Hoja de datos

Arbor Networks Spectrum™ con NETSCOUT ISNG

RANGO ÉPICO. COMPROBACIÓN MÁS RÁPIDA.

El panorama de ataques ha cambiado. Las herramientas de ataques como malware, usadas en general para comprometer inicialmente una red, ya no son las armas preferidas. Los atacantes de hoy en día acceden a las cuentas de los usuarios, manipulan las aplicaciones de TI o los sistemas operativos conocidos y eluden las defensas tradicionales de seguridad del perímetro. El tiempo promedio para detectar un ataque es generalmente superior a los 150 días, sin embargo, el tiempo que un adversario tarda en comprometer inicialmente una red son menos de 10 minutos.

Arbor Networks Spectrum™ puede reducir drásticamente el tiempo promedio de detección de todo el equipo de seguridad cuando un atacante ya ingresó y tomar acciones rápidas para expulsarlo o retenerlo. No solo brinda una mayor visibilidad de la actividad de la red y muestra rápidamente problemas de alta prioridad, sino que también los equipos de seguridad obtienen capacidad de escalado mediante la automatización y orquestación de flujos de trabajo claves de operaciones de seguridad y respuesta ante incidentes, lo que permite mayores logros con el personal y los recursos existentes.

Rango épico

Arbor Spectrum brinda una visibilidad completa de la red junto con la inteligencia de amenazas ATLAS™ (Active Threat Level Analysis System) de alta fidelidad derivada de una tercera parte de todo el tráfico de Internet mundial. La combinación de la visibilidad de ATLAS y las políticas de inteligencia de ATLAS, actualizadas continuamente con lo último en inteligencia de amenazas, les brinda a los clientes la vista con mayor fidelidad de las amenazas que ocurren en las redes, sobre y alrededor de estas.

Comprobación más rápida

Llegue a conclusiones relevantes, más rápido, con el archivo de tráfico de alto rendimiento y en tiempo real de Arbor Spectrum, ahora integrado con la tecnología de recopilación y análisis de metadatos de la aplicación y la red líder de la industria de NETSCOUT ISNG con tecnología ASI, para brindar una visibilidad generalizada sin igual de los datos de la red, la aplicación y el protocolo y la posibilidad de analizarlos. Flujos de trabajo de investigación integrados, una búsqueda rápida y referencias f[illegible]s de meses de actividades anteriores del usuario y de la red, transforman días y horas de trabajo en segundos.

—

"Ningún producto de seguridad es una fórmula mágica, pero Arbor Spectrum nos ha brindado una verdadera visibilidad integral que nunca antes habíamos tenido y que otras soluciones no brindan".

"Estamos muy felices con la solución y el servicio de Arbor Spectrum. Nos ha ayudado a reducir considerablemente nuestro tiempo promedio de detección".

INGENIERO DE SEGURIDAD PRINCIPAL, IMPORTANTE EMPRESA FINANCIERA

ARBOR NETWORKS

The Security Division of NETSCOUT

Cómo trabaja Arbor Spectrum

Arbor Spectrum potencia la visibilidad global de Arbor con la exclusiva inteligencia de amenazas de ATLAS y con sus propios datos de amenazas y patrones de tráfico para detectar, investigar y comprobar las amenazas más dañinas. Arbor Spectrum utiliza NETSCOUT ISNG con tecnología ASI o la Recopilación de flujos de Arbor Spectrum, con Active Directory, para mostrar la actividad de la red interna.

