

# Arbor SP Insight

Análise de big data na velocidade do pensamento para insights de rede mais rápidos e decisões de negócios mais inteligentes.

## PRINCIPAIS RECURSOS E BENEFÍCIOS

### Estende e melhora as implantações existentes do Arbor Networks SP

O valor do Arbor Networks SP é estendido e melhorado para manter o armazenamento de longo prazo e de alta fidelidade de seus dados anotados de fluxo bruto e permitir a análise visual multidimensional.

### Lago de big data fornece memória fotográfica de tráfego de rede

Armazene todos os fluxos brutos de rede, com suas anotações e metadados personalizados, pelo tempo que sua organização precisar mantê-los para análise não estruturada em tempo real ou de histórico.

### Tela única para análise ágil

Visualize as consultas complexas e as explorações casuais em formatos gráficos e tabulares a partir de uma única interface do usuário.

O Arbor Networks SP Insight se baseia na plataforma de visibilidade de rede Arbor Networks SP líder do setor, acrescentando novos recursos poderosos de big data que criam uma memória fotográfica de dados de tráfego de rede, além de uma nova análise visual para explorá-los na velocidade do pensamento. Aproveite as exclusivas anotações e enriquecimento de fluxo do Arbor SP para criar um contexto ao combinar esse contexto de memória fotográfica com sua topologia de rede, seus clientes e seus padrões de tráfego, permitindo que você conduza pesquisas ágeis e multidimensionais de dados brutos e enriquecidos com filtragem ilimitada, com a capacidade de manter a granularidade ao longo do tempo, as buscas detalhadas retrospectivas e os pivots fáceis de visualizações gráficas para tabulares, tudo isso enquanto mantém o estado no evento e no período de interesse.



A maioria dos provedores de serviços de internet, dos operadores de data centers e dos grandes operadores de rede do mundo confia na plataforma Arbor Networks SP para visibilidade ampla da rede, detecção de DDoS, engenharia de tráfego e análise avançada de rede ponto a ponto/trânsito. O Arbor SP os ajuda a manter o pico de desempenho e disponibilidade de serviços, expandir de forma inteligente sua capacidade de rede, entender seus custos operacionais e descobrir novas oportunidades de serviço. Agora, os operadores podem aproveitar o Arbor SP Insight para melhorar ainda mais sua visibilidade de rede e tomar decisões operacionais, de segurança e de negócios bem fundamentadas de forma mais rápida do que nunca.

## SP Insight melhora o desempenho de rede e os casos de uso forenses de DDoS

O Arbor SP Insight usa uma interface de usuário moderna e intuitiva, totalmente integrada ao Arbor SP, e aproveita a implantação existente do Arbor SP, garantindo fluxos de trabalho familiares e unificados, curva de aprendizado próxima de zero e nenhuma necessidade de configuração de rede adicional.



The Security Division of NETSCOUT

## Caso de uso: Cliente relata desempenho lento de rede

O Arbor Networks SP foi usado facilmente para determinar a causa-raiz desse problema. Usando um arsenal de relatórios pré-configurados, um usuário do SP pode pesquisar esse problema executando vários relatórios, como:

- Cliente por resumo, depois
- Cliente por <qualquer outro subcomponente>

Embora isso seja muito valioso, se o usuário não souber quais subcomponentes pesquisar, esse esforço pode facilmente tornar-se um processo com vários relatórios/várias telas.

Com o SP Insight, o usuário pode investigar a partir de uma única tela usando consultas flexíveis e multidimensionais e visualizações gráficas. Por exemplo, a partir do relatório de Resumo de cliente do Arbor Networks SP, o usuário clica no botão "Explorar com o SP Insight" para entrar na visualização do SP Insight.



Insight visual rápido e detalhado de problemas e origens.

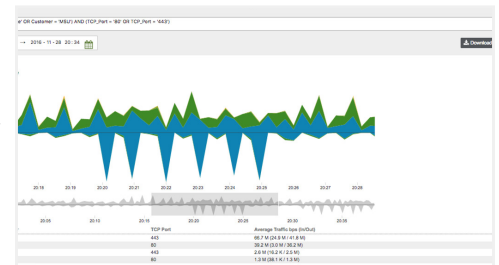
Uma única visualização do SP Insight é automaticamente carregada com um grande gráfico principal de todos os dados com base nos filtros definidos e no período desejado. Subgráficos adicionais abaixo exibem cada faceta (definida em "Contribuidores principais") dos dados filtrados acima.

