

Arbor TMS

Proteção contra ameaças abrangente e comprovada e Habilitação de serviço

PRINCIPAIS CARACTERÍSTICAS E BENEFÍCIOS

Mitigação Cirúrgica

Remova automaticamente apenas o tráfego de ataque sem interromper o fluxo de tráfego comercial não relacionado a ataques.

Portfólio completo de plataformas e capacidades de mitigação

Escolha entre uma variedade de plataformas e capacidades de mitigação, incluindo: dispositivos 2U (500 Mbps–400 Gbps), chassis 6U (10–100 Gbps); virtualizados no roteador Cisco ASR 9000 (10–60 Gbps) e hipervisor KVM e VMware (1–40 Gbps).

Comando e Controle Unificado de Oito Tbps de mitigação

Escale as defesas DDoS para um nível sem precedentes. Implante até oito terabits de capacidade de mitigação agregada e gerenciada centralmente por implantação.

Facilitador de serviços gerenciados

Atenda à demanda crescente por serviços de proteção contra DDoS. Use o Arbor TMS para fornecer serviços lucrativos de proteção contra DDoS na nuvem.

Lista abrangente de ataques Contramedidas

Proteja sua infraestrutura e/ou seus clientes dos maiores e mais complexos ataques volumétricos, de exaustão de estado TCP e DDoS na camada de aplicação.

Implantação flexível

Implante inteligência na camada de aplicação, detecção de ameaças e mitigação cirúrgica em diferentes partes da sua rede para proteção de infraestrutura e serviços de proteção DDoS gerenciados mais lucrativos.

Provedores de serviços de Internet (ISPs), provedores de nuvem e empresas enfrentam um problema comum. Ataques de Negação de Serviço Distribuído (DDoS) são um grande risco à disponibilidade do serviço. O poder, a sofisticação e a frequência dos ataques DDoS estão aumentando. Operadores de data center e provedores de rede precisam de uma defesa que seja eficaz, econômica e facilmente gerenciada. O Arbor TMS é o líder reconhecido em proteção contra DDoS. Mais provedores de serviços, provedores de nuvem e grandes empresas usam o Arbor TMS para mitigação de DDoS do que qualquer outra solução.

A solução Arbor para proteção DDoS

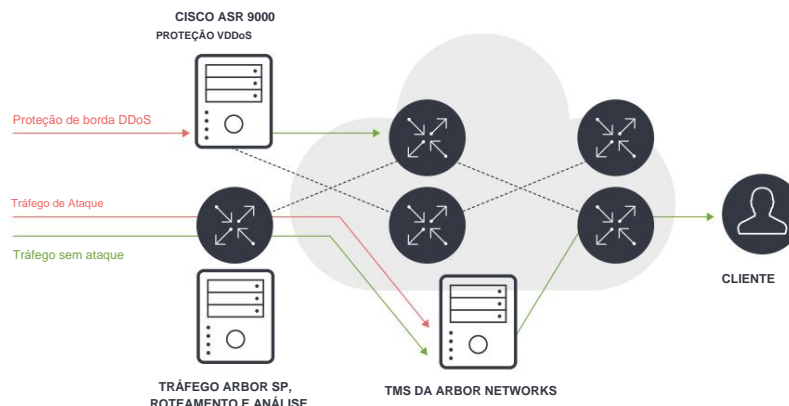
A solução Arbor integra inteligência em toda a rede e detecção de anomalias com gerenciamento de ameaças de nível de operadora para ajudar a identificar e interromper ataques volumétricos, de exaustão de estado TCP e DDoS na camada de aplicativo.

Os dispositivos de rede Arbor TMS fornecem o componente vital de depuração de tráfego da solução Arbor. O Arbor TMS pode ser implantado em linha para fornecer proteção "sempre ativa". Ao contrário de outros produtos, ele também oferece suporte a uma arquitetura de mitigação chamada "desvio/reinjeção". Nesse modo, apenas o fluxo de tráfego que carrega o ataque DDoS é redirecionado para o Arbor TMS por meio de atualizações de roteamento emitidas pela solução Arbor. O Arbor TMS remove apenas o tráfego malicioso desse fluxo e encaminha o tráfego legítimo para seu destino pretendido.

Isso é altamente vantajoso para provedores de serviços, grandes empresas e grandes provedores de hospedagem/nuvem. Ele permite que um único Arbor TMS localizado centralmente proteja vários links e vários data centers. Isso resulta em uso muito mais eficiente de mitigação e segurança totalmente não intrusiva.

