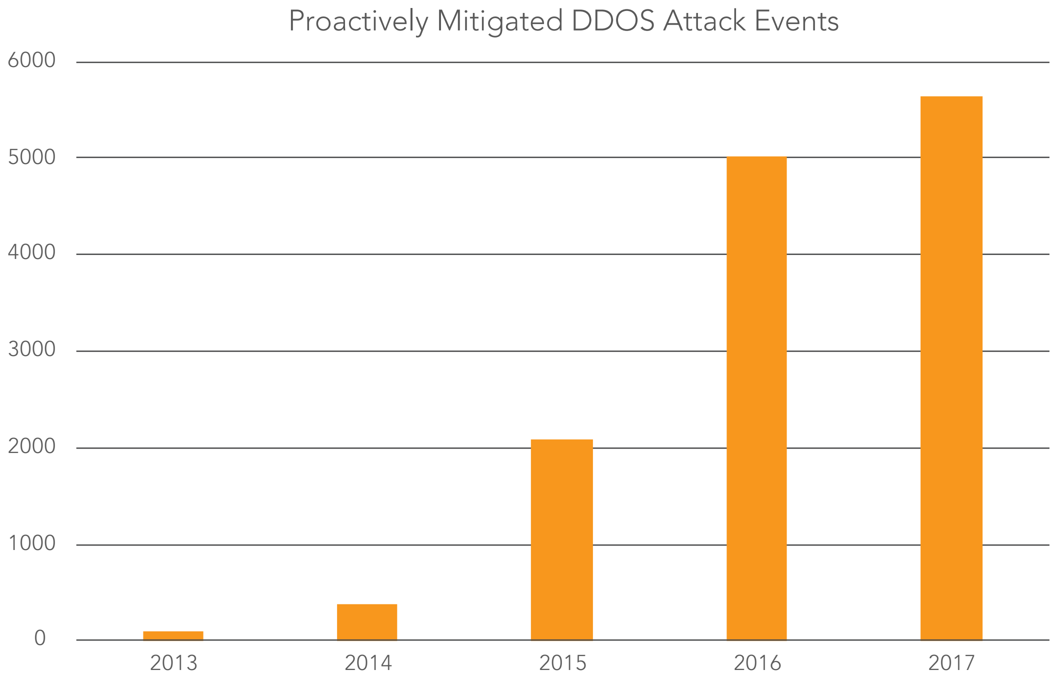
Mitigating DDoS Attacks in Zero Seconds with Proactive Mitigation Controls

Executive Summary

Akamai now mitigates the more than 65% of the 10,000-plus yearly DDoS attacks against its Prolexic platform via proactive mitigation controls, in 0 seconds and with no customer impact.

The number of DDoS attacks instantly mitigated via the Prolexic platform has increased exponentially over the past four years. We attribute this growth to our proactive engagement with customers, and the ability to implement and manage proactive mitigation postures based upon their baselined network traffic.

Akamai has been detecting and successfully mitigating DDoS attacks in an industry-leading SLA for 15 years. We will illustrate how Akamai continues to lead the industry with new capabilities including advanced customer traffic profiling and proactive mitigation controls to ensure the best possible results during an actual DDoS event.



This research covers the state of proactive mitigation with the Prolexic platform and its advantages over automated and hardware-based mitigation technologies, and describes how we manage and secure customers' mitigation policies to offer the best DDoS protection on the market today.

Terms

DDoS attack	A specific distributed denial of service attack against a customer's infrastructure.
DDoS attack event	A group of simultaneous DDoS attacks targeting a specific customer.
Proactive mitigation control	A proactive measure that is deployed in peacetime, offering the ability to block malicious traffic destined to a customer's network.
Proactive mitigation posture	The complete set of a customer's proactive mitigation controls.
Customer profile	Expected traffic mix across a customer's subnets or destination IPs, with respect to port, protocol, type, flags, TTL, etc.
Runbook	A set of instructions on how to contact customers and how to operate customers' subnets or destination IP addresses in the face of DDoS threats or attacks. This can include when to intervene and which defensive measures to take.
Service validation	The process of learning a customer's baselines and configuring their runbook.

