APRIL 2015 NEUSTAR DDOS ATTACKS & PROTECTION REPORT: NORTH AMERICA

THE RISE OF HYBRID PREVENTION STRATEGIES TO OUTPERFORM ATTACKERS

neustar®

CONTENTS

INTRODUCTION

IN THIS REPORT:

HOW U.S. ENTERPRISES ARE DEFENDING AGAINST DDOS ATTACKS

Neustar's 2015 DDoS Attacks and Protection Report spotlights the risks you face, and shows how companies throughout North America are aggressively defending themselves. The major change this year is the significant increase in the use of hybrid solutions (on-premises hardware plus cloud-based mitigation).

Over 500 executives and senior professionals—IT managers and directors, CTO, CIOs and others—participated in the research. Nearly three-quarters of their companies earn over $1 billion in annual revenue.

Today, few businesses doubt that DDoS attacks are a problem.

Most everyone knows the risks of distributed denial of service (DDoS) attacks. Here are some fresh reminders from this year's research:

40% 40% of businesses say DDoS attacks are a growing threat to their organization.

32% Nearly 1 in 3 companies would lose over **$100K** of revenue per hour.

33% Named by 33% of companies, customer support is the #1 area affected by DDoS attacks.

85% Most companies attacked are hit multiple times, with 30% attacked over 10 times annually.

26% 26% of companies attacked suffer loss of customer trust and brand damage.

The question now: what mix of protection strategies works best?

Companies in numerous industries are taking strong action, and many feel they should do more. But many also struggle with choosing the right course. They seek to invest in DDoS protection that aligns with potential losses, their budgetary constraints, and technical environments.

31% 31% of businesses now use hybrid DDoS protection—a 55% YOY increase.

94% When a DDoS outage would mean peak-hour losses of over **$100K**, 94% of financial companies rely on hybrid protection.

14% Only 14% of businesses use CDNs to block DDoS.

51% More than half of businesses are investing more in DDoS protection than they were a year ago.

As the following section shows, companies rely on a number of DDoS protection options.

UNDERSTANDING PROTECTION TRENDS

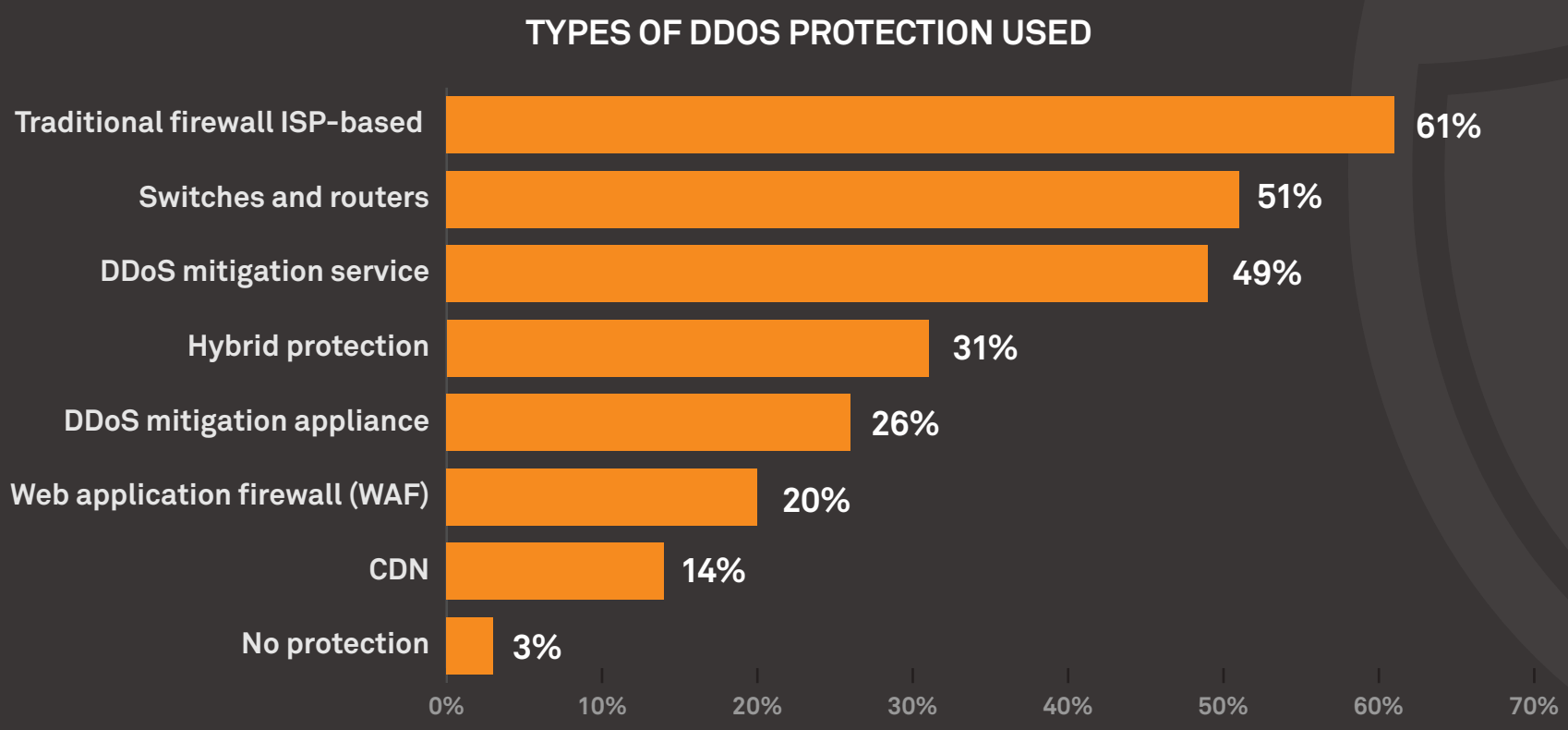
"As DDoS attack characteristics become more complex, organizations are finding value in 'hybrid' DDoS mitigation strategies, driving new alliances and acquisitions among complementary DDoS mitigation solution providers."