Os dispositivos inline devem inspecionar todo o tráfego o tempo todo nos links que monitoram. O Arbor TMS só precisa inspecionar o tráfego que é redirecionado para ele em resposta a um ataque a um alvo específico.

O Arbor TMS vem em uma variedade de plataformas e capacidades de mitigação, incluindo: dispositivos 2U (500 Mbps–400 Gbps de mitigação), chassis 6U (10–100 Gbps de mitigação), roteador Cisco ASR 9000 incorporado (10–60 Gbps de mitigação) e hipervisor KVM e VMware de suporte virtual (1–40 Gbps).



Detecção abrangente de ameaças

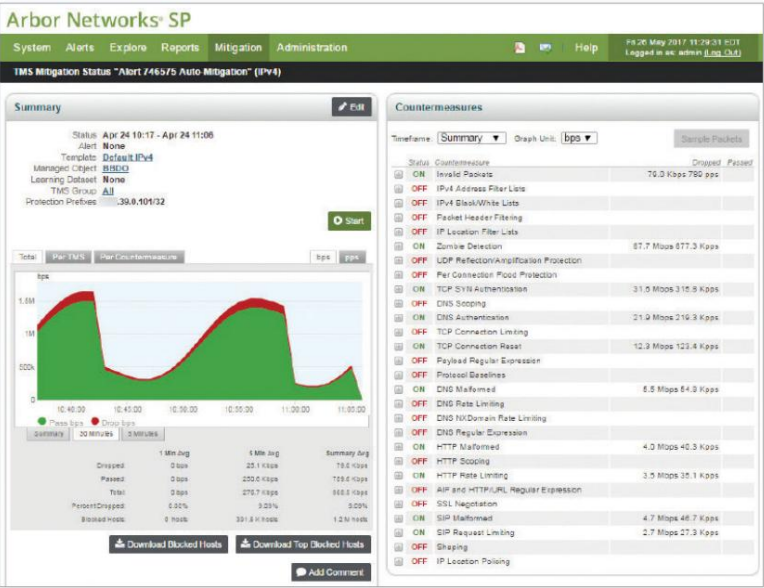
Data centers e redes públicas apresentam vários alvos para ataques DDoS. Esses alvos incluem dispositivos de infraestrutura (por exemplo, roteadores, switches e balanceadores de carga), Domain Name Systems (DNS), capacidade de largura de banda e aplicativos-chave, como web, comércio eletrônico, voz e vídeo. Até mesmo dispositivos de segurança, como firewalls e sistemas de prevenção de intrusão, são alvos de ataque. A solução Arbor fornece o conjunto mais abrangente e adaptável de recursos de detecção de ameaças do setor, projetado para proteger diversos recursos de ataques complexos e combinados. Esses recursos incluem detecção de anomalias estatísticas, detecção de anomalias de protocolo, correspondência de impressão digital e detecção de anomalias com perfil. Nossa solução aprende e se adapta continuamente em tempo real, alertando os operadores sobre ataques, bem como sobre mudanças incomuns na demanda e nos níveis de serviço.

Mitigação cirúrgica em segundos

A chave para uma mitigação eficaz é a capacidade de identificar e bloquear o tráfego de ataque, permitindo que o tráfego não relacionado a ataque flua para o destino pretendido. Ataques DDoS em larga escala afetam não apenas a vítima pretendida, mas também outros clientes infelizes que podem estar usando o mesmo serviço de rede compartilhado. Para reduzir esse dano colateral, os provedores de serviços e provedores de hospedagem geralmente fecham todo o tráfego destinado ao site da vítima, completando assim o ataque DDoS. Seja um ataque de inundação de alto volume projetado para esgotar a capacidade de largura de banda ou um ataque direcionado que busca derrubar um site, em alguns casos, o Arbor TMS pode isolar e remover o tráfego de ataque, sem afetar outros usuários, em apenas alguns segundos. Os métodos incluem identificar e colocar hosts maliciosos na lista negra, mitigação baseada em localização de IP, filtragem baseada em anomalias de protocolo, remoção de pacotes malformados e limitação de taxa (para gerenciar graciosamente picos de demanda não maliciosos). As mitigações podem ser automatizadas ou iniciadas pelo operador e as contramedidas podem ser combinadas para lidar com ataques mistos.

