KEY FINDINGS INTERACTIVE GUIDE

2016 IDG Connect DDoS Survey

As Attacks Intensify DDoS Defenses Require New Strategies

A10

IDG CONNECT

Introduction

IDG (commissioned by A10 Networks®) conducted a survey of over 120 North American IT/Security decision makers to gain insights into Enterprise capabilities to deal with the rise of multi-vector DDoS attacks. The study assessed how DDoS attacks impact these enterprises, steps to address such threats, effectiveness levels of existing protection solutions and perceived barriers to increased protection, desired capabilities, investment focus and desired vendor characteristics.

Survey Highlights

Survey Respondents Say:

A focus on the "worst case" scenarios is the best defense against a DDoS attack.

Attacks are becoming more complex and should not be ignored.

The effective downtime from an average attack is 17 hours.

The most effective DDoS defense solution is a hybrid approach on-premise with cloud bursting option.

DDoS leadership is primarily driven by the IT security teams and not by the Network teams.

The average peak bandwidth range of attacks is 30-40 Gbps.

Customer satisfaction is a critical metric to measure DDoS impact.

Over half of respondents plan to increase DDoS budgets in the next year.

Target Audience

Most respondents are from organizations with over 1,000 employees with 10 Gbps or more of Network Connectivity across their data centers.

Functional Focus

IT (Networking)
36%

IT (Security)
35%

IT (Management)
29%

Primary Role

50%
Technical Decision Makers

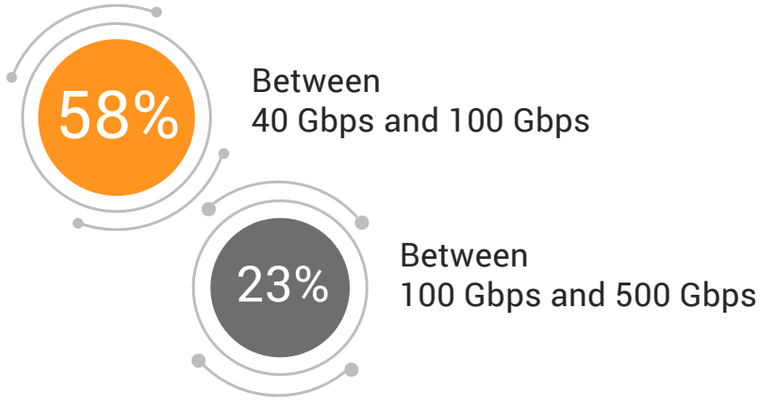
41%
Executive Decision Makers

8%
Others

Organization Size

68% 1000 - 4999 employees

Network Connectivity



Industry

The primary industries surveyed were:

GAMBLING, MEDIA/ENTERTAINMENT/RETAIL-ETAIL, AD-ECH/MARTECH

DDoS Attacks in the Past Year

NUMBER OF ATTACKS:
Respondents were aware of an average of 15 DDoS attacks during the past 12 months.

ATTACK FREQUENCY:
Highest percentage of organizations faced 1 to 5 Attacks. About a third faced over 25 Attacks.

AN AVERAGE

15 DDoS attacks

42% faced 1 to 5 Attacks

32% faced Over 25 Attacks

Average Peak Bandwidth for Attacks

Average range of DDoS attacks is 30-40 Gbps.

40%
30-40 Gbps

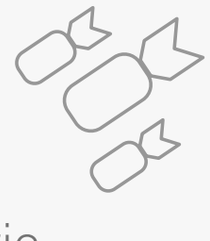
23%
40-50 Gbps

10%
More than 50 Gbps

14%
20-30 Gbps

Multi-Vector DDoS Attacks

Organizations face all three kinds of multi-vector DDoS attacks:



