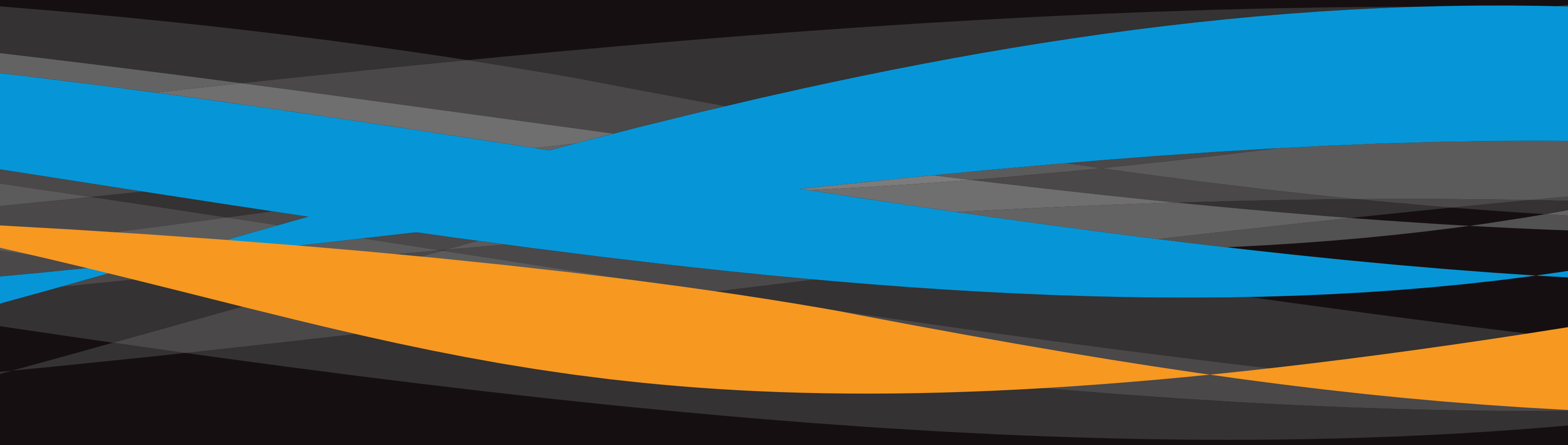


White Paper

Akamai Security Capabilities:
Protecting Your Online Channels and Web Applications

Table of Contents

Executive Summary

As companies continue to push their business-critical data and operations to the Internet, they must also take appropriate measures to protect these assets from the growing threats of the online world. From worms and viruses, to phishing and pharming, to botnets and denial-of-service attacks, the Internet's open infrastructure is an easy target for criminals looking to profit by stealing data, compromising systems, or otherwise disrupting the increasing amounts of business transacted online. To combat this proliferation of threats, enterprises need a multi-layered defense architecture that can protect their increasingly porous perimeter against potential attacks that are continually growing in sophistication and magnitude.

Situated at the entry point between end user requests and the enterprise's core infrastructure, the Akamai EdgePlatform can uniquely provide certain critical layers within a robust defense system. Leveraging its vantage point as the world's largest distributed computing platform, the EdgePlatform offers a broad range of flexible and highly scalable security capabilities to help customers extend their defenses out to the edges of the Internet and harden their infrastructure to the massive-scale attacks that are possible today.

This whitepaper gives a broad overview of the ways in which Akamai can help organizations bolster the security of their Web-based assets, with capabilities ranging across the application, network, and DNS layers, as well as solutions focused on Distributed Denial of Service (DDoS) mitigation and business continuity.

Introduction

The Threat Landscape

In recent years, there has been a dramatic rise in the scale and severity of attacks launched on Web sites and applications. Cyber crime has grown increasingly lucrative as companies migrate from mainframe to desktop to Web, relying more and more on the Internet for mission-critical data and operations. The Internet is now a virtual gold mine of sensitive data and valuable assets — but, unfortunately, its security stature has not yet caught up.

