AKAMAI WHITE PAPER

Akamai Cloud Security Solutions:

Comparing Approaches for Web, DNS, and Infrastructure Security

Akamai
FASTER FORWARD

TABLE OF CONTENTS

Introduction

Organizations today operate in a Faster Forward world. Over three billion people are connected to the Internet, often through multiple computing devices. People are spending a growing portion of their lives online – communicating, shopping, being entertained, and working. For both business and government organizations, this represents a significant shift in how they engage with their customers and employees.

For these organizations, more of their daily activities now take place outside of the traditional office. They engage with customers and collaborate with coworkers over the Internet, performing financial transactions, transmitting sensitive business data, and communicating over public networks. To do this, they are moving more of their applications onto Internet-facing networks, so customers can shop 24x7 and employees can access the resources they need at any time in the global work day.

As a result, attackers can more easily access a larger number of high-value corporate and government assets. Attackers have shifted their methods accordingly, developing new attacks that no longer rely purely on brute force to take a service offline, but rather probe for and then take advantage of application vulnerabilities to steal data or pursue financial gain.

The threat landscape is constantly evolving, and organizations must evolve to keep pace with the constant stream of new attacks. However, the increasing pace of change in the last few years requires a revolutionary, not evolutionary, approach to security. When comparing different approaches to security, organizations should consider the strengths and weaknesses of each solution – not just how it performs against the attacks of today, but also how well it will respond to those of tomorrow. Beyond the traditional metrics of scale and performance, architecture and adaptability will also help determine the efficacy of any security solution over the long term. How well will the platform's architecture lend itself to defending against new attacks that haven't yet been discovered? And how quickly will it detect and identify those new attacks before it can mitigate them?

For organizations operating online today, finding the right partner means much more than just protecting IT assets. The right partner can complement each organization's online strategy with the right blend of security and performance. And the right partner can help organizations operate online with less risk, while taking advantage of the medium to offer a better Internet experience for its users.

The Changing Threat Landscape

As long as organizations have operated online, attackers have looked for ways to target them. And as the Internet has evolved, the methods and techniques used have changed to take advantage of the vulnerabilities that exist. The challenge with web security lies in that changing nature. Attackers are always one step ahead of IT, constantly increasing the scale of attacks through massive botnets or looking for new ways to take down web applications and infrastructure.

Denial-of-Service Attacks Growing in Size

One of the most common and pervasive security threats today is the denial-of service (DoS) attack. DoS attacks attempt to disrupt a critical Internet service by overwhelming a supporting infrastructure component, such as a web server or network device or consuming available network bandwidth. The first publicly documented DoS attack took place on September 6, 1996, against Panix, a New York City ISP.[1] There, unidentified attackers employed a SYN flood to exhaust the available network connections and prevent legitimate users from connecting to Panix services.

The Panix attack used three computers to generate about 48 Kbps of network traffic. Since then, DoS attacks have steadily grown in size. Modern-day attackers employ either large botnets or reflection-style techniques to generate distributed denial-of-service (DDoS) attacks with attack traffic several orders of magnitude greater in size. In a recent example, attackers combined six different attack vectors to launch a DDoS attack against an Akamai customer in Europe that peaked at 363 Gbps and 57 Mpps.

Growth in DDoS Attack Sizes

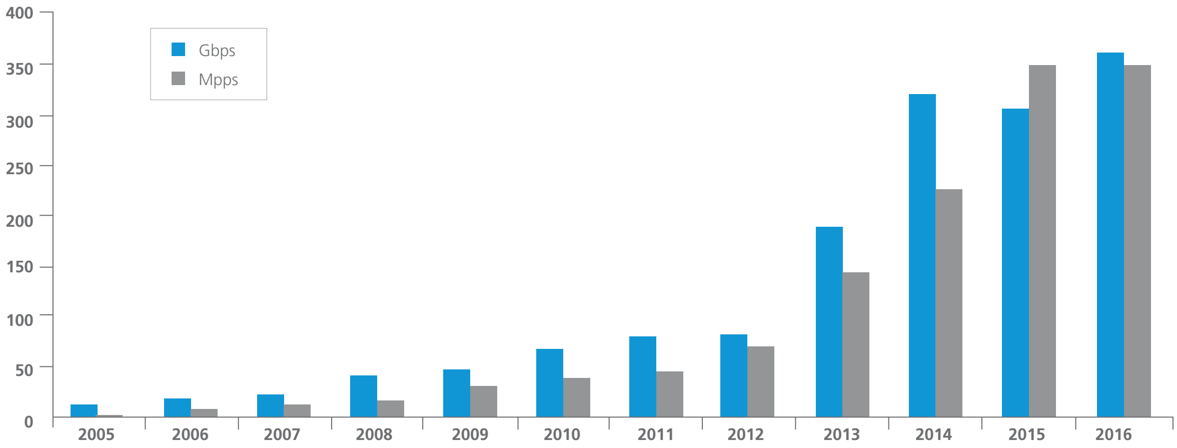


Figure 1: The size of DDoS attacks continues to grow every year, in terms of both bandwidth and the number of requests

Two trends are driving the increase in the size of volumetric DDoS attacks:

- The growth in the traffic-generating capacity of large botnets, deriving from both an increasing number of connected devices as well as the computing power of every connected device. Not only are botnets are increasing in size every year, but individual bots are also growing more powerful as the speed of computers increases and the cost of bandwidth decreases.
- The continuous discovery of new attack vectors such as DNS, NTP and SSDP reflection. Reflection-style techniques exploit vulnerabilities in existing Internet services to generate much larger attacks than otherwise possible. For example, DNS reflection generates 28x to 54x amplification in attack size, while NTP reflection generates 556.9x amplification.

This rapid growth highlights the difficulty in defending against volumetric DDoS attacks. Individual organizations can continue to invest in additional network bandwidth and higher performing network devices. However, they will always be hard-pressed to respond to the largest DDoS attacks of the time. These attacks harness the power of Internet to scale beyond the financial and technological resources of individual organizations.

Attacks Shifting to the Application Layer

While network-layer attacks will continue to present a significant challenge due to their scale, DDoS attacks targeting the application layer may prove to be a more vexing long-term challenge. For many attackers, the increasing number and complexity of web and other Internet-facing applications, coupled with a shortage of IT staff to adequately protect them, makes them highly attractive targets.

Application-layer DDoS attacks come in different forms and use a variety of methods and techniques to deplete a web or application server of the resources it needs to operate. Two common examples of application-layer attacks include:

- **HTTP –** As the underlying foundation for modern web applications, many application-layer attacks exploit HTTP vulnerabilities in order to incapacitate the targeted web server. For example, an HTTP flood targets a web server with high volumes of HTTP requests in order to consume its computational resources and prevent it from responding to requests from legitimate users.
- **DNS –** DNS has become another favorite target for attackers, not just because of its critical role in the IT infrastructure, but also because it is typically one of its least scalable components. Many organizations only deploy a small number of DNS servers, making it vulnerable to a volumetric attack that could easily overwhelm it.

