Security in a Faster Forward World: Respond to a constantly changing threat landscape using a website protection service with on-demand scale
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>THE CHANGING THREAT LANDSCAPE</td>
<td>1</td>
</tr>
<tr>
<td>Denial-of-service attacks growing in size</td>
<td>1</td>
</tr>
<tr>
<td>Attacks shifting to the application layer</td>
<td>2</td>
</tr>
<tr>
<td>Targeting applications for data theft</td>
<td>3</td>
</tr>
<tr>
<td>A multi-dimensional security threat</td>
<td>4</td>
</tr>
<tr>
<td>Increasing frequency and costs of cybercrime</td>
<td>5</td>
</tr>
<tr>
<td>COMMON APPROACHES TO SECURITY</td>
<td>6</td>
</tr>
<tr>
<td>On-premise hardware</td>
<td>6</td>
</tr>
<tr>
<td>Website Protection Service</td>
<td>7</td>
</tr>
<tr>
<td>THE AKAMAI INTELLIGENT PLATFORM™</td>
<td>7</td>
</tr>
<tr>
<td>A natural architecture for web security</td>
<td>7</td>
</tr>
<tr>
<td>Stopping Attacks at the Edge</td>
<td>8</td>
</tr>
<tr>
<td>Internet security with global scale</td>
<td>9</td>
</tr>
<tr>
<td>Always-on security</td>
<td>9</td>
</tr>
<tr>
<td>Protect and perform</td>
<td>10</td>
</tr>
<tr>
<td>Improving security with threat intelligence</td>
<td>10</td>
</tr>
<tr>
<td>INTRODUCING KONA SITE DEFENDER</td>
<td>11</td>
</tr>
<tr>
<td>Preventing Direct-to-Origin Attacks</td>
<td>11</td>
</tr>
<tr>
<td>Defending Against Network-Layer DDoS Attacks</td>
<td>11</td>
</tr>
<tr>
<td>Defending Against Application-Layer DDoS Attacks</td>
<td>11</td>
</tr>
<tr>
<td>Defending against data theft</td>
<td>12</td>
</tr>
<tr>
<td>INTEGRATING INTO THE SECURITY ECOSYSTEM</td>
<td>13</td>
</tr>
<tr>
<td>Open Platform Initiative</td>
<td>13</td>
</tr>
<tr>
<td>Managed security services</td>
<td>14</td>
</tr>
<tr>
<td>WHY AKAMAI</td>
<td>15</td>
</tr>
<tr>
<td>Innovate without fear</td>
<td>15</td>
</tr>
<tr>
<td>Security that grows with you</td>
<td>15</td>
</tr>
<tr>
<td>Simplify your web security</td>
<td>16</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>16</td>
</tr>
</tbody>
</table>
Introduction

Organizations today operate in a Faster Forward world. By the end of 2013, almost 3 billion people will be 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 24/7 and employees can access the resources they need at any time in the global work day.

Hackers can more easily access a larger number of high-value corporate and government assets. And they 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 changing, and organizations must evolve to keep pace with the constant stream of new attacks.

When comparing different approaches to web 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 web 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 web security partner means much more than just protecting IT assets. The right partner can complement each organization’s online strategy with the appropriate 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 web experience for its users.

The Changing Threat Landscape

As long as organizations have operated online, hackers have looked for ways to attack them. As the Internet has evolved, the methods and techniques used by hackers have changed to take advantage of the vulnerabilities that exist. The challenge with web security lies in that changing nature. Hackers and other bad actors 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 web 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. 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 large botnets to generate distributed denial-of-service (DDoS) attacks with attack traffic several orders of magnitude greater in size. In a recent example, a hacktivist organization known as the al-Qassam Cyber Fighters (QCF) launched a series of DDoS attacks against U.S. financial institutions, including one attack on March 5, 2013, that used 3,200 bots to generate 190 Gbps in peak network traffic.
Two trends are driving the increase in the size of volumetric DDoS attacks – the growth in the number of connected devices and that of the computing power of every connected device. Not only are botnets 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. By 2020, Akamai predicts that the average DDoS attack will generate 1.5 Tbps of network traffic.

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 applications, coupled with a shortage of IT staff to adequately protect them, makes them highly attractive targets. In 2013, Gartner expects that 25% of DDoS attacks will target the application layer. Akamai customers reported 768 application-layer DDoS attacks in 2012 and 807 in the first three quarters of 2013.
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 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 54% of the total hacking-based data breaches. Two 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.

- **Account-checker** – 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 or share passwords across multiple accounts, hackers can create scripts that make repeated login attempts in order to deduce the login credentials and compromise an account.