Essa tela única, projetada para simplificar a análise, substitui vários relatórios do Arbor Networks SP. A partir da visualização do SP Insight, o usuário pode aplicar um número ilimitado de filtros para reduzir a um conjunto de dados estritamente definido que pode, então, ser minado até os fluxos brutos.

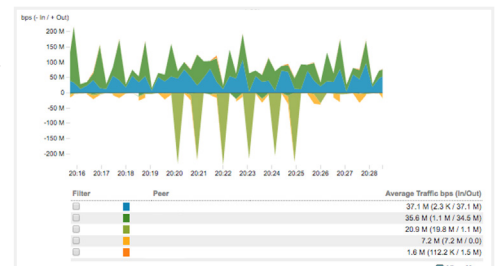
O Arbor SP Insight permite que os usuários examinem, de forma eficiente, os dados de tráfego multidimensionais e conduzam análises de causa-raiz refinadas enquanto investigam relatórios de desempenho prejudicado, reduzindo assim o tempo de resolução. A análise de hipóteses de links de rede ponto a ponto e de trânsito pode impulsionar o planejamento proativo de capacidade de rede e decisões de engenharia de backbone que reduzem custos e aumentam as receitas.

## COMO USAR O SP INSIGHT

1. No SP, use visualizações pré-filtradas em Explorar com o SP Insight (período e filtros).
2. Analise a relevância dos gráficos para sua investigação.
3. Clique em dados interessantes nos subgráficos de facetas ou adicione mais desses subgráficos.
4. Repita a etapa 2 até que sua investigação esteja concluída.



O gráfico superior mostra o tráfego por período e foi filtrado por combinações de facetas. Filtros adicionais permitem a redução em áreas de interesse específico.



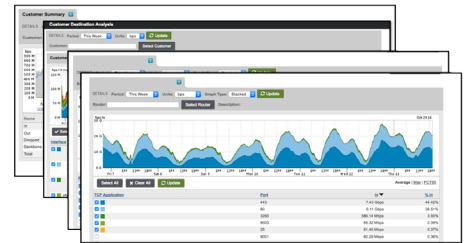
Exiba os dados filtrados por várias facetas (por exemplo, Cliente, Ponto, País, etc.) para visualizar o conjunto de dados dissecado por cada faceta. As facetas fornecem uma visualização adicional do conjunto de dados filtrados em uma única tela. Para explorar, adicionar, remover ou alterar facetas, clique em dados interessantes nos subgráficos para refinar os filtros.

