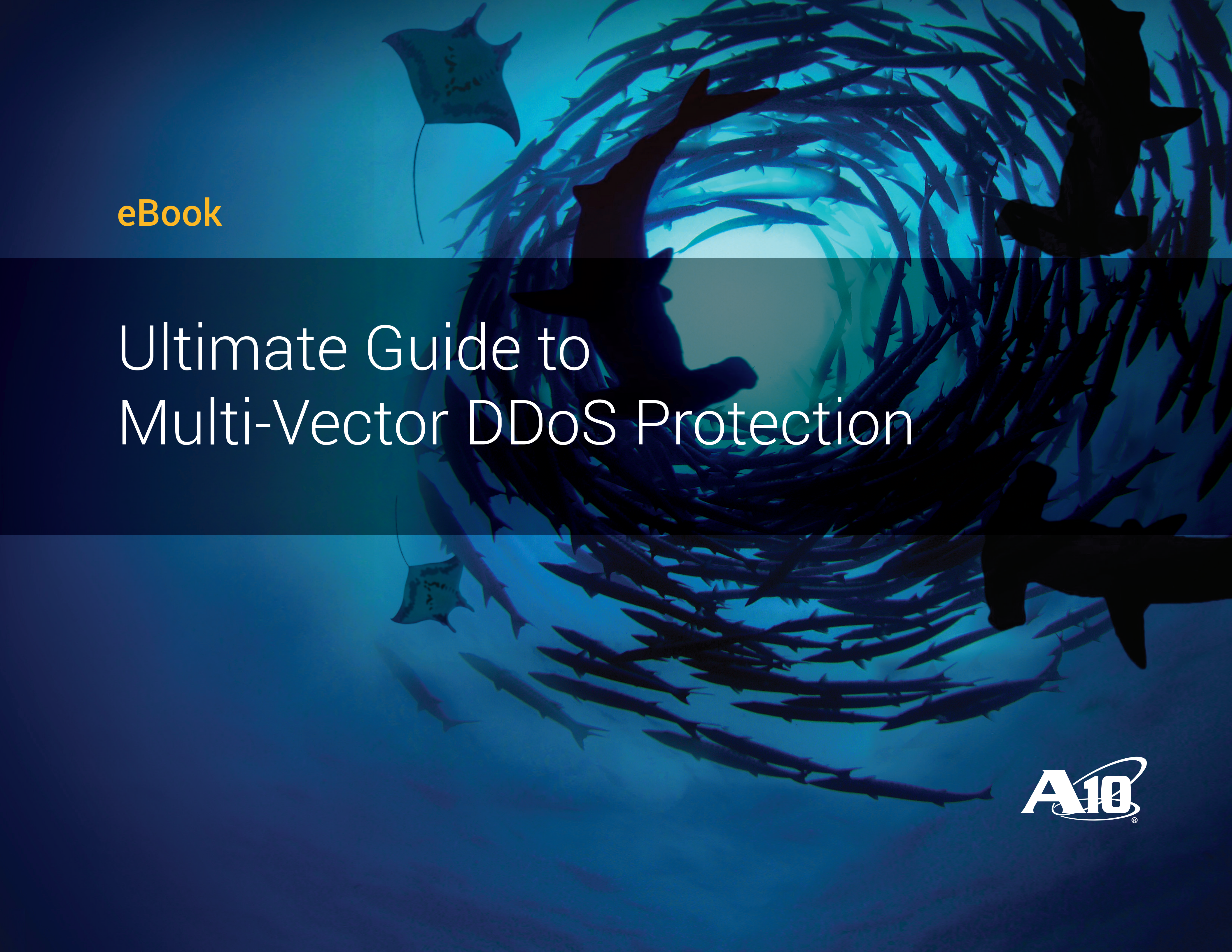
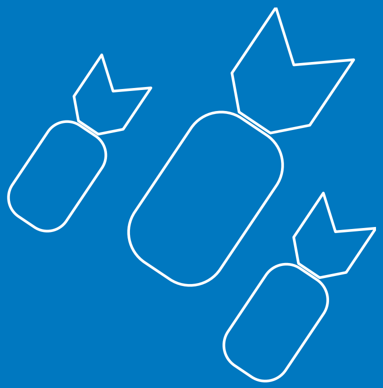