These types of attacks can be difficult to detect. Both SQL injections and account-checkers 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 one recent high-profile attack, a hacktivists group used SQL injection to steal account information for over 1.6 million accounts belonging to US government organizations, including NASA, the FBI and the Pentagon, and posted them online.
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 are only 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 true goal of data or financial theft. At least three financial institutions were attacked in such a manner in mid-2013, where attackers stole millions of dollars during the confusion. This scenario highlights the danger of focusing on just one aspect of web security. 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 U.S. 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 than 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 noncritical website. With no web security in place, the organization saw page view errors spike by 1,327%.

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 24/7 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 web attack have fallen. The distribution of attacker toolkits and the ease with which newly discovered vulnerabilities can be shared have greatly democratized cybercrime. As a result, companies are experiencing attacks more frequently – the Ponemon Institute recently reported an average of 1.8 successful attacks per company per week in 2012, a 42% increase from 2011.\(^x\)

These attacks are imposing an even greater financial cost. Businesses increasingly depend on a variety of web 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 riskier, 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](image)

*Figure 3: The annual cost of cybercrime in 2012, as reported by the Ponemon Institute using a benchmark sample of 56 organizations in the US*
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-premise within their data centers. With this approach, organizations manage their own devices and retain control of their security posture. From a financial perspective, on-premise 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.

As with any inline solution, the challenge for on-premise 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:

Case Study: On-Premises Hardware WAF

This national retail chain sells directly to consumers through brick-and-mortar stores as well as their e-commerce website. When the retail chain tested an on-premise hardware WAF in front of their website, they measured a 50% 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 e-commerce site.

• 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 predicted to exceed 1.5 Tbps in size by 2020, on-premise hardware will continue to be a potential single point of failure.

• Performance – Defending against application-layer attacks can be extremely resource-intensive. For example, web Application Firewalls require a large amount of computing resources to compare incoming application traffic against 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.

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. As the size of potential DDoS attacks continue to grow, organizations will have to continue provisioning additional bandwidth to ensure sufficient scale.
Website Protection Service

Website protection services provide a new approach to detecting and mitigating security threats. Here, organizations deploy a third-party cloud platform in front of their private infrastructure to deliver network traffic from users to their websites and applications. The cloud platform can examine network traffic for known attack patterns and pass only legitimate traffic through to the web application. In addition, it operates inline so organizations are protected at all times without any human interaction. In addition, a website protection service can operate under a positive security model, allowing it to mitigate attacks that are new and have not been seen previously. This also provides improved protection against non-DDoS attacks such as SQL injection.

Some website protection services also provide acceleration services in addition to security. Because the service already delivers network traffic from users to the application, it can apply acceleration technologies simultaneously to not just reduce the performance impact inherent to any security solution, but actually improve the end-to-end performance of the web application.

As with any inline security solution, organizations must consider additional factors:

1. **Scale and Performance** – Organizations must be confident that the selected vendor can easily handle the network traffic not just for their web applications, but for all of its other customers as well. Organizations should evaluate the total capacity of the cloud platform’s infrastructure – 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.

2. **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 website protection service also complies with all applicable legal regulations to which they are subject.

The Akamai Intelligent Platform™

Akamai offers an inline cloud security solution based on our Intelligent Platform. Originally founded as the leading content delivery network (CDN), the Intelligent Platform has evolved beyond acceleration to provide network and application-layer security for websites and 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 proxy, the Intelligent Platform sits in front of websites and applications, delivering requests from users to the application and content from the application back to users. Its inline and distributed architecture provides two advantages when defending against both network and application-layer attacks:

1. **Inline** – The proxy architecture offers a natural location from which to defend against any type of web security threat. As traffic passes through the Intelligent Platform to the web 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 Intelligent Platform to apply both positive and negative security models as appropriate for additional flexibility.

2. **Distributed** – Users access websites and applications through an Akamai edge server that serves content directly to the user. This provides a distributed platform for delivering content, with many thousands of delivery endpoints that an attacker must target in order to disrupt the application.
Case Study: 2012 London Olympics

During the 2012 London Olympics, Akamai partnered with the London organizing committee to deliver live streaming video of Olympic events to audiences across the globe. At any point in time, millions of users watched the games with video content delivered through the Intelligent Platform’s geographically-distributed edge servers. Some of the highlights of the games were:

- August 1: 850 Gbps for the table tennis, men’s synchronized 3m diving, cycling and men’s kayak finals
- August 3: 803 Gbps for the archery, badminton and men’s trampoline finals
- August 5: 873 Gbps for the men’s 100m final (Usain Bolt wins gold in 9.63 seconds)
- August 9: 833 Gbps for the basketball semi-final and beach volleyball, soccer and women’s water polo finals

Despite record-breaking online audiences, Akamai kept all sites up through a 40x increase in attack traffic with 23 different attack types, including SQL injections and XSS. In the first full day of activities alone, Akamai processed 5.6 billion requests, automatically blocking 36.4 million and warning on an additional 33.8 million requests. Gerry Pennell, CIO of the London organizing committee, said, “We use a content distribution network, so it is very hard to launch a DDoS on us, because our front end is so dispersed.”