Proactive Mitigation Stats – FY 2017

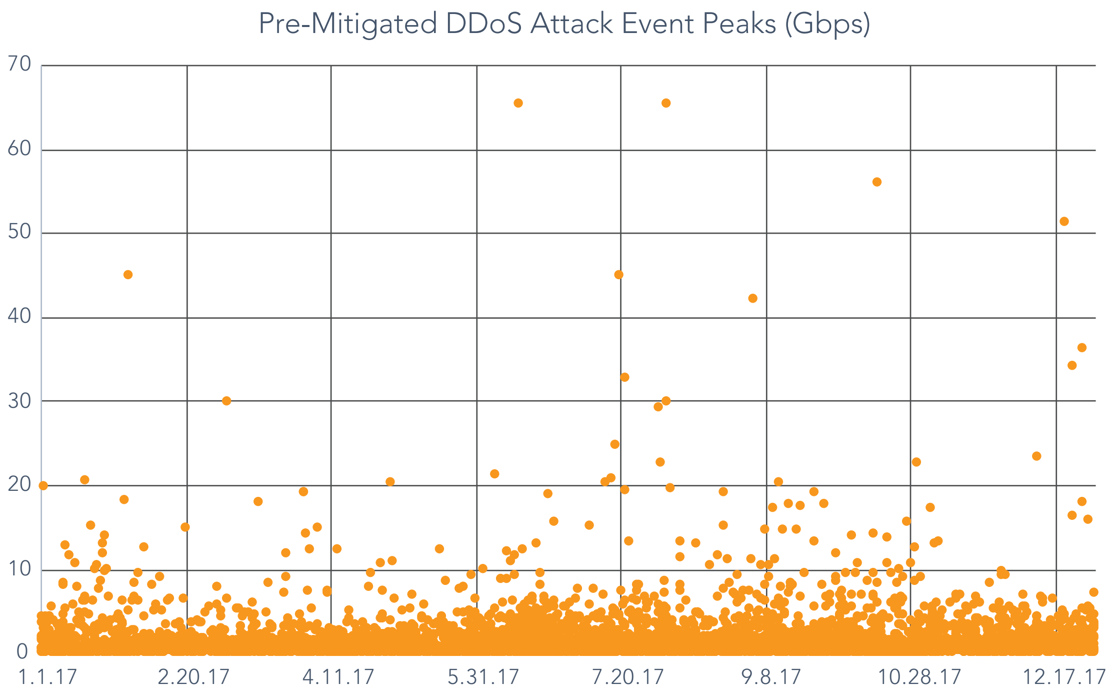
Proactively Mitigated Attacks	Mean Attack Event Peak Volume	Total Proactive Mitigation Volume
9,981	1.52 Gbps	> 1.2 Pb

Proactive DDoS Mitigation Peak Volumes

The bulk of attacks proactively mitigated in 2017 were under 10 Gbps, but there were many over that mark.

Higher-volume attacks can cause inbound link saturation and network gear overload, unless dealt with swiftly and sufficiently. Any delay or choke point during a high-volume attack can create a **backward-traveling wave** clogging a customer's upstream providers, making it more complex and time consuming to mitigate.

Pairing cloud-based DDoS protection with a proactive mitigation posture makes even large and quick-hitting attacks unnoticeable to customers.



