Hoja de datos de Arbor

ARBOR NETWORKS SPECTRUM™

Resuelva verdaderas amenazas más rápido que nunca conjugando una inigualable macrovisión del tráfico de Internet con una detallada microvisión de su red

BENEFICIOS

Investigaciones 10 veces más rápidas que las de los sistemas forenses tradicionales o SIEM

- Flujos de trabajo y capacidades de búsqueda inteligentes para validar amenazas
- Visión completa de indicadores de amenazas de todas las entidades, dentro y fuera de la red

Análisis optimizable de flujos y paquetes en tiempo real para detectar la actividad de amenazas presentes y pasadas

- Visibilidad y desempeño sin precedentes del análisis de flujos y paquetes
- Pivote/Zoom interactivo
- PCAP accesible
- Búsqueda en todas las conversaciones de red (días, semanas, meses)

Detección y conexión de las conversaciones de amenazas en toda la red: desde Internet hacia la red interna

- Indicadores de inteligencia de ATLAS®
- Inteligencia de terceros personalizada
- Políticas y aprendizaje del comportamiento de la red

Instalación y operación sencillas

- Implementación y capacitación en un día

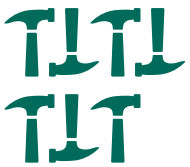
La verdadera amenaza avanzada

El panorama de amenazas a la seguridad ha cambiado radicalmente. El malware avanzado que las defensas tradicionales no pueden detectar ya no representa la mayor amenaza para las organizaciones.

La mayoría de los ataques de amenazas avanzadas que tuvieron éxito en los últimos dos años no se aprovecharon de una vulnerabilidad crítica, y muchos de ellos no utilizaron un malware como herramienta para atravesar las defensas del objetivo.

Arbor desarrolló una nueva plataforma para los equipos de seguridad que le permite analizar toda la red para luego buscar, detectar, investigar y demostrar la existencia de amenazas dentro y a través de ella como nunca antes.

- **Visualización de campañas de ataques globales en tiempo real en toda la red.** La inteligencia en tiempo real de amenazas globales de Arbor, recolectada de su red de proveedores de servicios, se conectará con los patrones de tráfico interno de una organización para detectar las amenazas más perjudiciales y peligrosas.
- **Búsqueda y detección de todo lo que se encuentra en la red.** Proporciona una visibilidad total de la actividad pasada y presente de su red, y a un costo mucho menor, lo que permite replantear y redefinir los modelos forenses de seguridad actuales.
- **Comprobación más veloz de la existencia de amenazas en la red.** Diseñados teniendo en mente el usuario de seguridad, los análisis y los flujos de trabajo inteligentes y en tiempo real, fortalecen y optimizan los equipos de seguridad para que puedan investigar y comprobar la existencia de amenazas 10 veces más rápido y con mayor eficiencia que las soluciones existentes en el mercado actual.



MÁS DE 7
KITS DE HERRAMIENTAS
se usaron para ataques avanzados en 2015, menos de la mitad se aprovechó de una vulnerabilidad crítica.

El 40 %
de los ataques avanzados en 2015 no involucró malware.

ARBOR NETWORKS
The Security Division of NETSCOUT

"Pudimos detectar un comando y control y hacer un seguimiento de toda la cronología del ataque y de los hosts afectados en siete minutos. Con las herramientas forenses existentes, nos hubiera llevado días."

Líder de Operación de Seguridad (Empresa Multinacional)

Descripción general de Arbor Spectrum

Arbor Spectrum ofrece una visibilidad total de la actividad de la red con un análisis de paquetes y flujos en tiempo real, y mediante una búsqueda rápida y sencilla en la actividad de los meses pasados. Este revolucionario enfoque permite a las organizaciones visualizar toda la red y realizar búsquedas mediante la conexión entre la visibilidad de ataques globales en Internet con la actividad de su propia red interna.