Gartner Research,
Competitive Landscape:
DDoS Mitigation Solutions, Oct. 2014
Sid Deshpande and Eric Ahlm, Authors

More businesses are using hybrid DDoS defense.

While the majority of companies still use firewalls to combat attacks, a significant number also use mitigation appliances, cloud-based third-party services, or hybrid solutions that combine both. Firewalls alone are not sufficient; during attacks, they often create bottlenecks and accelerate outages.

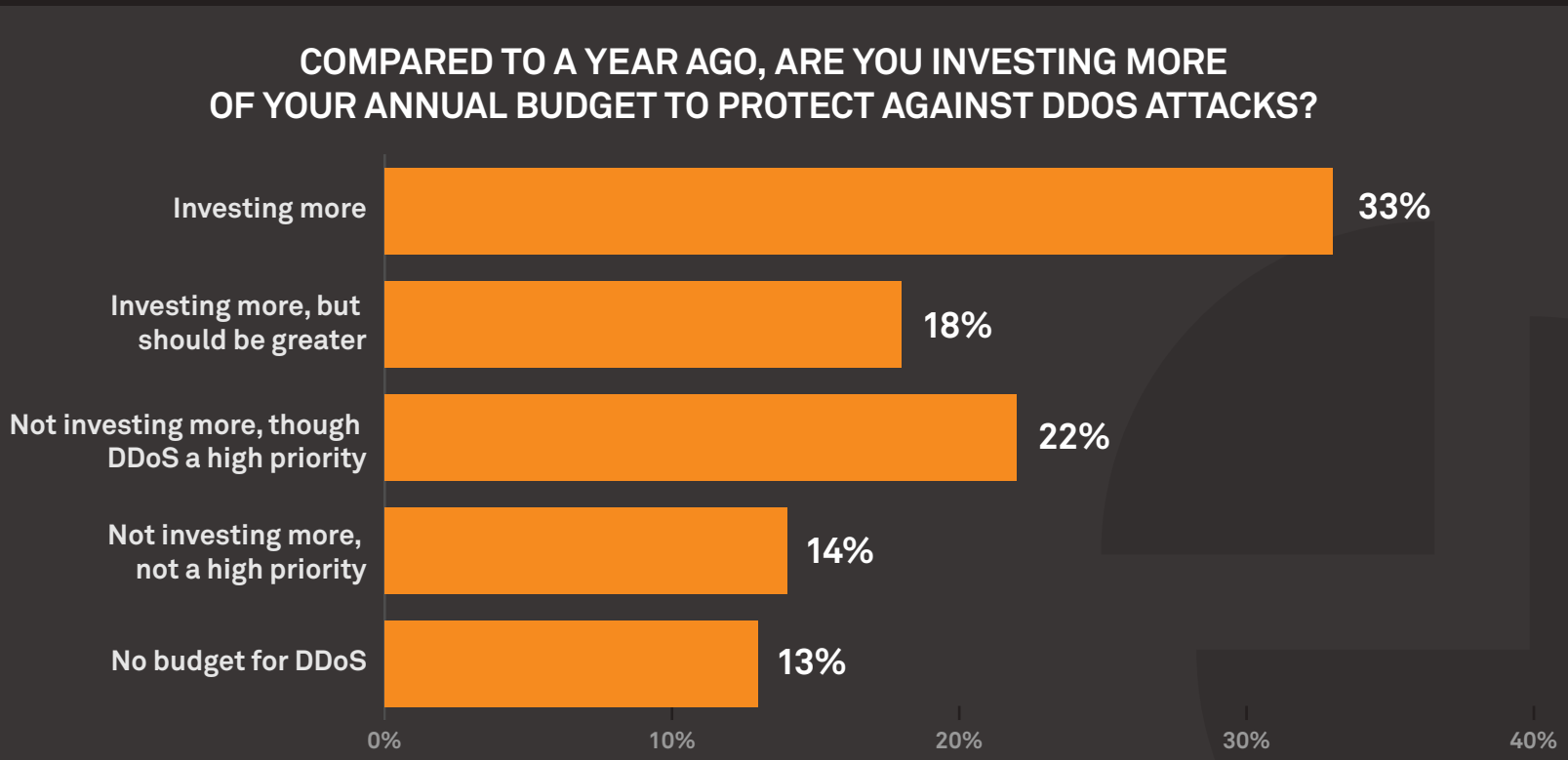
In fact, over 30% have adopted a hybrid defense. (In the EMEA version of this same report, that figure is 35%.) With always-on, on-premises hardware blocking attacks instantly, plus cloud-based traffic-scrubbing to handle larger strikes, hybrid solutions offer the best of both worlds.