Case Study: Proactive Mitigation of a Record Attack

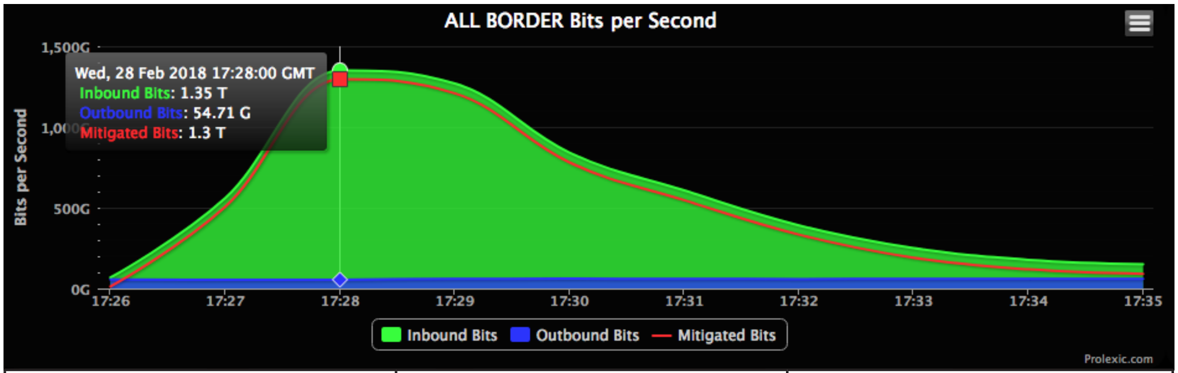
On February 28, 2018, an attack peaking at 1.3 Tbps was proactively mitigated by the Prolexic platform.

An on-demand customer was under a massive attack when it engaged the Prolexic SOCC (Security Operations Command Center) and initiated procedures to rapidly re-route traffic and enable the Prolexic protections. Until the BGP (Border Gateway Protocol) announcement propagated across the Internet, the customer's site was down. Once the customer's prefix was successfully routed on to the Prolexic platform, end users and the customer were no longer affected by the attack

This attack vector had first been spotted in the wild only a few days prior. It was seen seven times, across a number of customers and industries on the Prolexic platform, of which five had been proactively mitigated by customers' proactive postures. Akamai's SIRT and engineering teams were engaged to assess the risk and recommend proactive steps, which resulted in global mitigation controls being deployed by the SOCC.

This was a relatively unusual step, reserved for extremely dangerous vectors. When the customer routed its traffic onto the Prolexic platform, the attack against the customer essentially hit a defensive shield at Akamai's scrubbing centers around the world.

The attack was instantly mitigated, which can be seen below, while the customer's normal clean traffic was passed back to the customer origin, without impact.

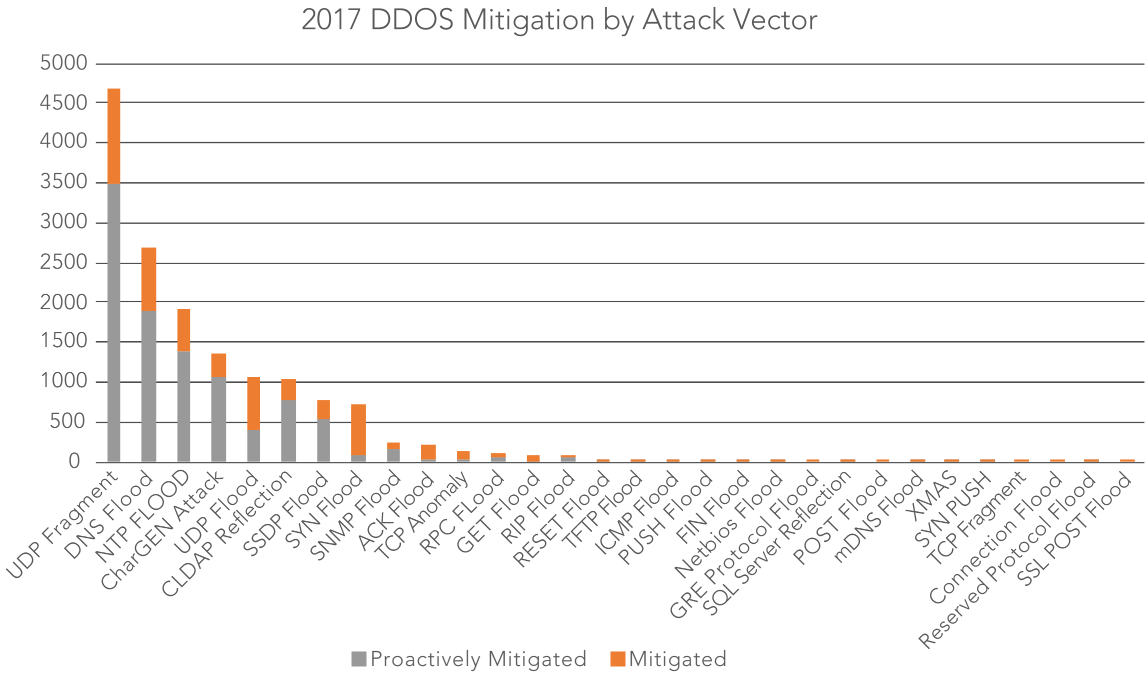


Green Area	Red Line	Blue Area
Total inbound traffic to Prolexic service	DDoS Attack traffic mitigated	Legitimate traffic delivered to customers

In addition, the network monitoring company, Thousand Eyes, published a detailed **write-up** on this event.