Stopping Attacks at the Edge

The Intelligent Platform is a distributed cloud platform comprising over 137,000 servers with points of presence in 87 countries and over 1,150 networks. The platform extends from the website or application to within one network hop of 90% of all Internet users. With this global reach, Akamai can detect and stop attacks at the edge of the network, closest to where they begin and before they reach their target.

With the Intelligent Platform, organizations no longer need to plan to defend against the largest potential DDoS attack. This allows them to reduce their capital and operational expenditures for on-premise hardware and network bandwidth. And when attacks do occur, the Intelligent Platform mitigates the attack before it reaches the application, helping organizations maintain their web experience for legitimate users.

Figure 4: As a distributed cloud platform, the Intelligent Platform stops attacks at the edge of the network before they reach the application.
Internet Security with Global Scale

Akamai architected the Intelligent Platform for a hyperconnected world, with the capacity to handle network traffic on a global scale. On any given day, Akamai delivers between 15 and 30% of total Internet traffic and has seen traffic in excess of 20 Tbps. This Internet scale provides a natural advantage when defending against the largest DDoS attacks today. For example, the QCF attack in March 2013 reached 190 Gbps of traffic and was one of the larger recorded DDoS attacks at the time. However, it was still several orders of magnitude lower than the average amount of traffic that Akamai handles on a daily basis.

<table>
<thead>
<tr>
<th>Absorbing the Largest DDoS Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>190 Gbps</td>
</tr>
<tr>
<td>Akamai Daily Traffic</td>
</tr>
</tbody>
</table>

![Figure 5: Akamai delivers daily average traffic almost 80 times larger than the peak traffic of the QCF attack in March 2013.]

Beyond raw bandwidth, the scale of the Intelligent Platform also provides a better defense against attacks at the application layer. 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 137,000 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.

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 the web application is 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% of all Internet 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 trade off 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 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 — that is protect web applications without requiring a tradeoff in application performance. The wide breadth of acceleration technologies also available for the Intelligent Platform allows it to protect web application infrastructures while improving application performance in order to maximize revenue and productivity at all times.

Improving Security with Threat Intelligence

The sophistication and complexity of application-layer 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 website and application deployments. Because of the global scale of the Intelligent Platform, Akamai can instantly detect new attack vectors as they are used. Akamai can then warn customers of an emerging threat or adjust the security posture of protected websites and applications. In addition, Akamai continuously develops rules to mitigate newly discovered attack vectors while refining existing ones to improve the accuracy of our website protection. Akamai sees the attacks against the largest and most popular web properties and brands, enabling all customers to benefit from any lessons learned. Akamai makes any rule changes available for all customers to leverage and contributes back to the OWASP and FS-ISAC organizations.

Case Study: SQL Injection

In Q3 2013, a major U.S. financial institution experienced an SQL injection attack. Over a three-hour period, an unidentified attacker in Southeast Asia used an SQL injection tool to send an average of 220 SQL injection requests per minute, hitting a peak of nearly 2,000 requests per minute. Akamai detected and blocked all of the SQL injection attempts without any intervention from IT staff, protecting the website from both data theft and potential denial of service.
Introducing Kona Site Defender

The Intelligent Platform provides the foundation for all Akamai solutions, including the Kona Security Solutions. Built on the Intelligent Platform, Kona Site Defender offers a comprehensive website protection service for the detection, identification and mitigation of DDoS and other application-layer attacks.

Preventing Direct-to-Origin Attacks

Providing the first layer of protection, Kona Site Shield cloaks the website or application server from the Internet, preventing users from directly connecting to it. Akamai then delivers web content to users through our globally distributed edge servers, preventing attackers from targeting the Origin directly and ensuring that all application traffic must pass through the Intelligent Platform, where it can be inspected for attack patterns by Kona Site Defender.

Defending Against Network-Layer DDoS Attacks

Users access websites and applications through globally distributed edge servers, which then proxy application traffic to the Origin. The Intelligent Platform 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 protection against the most common and bandwidth-consuming network-layer DDoS attacks.

Defending Against Application-Layer DDoS Attacks

Figure 6: Akamai continuously refines our Kona rule set to improve the accuracy and quality of web application security.

