Folha de dados da Arbor

Arbor NETWORKS Spectrum™

Resolva ameaças reais mais rápido do que nunca, conectando uma visão macro inigualável do tráfego de Internet com uma visão micro detalhada da rede

BENEFÍCIOS

Investigação dez vezes mais rápida do que com SIEM ou análise forense tradicional

- Recursos de pesquisa e fluxos de trabalho inteligentes para validar ameaças.
- Visão completa dos indicadores de ameaça em todas as entidades, dentro e fora da rede.

Análise escalonável de fluxos e pacotes em tempo real para trazer à tona atividades de ameaças atuais e passadas

- Visibilidade e desempenho sem precedentes da análise de fluxos e pacotes.
- Pivot/zoom interativo.
- PCAP acessível.
- Pesquisa de todas as conversas da rede (dias, semanas, meses).

Detecção e conexão de conversas de ameaça em toda a rede, da Internet à rede interna

- Indicadores de inteligência ATLAS®.
- Inteligência de terceiros personalizada.
- Políticas e aprendizado do comportamento de rede.

Instalação e operação fáceis

- Implantação e treinamento em um único dia.

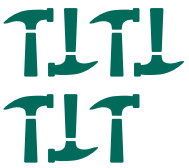
A verdadeira ameaça avançada

O cenário de ameaças de segurança mudou radicalmente. Não são mais os malwares avançados não detectados por defesas tradicionais que representam o maior risco para as organizações.

Em sua maioria, os ataques bem-sucedidos de ameaças avançadas nos últimos dois anos nunca exploraram uma vulnerabilidade crítica e muitos não usaram nenhum malware como parte das ferramentas para burlar as defesas do destino.

A Arbor desenvolveu uma nova plataforma para a equipe de segurança que permite realizar pesquisas para detectar, investigar e comprovar ameaças dentro e por toda a rede de maneira inédita.

- **Veja campanhas de ataque globais em tempo real em toda a rede**. A inteligência de ameaças globais em tempo real recebida a partir da rede de provedores de serviços da Arbor será conectada aos padrões de tráfego internos de uma organização para detectar as ameaças mais perigosas e danosas.
- **Pesquise e traga à tona qualquer elemento na rede**. Aprimoramento dos modelos de análise forense de segurança atuais, fornecendo visibilidade completa de todas as atividades passadas e presentes na rede por uma fração do custo.
- **Comprove ameaças na rede mais rapidamente**. Projetados com o usuário de segurança em mente, as análises e fluxos de trabalho inteligentes em tempo real capacitam e escalonam as equipes de segurança para investigar e comprovar ameaças com mais eficiência e dez vezes mais rapidamente que as soluções atualmente existentes no mercado.



Mais de 7
KITS DE FERRAMENTAS
foram usados para ataques avançados em 2015 e menos da metade explorava uma vulnerabilidade crítica.

40%
dos ataques avançados em 2015 não envolveram malware.

ARBOR® NETWORKS
The Security Division of NETSCOUT

"Conseguimos detectar um "command and control" e rastrear a cronologia de todo o ataque e os hosts afetados em sete minutos. Com nossas ferramentas de análise forense existentes, isso teria demorado dias."

Líder de operações de segurança (multinacional norte-americana)

Visão geral do Arbor Spectrum

O Arbor Spectrum fornece visibilidade completa de todas as atividades na rede, com análise de pacotes e fluxos em tempo real e pesquisa rápida e fácil de vários meses de atividades passadas. Essa abordagem inovadora permite que a organização visualize e pesquise toda a rede, conectando a visibilidade dos ataques globais na Internet com a atividade na rede interna.