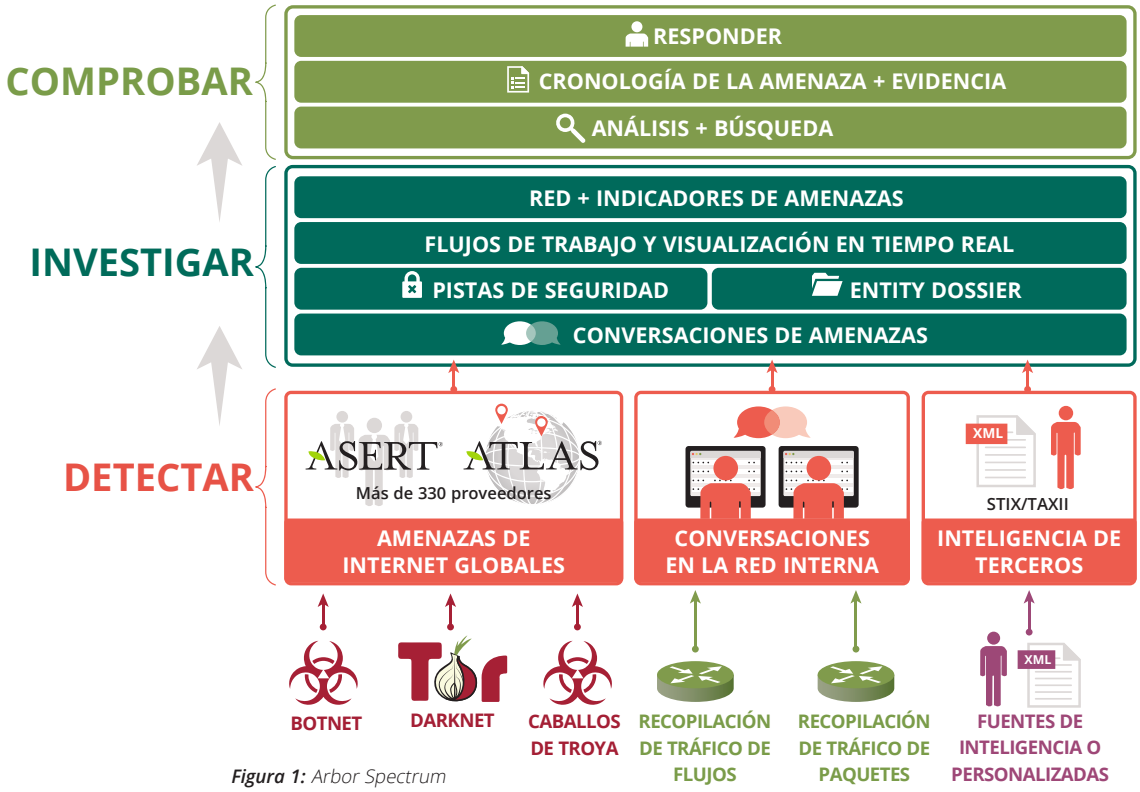


Figura 1: *Arbor Spectrum*

Características principales

DETECTAR

- **Flujos de trabajo de detección de amenazas**

  Proporciona una visión inmediata y en vivo de indicadores relevantes para comenzar a investigar a partir de las tendencias dinámicas en modo Pivote y Zoom Interactivo.

- **Indicadores de inteligencia de ATLAS**

  Lo que distingue a Arbor de otros proveedores es el modo en que aprovechamos la presencia ubicua en los proveedores de servicios para beneficiar a todos los clientes. ATLAS es un proyecto de colaboración con más de 330 clientes que acordaron compartir datos de tráfico anónimos con Arbor (aproximadamente un tercio de la totalidad del tráfico de Internet). Desde esta posición estratégica exclusiva, Arbor puede ofrecer inteligencia de amenazas ante los ataques que se están produciendo en tiempo real.

  La inteligencia de ATLAS se integra con Arbor Spectrum y equipa a los usuarios con políticas y tácticas defensivas que les permiten abordar ataques rápidamente como parte de una amenaza avanzada. La inteligencia de ATLAS y el Arbor Security Engineering and Response Team (ASERT) permiten a los clientes beneficiarse directamente de la capacidad y experiencia del equipo de investigación de Arbor.

INVESTIGAR

- **Host Dossier**
  Reúne rápidamente los datos relevantes acerca de una entidad (y dónde se encuentra) para actuar sobre sus operaciones de negocios.
- **Búsqueda de conversaciones en tiempo real**
  Permite al usuario detectar e investigar rápidamente las actividades para confirmar un ataque. Esto incluye información acerca de cómo, dónde y qué sucedió en el transcurso de minutos.
- **Tendencias de amenazas en tiempo real**
  Representación visual en tiempo real de tendencias en nuevos indicadores (orígenes y destinos de amenazas).

COMPROBAR

- **PCAP accesible de una amenaza**
  Comprueba si las amenazas de los últimos 3 a 6 meses fueron detectadas en la red, a una fracción del costo de los sistemas forenses de seguridad tradicionales.
- **Implementación y operación sencillas**
  Se puede implementar y capacitar al equipo en un día. Rápida recuperación de la inversión.