Figure 7: Akamai drops network-layer attacks at the edge of the network before it reaches the application.
Unlike with network-layer DDoS attacks, the Intelligent Platform 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, malformed or an excessive number of requests. Akamai defends against application-layer DDoS attacks in two ways. First, the global scale of the 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 Intelligent Platform’s 137,000 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 drop or throttle all application traffic from those IP addresses at the edge 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, a collection of rules based on OWASP and enhanced by Akamai security teams. 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 before they reach the application. Because of its distributed nature, the Kona WAF can inspect global traffic to the application without imposing any performance degradation. And because the Kona WAF scales with the Intelligent Platform, it ensures that websites and applications remain protected even as they grow.
Integrating into the Security Ecosystem

While Akamai provides website protection services, web security comprises only one part of any organization’s overall security posture. 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 web infrastructure on the 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 (APIs), organizations can automate how Kona Site Defender integrates with their existing security infrastructure or interacts 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 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 to enforce worldwide policies.

Case Study: Account Checkers

In the fall of 2012, a Vietnamese toolkit began spreading among organized criminal groups. Known as an account checker, this toolkit takes known user login information for an e-commerce site and attempts to gain access to other sites. Akamai discovered the toolkit shortly after it was first used by noticing patterns among login attempts at multiple e-commerce sites. Akamai then issued an alert to our ecommerce customers to warn them of this new type of attack and provided instructions on how to defend against it.

Because account checkers appear to make legitimate login attempts, this type of attack is difficult for individual organizations to defeat. Attackers can use anonymized IP addresses to quickly make a number of login attempts before moving to another target. However, the Intelligent Platform centralizes web security intelligence and provides the ability to detect patterns across all of Akamai’s customers.

Once Kona Site Defender detects a suspicious IP address, it can automatically apply rate controls to block or throttle either attempted logins from that IP address or attempts made to a specific account, while notifying the organization of a potential attack. Because account checking attacks are opportunistic, attackers will typically move on to another target once they see that they are being blocked or throttled.
**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 APIs 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 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 24/7 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 the leading acceleration platform, Akamai offers best-in-class website protection for organizations worldwide. The globally-distributed Intelligent Platform provides a natural architecture for web security, stopping attacks at the edge of the network before they reach websites and applications. Always on, the Intelligent Platform protects web infrastructure while helping organizations maintain the web experience for their users. By partnering with Akamai, organizations can augment their existing IT capabilities with a global web security posture that keeps pace with the latest security threats and grows with the needs of their business.

**Innovate without Fear**

In a hyperconnected world, websites and applications are increasingly becoming the face 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. As such, they are constantly changing, improving and innovating – not only with new websites and 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 inline at all times. Always-on protection frees organizations to continuously improve their web presence without the fear of exposing new vulnerabilities to attackers.

**Security that Grows with you**

Akamai front-ends many of the largest web 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 e-commerce sites. The Intelligent Platform is constantly growing – in both scale and performance – to meet the requirements of our global customers. In September 2013, the Intelligent Platform delivered a record amount of network traffic, peaking at 21.5 Tbps due to unprecedented demand. This was double the record set just one year prior, and six times the level set 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 web infrastructure. The Intelligent Platform provides organizations with the scale and performance necessary to defend against the largest network and application-layer attacks today, even as their web presence expands 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.

---

**Case Study: IBM Managed DDoS**

With over 20 years of cybersecurity assessment and response operations, IBM Security Services is a leading global provider of managed security services. IBM already offered a broad portfolio of security services, including firewall management, intrusion prevention and detection, identity and access management, and security information and event management. But with DDoS protection an increasing priority for its customers, IBM partnered with Akamai to combine their security expertise with Kona Site Defender and bring its Managed DDoS service to market.
Simplify your Web Security

With Akamai, organizations can simplify their web security posture by relying on a trusted third-party with a global security infrastructure. By stopping attacks at the edge of the network before they reach the application, Kona Site Defender reduces 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 Intelligent Platform also adapts to the changing threat environment, with Akamai security teams constantly developing and publishing new security rules 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 Intelligent Platform to simplify the web 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-premise hardware can lack sufficient scale and performance to protect web infrastructures as they continue to grow. As organizations move more of their operations online, they need a website protection service that can safeguard their websites and applications, business or customer data, and brand image from harm. Inline and always on, the Intelligent Platform not only provides the scale and performance to protect organizations’ web presence today, but also the adaptability to respond to new attacks as they emerge in the future.
I. Key ICT indicators for developed and developing countries and the world, International Telecommunications Unions, Feb 2013


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.