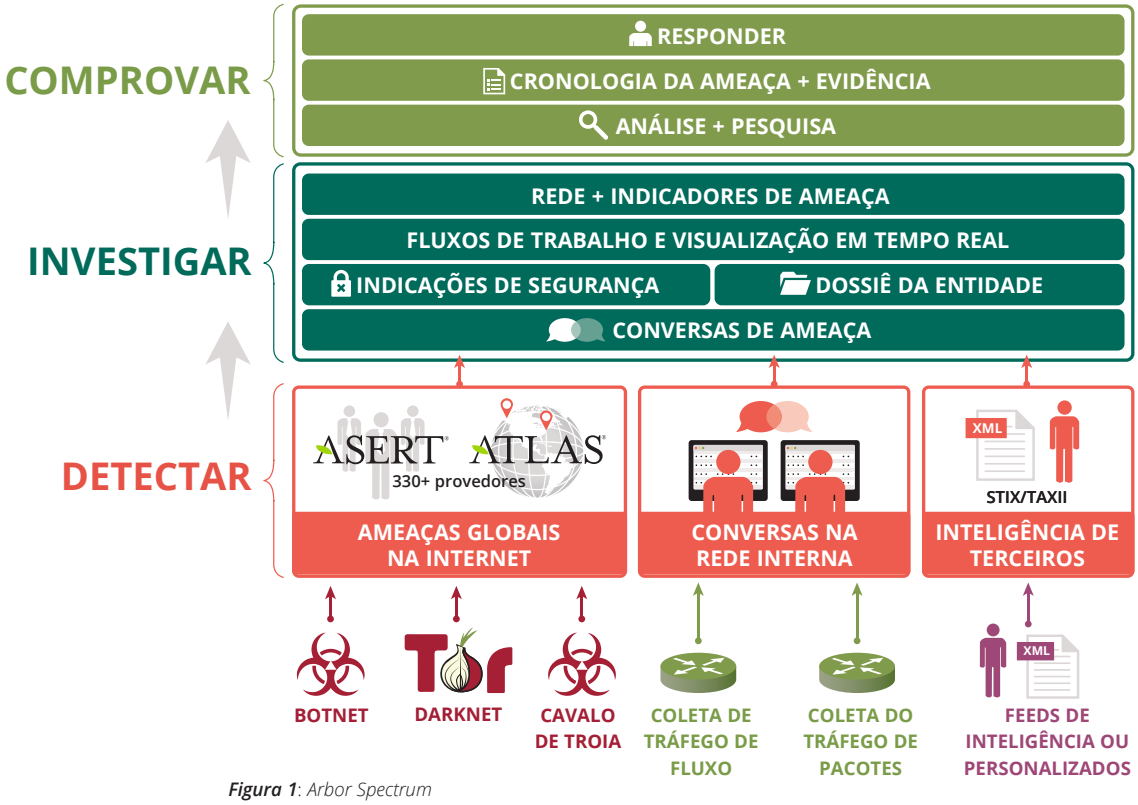


***Figura 1**: Arbor Spectrum*

Principais recursos

DETECTAR

- **Fluxos de trabalho de detecção de ameaças**

  Fornecem uma visualização imediata e dinâmica dos indicadores relevantes para começar a investigar a partir de zoom e pivot interativo, com atualização online.

- **Indicadores de inteligência do ATLAS**

  O que diferencia a Arbor de outros fornecedores é o modo como aproveitamos nossa presença de provedor de serviços global para beneficiar todos os nossos clientes. O ATLAS é um projeto colaborativo com mais de 330 clientes que concordaram em compartilhar dados de tráfego anônimos com a Arbor; aproximadamente um terço de todo o tráfego de Internet. Com base nessa posição privilegiada exclusiva, a Arbor pode fornecer inteligência de ameaças sobre ataques que estão ocorrendo em tempo real.

  A inteligência do ATLAS é integrada ao Arbor Spectrum e equipa os usuários com políticas e medidas defensivas que lhes permitem lidar rapidamente com ataques como parte de uma ameaça avançada. A inteligência do ATLAS e o Arbor Security Engineering and Response Team (ASERT) permitem que os clientes se beneficiem diretamente da visão detalhada e ampla da área de pesquisa da Arbor.

INVESTIGAR

- **Pesquisa de conversas em tempo real**

  Permite que o usuário detecte e investigue rapidamente uma atividade para confirmar um ataque, incluindo como, onde e o que aconteceu em um intervalo de poucos minutos.

- **Tendências de ameaças em tempo real**

  Representação visual em tempo real das tendências em novos indicadores (origens e destinos de ameaças).

COMPROVAR

- **PCAP acessível de uma ameaça**

  Comprove ameaças detectadas na rede de três a seis meses atrás, por uma fração do custo da análise forense de segurança tradicional.

- **Fácil de implantar e operar**

  É possível implantar e treinar a equipe em um dia, gerando ROI rápido.

"Um dos melhores pontos do Arbor Spectrum é que você realmente não precisa sequer de um nível de habilidade de principiante de análise forense de rede para usá-lo. A interface é objetiva, simplificando a extração de informações importantes relevantes para uma investigação."