35% Network-Layer

34% Network/Volumetric

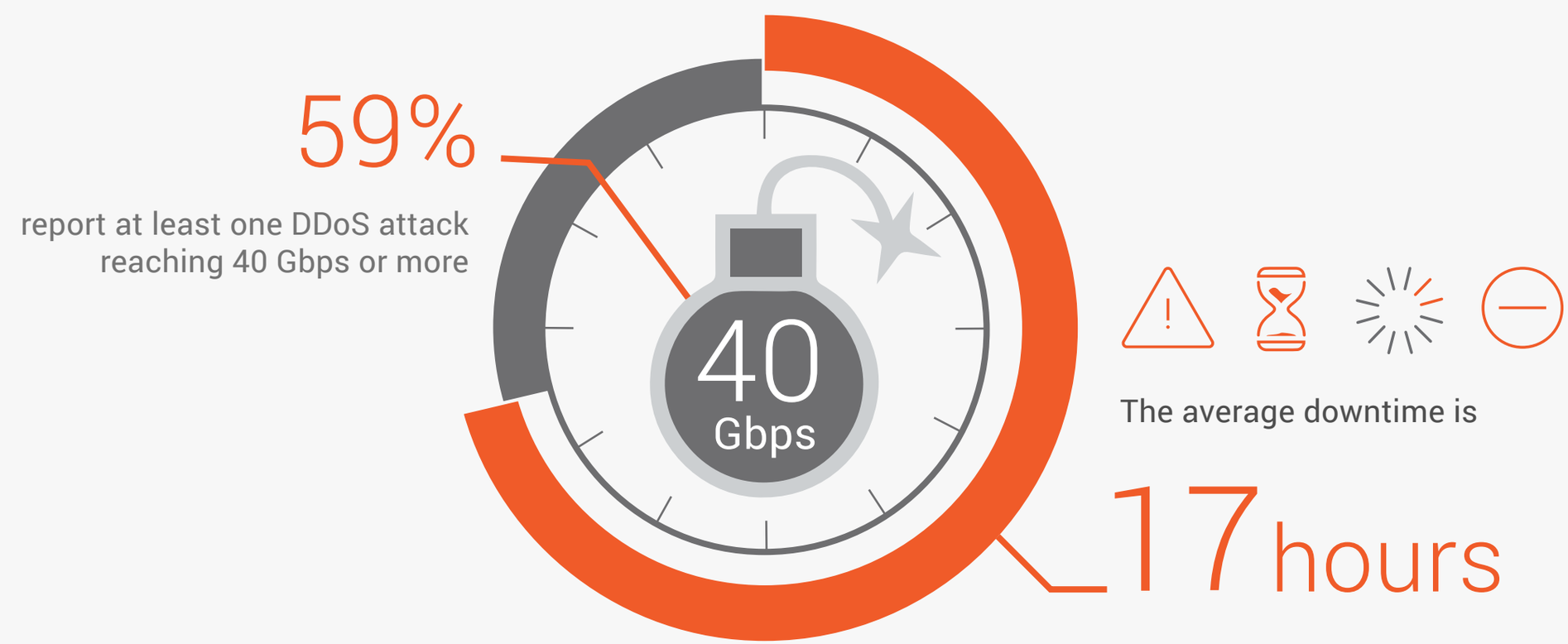
30% Application-Layer

Attack Size

While the average attack size is lower, a majority of organizations report at least one DDoS attack reaching 40 Gbps or more.

Downtime

Average effective downtime because of a DDoS attack is 17 hours.



Attack Types

23% UDP Flood (incl. DNS amplification)

16% Slow POST (Slowloris)

14% SYN Flood have the next most incidence

Most Effective Solutions

Most professionals are convinced that a combination of on and off site “Hybrid” protection (on premise with a cloud bursting option) is the most effective solution to address a multi vector DDoS threat.

34% Hybrid is the most effective solution

26% Outsourced to MSSP/Cloud-based Provider

21% Hosting Provider (including CDN)

19% On-premise Appliance

DDoS Decision Making

The research indicates that DDoS decisions are driven by Security Decision Makers. This probably occurs because the malicious intent of DDoS attacks makes it a security concern, not just a network issue.

92%

Security Teams

vs.

8%

Network Teams

Biggest Barrier

Cost of Detection and Mitigation Solutions is considered the biggest internal barrier to greater DDoS protection.

The **cost** is the biggest internal barrier

Capabilities

All features and capabilities received significant relative importance: Automated Detection and Mitigation followed by Threat Intelligence Feed are considered the most important, but makes it clear organizations are looking for a wide range of features.

