Data Sheet

Arbor Networks Spectrum™ com NETSCOUT ISNG

ALCANCE ÉPICO. COMPROVAÇÃO MAIS RÁPIDA.

O cenário de ataques mudou. As ferramentas de ataque, como o malware, geralmente utilizadas para comprometer inicialmente uma rede, não são mais as armas escolhidas. Os invasores atuais acessam contas de usuários e manipulam sistemas operacionais e aplicativos de TI conhecidos, ignorando as defesas de segurança de perímetro convencionais. O Tempo médio para detectar um ataque é geralmente superior a 150 dias, ainda que o tempo que seus adversários levam para comprometer inicialmente uma rede seja inferior a 10 minutos.

O Arbor Networks Spectrum™ pode aumentar significantemente o Tempo médio de descoberta de toda a equipe de segurança quando um invasor já estiver na rede e pode tomar medidas rapidamente para que ele seja excluído ou contido. Além de oferecer ampla visibilidade sobre as atividades na rede e encontrar rapidamente problemas de alta prioridade, ao automatizar e orquestrar a resposta a incidentes importantes e fluxos de trabalho de operações de segurança, as equipes de segurança também podem ajustar a escala, alcançando muito mais com a equipe e com os recursos existentes.

Alcance épico

O Arbor Spectrum oferece uma visibilidade completa da rede junto com a inteligência contra ameaças de alta fidelidade do ATLAS™ (Active Threat Level Analysis System, Sistema de análise de nível da ameaça ativa), obtida a partir de um terço de todo o tráfego de internet mundial. A combinação da visibilidade do ATLAS e suas políticas de inteligência, continuamente atualizadas com a inteligência contra ameaças mais recente, oferece aos clientes a mais alta perspectiva de fidelidade em relação às ameaças que estão acontecendo dentro ou ao redor das redes.

Comprovação mais rápida

Chegue a importantes conclusões de forma mais rápida com o arquivamento de tráfego de alto desempenho e em tempo real do Arbor Spectrum, agora integrado à tecnologia líder de setor do NETSCOUT de análise e coleta de metadados de aplicativos e redes, ISNG com Tecnologia ASI para oferecer uma visibilidade difundida e sem precedentes, além da análise de dados de rede, aplicativos e protocolos. Fluxos de trabalho de investigação integrados, pesquisas rápidas e pivots fáceis de meses de atividade antiga da rede e do usuário transformam dias e horas de trabalho em apenas alguns segundos.

—

"Nenhum produto de segurança é uma solução mágica, mas o Arbor Spectrum nos ofereceu uma visibilidade verdadeira e completa que nunca tivemos antes e que nenhuma outra solução foi capaz de oferecer."

"Estamos muito satisfeitos com a solução e os serviços do Arbor Spectrum. Ele nos ajudou a reduzir consideravelmente o Tempo médio de detecção."

ENGENHEIRO DE SEGURANÇA LÍDER, LARGE FINANCIAL

ARBOR® NETWORKS

The Security Division of NETSCOUT

Como o Arbor Spectrum funciona

O Arbor Spectrum utiliza a visibilidade global da Arbor em conjunto com a inteligência contra ameaças exclusiva do ATLAS e com seus próprios dados de ameaças e padrão de tráfego para detectar, investigar e comprovar as ameaças que causam mais danos. O Arbor Spectrum utiliza o NETSCOUT ISNG com a tecnologia ASI e/ou a Coleta de fluxo do Arbor Spectrum, com o Active Directory para trazer à tona a atividade de rede interna.

Figura 1

Como o Arbor Spectrum funciona

DETECÇÃO

- Indicadores relevantes para iniciar a investigação
- Novas ameaças com os Indicadores de inteligência do ATLAS
- Importação de feeds do STIX para aplicar a inteligência contra ameaças compartilhada
- Análise retrospectiva para pesquisar arquivos para os mais novos indicadores identificados

Indicadores de inteligência do ATLAS

O ATLAS é o maior conjunto de dados do mundo de telemetria de tráfego de internet atual (aproximadamente um terço de todo o tráfego de internet). O ATLAS permite que a Arbor monitore os níveis das atividades de ataques na internet e então transforme esses padrões de tráfego de ataque em indicadores de inteligência altamente controlados de hora em hora no Arbor Spectrum.

INVESTIGAÇÃO

Priorização de indicadores

Representação visual em tempo real das tendências em novos indicadores e atividades da rede. Elas podem ser mapeadas em grupos (incluindo usuários, funções de negócios, localização).

Módulo de investigações

Agregar referências, como indicadores relacionados, perfis de host e conexões de rede, em uma única visualização de uma ameaça avançada.

Dossiê do host com a integração de ID do usuário/Diretório de atividades

- Fluxos de trabalho exclusivos identificam e controlam o movimento lateral dentro da rede.
- Uma visão detalhada das conversas na rede entre hosts e pontos de interesse de conexão.

COMPROVAÇÃO

Captura de pacotes automática de qualquer indicador de compromisso

Permite uma análise forense agressiva e automatizada ao armazenar PCAPs de qualquer indicador identificado, tornando a análise forense escalonável e de custo reduzido.

Captura de pacotes manual de qualquer host ou conversa

Capacidade de carregar um PCAP no Arbor Spectrum.

Integração com as plataformas SIEM líderes

Envia os dados capturados em plataformas SIEM, incluindo HP Arcsight, IBM QRadar e Splunk Enterprise Security.