In fact, the opposite is occurring: vulnerabilities have multiplied as the Web becomes an increasingly complex and heterogeneous environment. Security plays second fiddle to the competitive pressures that drive unending cycles of rapid application development — so weaknesses and potential attack points are continually introduced. This means Web sites and applications are more susceptible to threats than ever. In fact, the Web Application Security Consortium recently found that more than 87% of Web applications carry a vulnerability classified as high risk or worse, with about half of the risks detectable through purely automated scanning.[1]

To make matters worse, malware has grown increasingly dangerous, as worms and viruses leverage ever more sophisticated techniques and become more difficult to detect and counteract. With stealthy use of advanced rootkits, social engineering, encryption, polymorphism, and the like, malware is propagating faster than ever across millions of unsuspecting hosts. As a result, botnets — the armies of infected zombie machines that carry out many of today's cybercrimes — have grown exponentially in recent years. The Georgia Tech Information Security Center estimates that as many as 34 million computers in the United States alone may now be part of a botnet.[2] Their numbers pose an enormous threat, because the zombie armies are both cheap and highly effective at executing any number of different cyber crimes, including DDoS attacks, data theft, spamming, phishing, and propagation of spyware and other malware.

No one is safe: recent, well-publicized attacks have crippled all types of establishments, from popular social networking sites to financial firms, from government organizations to the biggest names on the Web. With these attacks proving financially lucrative, a highly sophisticated criminal underground has formed, complete with an active black market for specialized services and clear ties to organized crime. While they deliberately fly under-the-radar, their impact is very real: cyber crime is estimated to now cost businesses an estimated $1 trillion a year.[3]

Defense Beyond the Perimeter

In order to mitigate operational risks and secure mission-critical infrastructure in such a challenging threat environment, enterprises need to employ a defense-in-depth strategy, using overlapping layers of protection to detect and deflect attacks across all tiers and access points of their infrastructure.

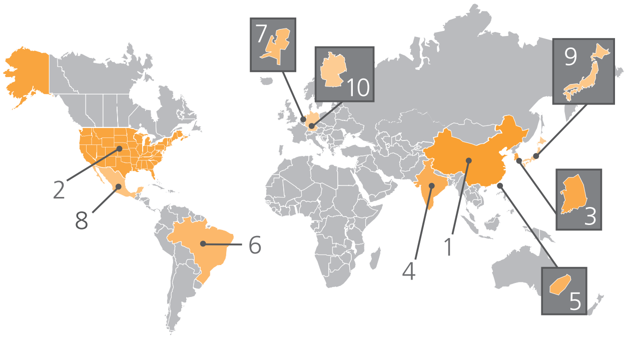
In addition to traditional perimeter-based solutions such as firewalls, intrusion detection systems, hardened routers, and other security appliances, a highly distributed, cloud-based defense system provides a necessary layer within the defense-in-depth approach, particularly as enterprise network perimeters become more porous to accommodate a growing variety of mobile devices, access methods, and client platforms.

An edge-based defense offers unique capabilities for combating the pervasive, distributed nature of the Internet's threats. It counteracts attacks at their source, rather than allowing them to reach the centralized perimeter. In addition, an edge architecture is the only one that can scale sufficiently to absorb and deflect the massive-scale attacks that today's botnets are capable of — including DDoS onslaughts that can barrage sites with traffic levels hundreds of times higher than usual.

Figure 1: Attack Traffic, Top Originating Countries

Data from Akamai's network shows that attack traffic sources continue to fluctuate, as the Internet's global, interconnected nature makes cybercrime an equal-opportunity employer. These and other Internet statistics are published quarterly in Akamai's State of the Internet reports.