*Multiple responses allowed.

Over 50% are investing more in DDoS protection versus last year.

And nearly 20% say their investment should be larger.



Investment follows risk.

Among companies whose annual revenue exceeds $500M, 51% are investing more in DDoS protection. 14% of businesses with revenues at these levels and who were attacked in 2014 experienced malware or virus installation; of this subset, 65% are investing more than last year.

THE FUTURE OF MITIGATION:

A DDoS Expert Weighs In

As one of the world's top authorities on DDoS and cyber security, Neustar's Rodney Joffe has advised the White House and federal agencies. He shared his thoughts about the future of DDoS mitigation:

"The use of website booter services, which lets anyone launch a DDoS attack for as little as six dollars an hour—has become a major source of DDoS attacks, with the sizes dramatically jumping during 2014. As such, it has become clear that that many companies are no longer able to "go it alone" when it comes to fighting off these attacks."

"At Neustar, we are working with both public and private organizations to strengthen our cyber protection as a nation. This includes working with the online community to develop industry-based mitigation technologies that incorporate mechanisms to distribute attack source information into ISPs, so they can squelch the attacks closer to the source. We also need to improve visibility and understanding of activities in the criminal underground, so their command and control structures can be disabled rapidly. Finally, it's important to improve attribution and law enforcement actions to identify perpetrators and bring them to justice."

"These improvements won't happen overnight or solve everything, but they could make a significant, positive difference."

Rodney Joffe
Neustar Senior Vice President and Fellow

A Lesson from the Financial Services Sector:

USING THE BEST OF THE BEST TO FIGHT THE WORST OF THE WORST

WHAT'S AT STAKE?

Financial companies are a prime DDoS target. Attackers sometimes take aim at banks to make a political or social statement, for example, the European Cyber Army attacks on major U.S. banks in early 2014. Also last year, the Federal Financial Institutions Examination Council (FFIEC) issued a set of DDoS protection steps for the industry to take.

43%

INVEST IN HYBRID DDoS PROTECTION
within the financial services industry.

94%

USE HYBRID WHEN BIG REVENUE IS ON THE LINE
When a DDoS outage would result in peak-hour losses of over $100K, 94% of financial companies choose a hybrid solution.

WHY? FASTER DETECTION & RESPONSE PAY OFF

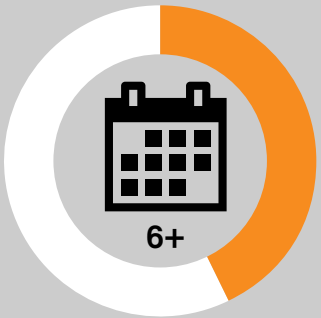
Financial companies with hybrid protection act faster to block attacks. Always-on hardware detects and mitigates immediately, even while security teams are confirming DDoS events.

88% **Detect** attacks in less than 2 hours, versus 77% of respondents overall.

72% **Respond** to attacks in less than 2 hours, versus 68% of respondents overall.

STRONGER PROTECTION FROM LARGER ATTACKS

With cloud capacity in the mix, financial companies with hybrid protection are poised to block larger attacks. Fifty percent of those able to measure attack size reported attacks of 5 Gbps or more.



43% OF THOSE ATTACKED GET HIT 6+ TIMES A YEAR

The financial sector has little choice but to be prepared.

THE BOTTOM LINE:

The financial services industry is balancing risk, impact, and investment in DDoS mitigation. Abundant data exists to make strong business cases for DDoS protection investments.