Proactive DDoS Attack Vectors

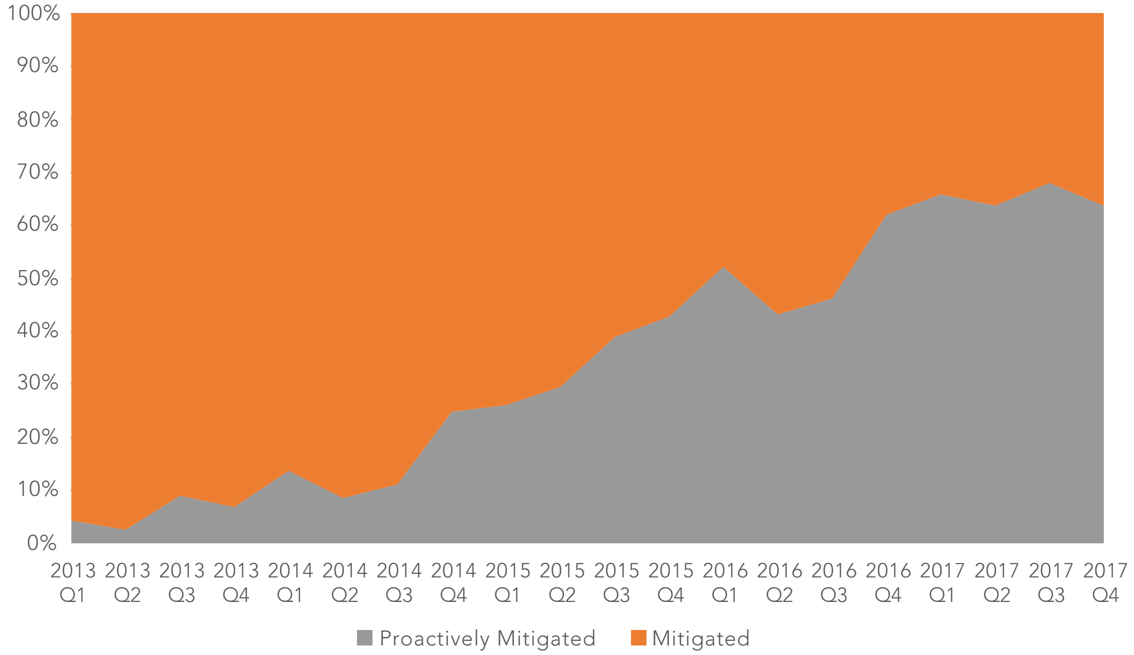
Proactive mitigation controls can be successfully leveraged to address a variety of DDoS attack vectors that target many ports and protocols, including UDP Fragments, DNS Floods, and even SYN Floods.



Proactive DDoS Mitigation: Trending

2017 was a banner year for attack mitigation via proactive mitigation controls on the Prolexic platform. The following shows the trend of steep and steady growth since these controls were first proactively applied in 2013.

Attack Events by Mitigation Type



Proactive DDoS Mitigation: Explained

Stop DDoS attacks before they start, at scale, in the cloud.

Proactive mitigation means putting controls in place to stop an attack — before an attack ever happens. A customer's proactive mitigation posture is developed as a result of a relationship between the customer and the Akamai SOCC, and involves the implementation of controls to drop traffic that does not match the criteria defined by the customer as expected (or normal) for its environment. Akamai can establish protective customer controls after examining, profiling, and learning about traffic patterns on a customer's network. Prior to deploying any controls, we work with customers to identify potential areas of risk — corner cases such as dormant backup systems and rare events — to avoid potential over-mitigation and to obtain formal customer approval and documented agreement on what will be proactively blocked from reaching the customer's network.

