# Redes corporativas: insights globais sobre os desafios de segurança atuais

Destaques do 11° *Relatório de Segurança de Infraestrutura Mundial* anual da Arbor Networks

## Principais descobertas

**34%** Sofreram ataques DDoS, metade dos quais excedeu a capacidade total de Internet.

**29%** Relataram um aumento na frequência dos ataques.

**23%** Testemunharam ameaças persistentes avançadas (APTs).

**17%** Detectaram pessoal interno mal-intencionado.

**53%** Indicaram que dispositivos IP ou firewalls falharam ou contribuíram para uma paralisação durante um ataque.

**38%** Não possuem ferramentas para monitorar dispositivos BYOD na rede, apesar do aumento de mais de 100% nos incidentes de segurança relacionados a BYOD.

**57%** Pretendem implantar soluções para acelerar a resposta a incidentes.

**43%** Usam sistemas de mitigação de DDoS inteligentes (IDMS).

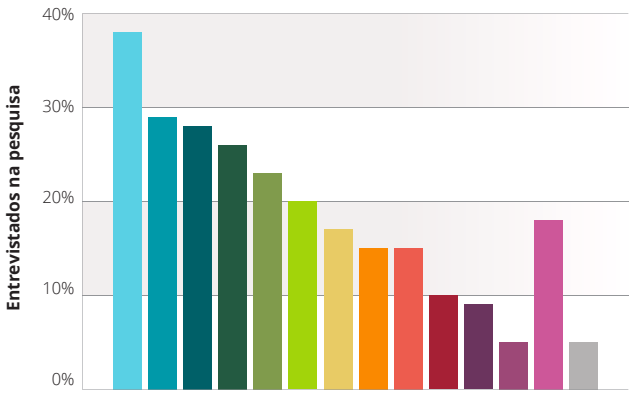
**25%** Mitigam ataques DDoS em menos de 15 minutos.

**O 11º *Relatório de Segurança de Infraestrutura Mundial* anual da Arbor Networks fornece insights sobre as ameaças de segurança de rede e técnicas de mitigação atuais. O relatório é baseado em uma pesquisa de 354 organizações representando operadores de redes corporativas e provedores de serviços em todo o mundo.**
**Ele abrange um período de 12 meses, de novembro de 2014 a outubro de 2015. Esse documento resume as respostas dos operadores de rede corporativa sobre os desafios de segurança mais críticos que eles enfrentaram em 2015 e aqueles que eles preveem no futuro próximo.**

## Preocupações e ameaças de segurança

O DDoS continua a ser a ameaça mais comum enfrentada pelas empresas entrevistadas (consulte a Figura 1). Metade desses ataques DDoS excedeu a capacidade total de Internet da rede de destino. A proporção dos entrevistados que mencionaram pessoal interno mal-intencionado e ameaças persistentes avançadas (APTs) aumentou para 17% e 23%, respectivamente. Quanto às preocupações para o próximo ano, os ataques DDoS e APT continuam no topo da lista.

**Principais ameaças de segurança de rede**




- **38%** Congestionamento na conectividade com a Internet devido a ataque DDoS
- **29%** Congestionamento na conectividade com a Internet devido a um crescimento/pico de tráfego genuíno
- **28%** Perda de dados acidental
- **26%** Hosts comprometidos por bots ou de outras maneiras em sua rede corporativa
- **23%** Ameaça persistente avançada (APT) na rede corporativa
- **20%** Interrupção acidental significativa dos serviços
- **17%** Pessoal interno mal-intencionado
- **15%** Exposição de dados confidenciais, mas não regulados
- **15%** Roubo
- **10%** Exposição de dados regulados
- **9%** Desfiguração da Web
- **5%** Espionagem industrial ou exfiltração de dados
- **18%** Nenhuma das alternativas acima
- **5%** Outros

*Figura 1 – Fonte: Arbor Networks, Inc.*

ARBOR NETWORKS
The Security Division of NETSCOUT

## Sobre a Arbor Networks

A Arbor Networks, a divisão de segurança cibernética da NETSCOUT, ajuda a proteger as redes das maiores empresas e provedores de serviços do mundo contra ataques DDoS e ameaças avançadas. A Arbor é o principal provedor de proteção contra DDoS do mundo nos segmentos de mercado de redes móveis, operadoras e empresas, de acordo com a Infonetics Research.