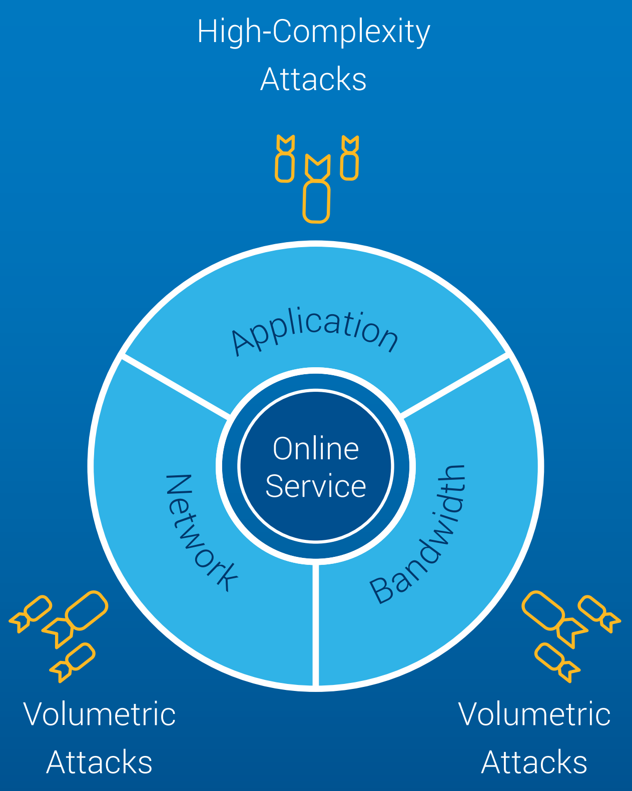
eBook

Ultimate Guide to Multi-Vector DDoS Protection

Table of Contents

What you need to know about DDoS Attacks





Highly Adaptive
Simple to Launch
Hard to Mitigate

Multi-Vector (MV) DDoS Attacks Are the New Norm

By simultaneously attacking the Network, Bandwidth and Application Layers, MV DDoS attacks have been effective disrupting the online services of organizations.

- Recent attacks like those targeting Spamhaus, Sony and Github indicate DDoS attacks are getting **larger, more sophisticated, and more destructive**.
- **3 out of every 4 DDoS attacks are now Multi-Vector** and most victims are attacked multiple times.
- MV DDoS attacks employ several techniques to target bandwidth, network devices, and applications. The combined attacks are difficult to stop and frequently overwhelm traditional DDoS defenses, consuming CPU resources rapidly.
- MV DDoS attacks find the weakest link to take down online services, which is devastating for organizations depending on their online presence for revenue.

DDoS attacks

Increased

for all vectors

Average attack

24+

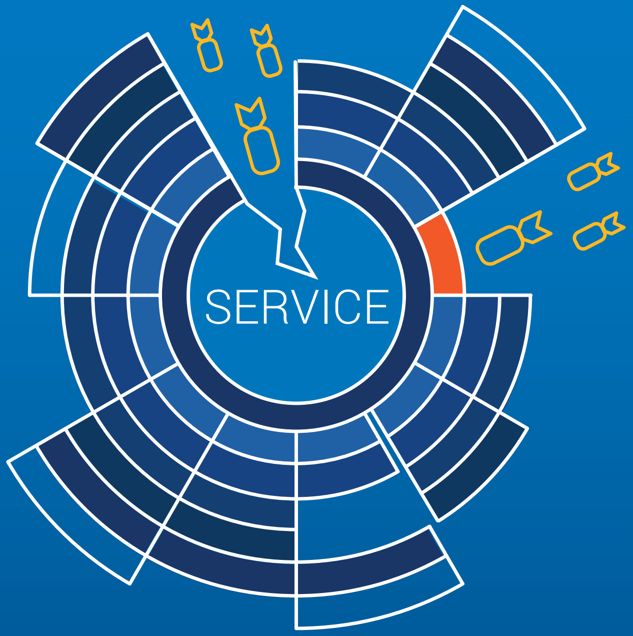
hours

MV DDoS Attacks Are on the Rise

One doesn't have to look far to see the rising risk of MV DDoS attacks to businesses everywhere:

- Network and Application layer DDoS attacks were both up sharply in Q2 2015 vs Q1 2014.
- Volumetric DDoS attacks also increased 15.5% in Q1 2015.
- At the same time, **average DDoS duration topped 24+ hours***, a nearly 19% increase over the same quarter a year before.
- In Q4 2015, a prominent MV DDoS attack was launched from the XOR DDoS botnet of infected Linux systems. It targeted the gaming sector as well as many educational institutions, demonstrating an ability to initiate up to **20 attacks per day** ranging from just a few to almost **150 Gbps in size**.