	Country	% Traffic	Q1 09 %
1	China	31.35%	27.59%
2	United States	14.63%	22.15%
3	South Korea	6.83%	7.53%
4	India	3.93%	1.60%
5	Taiwan	2.32%	2.22%
6	Brazil	2.29%	2.60%
7	Netherlands	2.06%	1.16%
8	Mexico	1.96%	1.21%
9	Japan	1.95%	1.79%
10	Germany	1.93%	2.95%
–	OTHER	30.75%	–



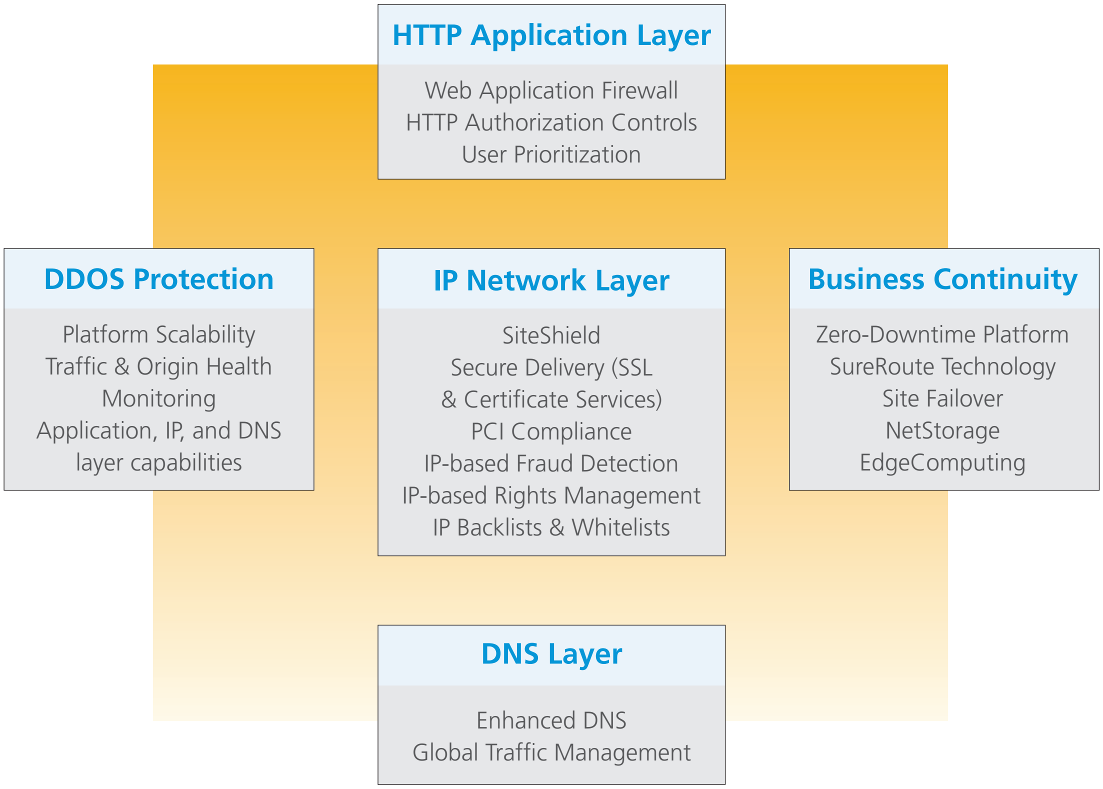
Akamai Security Capabilities

Akamai secures, monitors, and operates the Akamai EdgePlatform, the world's largest, on-demand distributed computing network, with more than 50,000 servers across more than 1,000 networks, located in 70 countries around the world. With a proven track record over a decade long, Akamai now delivers approximately one-fifth of all Web traffic and counts many of the world's leading enterprises as its customers, including:

- Three of the top five online brokerages
- Nine of the top 10 antivirus companies
- All the branches of the U.S. military
- Over 150 of the world's leading news portals
- 85 of the top 100 online U.S. retailers, delivering over $100 billion in e-commerce transactions annually through Akamai

Designed with security, resilience, and fault-tolerance at the forefront, Akamai's Edge-Platform is a proven platform for providing flexible and intelligent edge-based defense capabilities at all layers of the OSI stack, as shown in Figure 2. These cloud-based capabilities help organizations lock down their security perimeter and bolster their defense-in-depth architecture with the highly flexible and scalable protections needed to combat current day threats. Moreover, Akamai's innovative approach overcomes the traditional tradeoff of sacrificing performance and availability for increased security.