Nossas soluções de ameaça avançada fornecem visibilidade de rede completa por meio de uma combinação de captura de pacotes e tecnologia NetFlow, permitindo a detecção e mitigação rápidas de malware e pessoal interno mal-intencionado. Também fornecemos sistemas de análise líderes do mercado para resposta dinâmica a incidentes, análise de histórico, visualização e análise forense. A Arbor se esforça para ser um "multiplicador de forças", transformando os membros das equipes de segurança e rede em especialistas. Nosso objetivo é fornecer uma visão mais abrangente das redes e mais contexto de segurança para permitir que os clientes resolvam problemas mais rapidamente e reduzam os riscos para seus negócios.

Desenvolvido anualmente, o *Relatório de Segurança de Infraestrutura Mundial* da Arbor oferece uma visão singular do cenário de ameaças globais em evolução com base em uma série de pesquisas direcionadas a operadores de rede em todo o mundo. Para saber mais sobre os produtos e serviços da Arbor, visite nosso site da web em arbornetworks.com. As pesquisas, análises e insights da Arbor, juntamente com os dados do sistema global de inteligência de ameaças ATLAS®, podem ser encontrados no ATLAS Threat Portal.

## Descoberta, comunicação e correção de ameaças

Menos de 5% dos entrevistados afirmaram que os incidentes levavam mais de três meses para serem resolvidos. Quase 85% têm processos de notificação interna ou externa em caso de violação. Os principais mecanismos usados para acelerar a descoberta e a contenção de ameaças são novas ferramentas forenses, processos de triagem aprimorados e a integração da inteligência de ameaças à função de resposta a incidentes.

## Prontidão para resposta a incidentes

Três quartos dos entrevistados têm um plano de resposta a incidentes e pelo menos alguns recursos implementados, em comparação com dois terços no ano passado (consulte a Figura 2). No entanto, 38% não têm planos de aumentar seus recursos internos para melhorar a prontidão. Quase 50% contrataram uma organização externa para auxiliar na resposta a incidentes, especialmente na área de análise forense de TI. Somente 6% não fizeram nenhum preparativo para lidar com um incidente, contra 10% no ano passado. 57% estão considerando a implantação de soluções que acelerem o processo de resposta a incidentes, o que torna essas soluções a principal estratégia para melhorar a prontidão.

**Postura da resposta a incidentes**

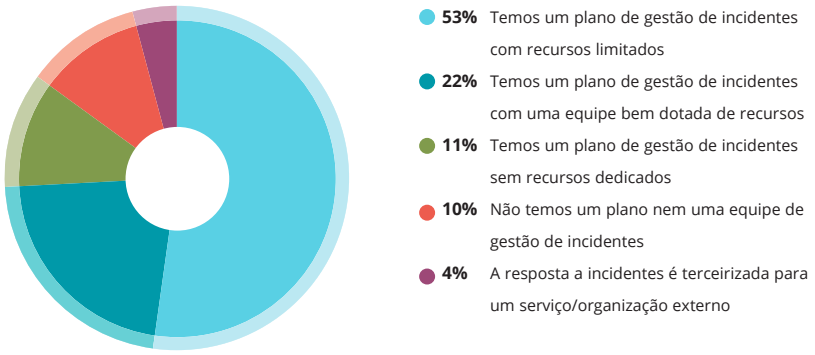



*Figura 2 – Fonte: Arbor Networks, Inc.*

## Detecção de ameaças

As ferramentas mais utilizadas para detectar ameaças são firewalls, SIEM e analisadores NetFlow. No entanto, o uso de ferramentas forenses de análise de pacotes e de tecnologias de sandbox aumentou significativamente, indicando um investimento contínuo em várias soluções pontuais para detecção. A detecção automática ainda é o método mais comum para detectar incidentes.