## Casos de uso: Análises forenses de ataque DDoS

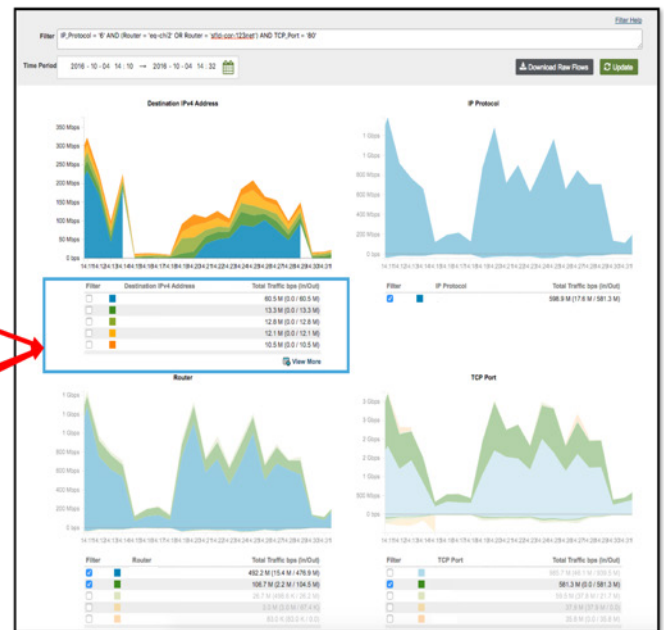
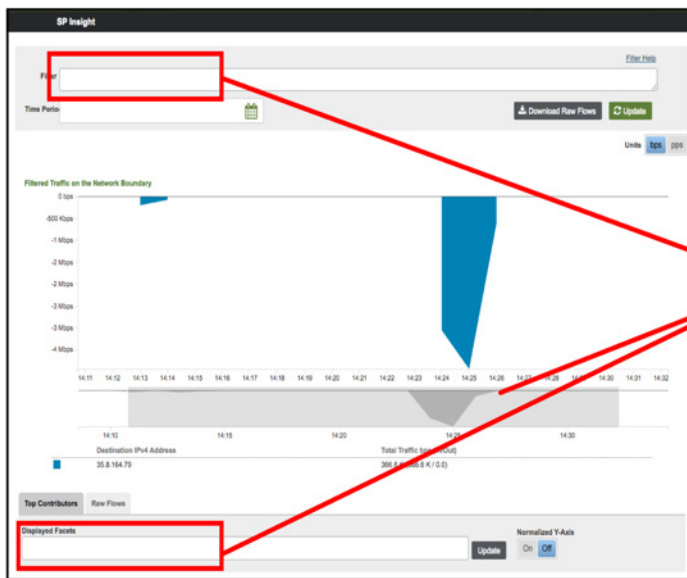
O Arbor Networks SP é incomparável na detecção de ataques DDoS. Usando relatórios pré-configurados, um usuário do Arbor SP pode começar a pesquisar um ataque DDoS a partir de um Alerta de host de DDoS com um alto volume de tráfego suspeito. Embora isso seja muito valioso, se o usuário não souber quais subcomponentes pesquisar, esse esforço pode facilmente se tornar um processo com vários relatórios/várias telas.

Com o Arbor SP Insight, o usuário pode ir diretamente do Alerta de host de DDoS, no Arbor Networks SP, para o fluxo de trabalho do SP Insight simplesmente clicando no botão "Explorar com o SP Insight". Em seguida, o usuário pode adicionar filtros à vontade, modificar filtros para fazer uma busca detalhada ou se mover lateralmente pelos dados para determinar mais informações sobre o ataque, como:

- Endereços IP dos destinos visados (Quais hosts foram mais afetados pelo ataque?)
- Intervalo de tempo expandido (Isso aconteceu mais de uma vez?)
- Portas TCP e UDP (Quais serviços foram alvo do ataque?)
- Roteadores e protocolos IP (Até que ponto o ataque foi "direcionado"?)



Com Arbor SP — uma investigação, 4 relatórios.



Uma investigação, opções ilimitadas.

O Arbor SP Insight permite que os usuários executem análises forenses de ataque DDoS de forma muito mais rápida e completa. Os usuários podem mudar facilmente entre visualizações gráficas e tabulares para investigar um alerta e um período de interesse do SP, descobrir os padrões de tráfego subjacentes e quaisquer fatores contribuintes e até mesmo expor os registros de fluxo individuais correlacionados ao evento. Esse fluxo de trabalho contínuo, combinado ao contexto de rede do SP Insight e aos dados de alta fidelidade, permite que os usuários aprendam mais sobre ataques passados, alvos e indicadores em menos tempo e se preparem melhor para eventos futuros. Os usuários liberam o potencial forense quando são capazes de filtrar e fazer a mineração dos próprios dados de fluxo.

## O QUE VOCÊ PRECISA SABER

1. O Arbor SP Insight usa uma arquitetura de armazenamento de big data para criar uma memória fotográfica de sua atividade de tráfego de rede, permitindo análise profunda e ampla.
2. As exclusivas anotações e enriquecimento de fluxo do Arbor SP (objetos gerenciados) criam um contexto no SP Insight ao combinar essa memória fotográfica com sua topologia de rede, seu cliente e seus padrões de tráfego.
3. O Arbor SP Insight melhora a visibilidade da rede e os casos de uso forenses de ataque DDoS, garantindo disponibilidade do serviço, reduzindo custos operacionais e expondo novas oportunidades de serviço.

## Comparação de Arbor SP e SP Insight

O Arbor SP Insight foi projetado para melhorar os recursos e fluxos de trabalho do Arbor SP. Juntos, eles permitem que os operadores de rede obtenham ainda mais visibilidade persuasiva da rede e conduzam análises visuais ágeis e multidimensionais em relação a uma combinação de fluxos agregados e brutos.