18%
Automated Detection and Mitigation

16%
Threat Intelligence Feed

Impact of DDoS Solutions

Impact of new DDoS solutions is almost evenly distributed:

27% Multi-vector Protection Metrics

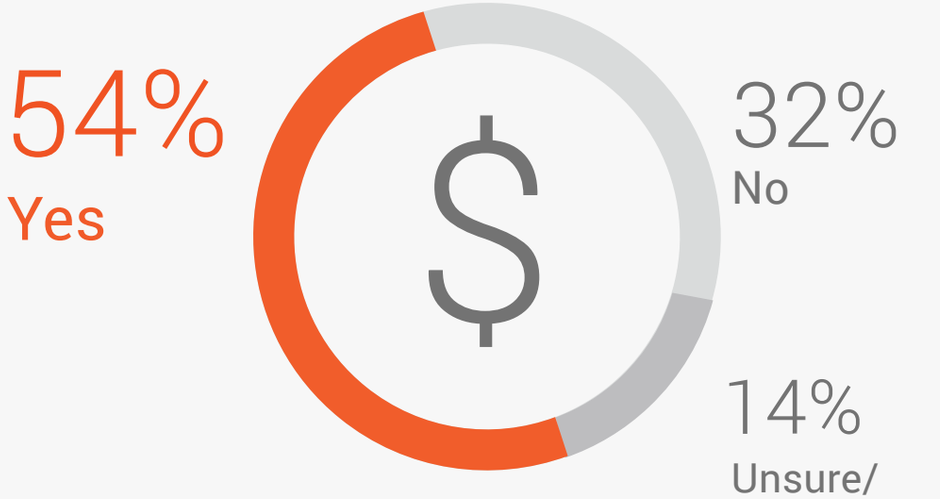
26% Throughput Performance

24% Reduced Data Center Footprint

23% TCO Savings

Budget

The majority of organizations claim they plan to increase DDoS budgets over the next six months.



Organizations that plan to increase DDoS budgets estimate a 22% increase.

Most Important Vendor Characteristics

Respondents consider Demonstrated Experience as relatively the most important vendor characteristic that makes them favor one over the other.

36%	Demonstrated Experience
19%	Known Brand
18%	Performance Guarantees
15%	Perceived Expertise
12%	Availability of Additional Services

Respondent Viewpoints

Respondents were quite vocal in their perceptions around the threat of DDoS. Here are the key statements, ranked by frequency.

93%

On Preparing for DDoS:

"A focus on worst case scenarios is the best preparation against high packet-per-second attacks."

88%

On DDoS Solutions:

"The best DDoS solutions are deep and detailed with an emphasis on factual reporting."

86%

On the Importance of Immediate Mitigation:

"An immediate DDoS mitigation of minutes is worth weeks and months of preparation."

83%

On Vendor reputation:

"The best DDoS solutions are those used by major, respected corporations who need to make an immediate, action-oriented response."

77%

On Multi-Vector DDoS Attacks:

"Multi-vector attacks, which include volumetric and application layer attacks, will be most dangerous in the future."

Key Takeaways

Organizations cannot ignore the hidden but present danger of DDoS attacks. Respondents confirm this in the frequency, magnitude and negative impact they face on an ongoing basis. From this research there are certain areas of insight that decision makers can use to avoid the disruptive impact of DDoS.

1 It's better to plan in advance than try to correct the problem after you've been attacked.

2 The true financial impact of DDoS is difficult to measure because slowdown and blocked service can go undetected without protection monitoring in place.

3 Consider protection for three reasons: lost orders, restoration of service costs and erosion of customer satisfaction levels.

4 Just because no one agrees there is a problem doesn't mean it's not there. Remember that denial and "let's ride it out mentality" are common when it comes to DDoS.

5 The best protection against multi-vector is hybrid protection (with cloud bursting option) and a preference for online mitigation.