Painel de mitigação em tempo real

O painel de mitigação em tempo real do Arbor TMS é uma tela única que mostra aos operadores exatamente o que está gerando um alerta de DDoS e qual efeito as contramedidas estão tendo no ataque. Ele fornece a capacidade de modificar contramedidas e fornece captura e decodificação completa de pacotes para obter uma visão detalhada dos fluxos de pacotes normais e de ataque. Essas informações são armazenadas para referência futura e relatórios de gerenciamento — dando aos operadores e gerentes visibilidade total e relatórios sobre ataques em suas operações comerciais.



Painel de alertas e mitigação em tempo real.

MÚLTIPLOS MÉTODOS DE AMEAÇA DETECÇÃO E MITIGAÇÃO

Bloqueie hosts maliciosos conhecidos usando listas brancas e negras

A lista branca contém hosts autorizados, enquanto a lista negra contém zumbis ou hosts comprometidos cujo tráfego será bloqueado.

Bloqueie explorações na camada de aplicação usando filtros complexos

O Arbor TMS fornece visibilidade e filtragem de carga útil para garantir melhor que ataques ocultos não consigam derrubar serviços críticos.

Defenda-se contra ameaças baseadas na web detectando e mitigando ataques específicos de HTTP

Esses mecanismos também ajudam a gerenciar cenários de multidões repentinas.

Proteja serviços DNS críticos

de envenenamento de cache, exaustão de recursos e ataques de amplificação. Adicione maior visibilidade em Serviços DNS.

Proteja os serviços VoIP

de scripts automatizados ou botnets que exploram inundações de pacotes por segundo e solicitações malformadas, empregando recursos de detecção e mitigação de ataques específicos de VoIP/SIP.

Pare grandes ataques de reflexão/ amplificação

Como NTP, DNS, Memcached, SNMP, SSDP, SQL RS ou Chargen, aproveitando até 400 Gbps de mitigação de ataques em um único chassi Arbor TMS.

ATLAS FEED DE INTELIGÊNCIA

Aproveitando uma rede global de monitoramento de tráfego e sensores, os pesquisadores da Arbor desenvolveram o ATLAS® Intelligence Feed, uma biblioteca de defesas direcionadas que fornece proteção automática contra a grande maioria dos ataques baseados em botnet. O ATLAS Intelligence Feed atualiza automaticamente o Arbor TMS com novas proteções conforme os pesquisadores da Arbor encontram e neutralizam ameaças emergentes.

Detecção e mitigação de ataques DDoS escaláveis

O Arbor SP escala em instâncias físicas e virtuais para fornecer detecção abrangente de DDoS em toda a rede do Provedor de Serviços, da borda do cliente à borda de peering, à borda do data center (ou borda da nuvem) à borda móvel, incluindo a rede de backbone intermediária. Com essa visibilidade incomparável, os fluxos de trabalho do Arbor SP permitem uma mitigação rápida e eficaz de qualquer ataque DDoS por meio da proteção vDDoS do Arbor TMS ou Cisco ASR 9000. As mitigações baseadas em contramedidas escalam até 400 Gbps por TMS HD1000 e até 8 Tbps em uma implantação.

A lista negra desbloqueia uma camada adicional de proteção antes de quaisquer contramedidas de mitigação.

A solução de proteção vDDoS Cisco ASR 9000 usa o OpenFlow para colocar na lista negra em grande escala até dezenas de Tbps de proteção em qualquer extremidade da sua rede, protegendo assim seus links principais contra ataques.

Gestão e Relatórios Abrangentes

O Arbor TMS simplifica e agiliza as operações ao fornecer a capacidade de visualizar e gerenciar até oito terabits de capacidade de mitigação a partir de um único ponto de controle. Isso fornece a capacidade de frustrar vários ataques em larga escala e produzir relatórios abrangentes que resumem o processo de mitigação para clientes e/ou gerência.

Uma plataforma para serviços gerenciados de DDoS

A solução Arbor permite que provedores de serviços e provedores de hospedagem/nuvem forneçam serviços de proteção contra DDoS aos seus clientes. O acesso personalizado ao portal, APIs e gerenciamento delegado dão aos provedores de serviços gerenciados (MSPs) a flexibilidade e o controle para personalizar os serviços para atender às necessidades de seus clientes. A Arbor é líder indiscutível em proteção contra DDoS gerenciada. É a solução de escolha para a grande maioria dos principais serviços gerenciados contra DDoS.