*Akamai



Ultimately, MV DDoS attacks look for the weakest link to bring the online service down

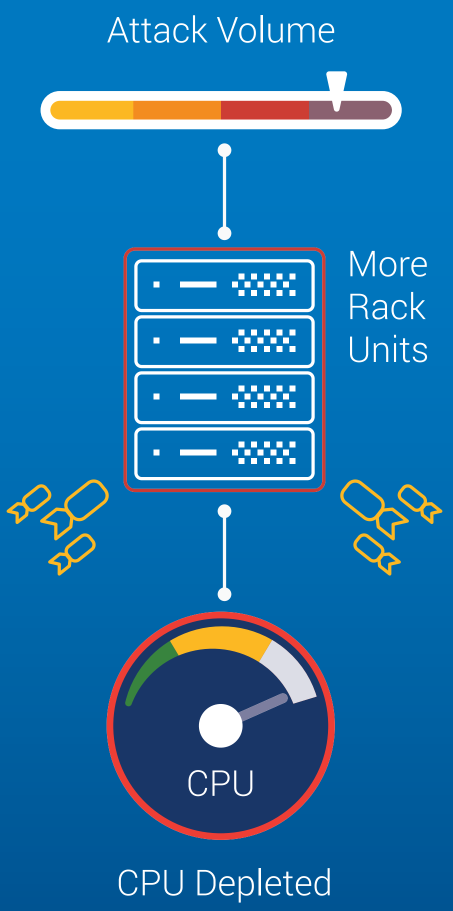
Many Possible Angles, Easy to Launch, and Difficult to Defend

The danger from MV DDoS attacks comes from their ability to explore many possible weaknesses across the network at once:

- **A volumetric attack saturates bandwidth**
- **A network infrastructure attack overwhelms devices**
- **An application layer attack drains CPU resources**

By leveraging these multiple angles, MV DDoS attacks increase the chances of the weakest one being discovered. For example, a Network layer attack by itself can be a blunt yet effective instrument against network devices; but paired with DDoS-related pressure on the application layer, it can become even more time and resource intensive for IT to deal with.

What you should know about Existing Solutions



Existing DDoS Solutions:

Inefficient

Ineffective

Not Agile

More Expensive

IT Teams Remain Challenged, Most Existing Solutions Fall Short

Volume and complexity of MV DDoS attacks overwhelm existing solutions (firewalls or legacy DDoS solutions) resulting in:

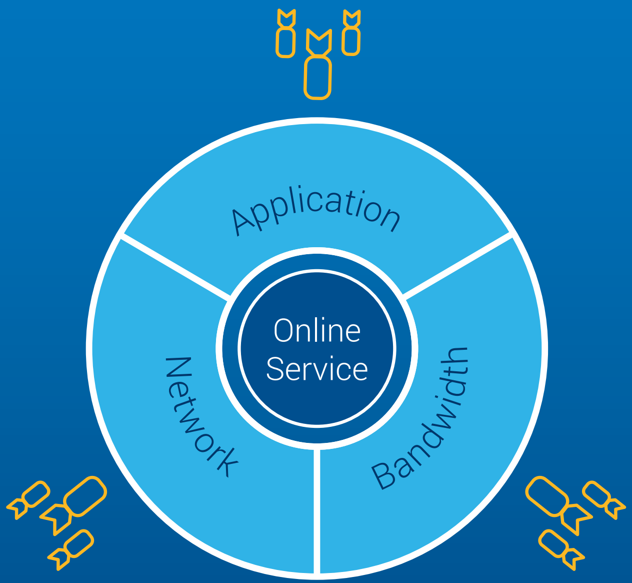
- **Rapid CPU depletion**
- **Inability to adapt quickly to new vectors** because they are not easily programmable and Dev-Ops ready
- **Poor scalability**

These shortfalls are usually addressed by adding more resources (rack units) which end up being more costly.

The need for a better and more efficient approach for MV DDoS protection is critical.