## Treinamento de segurança do usuário final

70% dos entrevistados acreditam que sua comunidade de usuários está devidamente informada sobre segurança básica. Além disso, 62% atualizam o treinamento de segurança de seus funcionários e exigem recertificação periódica.

## Monitoramento de dispositivos BYOD

13% dos entrevistados – mais que o dobro do ano passado – testemunharam incidentes de segurança relacionados a BYOD. No entanto, quase 40% ainda não têm ferramentas implantadas para monitorar dispositivos BYOD em sua rede. Embora a implementação de limitações de acesso para dispositivos de propriedade dos funcionários tenha aumentado entre as empresas, o uso do gerenciamento de dispositivos móveis (MDM) diminuiu 10%. Talvez seja um problema de custo, mas que precisa ser resolvido, porque o BYOD não desaparecerá.

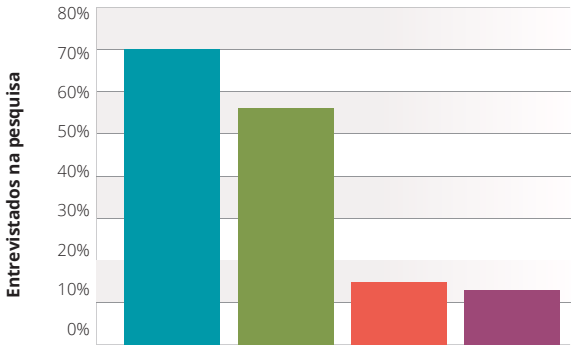
## Frequência de ataque DDoS

34% dos entrevistados testemunharam ataques DDoS durante o ano passado. No entanto, essa porcentagem varia de acordo com o setor. Para bancos e entidades governamentais, as porcentagens são maiores: 45% e 43% respectivamente. Mais de um quarto dos entrevistados observaram um aumento na frequência de incidentes. Entre todas as empresas entrevistadas que sofreram ataques, mais de um quarto sofreu mais de dez ataques por mês.

## Duração e alvos de DDoS

70% dos entrevistados sofreram ataques direcionados a serviços e aplicativos voltados ao cliente (consulte a Figura 3). Mais da metade observou ataques direcionados à infraestrutura, como roteadores, balanceadores de carga, firewalls e largura de banda da rede. Em mais da metade dos casos, dispositivos IP ou firewalls falharam ou contribuíram para uma paralisação durante um ataque, em comparação com apenas 35% no ano passado. A maioria dos entrevistados (88%) relatou ataques com duração inferior a um dia. Quase 60% indicaram que seu ataque mais longo terminou em sete horas ou menos.

**Alvos dos ataques DDoS**




- **70%** Aplicativos e serviços voltados ao cliente
- **56%** Infraestrutura
- **15%** Serviços de negócios
- **13%** Serviço de nuvem ou centro de dados terceirizado

*Figura 3 – Fonte: Arbor Networks, Inc.*

## Tipos de ataques DDoS

58% dos ataques DDoS relatados foram volumétricos e 24% foram direcionados à camada de aplicativo. Isso reforça a necessidade de uma defesa em camadas. O principal alvo dos ataques na camada de aplicativo foram os serviços da Web. Mais de 80% observaram ataques direcionados a HTTP e mais da metade ataques contra HTTPS e DNS. Quase metade observou ataques volumétricos direcionados a serviços da Web criptografados (UDP/TCP porta 443). Além disso, 37% testemunharam ataques direcionados ao serviço criptografado na camada de aplicativo e 42% observaram ataques direcionados ao protocolo SSL/TLS.

## Ataques multivetoriais

Os ataques DDoS multivetoriais combinam várias técnicas de ataque simultaneamente, direcionadas ao mesmo alvo, para aumentar a probabilidade de sucesso do atacante e a complexidade da mitigação. Neste ano, 43% dos entrevistados sofreram ataques DDoS multivetoriais em suas redes corporativas.