Arquiteto de segurança, grande varejista (América do Norte)

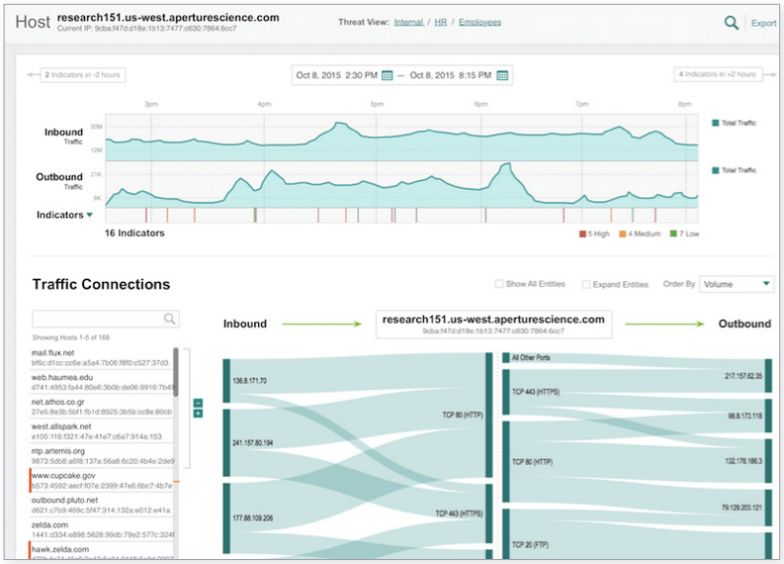


Figura 2: *Use o módulo Dossiê do host para investigar todas as atividades relacionadas a um host específico.*

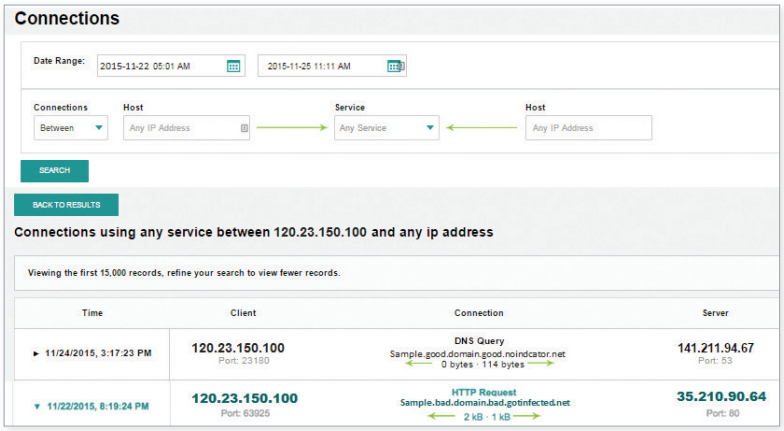


Figura 3: *Use o módulo Conexões para visualizar as comunicações de qualquer host para quaisquer hosts, ou entre hosts.*

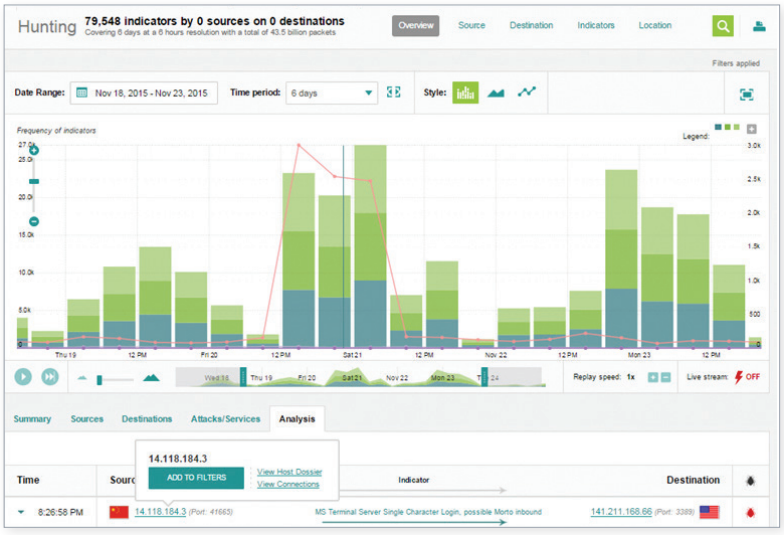


Figura 4: *Use o módulo Detecção para visualizar indicadores de ameaça ao longo do tempo.*