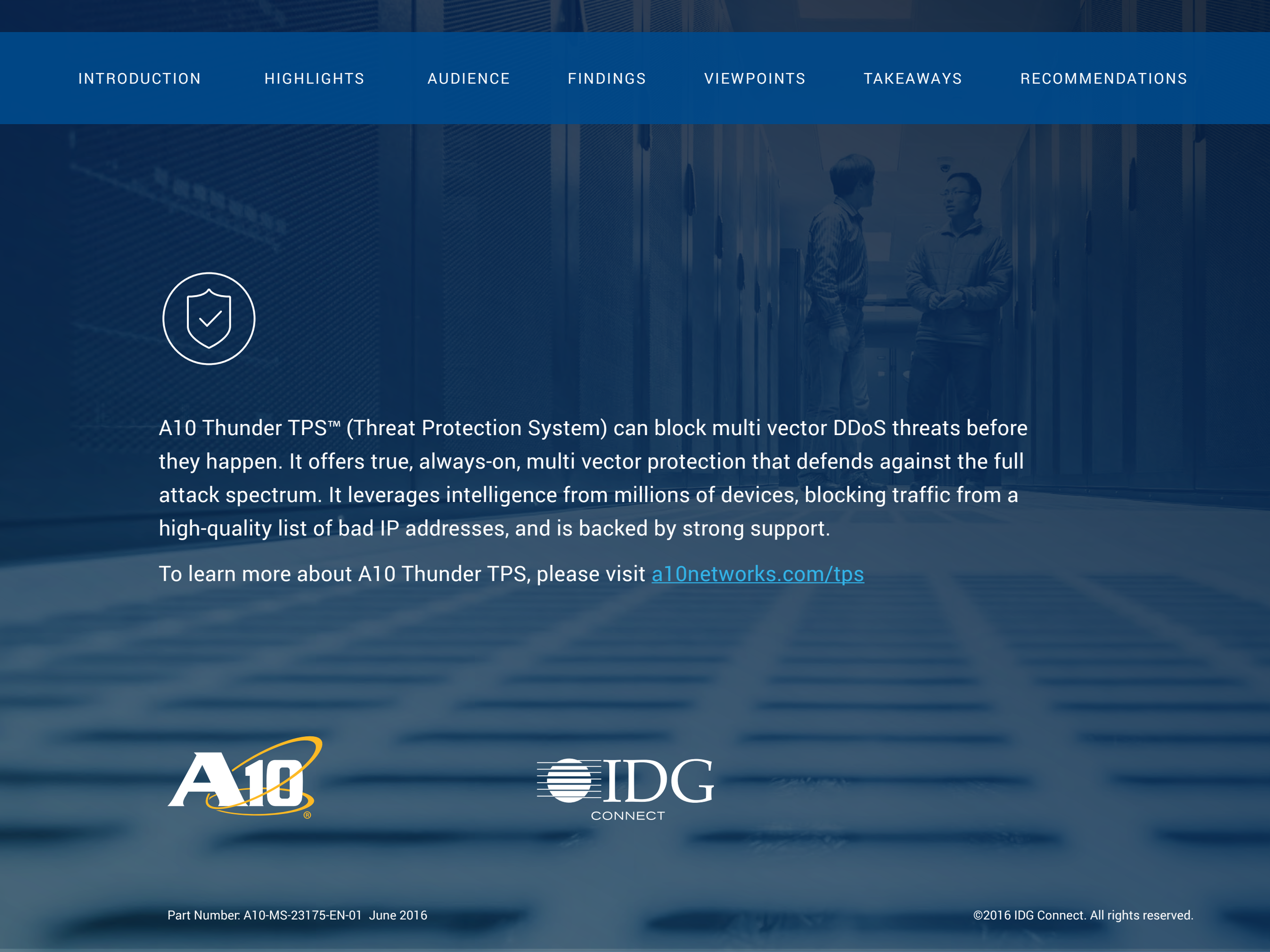
Four DDoS Strategy Recommendations

1. **Be proactive, not reactive.** Don't wait for a major crash. You may already be experiencing attacks with slowed or blocked customer access which can lose sales and/or create customer dissatisfaction.

2. **Hope for the best, but prepare for the worst**. Invest in sufficient DDoS protection early, before the organization has experienced a major attack.

3. **Beware of the "world of denial."** Ask the tough questions. What do your customer satisfaction metrics reveal? Do you see indicators of lost sales? What's the real cost of service restoration?

4. **Consider dedicated multi-vector DDoS protection** using in path mitigation coupled with integrate threat intelligence for best accuracy. Include hybrid protection with a cloud bursting service as an extra precaution to combat volumetric attacks.



A10 Thunder TPS™ (Threat Protection System) can block multi vector DDoS threats before they happen. It offers true, always-on, multi vector protection that defends against the full attack spectrum. It leverages intelligence from millions of devices, blocking traffic from a high-quality list of bad IP addresses, and is backed by strong support.

To learn more about A10 Thunder TPS, please visit a10networks.com/tps

Part Number: A10-MS-23175-EN-01 June 2016