdefender Network Traffic Security Analytics

Detección en tiempo real y retroactiva

Detecta brechas comprobando pasivamente el tráfico de red saliente en tiempo real en busca de comunicaciones maliciosas. Aplica nuevos elementos de inteligencia de amenazas sobre los metadatos grabados para detectar vulneraciones retroactivamente

Inteligencia de amenazas en la nube, Inteligencia Artificial/ Machine Learning y heurística

Combina la inteligencia de las amenazas en la nube de Bitdefender con el análisis del tráfico de red en tiempo real basado en Inteligencia Artificial, Machine Learning y heurística para lograr tasas de detección de amenazas superiores con pocos falsos positivos.

Cobertura extendida y visibilidad total

Cubre todos los endpoints de la red, independientemente del tipo o de las soluciones de seguridad preexistentes (dispositivos corporativos o administrados por el usuario, elementos de red, BYOD, IoT). Proporciona visibilidad total e información sobre la actividad de red relacionada con las amenazas y anomalías de tráfico en cualquier punto terminal

Reducción del ruido y búsqueda eficaz de las amenazas

Automatiza el análisis de seguridad, reduce el ruido para mejorar la eficacia de la búsqueda de amenazas por parte de los analistas y genera alertas útiles para facilitar la respuesta ante incidentes.

Comunicación cifrada y privacidad

El enfoque exclusivo en los metadatos del tráfico permite el análisis de las comunicaciones cifradas y elimina el problema de la privacidad en el tráfico sin cifrar.

Rápida implementación y resultados inmediatos

Se basa en una arquitectura sencilla y flexible (implementación física o virtualizada) con componentes plug-and-play para ofrecer resultados inmediatos.

Para conocer los requisitos detallados del sistema, consulte <https://www.bitdefender.com/business/enterprise-products/network-traffic-security-analytics.html>



Bitdefender es una compañía global de tecnología de seguridad que proporciona soluciones de seguridad cibernética de vanguardia y protección avanzada contra amenazas a más de 500 millones de usuarios en más de 150 países. Desde 2001, Bitdefender ha producido constantemente tecnología galardonada de seguridad para empresas y consumidores, y es un proveedor de elección tanto en seguridad de infraestructura híbrida como en protección de puntos finales. A través de I+D, alianzas y asociaciones, se confía en que Bitdefender está a la vanguardia y ofrece una seguridad sólida en la que puede confiar. Más información disponible en <http://www.bitdefender.es>

Todos los derechos reservados. © 2018 Bitdefender. Todas las marcas registradas, nombres comerciales y productos a los que se hace referencia en el presente documento son propiedad de sus respectivos dueños.
PARA MÁS INFORMACIÓN VISITE: www.bitdefender.es/business