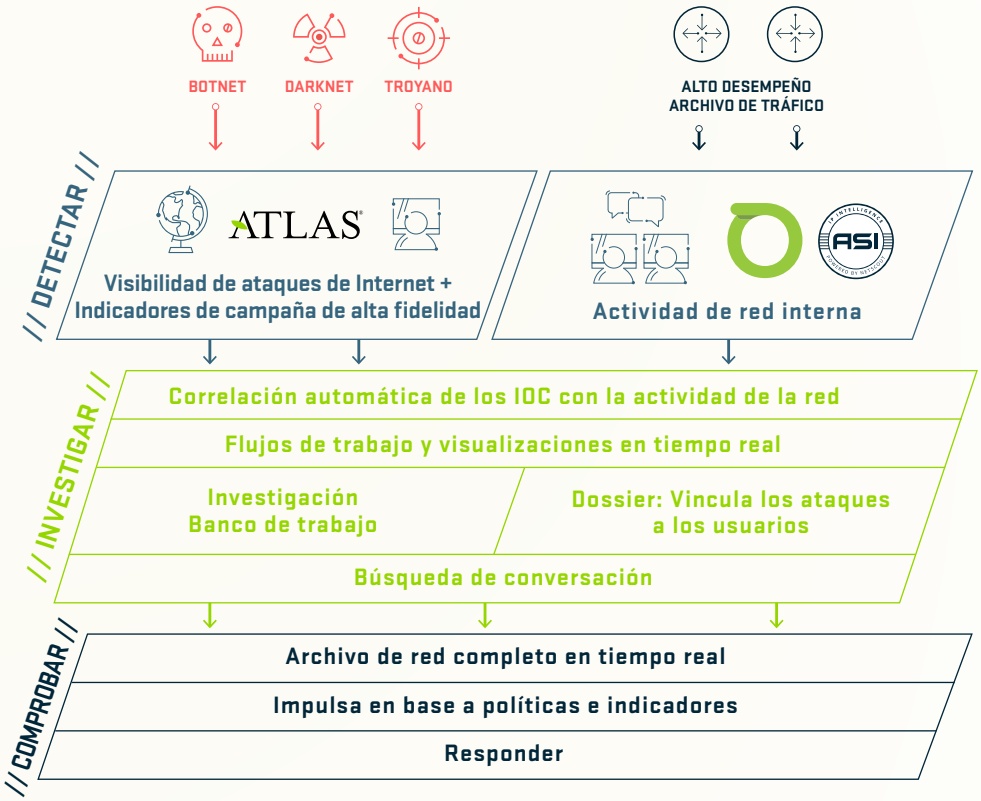

Figura 1

Cómo trabaja Arbor Spectrum

DETECTAR

- Indicadores relevantes para iniciar la investigación
- Nuevas amenazas con los indicadores de inteligencia de ATLAS
- Importar fuentes STIX para aplicar la inteligencia de amenazas compartida
- Análisis retrospectivo para buscar archivos de indicadores identificados recientemente

Indicadores de inteligencia de ATLAS

ATLAS es el mayor conjunto de datos de telemetría de tráfico de Internet activo del mundo (aproximadamente una tercera parte de todo el tráfico de Internet). ATLAS le permite a Arbor monitorear los niveles de la actividad de ataques en Internet y, luego, derivar esos patrones de tráfico de ataques en indicadores de inteligencia altamente an[illegible]dos cada hora en Arbor Spectrum.

INVESTIGAR

Priorización de indicador

Representación visual en tiempo real de tendencias en nuevos indicadores y actividad de la red. Se pueden asignar en grupos (incluidos usuarios, función comercial y ubicación).

Módulo de investigaciones

Agregado de pistas tales como indicadores relacionados, perfiles de host y conexiones de red, en una vista única de una amenaza avanzada.

Host Dossier con la integración del ID del usuario y el directorio de actividades

- Flujos de trabajo exclusivo identifican y rastrean movimientos laterales en la red.
- Una vista detallada de las conversaciones de red entre los hosts y los puntos de conexión de interés.

COMPROBAR

Captura automática de paquete de cualquier indicador de riesgo

Permite un análisis forense disruptivo y automatizado mediante el almacenamiento de interfaces PCAP de cualquier indicador identificado, lo que hace que los análisis forenses sean optimizables y rentables.

Captura manual de paquete de cualquier host o conversación

Capacidad de cargar un PCAP en Arbor Spectrum.

Integración con plataformas líderes de SIEM

Envía datos recopilados a las plataformas SIEM, incluidas HP Arcsight, IBM QRadar, Splunk Enterprise Security.