Preparation enables proactive mitigation.

The steps involved in setting up proactive mitigation are simple:

1. Customer coordinates a service validation exercise with the Akamai SOCC team.
2. Akamai profiles the customer's traffic during peacetime and establishes traffic baseline profiles.
3. The Akamai SOCC recommends proactive mitigation controls and an overall policy.
4. Recommendations are reviewed by the customer and Akamai SOCC in tandem.
5. Upon agreement of both parties, proactive mitigation policies are implemented.

This process is conducted with an agreed-upon cadence and/or as new attacks and vectors emerge and customer networks evolve.

Proactive Mitigation Postures

Proactive mitigation postures are used to reduce a customer's attack surface area. Locking down customer subnets and individual IP addresses against likely attack traffic allows Akamai to take away known favored lanes from attackers.

> *Example 1: After a period of service validation during which a customer's traffic is routed over the Prolexic network, it is observed that a specific subnet only serves UDP traffic. A recommendation to block all external TCP traffic is made; Akamai's SOCC team validates with the customer before applying a rule to allow only UDP traffic on the specific subnet.*
>
> *Example 2: After a period of service validation during which a customer's traffic is routed over the Prolexic network, it is observed that the customer is running publicly available DNS services from a handful of individual IP addresses across its protected space. A recommendation to restrict DNS traffic to these IPs is made, but during the Service Validation engagement with the customer it is uncovered that there are additional DNS servers on the customer's estate operating in standby mode. These servers are added to the list of allowed DNS servers before applying the rule to block traffic.*

While example 1 above is clear cut, example 2 showcases the need for a relationship between the Akamai SOCC and Services team and the customer's security and networking teams. The terms "never" and "not now" (or "not normally") cannot be confused in the world of proactive DDoS defenses.

While Akamai has significant insight into the traffic flowing across the Internet as a whole, each customer will have a significantly greater understanding of the traffic flowing across its unique network. In example 2, if Akamai had only allowed DNS traffic where it had been observed, and a DNS server had been taken down for maintenance (or failed, etc.) and replaced with a cold standby server, Akamai could have unnecessarily blocked traffic!

Effective Partnership

The Akamai SOCC successfully defends customers against dozens of DDoS attacks on any given day.

The SOCC team understands the DDoS landscape intimately, and closely interacts and coordinates with the Akamai Security Incident Research Team (SIRT) on the latest emerging threats.

Customers best understand their own networks and risk tolerance, as well as the value their organizations place on business continuity. Working in tandem to agree on establishing and actively managing the proactive mitigation policy is the critical step required to effectively reduce mitigation times to 0 seconds in the case where the controls match the attack vector.