Especificações de defesa DDoS do Arbor TMS

Sessões simultâneas	Não limitado por sessão	
Modos de Implantação	Ativo em linha, Monitoramento em linha, Porta SPAN, Desvio/Reinjeção	
Ações de bloco	Bloqueio de origem/suspensão de origem; bloqueio por pacote; combinação de bloqueio de origem, cabeçalho e taxa; BGP Flowspec automatizado Bloqueio de origem/destino	
Proteções contra ataques	Ataques de inundação de amplificação de reflexão (TCP, UDP, ICMP, DNS, mDNS, Memcached, SSDP, NTP, NetBIOS, RIPv1, rpcbind, SNMP, SQL RS, Chargen, L2TP, Microsoft SQL Resolution Service); Ataques de fragmentação (Teardrop, Targa3, Jolt2, Nestea); Ataques de pilha TCP (SYN, FIN, RST, ACK, SYN-ACK, URG-PSH, outras combinações de sinalizadores TCP, ataques TCP lentos); Ataques de aplicativos (inundações HTTP GET/POST, ataques HTTP lentos, inundações de convite SIP, ataques DNS, ataques de protocolo HTTPS); Ataques TLS (Inundações SSL Malformadas, Renegociação SSL, Inundações de Sessão SSL); Envenenamento de Cache DNS; Ataques de Vulnerabilidade; Ataques de Exaustão de Recursos (Slowloris, Pyloris, LOIC, etc.); Proteção de Multidão Flash; Ataques a Protocolos de Jogos	
Contramedida DDoS	Somente volumétrico Contramedidas	Conjunto completo de contramedidas
	Pacotes inválidos, endereço IP Listas de filtros, filtro preto/branco Listas, Filtragem de Cabeçalho de Pacote, Listas de filtros de localização de IP, Zumbi Detecção, Reflexão UDP/ Proteção de amplificação, por Conexão Proteção contra Inundações, Inundação TCP SYN falsificada, Autenticação TCP SYN, Limitação de conexão TCP, Redefinição de conexão TCP, Expressão regular de carga útil Filtro, Modelagem, Localização IP Policimento, Filtro Inline, Lista Negra Impressões digitais, linhas de base de protocolo	Autenticação HTTP, HTTP Malformado, Escopo HTTP, HTTP Limitação de taxa, HTTP/URL regular Expressão, Autenticação DNS, DNS malformado, escopo de DNS, Limitação de taxa de DNS, DNS regular Expressão, SIP malformado, Limitação de solicitação SIP, SSL Negociação, ATLAS Intelligence Alimentação (AIF)

13ª edição anual “Worldwide

Relatório de Segurança de Infraestrutura”

O 13º “Worldwide Infrastructure Security Report” (WISR) anual da Arbor abrange um período de 12 meses de novembro de 2016 a outubro de 2017. Para o relatório, a Arbor coletou 390 respostas de uma mistura de provedores de serviços de nível 1 e nível 2/3, hospedagem, dispositivos móveis, empresas e outros tipos de operadoras de rede do mundo todo. Ele foi projetado para coletar as experiências, observações e preocupações da comunidade de segurança operacional. Como nos anos anteriores, a pesquisa abordou tópicos como ameaças contra infraestrutura e clientes, técnicas empregadas para proteger infraestrutura e mecanismos usados para gerenciar, detectar e responder a incidentes de segurança.

Treze anos de relatórios de DDoS:

- O maior ataque DDoS relatado em 2017 foi de 800 Gbps. Isso é um aumento de 60X em relação ao ano passado. Em março de 2018, um ataque Memcached de 1,7 Tbps foi registrado. Os dados do ATLAS também mostram que a frequência de ataques extremamente grandes aumentou drasticamente este ano, já que um terço dos entrevistados deste ano relataram tamanhos de pico de ataque acima de 100 Gbps. Mais de 57% dos entrevistados de Enterprise e Data Center viram ataques que saturaram completamente sua conectividade com a Internet, acima dos 42% em 2016.
- Os entrevistados continuam observando um aumento no número de ataques DDoS; 45% dos provedores de serviços entrevistados viram mais de 21 ataques/mês; 29% dos entrevistados corporativos indicaram que sofreram mais de 20 ataques/mês.
- Os ataques DDoS continuam a aumentar em complexidade, já que 59% dos provedores de serviços e 48% das empresas, governos e educação (EGE) relataram ter visto ataques multivetoriais (ou seja, volumétricos, exaustão de estado TCP e camada de aplicação) em suas redes.