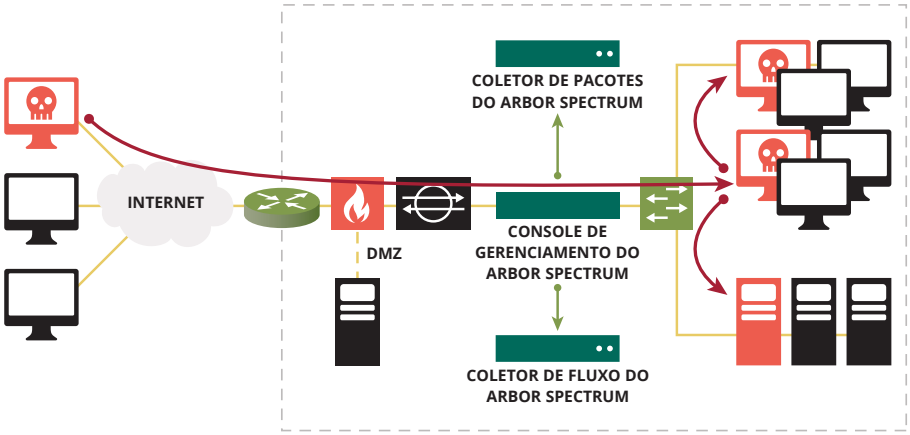


Figura 5: *Implantação do Arbor Spectrum*

Modelos de equipamento

	2200	2300
Opções de implantação	Console da plataforma, coletor de pacotes ou coletor de fluxo	Coletor de pacotes ou coletor de fluxo
Memória	64 GB	64 GB
Discos rígidos	8 x 2 TB SATA 7.200 RPM	16 x 4 TB SATA 7.200 RPM
Arquivo de tráfego	9,1 TB	44 TB
Máximo de fluxos por segundo *(como coletor de fluxo)*	25.000	100.000
Inspeção de pacotes máxima *(como coletor de pacotes)*	1,5 Gbps	5 Gbps
Opções de interface de captura	SFP de 4 portas ou SFP+ de 2 portas	
Interface de gerenciamento	2 x 10/100/1000 de cobre	
Processador	2 x XEON ES-2658; 2,1 Ghz/20 MB; processadores de oito núcleos	
Tamanho	2 RU	3 RU
Alimentação	CA ou CC dupla Unidade CA: 100 – 240 VCA; 47/63 Hz Unidade CC: -40 – -72 V/20-12 ACC	CA ou CC dupla Unidade CA: 100 – 127 – 200 – 240 VCA; 10 – 5 A; 50/60 Hz Unidade CC: -40 – -72 VCC; 31 – 15 A
Umidade relativa	8 – 90% sem condensação	8 – 90% sem condensação
Dissipação de calor	A 400 Watts, 1365 BTU/h	A 525 Watts, 1791 BTU/h
Ambiental	IEC 60950-1: 2005, 2ª Edição; Am 1:2009 CAN/CSA-C22.2 Nº 60950-1-07, 2ª Edição, Emenda 1: 2011 Norma ANSI/UL Nº 60950-1-2011, 2ª edição, FCC 47 CFR Parte 15, Subparte B: Verificação ICES-003 EN 55022: 2010 + AC: 2011 EN 55024: 2010 CISPR 22: Edição 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, 2ª Edição; Am 1:2009 CAN/CSA-C22.2 Nº 60950-1-07, 2ª Edição, Emenda 1: 2011 Norma ANSI/UL Nº 60950-1-2011, 2ª edição, FCC 47 CFR Parte 15, Subparte B: Verificação ICES-003 EN 55022: 2010 + AC: 2011 EN 55024: 2010 CISPR 22: Edição 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 USA
Chamada gratuita
dos EUA: +1 866 212 7267
Tel.: +1 781 362 4300

www.arbornetworks.com

Vendas na América Latina
Brasil
T: +55.11.4380.8035
brasil@arbor.net

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

América Latina do Norte
T: +57.1.508.7099
nola@arbor.net

América Latina do Sul
T: +54.11.5218.4007
sola@arbor.net

DS/SPECTRUM/PT/1016-LETTER