Figure 2:
Akamai's proven EdgePlatform offers a broad range of highly scalable security capabilities that combat cyber threats at the application layer, IP network layer, and DNS layer, and offer DDoS mitigation and Business Continuity solutions across all tiers of infrastructure.



HTTP Application Layer

Web Application Firewall
HTTP Authorization Controls
User Prioritization

DDOS Protection

Platform Scalability
Traffic & Origin Health Monitoring
Application, IP, and DNS layer capabilities

IP Network Layer

SiteShield
Secure Delivery (SSL & Certificate Services)
PCI Compliance
IP-based Fraud Detection
IP-based Rights Management
IP Backlists & Whitelists

Business Continuity

Zero-Downtime Platform
SureRoute Technology
Site Failover
NetStorage
EdgeComputing

DNS Layer

Enhanced DNS
Global Traffic Management

Application Layer Security

More and more cyber attacks are bypassing traditional firewall and email-specific security controls by using increasingly sophisticated HTTP-layer attacks to target Web sites and applications. Unfortunately, Web applications' heterogeneous nature, combined with continual, rapid development cycles, often leaves many doors open to exploit. In fact, security firm Sophos estimates that in 2008, there was a Web page infected every 4.5 seconds. [4]

This trend drives the needs for firewalls and other security defenses that can understand and analyze Web traffic payloads such as HTTP, HTTPS, and XML — and provide protection against treacherous application-layer threats such as cross-site scripting (XSS), buffer overflow exploits, and SQL injection attacks. Akamai delivers this type of protection at the edge of the network, augmenting traditional defense solutions with an unprecedented level of built-in redundancy and scalability.

Web Application Firewall (WAF)

Akamai's Web Application Firewall service is a highly scalable edge defense system with the ability to detect potential attacks in HTTP and SSL traffic as it passes through the EdgePlatform, before reaching the customer's origin data centers. The WAF service gives customers the ability to set up traffic blocks or alerts based on rules that either check for the presence of specific data like cookies, client certificates, and referrer fields, or detect anomalous and potentially malicious patterns in HTTP request headers. Based on a translation of the open source ModSecurity core rule set (CRS), Akamai WAF's protects against the most common and harmful types of attacks, including XSS and SQL injection.

WAF is unique in its highly distributed architecture, which enables both instantaneous scaling of defenses as needed as well as filtering of corrupt traffic as close to the attack source as possible. Moreover, unlike a centralized firewall, WAF does not create any performance chokepoints or single points of failure that often prove to be easy targets for attackers.

Akamai's Web Application Firewall uses configurable, rule-based application layer controls to prevent the following types of attack vectors:

- Protocol Violations
- Request Limit Violations
- HTTP Policy Violations
- Malicious Robots
- Generic and Command Injection Attacks
- Trojans Backdoors
- Outbound Content Leakage (Server Banners)

Not every type of Web application attack is best dealt with as it passes through Akamai's infrastructure. Some classes of attacks may be better addressed using detailed knowledge of the specific applications, databases and network infrastructure in the customer data center. Thus, WAF provides a highly flexible and efficient outer defense layer that works both as a stand-alone service and as a complement to other Web application protection systems — enhancing the robustness and scalability of those systems by migrating some of their functions to the Akamai platform so that centralized defenses can focus on more application-specific protections.

HTTP Authorization Controls

Akamai offers various authorization mechanisms that allow customers to retain full control over proper distribution of their access-controlled content, while still enjoying the enhanced performance and scalability offered by the Akamai network. The customer designates which content requires authentication and what authorization mechanism to use. These mechanisms include:

- **Centralized User Authentication.** The protected content resides on Akamai's edge servers but each end user request is authenticated by the customer origin server before delivery, enabling centralized control while taking advantage of the high performance of offloaded delivery.

- **Edge User Authentication.** Akamai's edge servers authenticate user requests for content on behalf of the customer origin server. This unique feature works based on a combination of encrypted cookies and special content URLs, dynamically generated by the customer origin server. The customer retains complete flexibility to choose the criteria with which to grant or restrict access, but the authentication and delivery process are completely offloaded to Akamai.