SABER MAIS

Para baixar o relatório mais recente, acesse: arborenetworks.com/report_____

Especificações do Arbor TMS 2600, 2800, 5000 e HD1000

	Árvore TMS 2600	Árvore TMS 2800	Árvore TMS 5000	Arbor TMS HD1000
Rendimento e mitigação <i>As séries 2600 e 2800 são licenças de software</i>	Licenças para 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps (complemento para 20 Gbps) até 15 Mpps	Licenças para 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps, todos até 30 Mpps	1 x APMe: Até 25 Gbps, 10 Mpps 2 x APMe: até 50 Gbps, 20 Mpps 3 x APMe: até 75 Gbps, 30 Mpps 4 x APMe: até 100 Gbps, 40 Mpps	Processamento de até oito pacotes Módulos (PPMs); Cada PPM adiciona 50 Gbps (25 Mpps) de rendimento de mitigação, Máximo 400 Gbps, 198 Mpps
Poder Requisitos	Fontes de alimentação redundantes CA: 100-240 VCA, 50/60 Hz, 12/6 A máx.; CC: -40 a -72 VCC, 28/14 A máx.	Fontes de alimentação redundantes CA: 100-240 VCA, 50/60 Hz, 12/6 A máx.; CC: -40 a -72 VCC, 28/14 A máx.	Fontes de alimentação Quad redundantes CA: 100-120 VCA/ 200-240 VCA, 50 a 60 Hz, 15 A; CC: -48/-60 VCC, 90A máx.	CA: Duas fontes de alimentação redundantes de 1500 watts; 100-240 V CA, 15-10 A, 50-60 Hz (x2); CC: Duas fontes de alimentação redundantes de 1500 watts; -48 a -60 V dc, 44 A (x2)
Poder Requisitos e Calor	325 Watts (máx.), 280 Watts (nom.): @ 280 Watts, 955 BTU/h	325 Watts (máx.), 280 Watts (nom.): @ 280 Watts, 955 BTU/h	1xAPMe: 1090 Watts (máx.), @ 610 Watts (nom.) 2081 BTU/h 2x APMe: 1125 Watts máx., @ 800 Watts nom. 2730 BTU/h 3 x APMe: 1440 Watts máx., @ 980 Watts nominais. 3344 BTU/h 4 x APMe: 1595 Watts máx., @ 1160 Watts nominais. 3.958 BTU/h	(1) MM, (5) ventiladores, (2) QSFP+, (4) QSFP28; (x1) PPM: @ 327 Watts, 1116 BTU/h; (x4) PPM: @ 569 Watts, 1940 BTU/h; (x8) PPM: @ 932 Watts, 3180 BTU/ hora
Dimensões	Chassi: altura do rack 2U Peso: 36,95 lbs (17,76 kg) Altura: 3,45 pol (8,76 cm) Largura: 17,14 pol (43,53 cm) Profundidade: 20 pol (50,8 cm)	Chassi: altura do rack 2U Peso: 39 lbs (17,7 kg) Altura: 3,45 pol (8,76 cm) Largura: 17,14 pol (43,53 cm) Profundidade: 20 pol (50,8 cm)	Chassi: altura do rack 6U Peso: Com CA: 77,15 lb (34,99 kg); Com CC: 58,52 lb (26,54 kg); Adicione 6 lb (2,72 kg) por lâmina APM-E Altura: 10,463 pol (265,76 mm) Largura: 19,00 pol (482,6 mm) Profundidade: 18,19 pol (462,00 mm) com alças	Chassi: altura do rack 2U Peso: 45,2 lbs (20,5 kg) com 1 PPM, adicione 1,6 lb (0,73 kg) por PPM (até oito) Altura: 3,5 pol (88,1 mm) Largura: 17,6 pol (449 mm) Profundidade: 21 pol (50,8 mm)
Rede Interfaces	4 portas 10G (SFP+) + 8x1G (SFP)	8 x 10 GigE (SFP+ para SR ou LR ou fibra mista)	32 x 10 GigE (QSFP+ com breakout cabos, SR4 ou 4LR); 8 x 40 GigE (QSFP+ SR4 ou LR4); 4 x 100 GigE (QSFP28 SR4 ou LR4)	4x100G + 8x10G = Um a quatro transceptores ópticos 100 GbE QSFP28 (LR) + Um ou dois 4 x 10 GbE QSFP+ (SR ou Transceptores ópticos LR Lite) com um cabo breakout 4 x 10 GbE em cada transceptor 16x10G = Um a oito 10 Transceptores ópticos GbE SFP+ (SR ou LR) + Um ou dois 4 x Transceptores ópticos 10 GbE QSFP+ (SR ou LR Lite) com um cabo breakout 4 x 10 GbE em cada transceptor
Armazenar	2 unidades SSD de 150 GB, RAID 1 2	unidades SSD de 240 GB, RAID 1 2	unidades SSD de 128 GB, RAID 1	2 unidades SSD de 480 GB, RAID 1
Temperatura operacional ambiental:	41° a 104°F (5° a 40°C) Humidade relativa (operacional): 5 a 85% sem condensação	Temperatura operacional: 41° a 104°F (5° a 40°C) Umidade relativa (operacional): 5 a 85%, (não operacional) 95% a 73° a 104°F (23° a 40°C)	Temperatura de operação: 23° a 104°F (-5° a 40°C) Humidade relativa (operação): 5% a 85% sem condensação	Temperatura operacional: 39,2° a 104°F (-5° a 40°C)