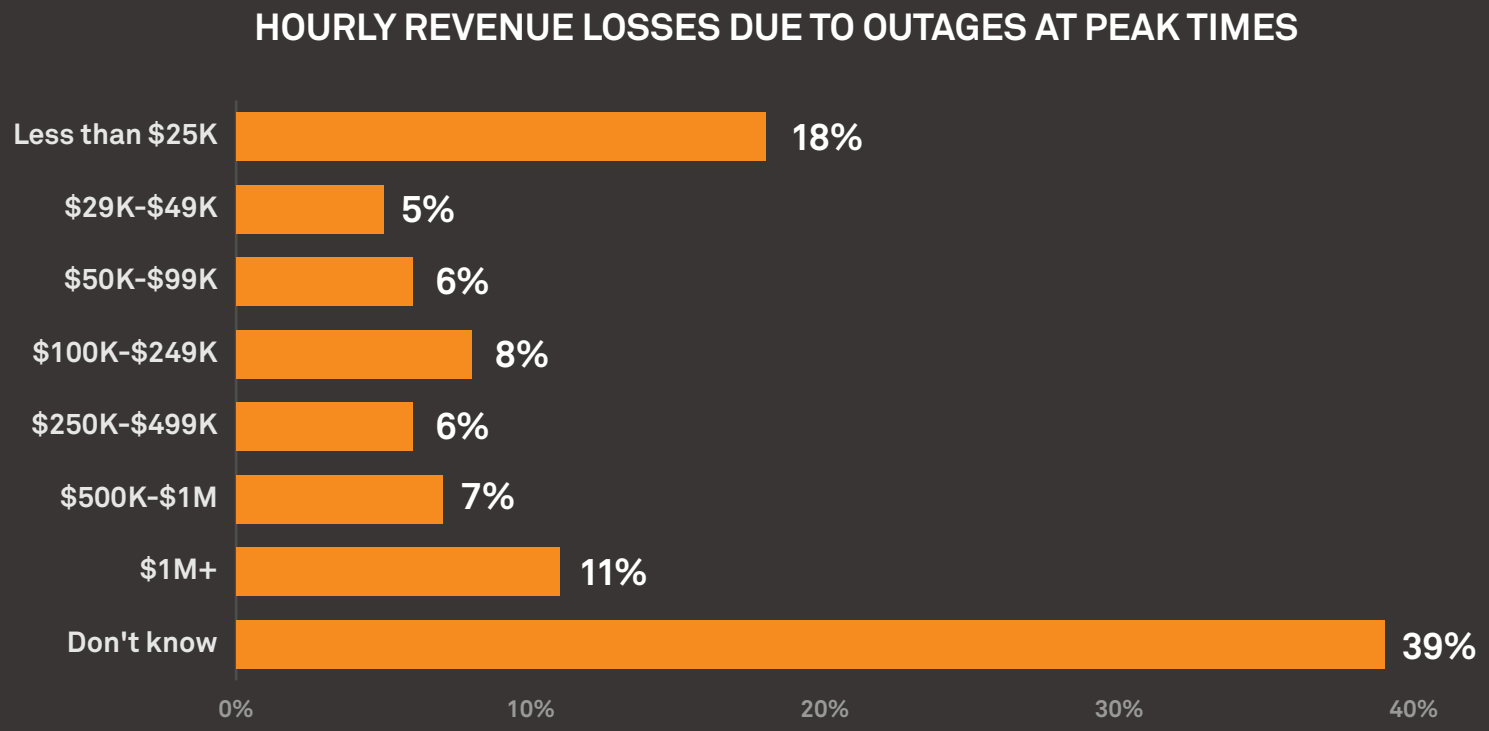
ASSESSING RISK

40% say DDoS attacks are a growing threat to their organization.

In fact...

Of those who say DDoS attacks are a smaller threat now, 46% are still investing more in protection compared to last year. This clearly indicates that organizations are more educated and committed in their approach to combating DDoS attacks. Awareness and action have moved beyond the IT department, all the way up to the C-suite.

The financial risk is great. For every hour their sites are down during peak business, 32% of companies would lose over $100K. Over 10% would lose $1M+.



A Lesson from One Gaming Company:

WHEN LIFE TURNED INTO A WAR GAME, THEY GOT MAX PROTECTION

Last year, few industries felt the sting of DDoS attacks like the video gaming industry, which suffered widely publicized outages.

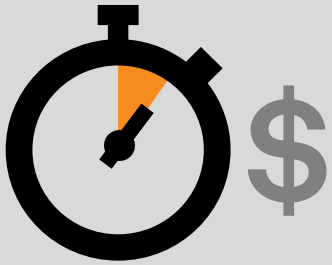
Let's put one (unnamed) gaming company under the microscope. Were they barraged like their industry neighbors? If so, what did they invest in to defend themselves?.

HOW MANY TIMES WAS THE COMPANY ATTACKED?

So often they lost count.

WHAT WAS THE SIZE OF A TYPICAL ATTACK?

10-19 Gbps
plenty big



HOW MUCH REVENUE WAS AT RISK DURING PEAK TIMES?

$100-250K per hour.

WHAT WERE THE MAJOR IMPACTS?

In its research responses, the company said it suffered ALL of these impacts:

- Damage to brand/customer trust
- Diminished call center efficiency
- Slower customer service
- Undermined online marketing

IS THE COMPANY INVESTING MORE IN DDOS PROTECTION THAN A YEAR AGO?

Absolutely, in proportion to threats.

WHAT DDOS PROTECTION SOLUTIONS IS THE COMPANY INVESTING IN?

Pretty much everything:

- Hybrid solution
- Firewall ISP-based prevention (blackholing)
- WAF
- CDN

HOW'S THAT WORKING OUT?

- Most attacks detected within 1 hour
- Most attacks responded to within 6-12 hours; below industry average, but explained perhaps by the sheer number and size of attacks and constant disruptions they caused
- Longest attack lasted 1-2 days