Not A Firewall In The Cloud

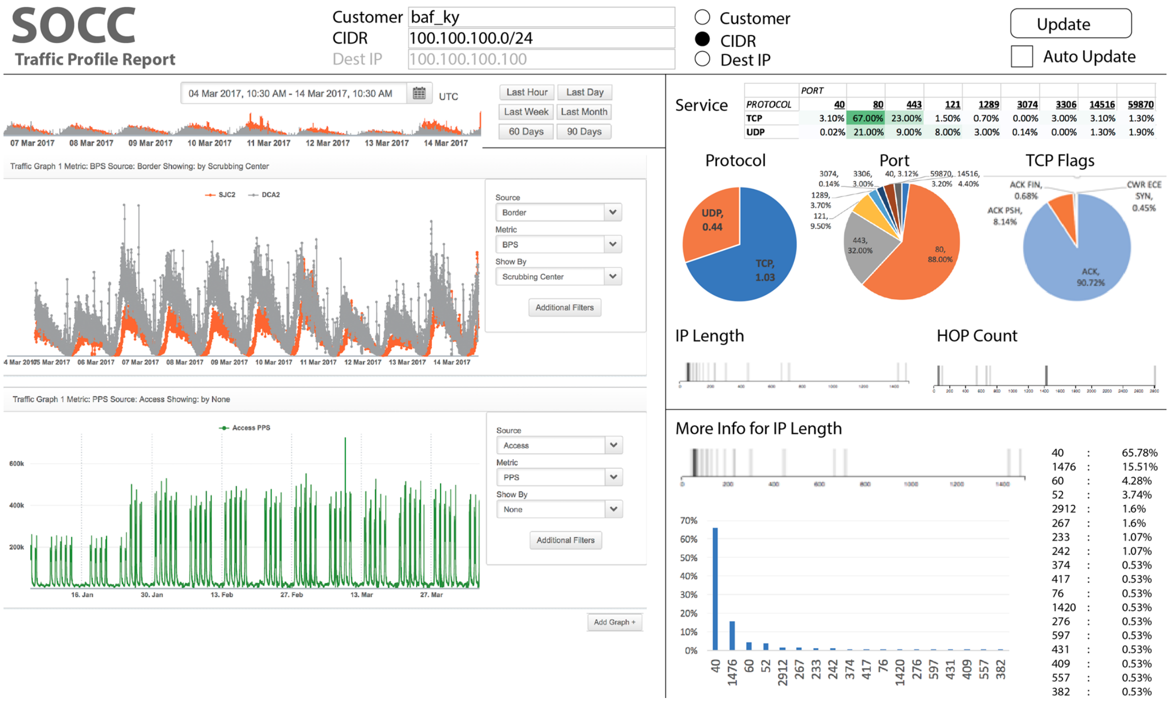
The aim of a proactive mitigation posture is not to create a cloud-based firewall, which — while feasible — is excessively cumbersome. Akamai customers run diverse and fluid networks. They don't want to have to go through a change control process with Akamai every time they want to make a simple change on their networks, such as swapping a DNS server's IP address.

Akamai's goal is to put protection in place for the most common and effective DDoS attacks, and to block unused ports, protocols, and services.

Akamai's proactive DDoS protection does not make customers less flexible or less agile. It simply and automatically protects them from DDoS attacks, so they can go about their business with one less thing to worry about.

Traffic Profiling

Effectively profiling customer traffic is the key to proactive mitigation.



SOCC
Traffic Profile Report

Customer: baf_ky
CIDR: 100.100.100.0/24
Dest IP: 100.100.100.100

○ Customer
● CIDR
○ Dest IP

Update
□ Auto Update

04 Mar 2017, 10:30 AM - 14 Mar 2017, 10:30 AM UTC

Traffic Graph 1 Metric: BPS Source: Border Showing: by Scrubbing Center

Source: Border
Metric: BPS
Show By: Scrubbing Center

Traffic Graph 1 Metric: PPS Source: Access Showing: by None

Source: Access
Metric: PPS
Show By: None

Service

	PORT								
PROTOCOL	40	80	443	121	1289	3074	3306	14516	59870
TCP	3.10%	67.00%	23.00%	1.50%	0.70%	0.00%	3.00%	3.10%	1.30%
UDP	0.02%	21.00%	9.00%	8.00%	3.00%	0.14%	0.00%	1.30%	1.90%

More Info for IP Length

40	:	65.78%
1476	:	15.51%
60	:	4.28%
52	:	3.74%
2912	:	1.6%
267	:	1.6%
233	:	1.07%
242	:	1.07%
374	:	0.53%
417	:	0.53%
76	:	0.53%
1420	:	0.53%
276	:	0.53%
597	:	0.53%
431	:	0.53%
409	:	0.53%
557	:	0.53%
382	:	0.53%

Akamai continuously updates traffic profiles for all customer subnets that are routed through the Prolexic platform in an "always on" deployment. For On-demand customers, the last known profile is kept once they route off (typically after an attack or a regularly scheduled service validation).

The Akamai SOCC, SIRT, and Threat research teams analyze customer traffic profiles and tie them back to the thousands of DDoS attacks we have mitigated. This approach enables Akamai to suggest effective proactive mitigation postures by leveraging thorough knowledge of not only the evolving DDoS attack landscape but also a customer's traffic profile.

Proactive Vs. Automated DDoS Mitigation

Proactive mitigation controls are often confused with automated or reactive controls.