Application-layer DDoS attacks are more difficult to detect than network-layer attacks because they look like legitimate network traffic. For example, HTTP floods generate high volumes of legitimate HTTP requests to the target web server, bypassing traditional security tools focusing on the network layer, while web servers typically do not have the ability to distinguish between normal and attack traffic today.

Targeting Applications for Data Theft

In addition to network- and application-layer DDoS attacks, organizations face an increasing number of web application attacks designed not to disrupt operations but rather to steal data. As organizations today increasingly interact with their suppliers, customers, and employees online, business and customer data is stored closer to the perimeters of the application where it can be easily accessed through a web browser. And because many organizations often lack sufficient resources or expertise to properly safeguard those application portals, hackers have increasingly focused on stealing data as an additional attack vector alongside traditional DDoS attacks.

Veracode, an application security testing vendor, predicts that three out of four companies will be targeted at some point by web application exploits and that web applications represent the approach through which 54% of the all hacking-based data breaches occur.[II] Some common attack vectors include:

- **SQL Injection –** According to Veracode, 30% of all data breaches are due to SQL injection. This type of attack exploits web applications that do not properly sanitize user inputs and tricks them into running database code that returns more data than they otherwise would have.
- **Remote File Inclusion (RFI)** – Similar to an SQL injection, this type of attack exploits web applications that do not properly sanitize user inputs. However, the immediate goal of a remote file inclusion is not to steal data, but rather trick the web server into executing the contents of a file stored in a remote location. In this manner, an attacker can then take control of a web server for malicious purposes.
- **Credential Abuse –** Public-facing websites and applications often require users to log in to access parts or all of the application. Because users often use passwords that are easy to guess and share passwords across multiple accounts, hackers can purchase stolen user login credentials for one site and make repeated login attempts against other sites in order to compromise an account.

Case Study: Remote File Inclusion

In December 2013, Akamai's Computer Security Incident Response Team (CSIRT) first detected unauthorized web scans against our customers looking for the remote file inclusion (RFI) vulnerability. Within two weeks, CSIRT pro-actively issued a threat advisory and provided a custom rule to block RFI scans using Akamai's WAF. A month later, Akamai introduced a new rule to identify and block RFI attempts in the Kona Rule Set, the common WAF rule set available for all customers, making it easy for any customers to enable protection against RFI exploits within their WAF configurations.

For a more detailed analysis of these attacks, read the blog post, *"A Two Week Overview of the Latest Massive Scale RFI Scanning,"* written by Ory Segal, Director of Threat Research at Akamai.

Web application attacks can be difficult to detect. SQL injections, remote file inclusions, and credential abuse attacks generate application traffic that appears legitimate to traditional network-layer security tools. As a result, organizations are often not aware of ongoing attacks until after large amounts of data have already been stolen. In an analysis of recent data breaches, Verizon found that 99 percent of attackers compromised their target within days or less, but only about 10 percent of breaches were discovered in that same time frame.[III]

A Multi-Dimensional Security Threat

While many security solutions focus on defending against a single type of attack, attackers are increasingly employing multiple different types of attacks in combination. Multiple-dimensional attacks have a higher chance of succeeding against organizations that may have limited IT resources or solutions focused on a single category of security threats. But even against well-protected applications, these attacks test their target's ability to respond to multiple parallel attacks occurring in different parts of their IT infrastructure.

In addition, attackers are beginning to combine DDoS attacks with SQL injections, using bandwidth-consuming and noisy DDoS attacks to distract limited security resources from the attacker's true goal of data or financial theft. This scenario highlights the danger of focusing on just one type of attack vector. In a rapidly changing threat landscape, organizations must be prepared to respond to a variety of potential attacks, including combinations of different types of attacks, in order to safeguard their IT infrastructure.

Case Study: Operation Ababil, Phase 3

In September, 2012, QCF launched Operation Ababil, a year-long campaign of DDoS attacks against a number of US financial organizations in response to an inflammatory video produced by a third-party individual. To conduct the attacks, QCF deployed its own botnet, with 9,200 bots, to target the organizations' public-facing websites. One attack on March 5, 2013, generated 190 Gbps in peak attack traffic, including 110 Gbps against a single bank.

Among the targeted organizations, one Akamai customer reported a multi-dimensional attack employing three different attack vectors over the course of two days.

1. The attack began on March 5 with 2000 bots generating an HTTP flood with peak attack traffic of 30 Gbps and 4 million HTTP requests per minute, 75 and 25 times their respective normal levels. Because their website was behind Akamai, this organization was able to maintain normal customer traffic through the attack, with no impact to website availability or performance.
2. The next day, the attackers adjusted their vector to a DNS-based volumetric attack. Using fewer than 40 bots, this attack attempted to overwhelm the DNS infrastructure with bad DNS requests, generating peak attack traffic of 40 Gbps and 1.8 million requests per second. Again, this organization maintained 100% availability, despite DNS traffic ten times greater normal, and facilitated customer access to their site throughout the day.
3. Later that afternoon, the attackers adjusted again, this time changing the target to an unprotected but non-critical website. With no web security in place, the organization saw page view errors spike by 1,327 percent.

Financial institutions increasingly rely on their public-facing websites to maintain relationships with customers. Many of these customers perform all of their banking activities through online branches. They expect to have access to their financial assets 24x7 and do not care that the organization may be under attack. With low barriers for customers to switch banks, any drop in customer satisfaction caused by DDoS-related outages can carry a significant financial cost.

Increasing Frequency and Costs of Cybercrime

Not only has the number, variety, and financial value of online targets proliferated, but the barriers to conducting a successful attack have fallen. The distribution of attacker toolkits and the ease with which newly discovered vulnerabilities can be shared have greatly democratized cybercrime. And these attacks are imposing a financial greater cost. Businesses increasingly depend on a variety of Internet-facing applications to capture revenue from customers, and even short disruptions can result in significant loss of revenue as customers postpone purchases or turn to competitors. But perhaps even risker, businesses often store sensitive information in centralized repositories that can be accessed through a web browser. These repositories present attractive targets for attackers seeking financial gain. Once rare, data breaches are now the most publicized type of cybercrime, as businesses suffer financial penalties and long-term damage to their corporate brand.