5 Things to look for in an Ultimate Solution for MV DDoS Protection

Slowloris
R.U.D.Y
HTTP GET



Fragmentation
SYN Flood
Ping of Death

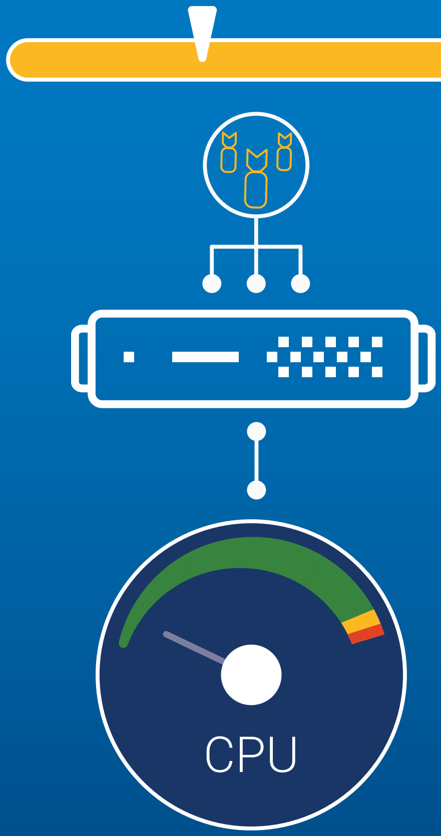
Reflection
DNS Reflection
UDP Flood/ICMP Flood

1 Support Against the Full Spectrum of MV DDoS Attacks

An ultimate MV DDoS protection solution must provide support for a wide variety of attacks that could hit simultaneously:

- Bandwidth (volumetric) attacks such as DNS/NTP reflection, UDP floods, ICMP floods, etc.
- Network Protocol Attacks such as TCP SYN floods, Ping of death.
- Application resource attacks to exhaust application resources such as Slowloris, R.U.D.Y.
- Application exploit attacks such as buffer overflows.

Offloading common attacks to hardware



Results in more CPU availability, fewer rack units and ultimately in lower costs

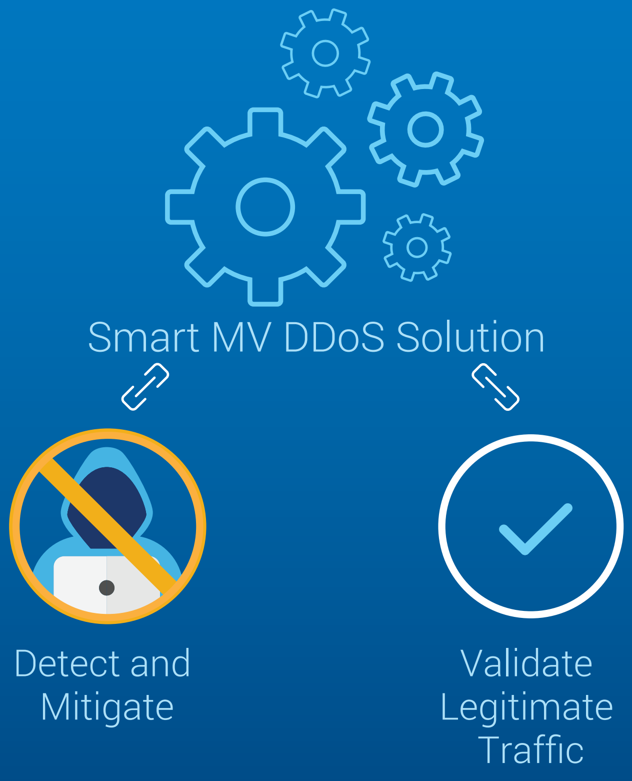
2 High Performance at a Low Cost

MV DDoS attacks are complex and adaptable, straining limited CPU resources between the high volume, low-complexity volumetric attacks and low volume, high-complexity application attacks.

Most solutions in the market respond to this by continuing to add additional processing capacity, resulting in a large data center footprint. As a result, costs just keep adding up, both to acquire new processing capacity and increased operational costs. This approach is both inelegant and unsustainable.

A more efficient approach is to **offload processing of high volume, low complexity network level attacks to purpose-built embedded hardware**, relieving the CPU resources for dealing with more complex and low-volume application attacks. All of this can be done within an efficient appliance size.

3 Smart Attack Detection and Automated Mitigation



Smart MV DDoS Solution

Detect and Mitigate

Validate Legitimate Traffic

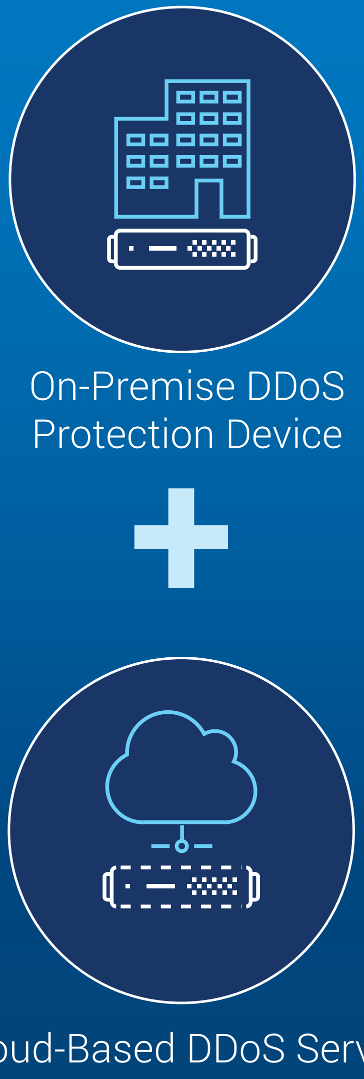
A good solution should also allow for the intelligent detection of DDoS attacks.