### Faça download do *Relatório de Segurança de Infraestrutura Mundial* de 2015 completo

Desde sua criação há 11 anos, o *Relatório de Segurança de Infraestrutura Mundial* tem sido baseado em dados de pesquisa coletados daqueles que estão envolvidos diretamente com a segurança operacional diária. Os mais de 350 operadores de rede que participaram do relatório deste ano representam um amplo espectro de localizações geográficas e focos de negócios, proporcionando um insight do mundo real sobre segurança de infraestrutura do ponto de vista operacional. Nosso relatório de 2015 captura as principais tendências nas ameaças de segurança voltadas para quatro setores principais: provedores de serviços, empresas, centros de dados e operadoras de redes móveis. Ele também revela as tecnologias que cada um desses setores está usando para identificar e mitigar as ameaças de segurança.

**Para fazer download de uma cópia gratuita desse relatório, acesse arbornetworks.com/report**

## Técnicas de mitigação de DDoS

Entre os entrevistados deste ano, os firewalls continuaram a ser a técnica de mitigação de DDoS mais comum. Seu uso, porém, diminuiu significativamente: de 72% no ano passado para 53% neste ano. Esse é um sinal positivo, uma vez que os firewalls são suscetíveis ao ataque DDoS de exaustão de estado, como evidenciado pelos 53% de empresas entrevistadas que viram seus firewalls falharem devido a ataques DDoS durante o período da pesquisa. Um aspecto positivo é que 43% agora usam sistemas de mitigação de DDoS inteligentes (IDMS), em comparação com um terço no ano passado. No entanto, somente 23% possuem uma estratégia de mitigação de DDoS em camadas, que é atualmente a melhor prática.

## Tempo de mitigação de ataques DDoS

Em uma melhoria significativa em relação ao ano passado, aproximadamente o dobro da porcentagem de entrevistados é capaz de mitigar imediatamente um ataque por meio de um serviço ou dispositivo "sempre ativado" (consulte a Figura 4). E pouco mais de um quarto consegue fazer essa mitigação em menos de 15 minutos. No entanto, não houve mudança na porcentagem de entrevistados que medem seu tempo de resposta em horas, não em minutos. Conforme as empresas se tornam mais dependentes da Internet e o tempo de inatividade se torna mais caro, a redução do tempo de mitigação torna-se cada vez mais importante.

**Tempo de mitigação de ataques DDoS**

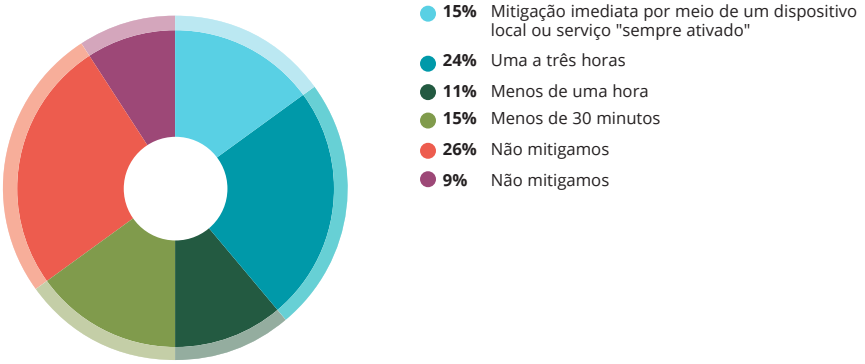



*Figura 4 – Fonte: Arbor Networks, Inc.*

## Impacto nos negócios e custo dos ataques DDoS

Quando solicitados a identificar os impactos nos negócios resultantes dos ataques DDoS, os entrevistados citaram despesas operacionais (64%), danos à reputação/marca (36%), perda de receita (30%) e perda de clientes (17%). Aproximadamente dois terços dos entrevistados estimam o impacto associado à perda da conectividade com a Internet em mais de US$ 500/minuto, com alguns indicando um custo muito maior.

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

**Vendas na América do Norte**
Chamada gratuita: +1 (855) 773-9200

**Europa**
Tel.: +44 (207) 127-8147

**Ásia-Pacífico**
Tel.: +65 6809-6226

**www.arbornetworks.com**



SR/WISR/ENTEPRISE/EN/0216-LETTER