Cost of Cyber Crime ($Millions)

Ponemon Institute, October 2015

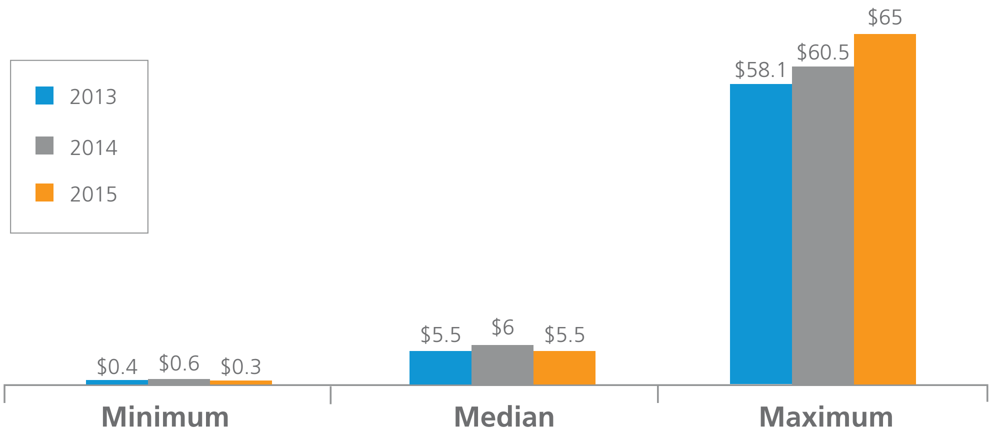


Figure 2: The annual cost of cybercrime increased from 2013 to 2015, as reported by the Ponemon Institute [IV]

Common Approaches to Security

The changing focus of security threats – from network to applications, disruption to data theft, and one-dimensional to multi-dimensional attacks – is driving an architectural shift in the security industry. While DDoS attacks will continue to command the greatest attention, many of the most damaging attacks are also the most difficult to detect, and provide little to no advance warning. This necessitates a security posture that is always on, but still provides the performance and scale to respond to the largest network- and application-layer attacks prevalent today.

On-Premises Hardware

Many organizations rely on hardware devices, such as network firewall, DDoS mitigation, and web application firewall (WAF) appliances, deployed on-premises within their data centers. With this approach, organizations manage their own devices and retain control of their security posture. From a financial perspective, on-premises hardware requires a large upfront capital expenditure with a typical hardware lifecycle and depreciation of two to three years, as well as operational expenditures for IT management costs. Deploying applications across multiple data centers can further increase costs as these solutions often must be deployed wherever the applications are located.

As with any inline solution, the challenge for on-premises hardware is ensuring sufficient scale and performance to remain resilient against attacks that are growing in size. This challenge is particularly acute for hardware devices, which are typically limited by the capabilities of the individual device, as opposed to those of the entire security system:

- **Scale** – While hardware devices are always increasing in scale, hardware-based security systems can still be overpowered by the vast amount of attack traffic generated by today's massive botnets. With the average DDoS attack peaking at 6.9 Gbps in Q1 2016, on-premises hardware continues to be a potential single point of failure.[V]
- **Performance** – Defending against application-layer attacks can be extremely resource-intensive. For example, For example, web application firewalls require a large amount of computing resources to compare incoming application traffic against known attack profiles. Even normal application traffic can require a significant amount of processing, which can reduce the published performance of hardware-based WAF devices and, subsequently, the amount of traffic that makes it through to the applications behind them.

Average size of DDoS attacks

State of the Internet – Security, Q1 2016

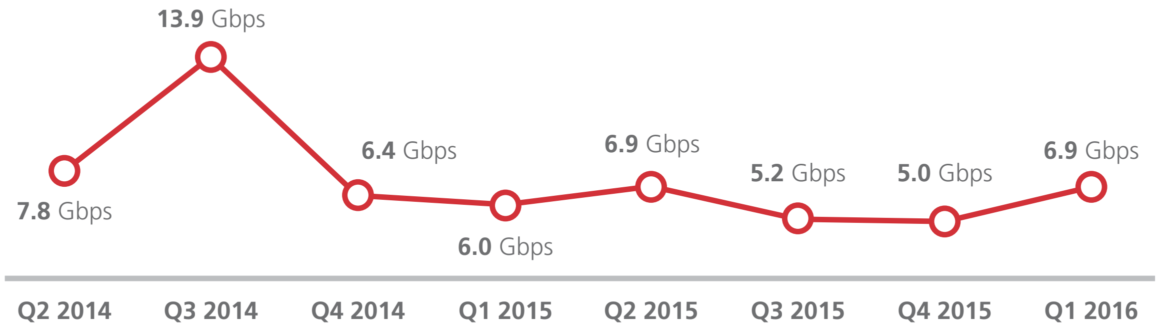


Figure 3: The average size of DDoS attacks exceeds the scale of on-premises hardware to mitigate

Case Study: On-Premises Hardware WAF

This national retail chain sells directly to consumers through brick-and-mortar stores as well as their eCommerce website. When the retail chain tested an on-premises hardware WAF in front of their website, they measured a 50 percent drop in performance due to the number of rules that needed to be processed. They compared that result with the Akamai solution, which resulted in no performance degradation. This allowed them to preserve their user web experience and continue to grow the revenue captured from their eCommerce site.

When considering a hardware-based approach, it is important to remember that no hardware device operates in isolation. Individual devices may have respectable specifications for scale and performance. However, multiple different types of devices are often deployed in sequence. A DDoS attack needs only to overpower the weakest link in the chain in order to cause an outage for the entire system. For example, network firewalls are often deployed behind routers. Routers are typically not designed to defend against a volumetric attack and can be easily overwhelmed by a volumetric attack, resulting in a denial of service for the entire system behind it.

A final disadvantage of a hardware approach is that it attempts to stop a DDoS attack only after it has entered the data center. If an organization does not have a sufficiently large Internet link, then the attack will saturate the available bandwidth, causing an outage for the entire data center. Even when attacks are successfully defended against, bandwidth-intensive attacks may degrade the performance for legitimate users. And as the size of potential DDoS attacks continue to grow, organizations will have to continue provisioning additional bandwidth to ensure sufficient scale.

Internet Service Providers

Another common approach to protecting Internet-facing applications is to implement a service through an organization's Internet service provider (ISP). Many ISPs offer DDoS mitigation services to complement their primary business of providing network bandwidth. These services take advantage of the ISP's role and location in delivering network traffic between remote users and applications to mitigate DDoS attacks against their customers' infrastructures.

For many organizations, this approach can be attractive for several reasons. First, it enables them to transfer the responsibility for mitigating a DDoS attack to a third-party. Network traffic to the organization's applications is already transiting the ISP's network, making the ISP a logical location in which to implement a DDoS mitigation service. And finally, ISPs typically offer DDoS mitigation services at a low monthly cost. The combination of these factors makes an ISP-based DDoS mitigation service an easy solution for organizations to purchase and deploy. However, there are several considerations that may not be apparent at first glance:

- **Multiple ISPs** – from an architectural perspective, ISPs can only mitigate DDoS attack traffic transiting their network. Many organizations purchase bandwidth from multiple ISPs in order to increase availability, improve performance, and reduce bandwidth costs. However, this can significantly increase the complexity of responding to any DDoS attack. Attack traffic can now arrive over the networks of multiple ISPs, meaning that organizations must deploy and manage multiple DDoS mitigation solutions, as well as coordinate any DDoS attack response across multiple vendors.
- **Scale** – with the largest DDoS attacks exceeding 300 Gbps in peak bandwidth, most ISPs simply do not have sufficient network capacity to properly mitigate potential attacks directed at their customers. However, even smaller attacks can present a risk to the ISP's network, consuming network capacity and impacting performance for other customers. Faced with this situation, an ISP will often choose to "black hole" traffic to the intended target of any DDoS attack over 10 Gbps in size in order to preserve the stability of the ISP's network at the expense of the target organization.
- **Security Expertise** – most ISPs do not regard security as a core component of their business, but rather an additional capability to augment their primary business of providing network bandwidth. As a result, ISPs typically have limited security expertise and do not employ best-of-breed security solutions, and may have difficulty stopping attacks that are too complex or large in size.