"Una de las ventajas más destacadas de Arbor Spectrum es que realmente no se necesita siquiera un nivel de conocimiento de principiante en sistemas forenses de red para usarlo. La interface es sencilla y resulta muy fácil extraer información relevante para una investigación."

Arquitecto de Seguridad
(Empresa de Retail)

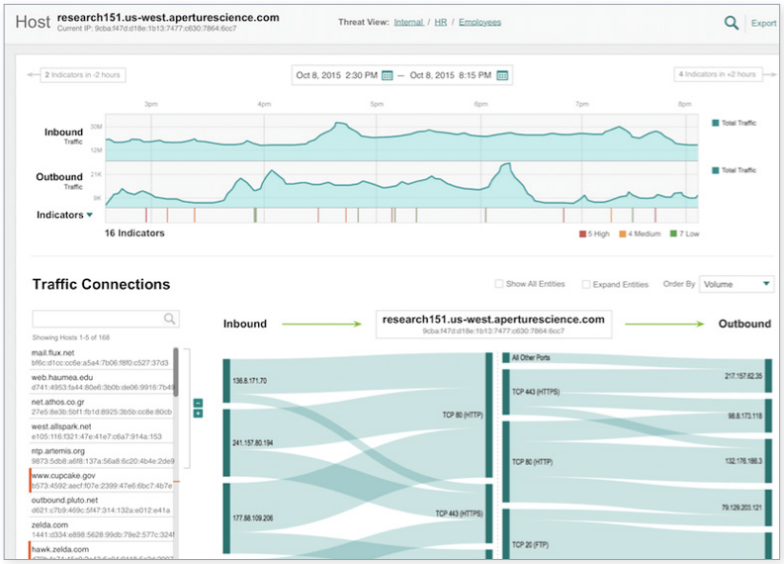


Figura 2: *Use el módulo Host Dossier para investigar todas las actividades relacionadas con un host específico.*

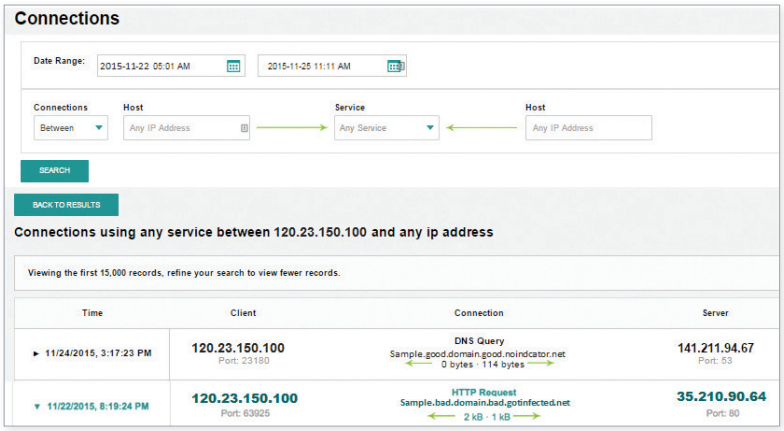


Figura 3: *Use el módulo Conexiones para ver comunicaciones de un host hacia otro, o entre hosts.*

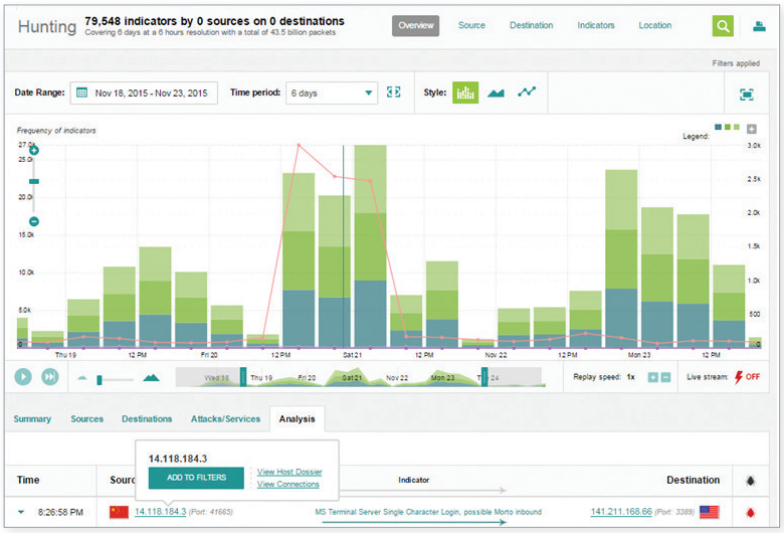


Figura 4: *Use el módulo Detección para ver indicadores de amenazas en el tiempo.*