	GERAÇÃO DE RELATÓRIOS	FILTRAGEM	ACESSO DE DADOS
ARBOR SP	Fluxo de trabalho estruturado Pré-configurado Combinações de 2 filtros	Máx. = 2 Formato de relatório Determina a combinação Investigações estruturadas	MO - Agrupado e dependente Consultas rápidas Detecção rápida
ARBOR SP INSIGHT	Ad-hoc, interativa Combinações ilimitadas de filtros	Visualização ilimitada de filtros Visualização ilimitada de intervalos de tempo Permite combinações intuitivas	Determinado pelas necessidades de armazenamento do usuário Consultas detalhadas Fluxos brutos

## O SP Insight transforma o SP em um lago de big data

O Arbor SP Insight é um complemento para uma implantação do Arbor SP. Todos os fluxos brutos de rede, incluindo anotações e metadados do Arbor SP, são enviados ao armazenamento fornecido pelo usuário para análise não estruturada e altamente visual, em tempo real ou de histórico.

**ARBOR**  
NETWORKS

The Security Division of NETSCOUT

### Sedes corporativas

76 Blanchard Road  
Burlington, MA 01803 USA  
Chamada gratuita dos EUA: +1 866 212 7267  
Tel.: +1 781 362 4300

### Vendas na América do Norte

Chamada gratuita: +1 855 773 9200

### Europa

Tel.: +44 207 127 8147

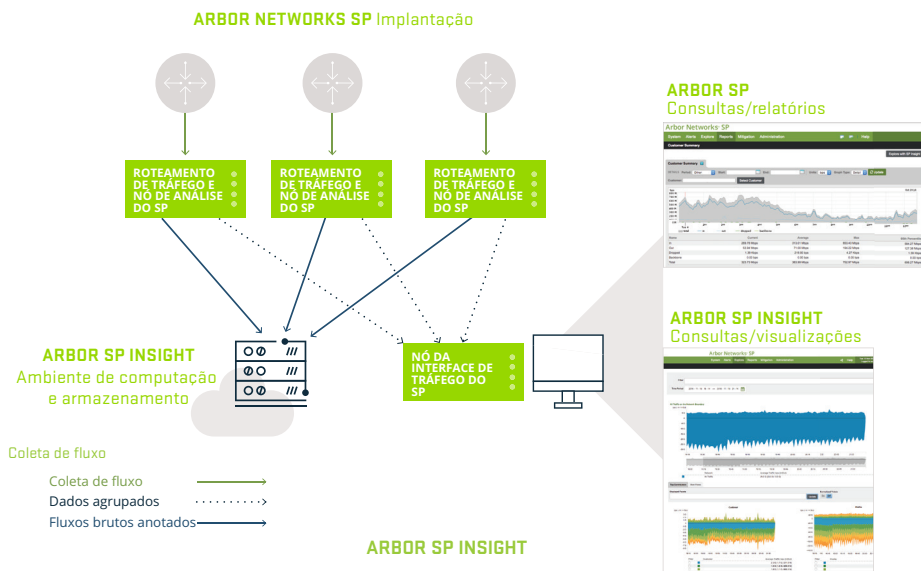
### Ásia-Pacífico

Tel.: +65 68096226

[www.arbornetworks.com](http://www.arbornetworks.com)

©2017 Arbor Networks, Inc. Todos os direitos reservados. Arbor Networks, Arbor Networks Logo, ArbOS, Cloud Signaling, Arbor Cloud, ATLAS e Arbor Networks são marcas registradas da Arbor Networks, Inc. Todas as outras marcas podem ser marcas registradas de seus respectivos proprietários.

PB/ARBORSPINSIGHT/BR/1216-LETTER



## Requisitos

- Arbor SP v8.1 com licenciamento Flex
- O SP Insight é uma extensão opcional de software do Arbor SP e exige infraestrutura externa de armazenamento e computação fornecida pelo usuário.
- A escala do ambiente de hardware de computação/armazenamento necessário é uma função de:
  - Taxas de fluxo de rede
  - Armazenamento desejado do fluxo histórico
  - Tempos e volumes desejados para consultas