Beyond DDoS mitigation, organizations must also consider the threat of posed by data exfiltration attempts such as SQL injections and XSS. Organizations that have deployed an ISP-based DDoS mitigation service must still implement a WAF solution in order to protect their websites and applications from data theft. This requires augmenting the ISP-based DDoS mitigation with a separate solution from another vendor – either an on-premises or a cloud-based WAF. In addition to the cost of acquiring and managing multiple solutions, this can increase the complexity of responding to multi-dimensional attacks that combine DDoS with data theft.

Cloud Security Providers

Cloud-based security solutions provide a new approach to detecting and mitigating security threats. Here, organizations deploy a third-party cloud platform in front of their private infrastructure and inline between remote users and their websites and applications. The cloud security provider can examine network traffic for known attack patterns and pass only legitimate traffic through to the application. This allows the solution to stop attacks in the cloud, before they reach the target organization's data center or applications.

For many organizations, the concept of stopping attacks in the cloud represents a paradigm shift. This approach moves the point of mitigation from the data center to the cloud platform and offloads the responsibility for mitigation from an organization's IT staff to that of the cloud provider. This provides several advantages over traditional approaches:

- **Simplicity** – defending against DDoS attacks within the data center requires scaling and hardening many infrastructure components. By moving the point of mitigation to a third-party cloud platform, organizations can remove the complexity of securing every part of their infrastructure from different types of DDoS attacks.
- **Scale** – by leveraging the economies of scale that come from protecting many organizations at once, cloud providers can build a much larger infrastructure than what individual organizations can on their own. However, not all cloud security solutions are created equal – even between different cloud providers, the scale of their platforms can vary greatly. Organizations should evaluate the total capacity of the cloud platform – how much traffic it delivers on a daily basis as well as how much extra capacity it has to mitigate potential attacks and handle future growth.
- **Performance** – some cloud-based security solutions can improve performance while protecting applications against DDoS and web application attacks. These solutions often share a common underlying platform with a content delivery network (CDN) that is designed to accelerate access to web applications. Because many performance-sensitive applications may already be behind by a CDN, this approach can help secure those applications without requiring a tradeoff in performance.
- **Threat intelligence** – cloud security providers typically have greater visibility into attacks and attack trends than individual organizations. Because of their position in the network, they can see an attack as it is first used against one of their customers and then leverage the technologies and techniques used to defend against that attack to improve security for other customers. Cloud security providers can make threat intelligence available to organizations in different ways, including through improved WAF rules, new attack signatures, customer-facing threat advisories, and better internal response processes.
- **Expertise** – the effectiveness of any organization's ability to respond to DDoS or web application attacks is greatly influenced by its experience at mitigating other similar attacks. By defending against attacks directed at many individual organizations over time, cloud security providers can develop significant expertise and experience. They can draw on this experience when mitigating future attacks to reduce mitigation times and any impact on their customers.
- **Compliance** – many organizations operate websites and applications that are subject to various legal regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) for any site that handles credit card information. Organizations must ensure that their cloud security solution also complies with all applicable legal regulations to which they are subject.
- **Cost** – with a cloud-based security solution, organizations can trade an upfront capital expenditure with a much lower recurring operational expenditure. Considering the size of the infrastructure required to protect against the largest attacks, the savings from such a cost model can be significant.

Case Study: Cloud-Based DDoS Mitigation Solution

This gaming company provides a range of online games to consumers through its websites. Recently, the company was targeted with a month-long DDoS attack campaign comprising 26 distinct attacks against their application, network, and DNS infrastructures. Of the 26 attacks, eight saw peak bandwidth of over 100 Gbps, and one peaked at 321 Gbps. By deploying a cloud-based security solution from Akamai in front of their data center, the gaming company was able to leverage the scale of the Akamai cloud platform instead of incurring the costs required to build out a private infrastructure capable of absorbing 300+ Gbps of attack traffic. In addition, they were able to rely on staff from Akamai's 24x7 security operations center (SOC) to respond to these attacks.

The Akamai Intelligent Platform™

Akamai offers an inline cloud security solution based on our Akamai Intelligent Platform. Originally founded as the leading CDN, the Akamai Intelligent Platform has evolved beyond acceleration to provide network- and application-layer security for websites and other Internet-facing applications. Its global scale and connectivity provides several inherent advantages when defending against many of today's most prevalent security threats.

A Natural Architecture for Web Security

As a cloud-based security solution, the Akamai Intelligent Platform sits in front of websites and other Internet-facing applications, delivering network and application traffic from users to applications, and content from applications back to users. Its inline and distributed architecture provides two advantages when defending against both network- and application-layer attacks:

1. **Inline** – The inline architecture offers a natural location from which to defend against any type of DDoS or web application attack. As traffic passes through the Akamai Intelligent Platform to the application, the platform can identify and analyze attacks as well as take the appropriate actions to mitigate them. In addition, its inline architecture enables the Akamai Intelligent Platform to apply both positive and negative security models as appropriate for additional flexibility.

2. **Distributed** – Users access websites and other Internet-facing applications through the Akamai Intelligent Platform's globally distributed resources, including over 200,000 edge servers and seven global scrubbing centers. This provides a distributed platform for securing Internet-facing applications, with many locations in the network where mitigation activities can be performed.

Multiple Perimeters of Defense

Websites and other Internet-facing applications depend on a variety of infrastructure elements in order to function. These include the physical servers on which they run, the network infrastructure through which they communicate, and even the DNS infrastructure that directs client systems to the application. Protecting applications from downtime and data theft requires protecting all of these supporting elements from potential attack – a task that has become increasingly challenging as the IT landscape has shifted. Globalization and the resulting distribution of IT assets around the world, the adoption of cloud services and infrastructure, and increasing reliance on the Internet for business operations have all contributed to a diffusion of the traditional IT perimeter.

Akamai architected the Akamai Intelligent Platform as a distributed cloud platform in order to help organizations better protect their new, smaller, and more diffused perimeters wherever their IT assets are deployed and data is stored. The Akamai Intelligent Platform comprises multiple different technologies and networks that protect different parts of the application infrastructure, including:

- **Websites and Applications** – with over 215,000 servers deployed in 127 countries and over 1,500 networks, Akamai's edge network extends from the website or application to within one network hop from 90 percent of all web users. This provides Akamai with global reach to detect and stop both DDoS and web application attacks at the edge of the network, closest to where they begin and before they reach their target.
- **Origin Infrastructure and Non-Web Applications** – with seven high-capacity scrubbing centers located around the world, the purpose-built Prolexic DDoS mitigation network provides the capability to protect the entire origin infrastructure from DDoS attack. It employs over 20 different security technologies to detect, identify, and mitigate any type of DDoS attack targeting both the infrastructure as well as any type of Internet-facing application.
- **DNS** – an independent DNS platform architected for both performance and availability, Akamai's DNS platform includes thousands of name servers deployed in over 200 points of presence around the world to improve DNS performance and provide the capacity to absorb the largest DNS-based DDoS attacks.