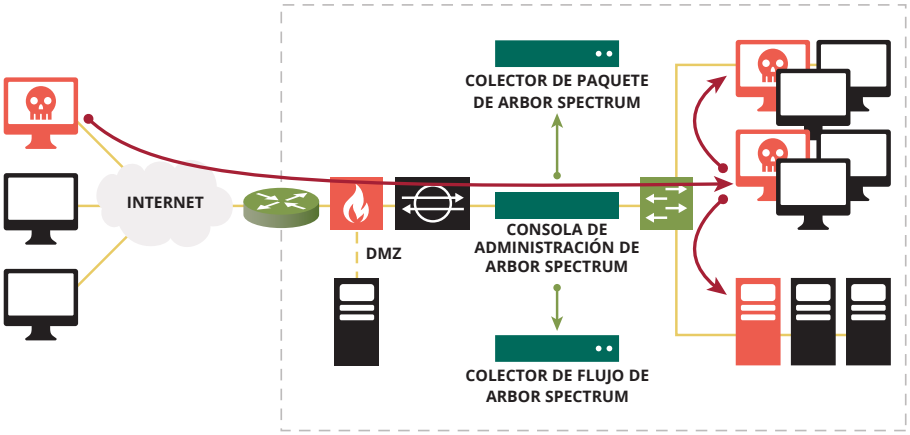


Figura 5: *Implementación de Arbor Spectrum*

Modelos de dispositivos

	2200	2300
Opciones de implementación	Consola de la plataforma, Colector de paquete o Colector de flujos	Colector de paquete o Colector de flujo
Memoria	64 GB	64 GB
Discos duros	8 x 2 TB SATA 7200 RPM	16 x 4 TB SATA 7200 RPM
Archivo de tráfico	9,1 TB	44 TB
Flujos máx. por segundo *(como Colector de flujo)*	25,000	100,000
Inspección máx. de paquetes *(como Colector de paquete)*	1,5 Gbps	5 Gbps
Opciones de interface de captura	4 puertos SFP o 2 puertos SFP+	
Interface de gestión	Cobre de 2 puertos de 10/100/1000	
Procesador	2 x XEON ES-2658; 2,1 Ghz/20 MB; procesadores de 8 núcleos	
Tamaño	2 U	3 U
Potencia	CA o CC dual Unidad de CA: 100 a 240 VCA; 47/63 Hz Unidad de CC: -40 a -72 V/20 a 12 ADC	CA o CC dual Unidad de CA: 100 – 127 –200 – 240 VCA; 10 a 5 A; 50/60 Hz Unidad de CC: -40 a -72 VCC; 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
Condiciones ambientales	IEC 60950-1: 2005 2.ª Edición; Am 1:2009 CAN/CSA-C22.2 N.º 60950-1-07, 2.ª Ed., Enmienda 1: 2011 Norma ANSI/UL N.º 60950-1-2011, 2.ª Ed. FCC 47 CFR Parte 15, Subparte B – Verificación ICES-003 EN 55022: 2010 + AC: 2011 EN 55024: 2010 CISPR 22: Edición 6.0 2008-09 AS/NZS CISPR 22: 2009 EN 61000-3-2: 2006 + A1: 2009 + A2: 2009 EN 61000-3-3: 2008	IEC 60950-1: 2005 2.ª Edición; Am 1:2009 CAN/CSA-C22.2 N.º 60950-1-07, 2.ª Ed., Enmienda 1: 2011 Norma ANSI/UL N.º 60950-1-2011, 2.ª Ed. FCC 47 CFR Parte 15, Subparte B – Verificación ICES-003 EN 55022: 2010 + AC: 2011 EN 55024: 2010 CISPR 22: Edición 6.0 2008-09 AS/NZS CISPR 22: 2009 EN 61000-3-2: 2006 + A1: 2009 + A2: 2009 EN 61000-3-3: 2008

ARBOR NETWORKS

The Security Division of NETSCOUT

Sede corporativa
76 Blanchard Road
Burlington, MA 01803 EE. UU.
Llamada gratuita en los
EE. UU.: +1 866 212 7267
Tel.: +1 781 362 4300

www.arbornetworks.com

Ventas en Latinoamérica
Brasil
Tel.: +55.11.4380.8035
brasil@arbor.net

México, Caribe y América Central
Tel.: +52.55.4624.4842
mxcca@arbor.net

América Latina del Norte
Tel.: +57.1.508.7099
nola@arbor.net

América Latina del Sul
Tel.: +54.11.5218.4007
sola@arbor.net

DS/SPECTRUM/ES/1016-LETTER