- **Akamai Authentication.** This is a flexible and robust mechanism to authenticate Akamai's edge servers to the customer's origin server using a shared secret key. This means the origin server can securely authenticate requests from any server in the Akamai network without using a preset list of IPs or other more rigid mechanism.

User Prioritization

Akamai offers the capability to manage flash crowd situations where the customer's application server is at risk of failure. By monitoring application server health, Akamai is able to throttle load to the server when necessary, redirecting excess users to alternate, cached content — a virtual waiting room which keeps them engaged on the site and keeps the origin server from becoming overloaded. This offers a double benefit, as case studies show that recovering traffic levels after a site failure (where the site is completely inaccessible) takes much longer than recovering from a site slowdown.

Network Layer Security

While cyber attacks are growing in sophistication and an increasing number of the most devastating attacks are focused on the application layer, the IP layer still accounts for nearly two-thirds of attacks today.[5] Accordingly, defenses that harden this fundamental layer of Internet communications are essential to the security of any Web infrastructure. Akamai leverages its unique architecture and real-time Internet knowledge base to offer a number of capabilities that help secure the network layer.

SiteShield

Akamai's SiteShield service helps protect the customer origin server by cloaking it from the public Internet — that is, removing it from the Internet-accessible IP address space. This mitigates risks associated with network-layer threats, including lower layer DDoS attacks that direct target the origin server.

SiteShield works by allowing the customer's firewall to restrict incoming connections to Akamai SiteShield servers only, rather than leaving the standard HTTP/S ports 80 and 443 open and vulnerable to all incoming connections. SiteShield servers can be configured to communicate with the origin on non-standard ports as well to provide additional port masking protection. Akamai's EdgePlatform intercepts and fulfills each end user request, on the customer's behalf, communicating securely and "invisibly" with the origin server as necessary to retrieve content that is not in cache.

Customer Case Study: SiteShield

Akamai SiteShield protects U.S. Citizen and Immigration Services

When the U.S. Citizen and Immigration Servers (USCIS) wanted to both streamline its infrastructure and provide cost-effective protection against denial-of-service attacks, it choose Akamai, leveraging both the Dynamic Site Accelerator and SiteShield solutions. According to Stephen Schillinger, Chief of Web Services Branch, USCIS, "SiteShield provides us with peace of mind. With it, we know our Web infrastructure will be safe from attack, and will remain available despite any issues that may happen within the USCIS environment."

"Akamai guarantees that our site is always available and that our users will have as good an experience as possible."

— Stephen Schillinger, Chief of Web Services Branch, USCIS

Secure Delivery (SSL & Digital Certificates)

Akamai delivers SSL-secured content over a network that is engineered to meet stringent financial services industry standards. The Secure Delivery service enables customers to enjoy Akamai's performance, reliability, and offload benefits while delivering content protected by SSL encryption and authentication.

Digital Certificates. In order to facilitate secure and trusted transactions, Akamai provides a number of SSL certificate options to meet different customer business requirements. These include single hostname, wildcard, and Extended Validation certificates, as well as a seal option that displays a trust logo on the secure Web site or application.

Cipher Strength. Akamai edge servers can be configured to require a minimum cipher strength in any SSL connection request. Requests that do not meet the minimum can be denied or sent to an alternate page with upgrade requirements.

PCI Compliance

The Akamai SSL network is certified to the Payment Card Industry Data Security Standard (PCI DSS) Level 1 Service Provider guidelines. The Akamai SSL network is scanned quarterly by an Approved Scanning Vendor (ASV), plus assessed and audited annually by an independent Qualified Security Assessor (QSA). PCI compliance is required of all systems worldwide that process, store, or transmit credit card data. Akamai's PCI certification allows customer organizations to streamline their own certification process and ensure protection of their sensitive user transaction data.