Internet Security with Global Scale

Akamai architected every aspect of the Akamai Intelligent Platform for a hyperconnected world, with the capacity to handle network traffic on a global scale:

- On any given day, the Akamai edge network delivers between 15 and 30 percent of global web traffic and has seen traffic in excess of 35.7 Tbps. On any given day, the Akamai edge network delivers around 24 Tbps of web traffic, leaving well over 10 Tbps of available capacity. This Internet scale provides a natural advantage when defending against the largest DDoS attacks.
- The Prolexic network provides over 3.2 Tbps of network capacity dedicated to mitigating DDoS attacks. This was nine times the size of the largest attack experienced on the Prolexic network – the 363 Gbps attack against a European media company.
- The typical amount of traffic on Akamai's DNS platform represents less than one percent of its overall capacity, with spare capacity to absorb the largest DDoS attacks, including the 90 Gbps attack against a media company.

Beyond bandwidth-intensive DDoS attacks, the scale of the Akamai Intelligent Platform also provides a better defense against web application attacks. Detecting these attacks requires significant processing power, as every incoming application request must be compared to known attack profiles through matching rules on a WAF. With over 215,000 servers distributed around the world, Akamai's cloud platform has the capability to protect against application-layer attacks without degrading the performance of the web applications behind it.

By leveraging the Akamai Intelligent Platform , organizations no longer need to plan to defend against the largest potential attacks. This allows them to reduce their capital and operational expenditures for on-premises hardware and network bandwidth. And when attacks do occur, the Akamai Intelligent Platform mitigates the attack at the appropriate network location in the cloud before it reaches the application, helping organizations maintain the availability and performance of their Internet-facing applications for legitimate users.

Always-on Security

Originally designed to deliver network traffic on a global scale, the Akamai Intelligent Platform provides a notable advantage over other security solutions – it is always on. Many solutions provide a passive and reactive defense. The target organization must first detect an attack before it can contact the security vendor to enable DDoS protection. Not only does a window exist in which applications are impacted, but this type of solution cannot effectively protect against many application-layer attacks that focus on data theft and blend in with legitimate traffic to go undetected.

The Akamai Intelligent Platform already delivers between 15 and 30 percent of all web traffic on a daily basis. It can inspect incoming network traffic for attack profiles while delivering it to the web application, providing both acceleration and security. With Akamai, IT organizations do not need to know that they are being attacked before they can defend against them. Akamai provides proactive Internet security that automatically detects new attacks as they begin, before they impact the target application, and without any outside intervention.

Protect and Perform

Most security solutions were designed for a single purpose – to defend against one or more types of attack. Because of this narrow focus, these solutions require organizations to tradeoff performance for security, resulting in lower traffic, lost lead conversion, and potentially reduced brand equity. For example, deploying hardware-based WAF (see case study, above) can result in significant performance degradation for web applications. As a result, organizations often choose to deploy these security solutions out of band, despite the original design and greater security benefit of an inline solution.

Unlike many security solutions, the Akamai Intelligent Platform is architected with both security and performance in mind. Akamai views security and performance as complementary goals and helps organizations both protect and perform – protect web applications without requiring a tradeoff in application performance. The wide breadth of acceleration technologies also available for the Akamai Intelligent Platform allows it to protect web application infrastructures while improving application performance in order to maximize revenue and productivity at all times.

Case Study: 2014 World Cup

In Summer 2014, the World Cup brought sporting audiences around the world together in heavily broadcasted soccer matches in which various countries competed against another. Beyond the competitions on the field, Akamai's threat research team found that attackers around the world targeted organizations in other countries corresponding with scheduled soccer matches. For example, four matches that saw corresponding attack campaigns:

- August 1: 850 Gbps for the table tennis, men's synchronized 3m diving, cycling, and men's kayak finals
- Brazil vs. Croatia: this match corresponded with a spike in SQL injection attacks originating from Croatia and targeting a major Brazilian financial institution.
- Spain vs. Netherland: after Spain's loss to the Netherlands, an attacker in Spain targeted the sports section of a Dutch news website with a DDoS attack.
- Chile vs. Australia: Akamai saw an increase in attack traffic originating in Australia and targeting sites in Chile two days after the event.
- Cote D'Ivoire vs. Japan: similar to Chile vs. Australia, Akamai saw an increase in attack traffic originating in Australia and targeting sites in Chile two days after the event.

For a more detailed analysis of these attacks, read the blog post, "Hackers 'Join' World Cup 2014 Matches on the web," written by Ory Segal, Director of Threat Research at Akamai.

Improving Security with Threat Intelligence

The sophistication and complexity of attacks are increasing every day, as hackers develop new tools and discover new vulnerabilities to exploit. To keep up with attackers, security vendors must have granular visibility into emerging threats as they are developing anywhere in the world. In addition, vendors need the capability to quickly develop new rules to mitigate emerging threats and push them into global application deployments.

Because of the global scale of the Akamai Intelligent Platform, Akamai has unmatched visibility into attacks against the largest, most trafficked, and most frequently attacked online properties and brands, and leverages this visibility in several ways:

- Identify new attack trends as they develop or new attack vectors as they are first used.
- Proactively warn at-risk customers of an emerging threat or adjust the security posture of protected websites and other Internet-facing applications.
- Develop WAF rules to mitigate newly discovered attack vectors while refining existing ones to improve the accuracy of our protection against web application attacks.
- Improve the tools and processes utilized by Akamai's global SOC to detect, identify, and mitigate future attacks more quickly and effectively.
- Issue specific threat advisories to customers through Akamai's threat intelligence services.

Improving WAF Rule Accuracy

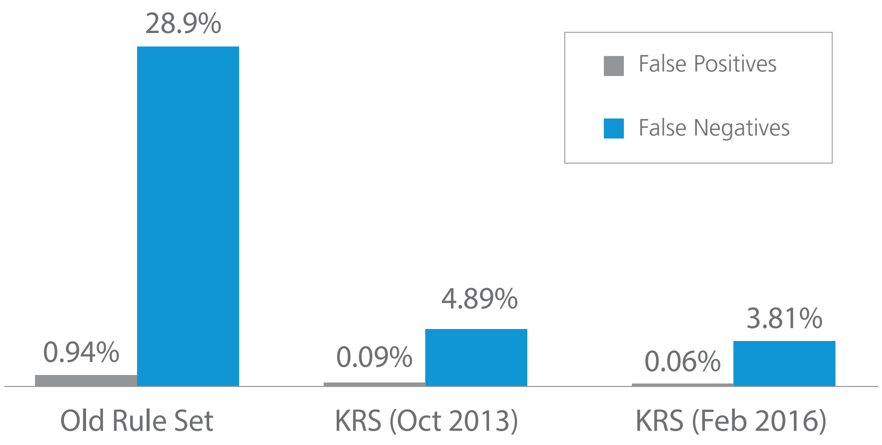


Figure 4: Akamai continuously refines our Kona Rule Set to improve the accuracy and quality of web application security.