	Árvore TMS 2600	Árvore TMS 2800	Árvore TMS 5000	Arbor TMS HD1000
Regulatório	UL60950-1/CSA 60950-1 (EUA/Canadá); EN60950-1 (Europa); IE60950 (Internacional), Certificado CB & Relatório incluindo todos os desvios internacionais; GS Certificado (Alemanha); EAC-R Aprovação (Rússia); CE – Baixo Diretiva de Tensão 73/23/EEE (Europa); BSMI CNS 13436 (Taiwan); KCC (Coreia do Sul); Diretiva RoHS 2002/95/CE (Europa)	UL 60950-1 2ª edição/ CSA C22.2 No. 60950-1-07 2ª edição, Diretiva de baixa tensão 2006/95/EC, Diretiva de segurança 2001/95/EC, Certificado CB e relatório para IEC60950-1, 2ª edição e todos os desvios internacionais, FCC 47CFR Partes 15, Limite de classe A verificado, Limite de classe A ICES-003, Diretiva EMC, 2004/108/EC, EN55022, EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, EN61000-3-2, EN61000-3-3, VCCI Classe A ITE (CISPR 22, Limite de Classe A), Aprovação BSMI, CNS 13438, Segurança de Classe A e CNS13436, Aprovação KCC, Aprovação Gost, CISPR 22 Limite de Classe A, Imunidade CISPR 24, Diretiva RoHS (reformulada) 2011/65/UE	RoHS 6/6, IEC/EN/UL 60950-1, FCC Parte 15 Subparte B Classe A, ETSI EN 300 386, Marca UL, Marca CE	RoHS 6/6, IEC/EN/UL/ CSA 60950-1, FCC Parte 15 Subparte B Classe A, EN 55022, EN55024, ETSI EN 300 386, Marca cCSAus, Marca CE, KN22, KN24, Marca RCM, Marca KCC, Marca EAC, BIS, Marca CCC (pendente).
Hardware Ignorar	Externo			

TMS virtual (vTMS)

Suportado Hipervisor	VMware ou KVM em execução em qualquer distribuição Linux moderna, x86_64
Máquina Virtual Especificações	Núcleos: 3-32, RAM: 9,5-56 GB, Interfaces de mitigação: 1-8, Interfaces de gerenciamento: 1-2
Configuração Mitigação Taxa de transferência	3 núcleos sem passagem de hardware: 3 vCPU, 9,5 G de RAM, 100 GB de espaço em disco, 2 interfaces de gerenciamento virtio, 2 interfaces de mitigação virtio = 1 Gbps 3 núcleos com passagem de hardware: 3 vCPU, 9,5 G de RAM, 100 GB de espaço em disco, 2 interfaces de gerenciamento virtio, 8 interfaces de mitigação Intel 82599 PCI Passthrough = 6 Gbps 16 núcleos com passagem de hardware: 16 vCPU, 29 G de RAM, 100 GB de espaço em disco, 2 interfaces de gerenciamento virtio, 8 interfaces de mitigação Intel 82599 PCI Passthrough = 40 Gbps
NFV suportado Gestão e Orquestração	Openstack (Heat, Rastreador), Ansible, Cisco NSO/ESC, Nokia CloudBand, AWS CloudFormation



Sede Corporativa
Sistemas NETSCOUT, Inc.
Westford, MA 01886-4105
Telephone: +1 978-614-4000
www.netscout.com

Informações de vendas
Ligação gratuita nos EUA: 800-309-4804
(Números internacionais abaixo)

Suporte ao produto
Ligação gratuita nos EUA: 888-357-7667
(Números internacionais abaixo)

A NETSCOUT oferece vendas, suporte e serviços em mais de 32 países. Endereços globais e números internacionais estão listados no site da NETSCOUT em: www.netscout.com/company/contact-us