Reactive controls require traffic to be observed for a certain amount of time or reach a certain volume before an attack is confirmed and mitigation is attempted. Potential attack traffic must be inspected and deemed malicious before mitigation controls can be applied, let alone become effective. Whether it is a human-driven or automated response process, it takes time. Hence, DDoS SLAs are often measured as time to apply mitigation with caveats like "once activated," "post detection," or "in the event of a sustained DDoS attack."

What good is a 10-second SLA if it takes minutes for mitigation to kick in?

Effective **Time To Mitigation (TTM) = time to detect attack + time to apply mitigation + time for mitigation to become effective**

During the auto-mitigation analysis and deployment period, DDoS victims have very limited options:

1. Employ arbitrary rate limiting (blocking legitimate and illegitimate traffic alike).
2. Wait it out while attack traffic bleeds through and likely causes impact on availability.

Both of these options are problematic and tend to have significant impact — exactly the type of impact the attacker was trying to generate. Proactive mitigation policies do not require analysis and deployment periods. They become effective from the moment an attack begins. Additionally, proactive mitigation controls don't rely on historic signature stores and are effective on zero-day attacks (as these emerging attacks tend to use network services that don't normally interact with customer environments).

With proactive mitigation in place, effective TTM is truly 0 seconds.

This is particularly important with the advent of modern DDoS attack networks that can generate traffic spikes very quickly, and pulse wave DDoS attacks that are meant to exploit weaknesses in automated cloud and hybrid on-prem/cloud DDoS defenses.

Akamai's most-attacked customers make heavy use of Akamai's proactive mitigation policies as a no-hassle solution to a persistent DDoS problem. Akamai's less-frequently attacked customers rest easy knowing that, by partnering with Akamai to deploy proactive mitigation postures, they have greatly decreased their attack surface and will have an effective 0-second TTM on many potential attacks.

Proactive Mitigation Safeguards

Proactive mitigation postures seem pretty straightforward: *Deny some traffic type(s) from somewhere (or anywhere) to somewhere within a customer's protected space.* Managing these controls constitutes the real challenge. Many of Akamai's customers run complex networks with millions of IP addresses, dozens of Internet-facing services, and myriad use cases.

Fortunately, Akamai operates a multi-site SOCC staffed 24/7 with security experts who have been extensively trained to work in these complex and ever-changing environments. Akamai's mitigation policy implementation tools are built for multi-tenant operations — meaning all changes are customer-bound, effectively eliminating the chance of one customer's mitigation posture impacting another's (a.k.a. cross contamination).

Mitigation Control Updates

Need a review of your mitigation posture before a big event or after a specific threat? Rest assured — a SOCC specialist is always available and ready to help. They can add, alter, or remove mitigation postures as needed, around the clock, seven days a week.

Mitigation Control Peer Review

All mitigation policies are subject to an audited peer review process within the Akamai SOCC and are continuously monitored for effectiveness. This is true whether the policies are deployed during an active DDoS attack or proactively during peacetime.

Mitigation Control Monitoring

Akamai's 24/7 global SOCC monitors all DDoS activity regardless of mitigation stance. Customers receive the same attack reporting whether attacks are actively or proactively mitigated. Monitoring of proactive mitigation controls helps identify changes on customer subnets and allows for appropriate tuning.

Best DDoS Defense You Can Buy

Akamai's cloud security platform has withstood the test of time and continues to serve the security needs of our customers by providing unequalled DDoS detection, response, and SLA-backed mitigation times. When combined with Akamai's web acceleration and delivery services, Akamai's cloud security platform can yield the highest uptime possible while delivering industry-leading performance.

Working with customers to deploy proactive mitigation controls has proven to be an extremely effective way to increase mitigation effectiveness for a large segment of attacks. However, proactive mitigation is just one example of the many tools and capabilities that Akamai's SOCC team employs as Akamai continually improves DDoS detection times and mitigation effectiveness.

Please contact your Akamai account team for additional information about proactive mitigation controls or any of our DDoS mitigation product capabilities.

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with more than 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, online retail leaders, media & entertainment providers, and government organizations trust Akamai, please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 04/18.