Arbor Spectrum com implantação do NETSCOUT ISNG

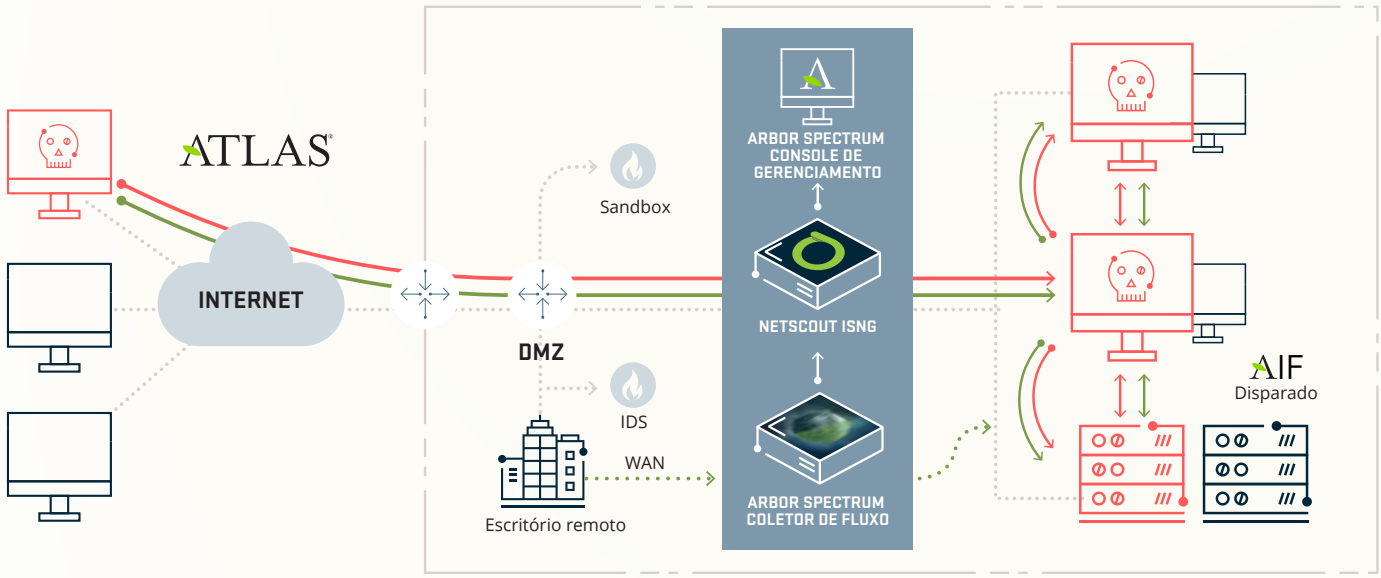

Figura 2 *Arbor Spectrum com NETSCOUT ISNG*

Principais recursos

Indicadores de campanha de alta confiança

Com a Inteligência do ATLAS.

Fluxos de trabalho exclusivos

Encontre e conecte rapidamente indicadores de ameaçasa atividades suspeitas.

Arquivo de tráfego de rede de alto desempenho

Acesso a meses de dados da rede na palma da sua mão com o NETSCOUT ISNG.

Pesquisa e pivot

Meses de dados da rede em apenas alguns segundos.

Implantação em menos de um dia

Equipamento e fatores de forma virtuais.

Modelos preferidos do NETSCOUT ISNG

Modelo ISNG	Nº de interfaces	Tipo de interface	Armazenamento	Núcleos	RAM
ISNG 9895	4	4 portas de 10 G/1 G	96 TB	36	256 GB
ISNG 9795	4	4 portas de 10 G/1 G	64 TB	24	128 GB
ISNG 4895	4	4 portas de 10 G/1 G	32 TB	36	256 GB
ISNG 4795	4	4 portas de 10 G/1 G	24 TB	24	128 GB

Console de gerenciamento do Arbor Spectrum e modelos do coletor de fluxo

	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 7200 RPM	16 x 4 TB SATA 7200 RPM
Capacidade de armazenamento	15 TB	64 TB
Arquivo de tráfego	9,1 TB	44 TB
Máximo de fluxos por segundo (como coletor de fluxo)	25.000	100.000
Inspeção máxima de pacotes (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 8 núcleos	
Tamanho	2 RU	3 RU
Alimentação	AC ou DC dupla **Unidade AC:** 100 – 240 VAC, 47 – 63 Hz, 10 – 5 A **Unidade DC:** -40 a -72, 20 – 12 A	AC ou DC dupla **Unidade AC:** 100 – 127/200 – 240 VAC, 50/60 Hz, 10/5 A; **Unidade DC:** -36 a -72, 31 – 15 A
Umidade relativa	8 a 90% sem condensação	8 a 90% sem condensação
Dissipação de calor	A 400 Watts, 1365 BTU/h	A 525 Watts, 1791 BTU/h

Recomendações de hardware para a VM do Arbor Spectrum

A Arbor faz as seguintes recomendações de hardware:

Implantações de VM	Console	Coletor de pacotes	Coletor de fluxo
Versão VMware com suporte	Software vSphere Hypervisor (conhecido anteriormente como ESXi), versão 5.5		
Alocação de núcleo	8 – 32	8 – 32	8
Alocação de memória	16 – 64 GB	16 GB	16 GB
Alocação de disco	**Sistema operacional:** 150 GB/**Dados:** 1 – 4 TB	**Sistema operacional:** 150 GB/**Dados:** 1 – 40 TB (máximo testado; criado para escala além de 40 TB)	
Interfaces de rede	1 – 2	3 – 15	1 – 15
Máximo de fluxos por segundo			250.000 FPS
Inspeção máxima de pacotes		Até 2 Gbps	

Requisitos e desempenho fornecidos como documentação para implantações de produção.
O Arbor Spectrum oferece suporte a outras opções para menor prova de escala de implantações de conceito.

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: +571.508.7099
nola@arbor.net

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

www.arbornetworks.com

DS/SPECTRUM/PT/0817-LETTER