The solution should be smart enough to distinguish between malicious activity and traffic that might look like an attack, but is really legitimate.

To accomplish this:

- The solution should employ **network behavior anomaly detection** with progressive escalation to block MV DDoS attacks while at the same time letting legitimate traffic get through. Once an attack is detected it must be stopped.
- The system should **automatically mitigate such attacks via a dynamic policy-based system** that can be programmed in advance.

The Right Formula for Smart DDoS Solution


On-Premise DDoS Protection Device

+

Cloud-Based DDoS Service

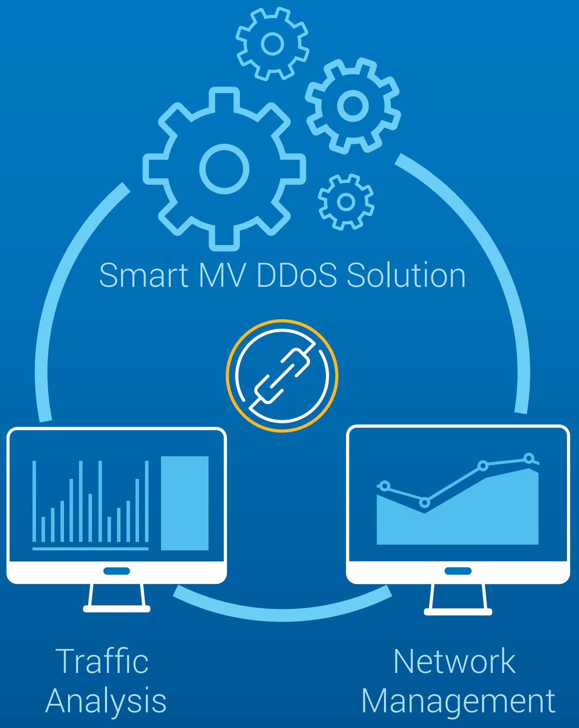
4 Hybrid Solution for Customers with Limited Internet Bandwidth

Organizations of all sizes are going to be targets of MV DDoS attacks. It's no longer a matter of if but when.

For smaller organizations with limited Internet bandwidth, large DDoS attacks can be devastating and bring their web applications to a standstill.

To prevent such a scenario, **a smart MV DDoS protection solution should leverage a hybrid approach**. An on-premise DDoS protection device detects the start of an attack and mitigates attacks until the volume exceeds the bandwidth capacity.

When this happens, the device signals to a cloud-based scrubbing service for mitigation, ensuring continued operation of the enterprise's Web operations.



Flexible Integration through Open APIs and Signaling

5 Easily Integrates with Existing Traffic Analysis and Network Management Solutions

An Ultimate MV DDoS protection solution must be open and flexible.

Enterprises already have traffic analysis and network management solutions in place that are leveraged for analysis.

A smart MV DDoS protection solution should be accessible with open APIs and signaling features, enabling it to be integrated with the systems already in place. This ensures minimal disruptions to existing solutions and faster time to deployment of the MV DDoS protection solution.

An alternative approach to

Ultimate MV DDoS Protection

THUNDER TPS
IS A TRUE MVP

✓ Efficient

✓ Flexible

✓ Comprehensive

✓ Powerful

A10 Thunder TPS from A10 Networks

The A10 Thunder TPS Threat Protection System brings many unique capabilities to the table in the fight against MV DDoS attacks.

A10 Thunder® TPS offers true Multi-Vector protection. It helps defend against the full spectrum of MV DDoS attacks, provides smart detection and automated mitigation capabilities, and is backed by A10 Threat Intelligence Service to minimize attacks before they happen.

These are some of the main features offered by A10 Thunder TPS:

- Efficiency: 1 rack unit for 200M packets per sec. Includes hardware offload to a field-programmable gate array/FPGA and features 100 GbE ports and high performance CPUs.
- Flexibility: highly programmable, full control for agile protection.
- Comprehensive: protects against full attack spectrum including 60 hardware mitigations.
- Powerful: 155 Gbps attack throughput.

To learn more visit a10networks.com/tps

Part Number: A10-EB-14103-EN-01