Introducing Kona Site Defender

Built on the same edge network as Akamai's Web Performance solutions, Kona Site Defender offers a comprehensive website protection service for the detection, identification, and mitigation of DDoS and web application attacks targeting protected websites and applications.

Defending Against Network-Layer DDoS Attacks

Users access websites and applications through the Akamai Intelligent Platform's globally-distributed edge servers, which then proxy application traffic to the application origin. The Kona Site Defender automatically drops all non-application traffic, such as SYN packets, ICMP packets, or UDP packets without application payloads, at the edge server. This provides organizations with instant protection against the most common and bandwidth-consuming network-layer DDoS attacks.

Defending Against Application-Layer DDoS Attacks

Unlike with network-layer DDoS attacks, Kona Site Defender cannot automatically drop attacks at the application layer. These attacks typically communicate with websites and applications using legitimate requests. However, they attempt to overwhelm the application server through either incomplete or malformed requests or an excessive number of requests. Kona Site Defender defends against application-layer DDoS attacks in two ways. First, the global scale of the Akamai Intelligent Platform provides the capacity to absorb the largest attacks, including HTTP and DNS floods, before they reach the application. Then, Kona Site Defender provides granular controls to automatically identify attackers and block them from sending traffic to the application. These controls include:

- **Static and Advanced Caching** distribute web content across the Akamai Intelligent Platform's 215,000 edge servers, making it difficult for attackers to disrupt protected websites and applications.
- **Adaptive Rate Controls** monitor the behavior of application clients and automatically block or throttle those demonstrating suspicious behavior, such as issuing an excessive number of requests or a pattern of requests identical to other clients. In addition, rate controls automatically sanitize requests before they are delivered to the application, protecting it from DDoS attacks that rely on malformed or incomplete requests, such as Slowloris, Slow POST, and RUDY.
- **IP Whitelists and Blacklists** allow or deny requests from specific IP addresses, offering flexibility in configuring access to the protected web application.
- **Geo Blocking** can block traffic originating from specific geographic regions to mitigate localized DDoS attacks.

Once specific IP addresses are identified, Kona Site Defender can block all application traffic from those IP addresses at the edge and before it reaches the application.

Defending Against Data Theft

To help organizations defend against data theft, Kona Site Defender combines:

- **Web Application Firewall** to identify and block an attempted attack, such as an SQL injection attack; with
- **Adaptive Rate Controls** to block identified attackers from connecting to the application or throttle back the number of requests they are allowed to make.

Like any WAF, Kona Site Defender inspects incoming application traffic, comparing it to known attack profiles through matching rules and either alerting on or blocking detected attacks. Comprehensive protection against a wide range of known attacks, such as SQL injection and XSS, is enabled by default in the Kona rule set, Akamai's proprietary WAF ruleset. Organizations can also further customize their security posture with the addition of custom rules.

Kona Site Defender implements the WAF on the edge servers, identifying, analyzing, and mitigating application-layer attacks at the edge of the network and before they reach the application. Because of its distributed nature, Kona Site Defender can inspect global traffic to the application without imposing any performance degradation. And because the Kona Site Defender scales with the Akamai Intelligent Platform, it ensures that websites and applications remain protected even as they grow.

Introducing Prolexic Routed

While Kona Site Defender provides a deep layer of website protection for critical websites and applications, Prolexic Routed provides broad protection against DDoS attacks for the entire origin infrastructure. Prolexic Routed leverages a dedicated network with seven scrubbing centers and over 3.2 Tbps in dedicated network capacity and Akamai's 24x7 SOC to detect, inspect and mitigate DDoS attacks.

Protecting the Origin Infrastructure

Modern DDoS attacks employ a variety of attack vectors to target different areas of the origin infrastructure. In order to protect the origin against all possible attack vectors in the most efficient manner, Prolexic Routed leverages BGP to route network traffic to entire subnets through Akamai's global scrubbing centers. There, Akamai SOC staff can easily inspect the network traffic, identify suspected attack traffic, and mitigate any type of DDoS attack before it reaches the origin.

Combining Best-of-Breed Security Technologies

Within every scrubbing center, Akamai utilizes over 20 different security technologies to identify and mitigate different types of DDoS attacks in the most efficient manner. Akamai SOC staff always applies the technology best suited to mitigating a specific attack vector and can combine multiple technologies as attack vectors change over time. With Prolexic Routed, organizations can benefit from Akamai's experience in selecting and managing best-of-breed DDoS mitigation technologies for the most effective response to any type of DDoS attack.

People-Driven DDoS Mitigation

Prolexic Routed utilizes a people-driven security strategy, relying on dedicated security staff to inspect for and mitigate DDoS attacks originating anywhere in the world from Akamai's 24x7 SOC. SOC staff perform real-time analysis of ongoing attacks and provide the ability to respond to changing attack vectors and multi-dimensional threats. Mitigating 10 to 15 attacks every day, Akamai security experts provide the experience necessary to respond quickly and effectively to new and developing DDoS attacks.

Introducing Fast DNS

Fast DNS offers a cloud-based DNS infrastructure to help organizations protect their DNS services from DDoS attack. Organizations can deploy Fast DNS as a primary or secondary DNS solution to either replace or augment their existing infrastructure.

Architected for Performance and Availability

Providing DNS services for Akamai's Akamai Intelligent Platform, Akamai architected Fast DNS to provide an optimal combination of performance and availability. Fast DNS combines 20 independent DNS networks, or clouds, including one performance cloud and 19 availability clouds. While the globally-distributed performance cloud deploys name servers into a larger number of smaller points of presence in order to get closer to end users, the availability clouds provide concentrated capacity from a smaller number of larger points of presence in order to absorb DDoS attacks.

Defending Against DNS-Based DDoS Attacks

Fast DNS protects against DNS-based DDoS attacks in several ways:

- **Capacity** to absorb the largest attacks – with normal traffic less than one percent of its total capacity, Fast DNS has the capacity to handle spikes in both bandwidth and the number of requests.
- **Rate Controls** block specific IP addresses responsible for generating unusually large amounts of DNS traffic.
- **IP Whitelists and Blacklists** deny DNS requests from specific IP addresses for a more granular response to attacks. In addition, Fast DNS can automatically block DNS traffic from any server not on a predefined list of known name servers.