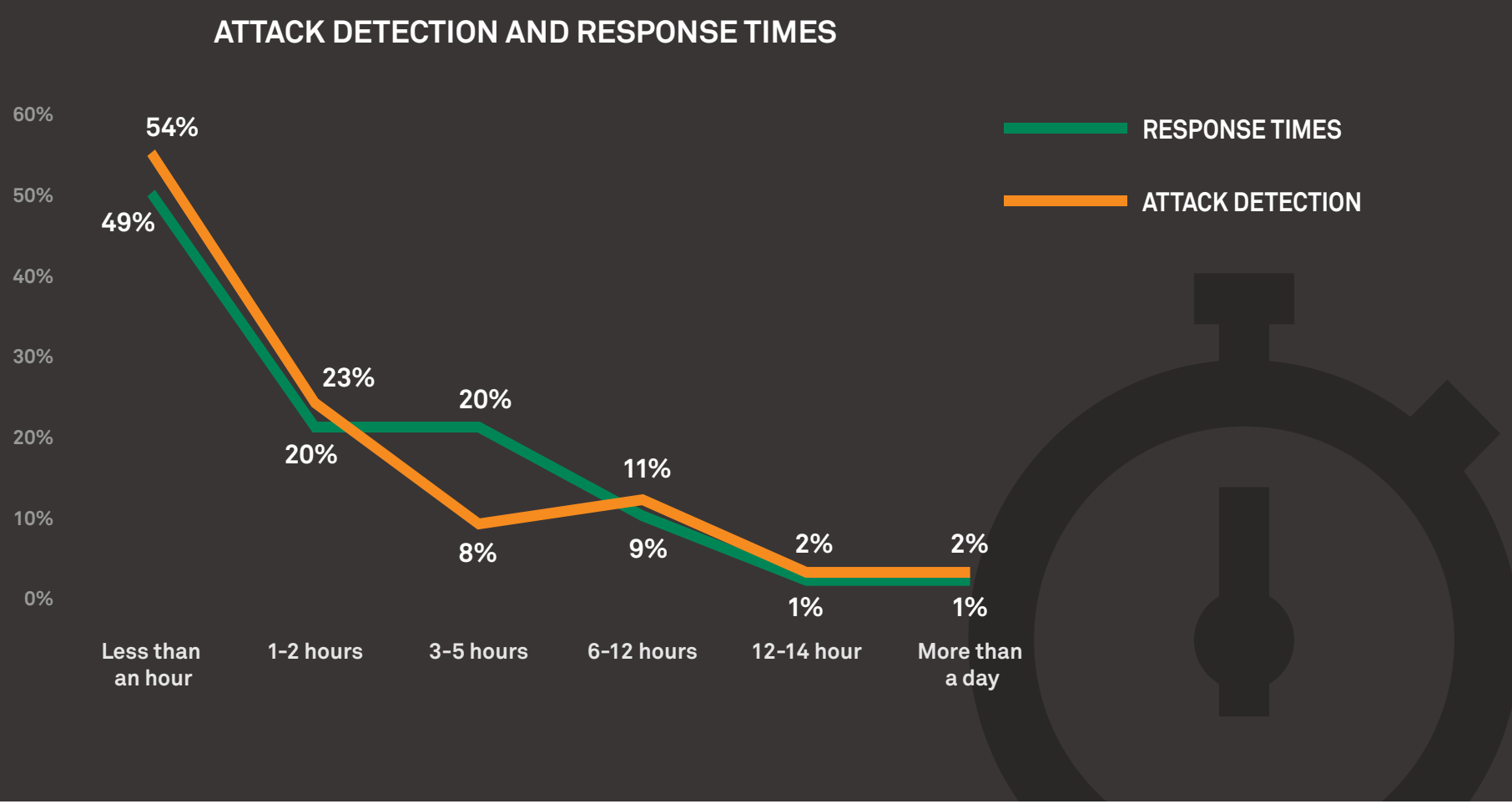
THE BOTTOM LINE:

In an industry under siege, this company anchors their defenses with hybrid and, just to be sure, layers in other solutions.

RESPONDING TO ATTACKS

45% of businesses take more than 1 hour to detect a DDoS attack.

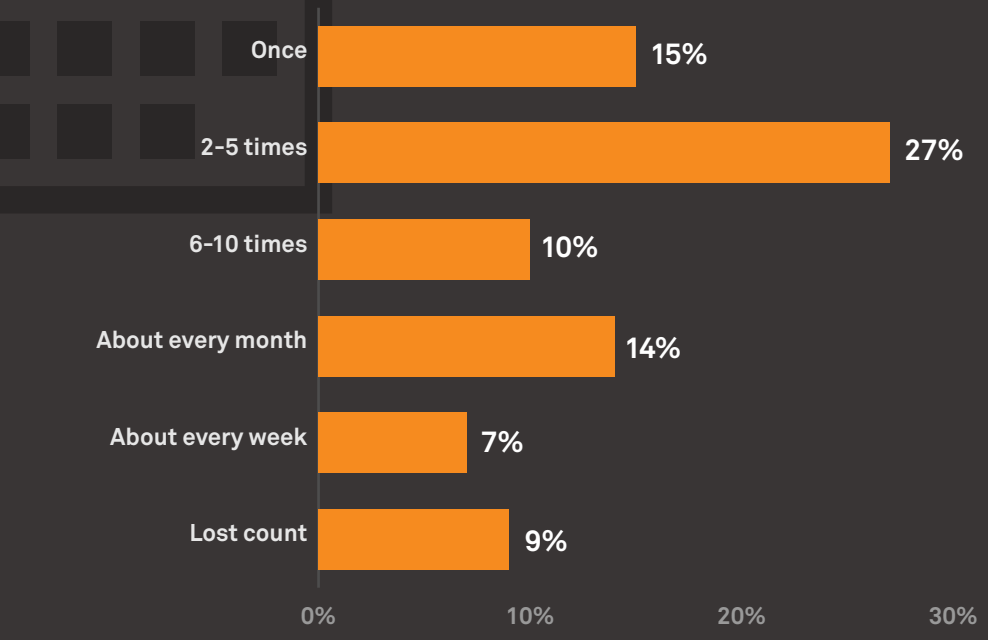
After detection, 51% take more than an hour to respond.