IP-Based Fraud Detection

Akamai offers fraud detection capabilities based on its ability to provide real-time geographic data (such as country, state/region, city, latitude and longitude, or zip code) for each end user request, based on IP information. This data is made available via a simple API that can be integrated into the content provider's Web application server. The data can be used, for example, to verify address information entered by the end user; mismatched locations may signal the need for a second level of verification. IP-based fraud detection also enables blocking of requests from open or anonymous proxies that are a high security risk.

IP-Based Rights Management

Similar to its IP-based fraud detection capabilities, Akamai's ability to validate end user geography in real time helps content providers ensure that digital goods and information are delivered only to users in authorized geographies. With this capability, customers are able to enforce contractual or legal obligations, protecting their assets while reducing the occurrence and expense of distributing products to unauthorized locations and users.

IP Blacklisting/Whitelisting

Akamai offers the capability to allow or deny a request based on IP address:

- Blacklist: deny access to a list of specific IPs (and/or CIDR blocks)
- Whitelist: allow access to a list of specific IPs (and/or CIDR blocks) without further inspection
- Strict Whitelist: allow access to a list of specific IPs without further inspection; all other IPs are denied

This capability can be leveraged both for access control as well as mitigation of DOS attacks.

DNS Security

A Web site or application's DNS (Domain Name System) infrastructure is a critical but often under-deployed part of its overall infrastructure. DNS failure can devastate an organization's Web operations, yet many enterprises rely on just two or three DNS servers, often residing in the same network or even the same data center — making them vulnerable to server failures, power losses, or network outages, as well as DNS-based attacks. Akamai offers a number of options for customers looking to fortify their DNS system against such vulnerabilities.

Enhanced DNS (EDNS)

Akamai's Enhanced DNS service provides a secure, robust and scalable outsourced DNS solution to reliably direct end users to an organization's Web sites and applications. Configured as an authoritative Secondary DNS service, EDNS enables the customer to leverage the unparalleled performance, scalability, and reliability of Akamai's distributed global nameserver platform without changing their existing DNS administration processes.

Using EDNS, the customer's primary DNS servers are not directly exposed to end users, therefore mitigating the risk of cache poisoning and denial-of-service attacks. Moreover, EDNS leverages a number of technologies, including IP Anycast, secured zone transfers, router-protected name servers, and non-BIND-based DNS to provide customers with a highly secure and fault-tolerant solution.

Global Traffic Management (GTM)

Akamai's Global Traffic Management is a highly scalable, cloud-based offering that enables companies with origin servers in multiple geographies to optimize the availability and performance of their Web applications. GTM leverages Akamai's globally distributed dynamic DNS system to direct user requests to the best origin location based on customer-configured rules that encompass business policy and real-time Internet and origin server performance conditions that are continually monitored by Akamai's EdgePlatform. Dynamically configurable business policies include automatic failover, weighted load balancing, or IP-based routing.

GTM can also be employed to help mitigate DDoS attacks that are emanating from localized regions. By leveraging real-time geographic information about each request, GTM can be used to set up a black hole — directing traffic from attack regions to nonexistent or nonresponsive machines — while directing legitimate traffic to the true origin servers.

Denial-of-Service Mitigation

Distributed Denial of Service (DDoS) attacks have become one of the most visibly disruptive forces in cyberspace. While some DDoS attacks are politically or socially motivated, many are financially driven — either by companies hiring cyber criminals to attack competitor sites, or by the criminals themselves blackmailing companies with the threat (or reality) of severe business disruption.

Unfortunately, with the proliferation of botnets, the size and scale of DDoS attacks has skyrocketed. According to Arbor Networks, the largest DDoS attacks grew a hundred-fold in seven years, from 400 Mbps in 2001 to 40 Gbps in 2007.[6] The July 4th attacks of 2009 were yet another order of magnitude larger, as Akamai Technologies absorbed attack traffic in excess of 200 Gbps on behalf of its under-siege customers.