Case Study: DNS-Based DDoS Attack Against a Media Company

In 2014, a media company in APJ experienced a volumetric attack targeting their DNS infrastructure. The attack unfolded in three phases over the course of two weeks:

- The first phase lasted over 18 hours, with attack traffic peaking at 68 Gbps and 20 Mpps.
- The second phase occurred five days later and lasted over 30 hours, with attack traffic peaking at 73 Gbps and 40 Mpps.
- The third phase occurred six days later and only lasted three hours, but attack traffic peaked at 91 Gbps and 53 Mpps.

This attack highlighted the attractiveness of DNS as a target for attackers attempting to disrupt web operations. Even if the primary web target is well protected, attackers often target the supporting DNS infrastructure in order to prevent users from reaching the site. In this case, Akamai's Fast DNS absorbed the attack while maintaining the availability of DNS services for all customers.

Integrating into the Security Ecosystem

In addition to protection from DDoS and web application attacks, most organizations operate a number of additional security solutions, including intrusion protection systems (IPS), authentication, authorization, and accounting (AAA) solutions, and security information and event management (SIEM) solutions. Akamai easily integrates into the broader security ecosystem to help organizations establish a layered defense, centralize security intelligence, and build additional services that include web security.

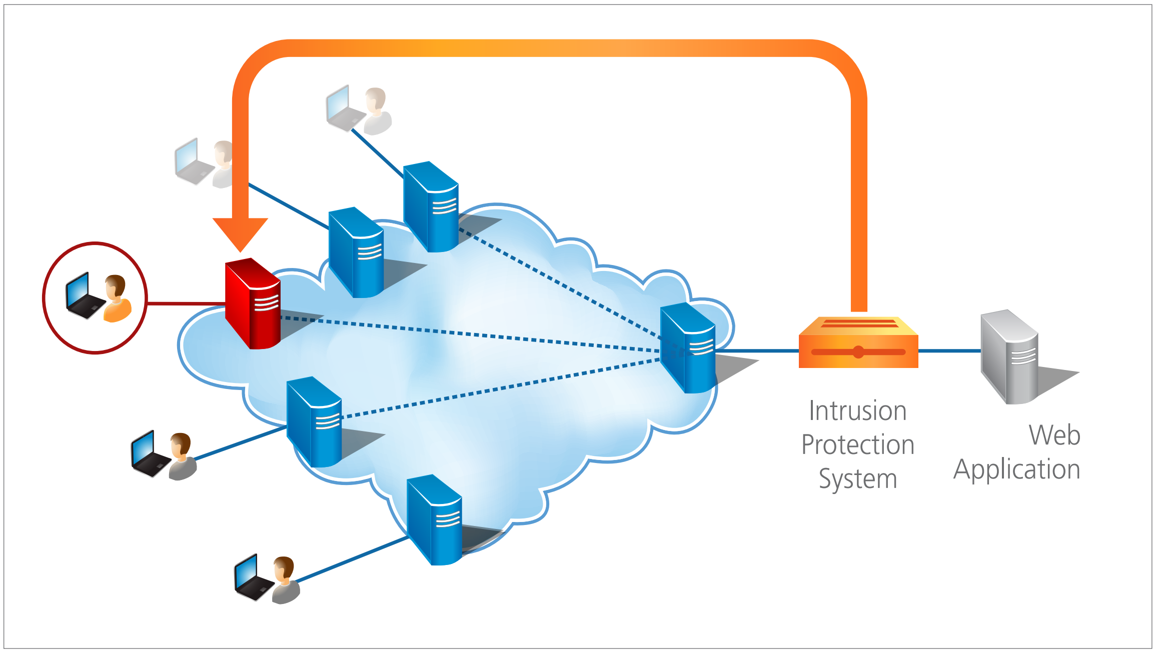
Open Platform Initiative

Organizations running their application infrastructure on the Akamai Intelligent Platform can take advantage of Akamai's Open Platform Initiative to control their Akamai solutions on a more granular level, as well as gain additional insight into their applications. Through the {OPEN} framework of application programming interfaces (API), organizations can automate how Akamai solutions integrate with their existing security infrastructure or interact with other security solutions. For example, organizations can:

- Automatically adapt their web security posture using data collected by complementary security solutions to adapt their Kona Site Defender configuration or create new security rules.
- Centrally manage their security infrastructure by exporting data collected by Kona Site Defender and Fast DNS to a SIEM tool, where it can be correlated with data from other security solutions.
- Offload or minimize additional investments in expensive hardware solutions, instead relying on Kona Site Defender and Fast DNS to enforce worldwide policies.

Case Study: Insurance Company

This insurance company had deployed a hardware-based IPS solution to defend the perimeter of their data center. Kona Site Defender complemented the existing IPS solution with protection for their websites and applications. The insurance company utilized the {OPEN} framework API's to connect the two solutions and create a more responsive and intelligent security infrastructure. If an IPS detects a suspicious IP address attempting to gain access to an application, it pushes the IP address to the IP blacklist on Kona Site Defender, thereby blocking the intruder from accessing the application.



Managed Security Services

Kona Site Defender provides managed security service providers (MSSP) with an ideal technology platform on which to build value-added security services. The distributed cloud architecture of the Akamai Intelligent Platform enables MSSP's to offer global security services based on human expertise without needing to invest in an expansive hardware infrastructure.

In addition, the {OPEN} API's facilitate integration with:

- **Existing Management Solutions** – MSSP's can retrieve data collected by Kona Site Defender to enhance their visibility into developing security threats and provide 24x7 monitoring of websites and applications
- **Existing Response Processes** – MSSP's can use retrieved data or other alerts integrate Kona Site Defender with existing response processes and ensure that security personnel always have the latest situational intelligence.
- **Other Security Solutions** – MSSP's can integrate Kona Site Defender with other security solutions to increase the cohesiveness of their entire security service portfolio.

Why Akamai

Built on a globally-distributed cloud platform, Akamai offers best-in-class protection against DDoS and web application attacks for organizations worldwide. The Akamai Intelligent Platform provides a natural architecture for protecting websites and other Internet-facing applications, stopping attacks in the cloud before they reach the application and origin infrastructure. Always on, the Akamai Intelligent Platform protects the Internet-facing application infrastructure while helping organizations maintain application performance and availability for their users. By partnering with Akamai, organizations can augment their existing IT capabilities with a global security posture that keeps pace with the latest Internet security threats and grows with the needs of their business.

Innovate Without Fear

In a hyperconnected world, websites and other Internet-facing applications are increasingly becoming the external and internal faces of corporate, public sector, and non-profit organizations alike. They provide the primary conduit between organizations and their customers, maintaining relationships and presenting the best possible brand experience. In addition, they help integrate the activities of an increasing number of global employees with the rest of the organization. As such, applications are constantly changing – improving and innovating – not only with new applications but also a constant stream of updates to existing ones.