Among companies surveyed, 31% of their longest attacks lasted more than a day. 13% lasted over 3 days.

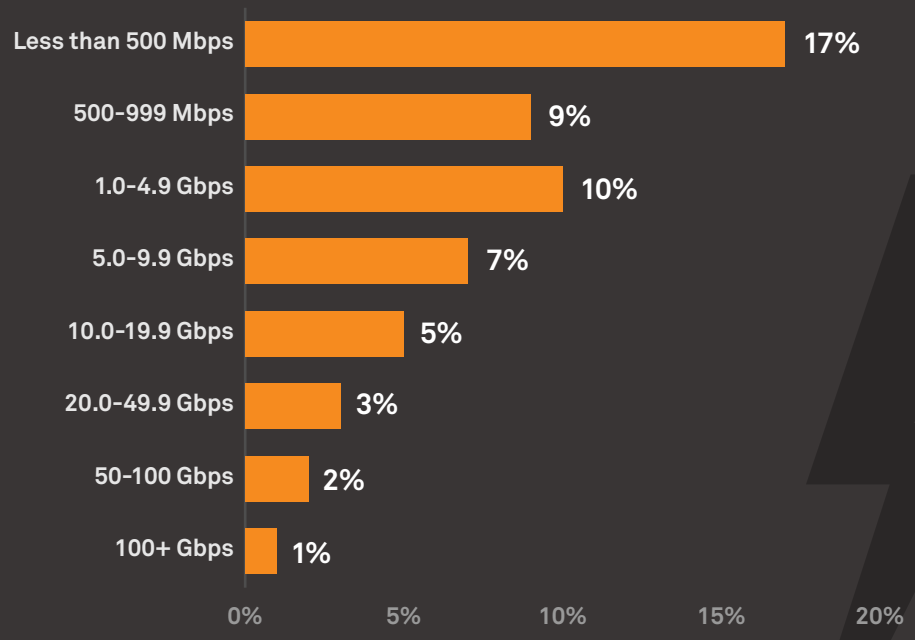
Most companies that are attacked are hit multiple times. Most attacks are large enough to disable sites with little or no protection. These realities are driving heavier investments in cloud or hybrid mitigation. Again, companies with **hybrid solutions detect and respond to attacks faster** while offering the bandwidth to counter large attacks.

ATTACK FREQUENCY
Among companies attacked in 2014



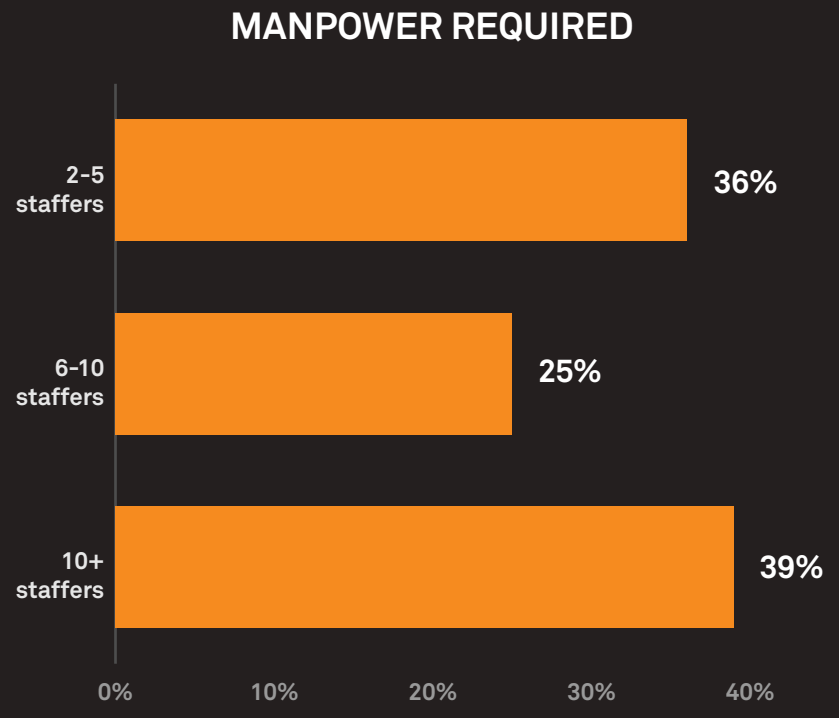
Some companies were unable to pinpoint attack frequency.

ATTACK SIZE IN BANDWIDTH
Among companies attacked in 2014



Some companies were unable to pinpoint attack size.

When attacked, 64% of businesses use more than 6 staffers to mitigate.
In fact, 39% use more than 10. Of course, attackers count on this—the more people focused on a DDoS attack, the fewer eyes watching for other threats like malware or virus installation.



A Lesson from the Tech Sector:

HYBRID IS NOW THEIR #2 MOST POPULAR DDOS PROTECTION

No wonder. Technology companies that get attacked tend to get smacked repeatedly. They're also more likely to lose big during outages—many risk losses of a quarter million dollars per hour or more during peak business.