The First Line of Defense: Massive Scale

Akamai's highly distributed global network of 50,000 security-hardened servers routinely delivers worldwide Web traffic at an aggregate rate ranging from 800 Gbps to over 2 Tbps. With its massive scale and real-time dynamic resource allocation capabilities, Akamai's EdgePlatform is uniquely able to help its customers successfully withstand DDoS storms that can drive traffic levels to hundreds of times higher than normal. Moreover, Akamai's intelligent load balancing and routing system ensures that the attack traffic does not degrade performance for legitimate end user requests — for any of Akamai's customers.

Traffic and Origin Health Monitoring

With servers in 3,000 locations across 1,000 networks worldwide, the EdgePlatform continually monitors and analyzes Internet health in real time. This includes data on traffic levels across different geographies, backbone health, DNS server health, and BGP churn. With aggregate and customer-specific alerting mechanisms triggered by unusual traffic patterns, Akamai's unique, up-to-the-minute view of the global Web enables proactive identification of traffic attacks and their sources. Akamai can also provide origin health monitoring for customers, which detects slowdowns in origin response times due to overload.

Additional DDoS Mitigation Capabilities

Because there is no simple, one-size-fits-all solution to combat the many varieties of DDoS attacks, it is critical to have a defense system that can quickly be tailored to the characteristics of each specific attack. Akamai's flexible, metadata-driven EdgePlatform does this, offering a broad suite of potential protective responses and the ability to dynamically employ any number of them in the midst of an attack.

DDoS mitigation spans all the tiers of an application's infrastructure, including the application, network, and DNS layers. Thus, many of the services we have already covered — including Web Application Firewall, SiteShield, Enhanced DNS, and Global Traffic Manager — provide specific DDoS mitigation capabilities as mentioned in their descriptions above. The EdgePlatform's other DDoS capabilities include:

- Blocking or redirecting requests based on characteristics like IP address, originating geographic location, or query string patterns
- Black-holing attack traffic through DNS responses
- Using slow responses (tarpits) to shut down attacking machines while minimizing effects on legitimate users
- Directing traffic away from specific servers or regions under attack
- Limiting the rate at which requests are forwarded to the origin server in order to safeguard its health
- Quarantining suspicious traffic to a small set of servers
- Serving customized error pages during the attack (cached on the Akamai network)
- Cookie-checking to identify abnormally high levels of new users, which may indicate an attack
- Directing illegitimate traffic back to the requesting machine via a DNS response.

Customer Case Study: DDoS Mitigation

Akamai protects U.S. government from unprecedented DDoS attacks: Targeted site sees eight years' worth of traffic in a single day

On July 4th, 2009, the U.S. government faced the largest DDoS attack in its history, with the top-targeted site receiving nearly 8 billion page views in a day, resulting in traffic levels that peaked to nearly 600 times normal. The attack came in several waves and lasted more than a week, with 48 sites targeted in all. Despite the unprecedented scale of the attack, all of the U.S. government sites delivered via Akamai — including sites for the White House and 13 of the 15 Federal Cabinet level agencies — remained online, thwarting the attacker's goals.

At the peak of the attack, Akamai absorbed more than 200 Gbps of attack traffic targeted at the government sites. At the same time, Akamai continued serving traffic to legitimate users and maintained 100% availability for all of its customers, delivering traffic at over a Terabit per second for the rest of its customer base.

Business Continuity

Web site downtime can cost companies millions of dollars in lost revenue and productivity, making business continuity and disaster recovery planning more important than ever. Enterprises that rely on traditional, centralized Web infrastructure are particularly vulnerable to disasters both natural and man-made — from earthquakes and denial-of-service attacks to cable cuts, power outages, and misconfigured routers. In contrast, Akamai's highly distributed architecture provides multiple layers of protection that help to ensure the uptime of business-critical Web infrastructure.

Like DDoS mitigation, business continuity spans all the different tiers of an application's infrastructure. Previously described services such as **Global Traffic Management** and **User Prioritization** are part of the arsenal of disaster recovery tools offered by Akamai. These capabilities, as well as the following ones, help enable our customers to continue their business operations — delivering site and application functionality — in the face of serious network, routing, or origin server failures.