While any change can introduce new vulnerabilities, Akamai can help organizations innovate their web experience faster without lower risk. Like any WAF solution, Kona Site Defender provides protection against many common attack vectors that lead to data breach, including SQL injections and cross-site scripting. But unlike other WAF solutions, Kona Site Defender comes with the scale, performance, and accuracy to remain in-line at all times. Always-on protection frees organizations to continuously improve their web presence without the fear of exposing new vulnerabilities to attackers.

In addition, Prolexic Routed helps organizations deploy new Internet-facing applications faster by reducing the much of the complexity involved with securing them. By using BGP to route network traffic to entire protected subnets through Akamai scrubbing centers, Prolexic Routed provides blanket DDoS protection for hundreds of applications at a time. Organizations no longer need to consider DDoS protection on an application-by-application basis, but can easily meet their corporate mandate for DDoS protection even as existing applications are updated or new applications are deployed.

Security that Grows with You

Akamai front-ends many of the largest online properties in the world, including one out of every three Global 500® companies, the top 30 media & entertainment companies, and all of the top 20 global eCommerce sites.[VI] The Akamai Intelligent Platform is constantly growing – in both scale and performance – to meet the requirements of our global customers. In April 2016, the Akamai Intelligent Platform delivered a record amount of network traffic, peaking at 35.7 Tbps due to unprecedented demand. This was double the record set just three years prior, and almost eight times the level in 2010.

By growing with the Internet, Akamai ensures that individual organizations don't have to. By partnering with Akamai, organizations always have a global platform supporting their Internet-facing application infrastructure. The Akamai Intelligent Platform provides organizations with the scale and performance necessary to defend against the largest network- and application-layer attacks both today and as they grow in the future. And using either the Akamai Luna Control Center or the {OPEN} APIs, organizations can easily manage online security for their global website and applications, without needing to invest in a global security infrastructure themselves.

Growth in Record Traffic on the Akamai Platform

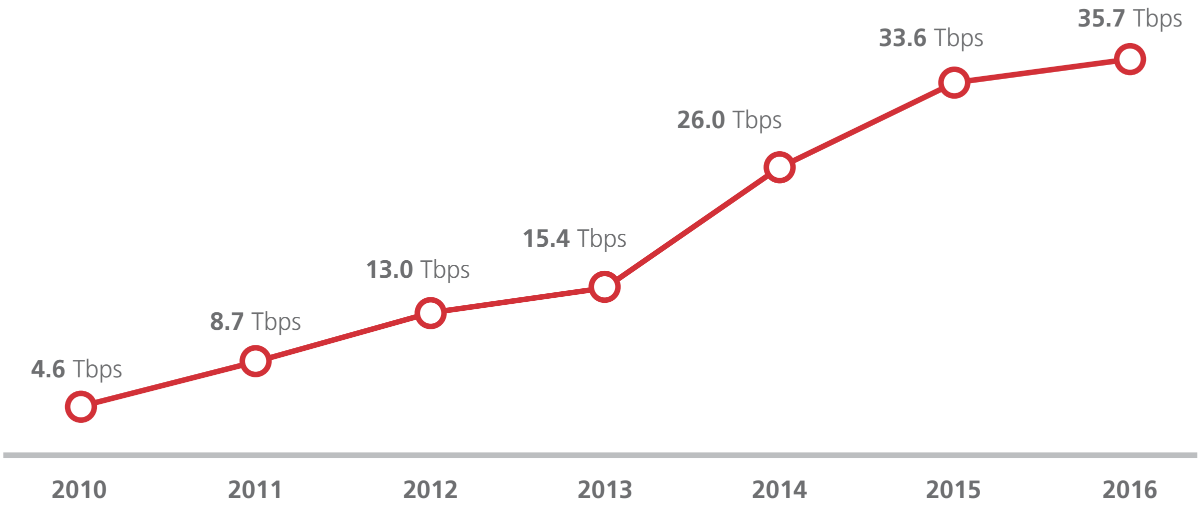


Figure 5: Akamai delivered a record 35.7 Tbps of traffic in 2016

Case Study: Motorcycle Superstore

Listed in the top 200 on the Internet Retailer 500 list, Motorcycle Superstore had always taken online security seriously. It originally deployed a hardware WAF out-of-band, but had to reevaluate when a new PCI rule required WAF solutions to operate inline. With highly dynamic content, managing a hardware WAF became unwieldy and limited its ability to take advantage of acceleration solutions to drive additional revenue from their website. Motorcycle Superstore upgraded their WAF solution with Akamai, which provided the additional flexibility and scale that they needed. Instead of regularly upgrading security hardware and network bandwidth, Motorcycle Superstore saved 15 percent in capital expenditures and reduced network bandwidth costs by 10 percent while positioning their web infrastructure for future growth.

Simplify Your Web Security

With Akamai, organizations can simplify their security posture by relying on a trusted third-party with a global security infrastructure. By stopping attacks in the cloud before they reach the application, Kona Site Defender, Prolexic Routed, and Fast DNS reduce the burden on organizations' infrastructure and internal IT resources. Organizations can offload the resource requirements of deploying a global physical security infrastructure and focus instead on how to customize it to meet the security needs of their business.

The Akamai Intelligent Platform also adapts to the changing threat environment, with Akamai security teams constantly developing and publishing new security rules and processes in response to the latest threats. Akamai has invested in building relationships within the security community, such as with OWASP, FS-ISAC, FIRST, NANOG, and government law enforcement agencies. Akamai combines this external intelligence with the threat data made available by the Akamai Intelligent Platform to simplify the security posture for individual organizations.

Summary

The Panix attack in 1996 first highlighted the security threats that organizations face online. However, the threat landscape has changed dramatically since then – starting at the network layer and moving to applications, the range of possible attack vectors continues to expand with no end in sight. With this shift, legacy security solutions are no longer as effective, while on-premises hardware can lack sufficient scale and performance to protect Internet-facing application infrastructures as they continue to grow. As organizations increasingly move more of their operations online, they need a cloud-based security solution that can defend their websites and other Internet-facing applications, safeguard business or customer data, and protect their brand image from harm. Inline and always on, the Akamai Intelligent Platform not only provides the scale and performance to protect organizations' Internet-facing presence today, but also the adaptability to respond to new attacks as they emerge in the future.

Sources:

I. Patrikakis, Charalampos, Masikos, Michalis, Zouraraki, Olga (Dec 2004). Distributed Denial of Service Attacks. The Internet Protocol Journal – Volume 7, Number 4. Retrieved from http://www.cisco.com/Web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

II. DuPaul, Neil (July 2013). The Real Cost of a Data Breach Infographic. Retrieved from http://blog.veracode.com/2013/07/the-real-cost-of-a-data-breach-infographic/

III. 2016 Data Breach Investigations Report. Verizon. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

IV. 2015 Cost of Cybercrime Study (Oct 2015). Ponemon Institute. Retrieved from http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states

V. Akamai State of the Internet - Security Report (Q1 2016). Akamai. Retrieved from https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/

VI. Facts and Figures. Akamai. Retrieved from http://www.akamai.com/html/about/facts_figures.html

Akamai FASTER FORWARD

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on www.akamai.com/locations.