Types of Protection Tech Companies Use

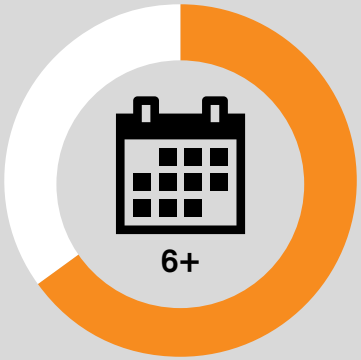
Firewalls	**53%**
Hybrid solutions	**40%**
DDoS mitigation service	**16%**
DDoS mitigation appliance	**12%**
CDN	**11%**
WAF	**5%**

*Multiple responses allowed.

OVERALL, THE INDUSTRY IS INCREASING ITS DDOS PROTECTION INVESTMENT.

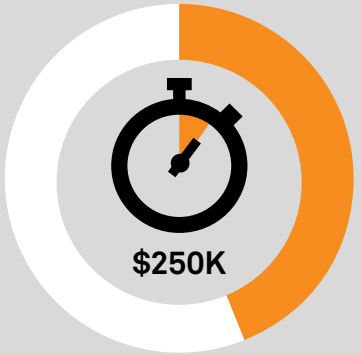
51% are investing more than they did a year ago in various types of DDoS protection.

Here's why the tech sector is embracing best-of-breed hybrid:



65%

65% of tech companies attacked are targeted 6+ times a year.



44%

Nearly half of all tech companies attacked would lose $250K+ per hour if their sites went down during prime time.

47%

Nearly half of all tech companies attacked experienced a data breach.

THE BOTTOM LINE:

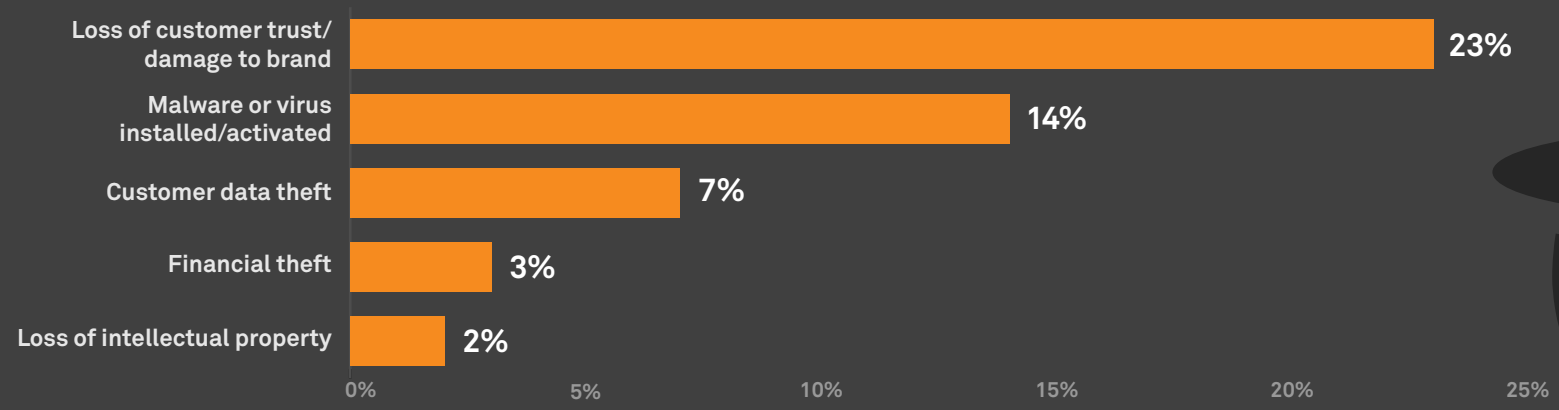
Dealing with a precarious mix of online risk and threats, tech companies not only defend with traditional firewalls but are quickly embracing hybrid as the gold standard.

MEASURING BUSINESS IMPACT

Following DDoS-related data breaches, 23% of companies report loss of customer trust and damage to the brand.

In "smokescreen" attacks DDoS is just a distraction. The real objective is installation of malware and theft.