Arbor Spectrum con implementación de NETSCOUT ISNG

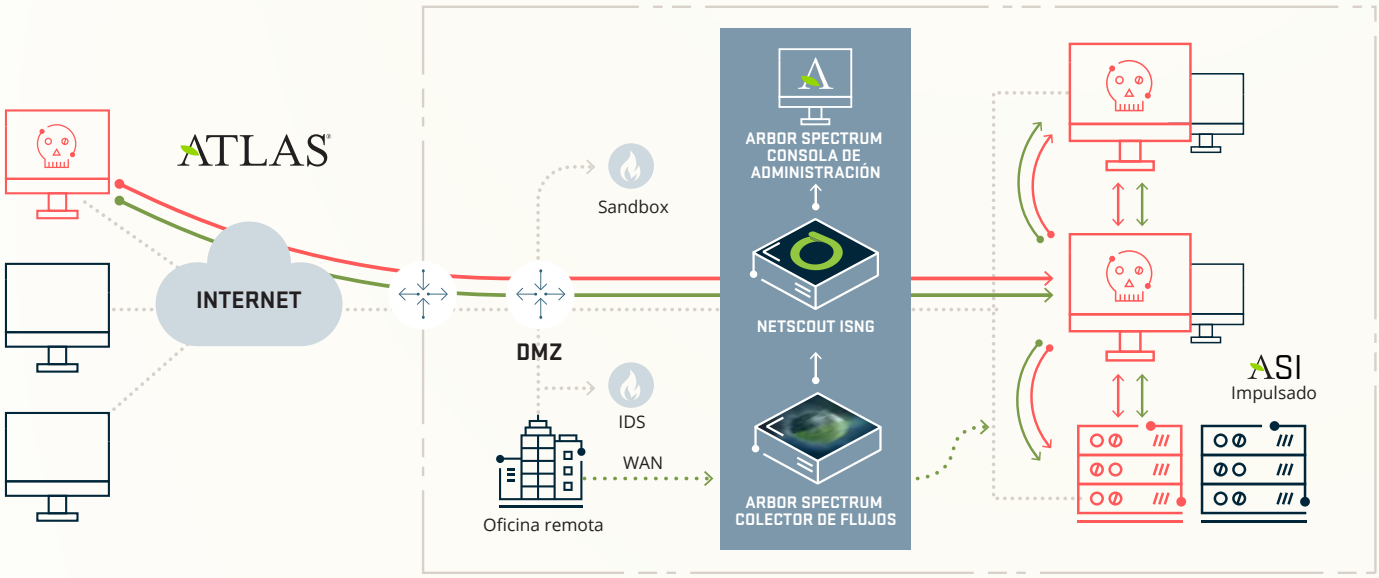

Figura 2 *Arbor Spectrum con NETSCOUT ISNG*

Características principales

Indicadores de campaña altamente confiables

Con inteligencia de ATLAS.

Flujos de trabajo exclusivos

Muestra rápidamente y vincula los indicadores de amenazasa la actividad sospechosa.

Archivo de tráfico de red de alto rendimiento

Acceso a meses de datos de la red a su alcance, ahora con NETSCOUT ISNG.

Buscar y pivotar

Meses de datos de la red en segundos.

Implementado en menos de un día

Factores de forma virtuales y de dispositivo.

Modos preferidos de NETSCOUT ISNG

Modelo ISNG	N.º de interfaces	Tipo de interfaz	Almacenamiento	Núcleos	RAM
ISNG 9895	4	4 puertos 10 G/1 G	96 TB	36	256 GB
ISNG 9795	4	4 puertos 10 G/1 G	64 TB	24	128 GB
ISNG 4895	4	4 puertos 10 G/1 G	32 TB	36	256 GB
ISNG 4795	4	4 puertos 10 G/1 G	24 TB	24	128 GB

Consola de administración de Arbor Spectrum y Modelos de colector de flujos

	2200	2300
Opciones de implementación	Consola de la plataforma, Colector de paquetes o Colector de flujos	Colector de paquetes o Colector de flujos
Memoria	64 GB	64 GB
Discos duros	8 × 2 TB SATA 7200 RPM	16 × 4 TB SATA 7200 RPM
Capacidad de almacenamiento	15 TB	64 TB
Archivo de tráfico	9.1 TB	44 TB
Flujos máx. por segundo (como colector de flujos)	25,000	100,000
Inspección máx. de paquetes (como colector de paquete)	1.5 Gbps	5 Gbps
Opciones de interfaz de captura	4 puertos SFP o 2 puertos SFP+	
Interfaz de gestión	Cobre de 2 puertos de 10/100/1000	
Procesador	2 procesadores XEON ES-2658; 2.1 Ghz/20 MB; 8 núcleos	
Tamaño	2 U	3 U
Potencia	CA o CC dual **Unidad de CA:** 100 a 240 VCA, 47 a 63 Hz, 10 a 5 A **Unidad de CC:** -40 a -72, 20 a 12 A	CA o CC dual **Unidad de CA:** 100 a 127 / 200 a 240 VCA, 50/60 Hz, 10/5 A; **Unidad de CC:** -36 a -72, 31 a 15 A
Humedad relativa	De 8 a 90 % sin condensación	De 8 a 90 % sin condensación
Disipación del calor	A 400 W, 1365 BTU/h	A 525 W, 1791 BTU/h

Recomendaciones de hardware para Arbor Spectrum VM

Arbor realiza las siguientes recomendaciones de hardware:

Implementaciones de VM	Consola	Colector de paquetes	Colector de flujos
Versión de VMware compatible	Software vSphere Hypervisor (anteriormente conocido como ESXi), versión 5.5		
Asignación de núcleos	8 a 32	8 a 32	8
Asignación de memoria	16 a 64 GB	16 GB	16 GB
Asignación de disco	**SO:** 150 GB / **Datos:** 1 a 4 TB	**SO:** 150 GB / **Datos:** 1 a 40 TB (máximo probado; diseñado para ampliarse a más de 40 TB)	
Interfaces de red	1 a 2	3 a 15	1 a 15
Flujos máx. por segundo			250,000 FPS
Inspección máx. de paquetes		Hasta 2 Gbps	

—

Requisitos y rendimiento proporcionados como documentación para las implementaciones de producción. Arbor Spectrum es compatible con otras opciones de implementaciones de prueba de concepto de menor escala.

ARBOR NETWORKS
The Security Division of NETSCOUT

Estados Unidos
T: +1 781 362 4300
contact@arbor.net

Brasil
T: +55.11.4380.8035
brasil@arbor.net

Mexico, Caribe & Central America
T: +52.55.4624.4842
mxcca@arbor.net

North of Latin America
T: +57.1.508.7099
nola@arbor.net

South of Latin America
T: +54.11.5218.4007
sola@arbor.net

www.arbornetworks.com

—

DS/SPECTRUM/ES/0717-LETTER