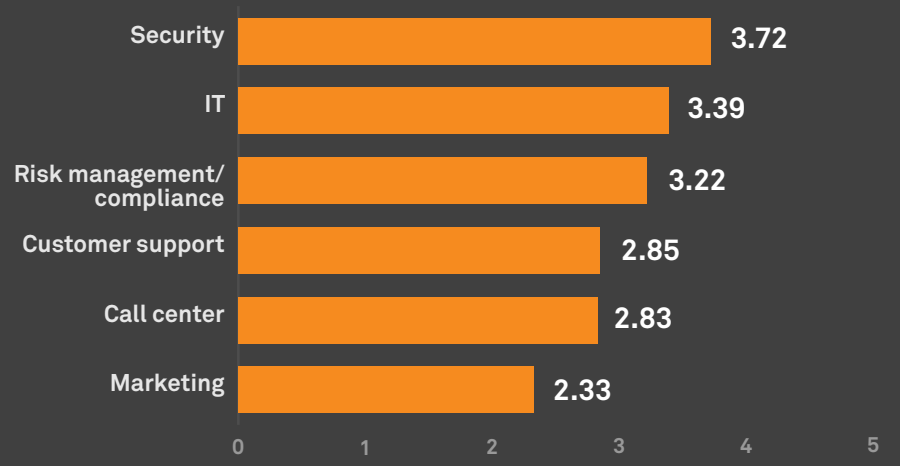
RESULTS OF DDOS-RELATED DATA BREACHES



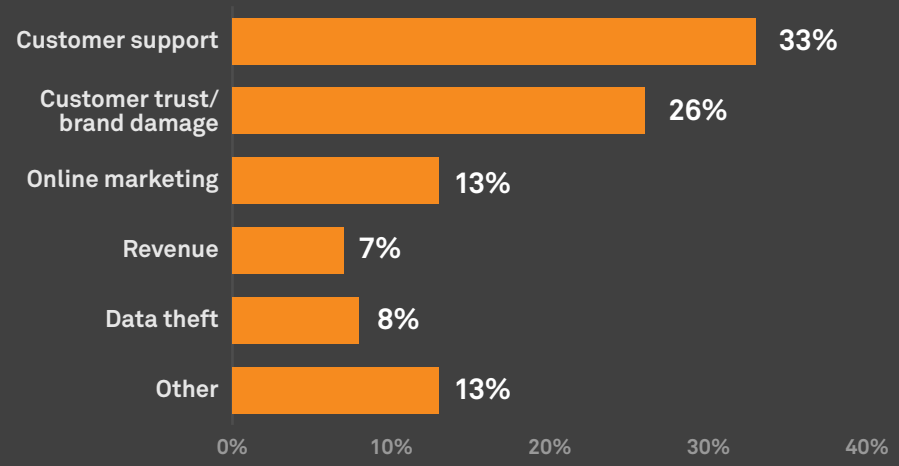
Some companies breached could not pinpoint impact.

Security and IT absorb the greatest DDoS-related cost increases. But areas strongly impacted by DDoS are found throughout the enterprise.

DEPARTMENTS WITH GREATEST DDOS-RELATED COST INCREASES (Scale of 1 to 5)



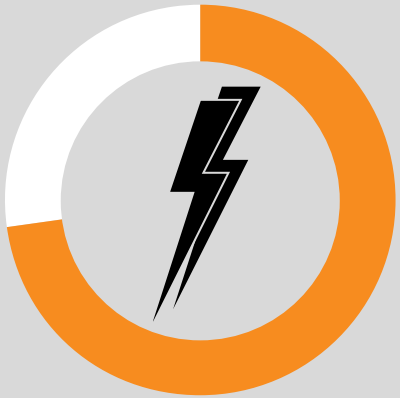
AREAS MOST IMPACTED BY DDOS



A Lesson from the Retail Sector:

REPEAT ATTACKS SPUR HYBRID ADOPTIONS

In retail, most companies are attacked repeatedly.
Most retailers also have high levels of online revenue risk.



73%

LIGHTNING OFTEN STRIKES MORE THAN TWICE.

73% of retailers attacked in 2014 were hit multiple times.

57%

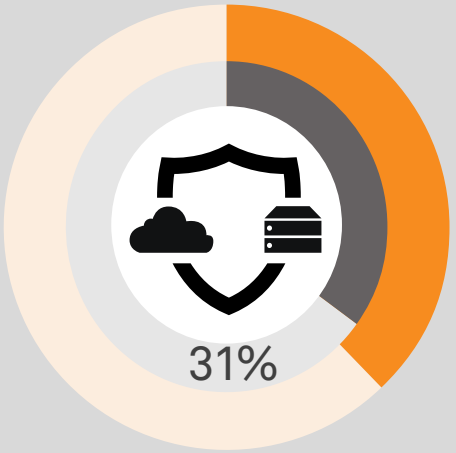
BIG TARGETS ARE FREQUENT TARGETS.

57% of retailers with $1B+ in annual revenues were attacked multiple times.

46%

A LOT TO LOSE.

46% of retailers attacked had annual revenues of $1B+.



38%

TO LOWER RISK, RETAILERS USE HYBRID PROTECTION AT AN ABOVE-AVERAGE RATE: 38% HYBRID ADOPTION.

The cross-industries average: 31%

THE BOTTOM LINE:

Faced with recurring attacks and substantial revenue to protect, retailers are adopting hybrid solutions at a brisk clip.

SUMMARY

5 KEY TAKEAWAYS FROM THIS REPORT

1. Acceptance of Threat: Most U.S. businesses are aware that the DDoS threat is real—nearly 1 in 3 would lose at least $100K due to a DDoS outage during peak business.

2. Increasing Investment: over 50% are investing more in protection than a year ago.

3. Hybrid Strategies: More companies are layering types of protection, with many (31%) adopting hybrid models. In key industries like technology and financial services, the adoption rate is higher (40% or more).

4. Outperforming Attackers: Companies with advanced mitigation solutions, such as hybrid models, are detecting and responding to attacks at a faster-than-average rate.

5. Business Impact: The impact of DDoS is felt throughout the enterprise—33% of companies say that customer support is the #1 problem.

To mitigate DDoS attacks, Neustar blends expertise, proven responses, and diverse technologies. Neustar SiteProtect, our DDoS mitigation service, offers options to meet your level of risk, budget, and technical environment: cloud-based protection; on-premise, always-on hardware; or a hybrid of both, fully managed by us. SiteProtect is backed by the Neustar Security Operations Center, whose experts bring years of experience to blocking every attack.

ABOUT NEUSTAR

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at **www.neustar.biz**.