Zero-Downtime Delivery Platform

Akamai's massively distributed network was built from the ground up with redundancy and fault tolerance at every level. Designed to self-heal from all types of failures — whether at the machine, data center, network, or Internet-wide level — Akamai's network provides a true high-availability platform for Web content and application delivery, reducing the customer's need to maintain their own failover infrastructure. The EdgePlatform dynamically routes around failures and trouble spots to continually deliver content, quickly and reliably, from optimal edge servers near end users.

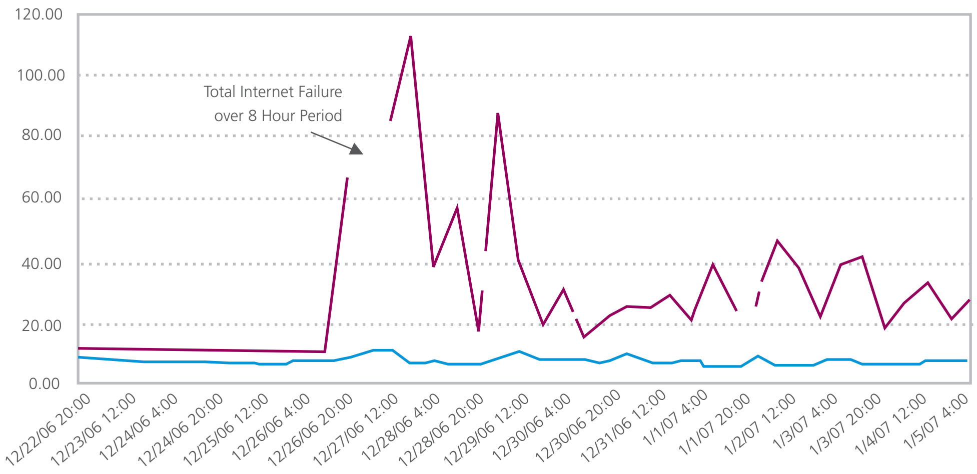
Improved Reliability for Dynamic Content

With its Dynamic Site Solutions and Application Performance Solutions, Akamai offers the ability to enhance reliability and performance even for dynamic, uncacheable content and applications. Leveraging its SureRoute technology, the EdgePlatform can route dynamic content around major Internet problems that can otherwise cut off connectivity.

During the Taiwan earthquake of 2006, for example, Akamai measured an 8-hour Internet outage as undersea network cables were severed. However, Akamai was able to route around the problem and continue delivering dynamic content without performance degradation, while online business not leveraging Akamai experienced total failures or severe degradation for weeks.

NetStorage

Web Transaction Times Following the December 26 Earthquake in Taiwan



While other Internet transactions across Asia suffered for weeks after an earthquake severed undersea network cables, Akamai continued delivering dynamic content without interruption or performance degradation.

NetStorage is Akamai's secure, distributed, high-availability storage service. Customers can host any type of content, including media libraries, software downloads, or entire Web sites through this scalable, on-demand service. NetStorage will automatically replicate the content to multiple locations. This ensures robust fault tolerance as well as improved performance as content requests are directed to the optimal location. NetStorage is an ideal solution for companies looking to manage the most minimal, streamlined in-house infrastructure possible.

Site Failover

By taking the first hit and absorbing traffic spikes for the origin infrastructure, Akamai provides a strong layer of protection from flash crowds and denial-of-service attacks. However, with its Site Failover solution, Akamai also provides multiple options for Web site continuity in case of origin server failure.

Site Failover offers three main options in case of origin failure:

- **Failover to edge servers.** Customers can opt to either have Akamai's edge servers serve a default failover page or serve the most recent (expired) content in cache.

- **Failover to alternate site.** Akamai will direct users to a backup site, which may have reduced functionality or otherwise be different from the original site

- **Failover to Akamai NetStorage.** Customers can host a full backup version of their site on Akamai's high-availability NetStorage service. In case of origin server failure, Akamai will direct end users to the customer site on NetStorage, so that, companies are guaranteed a robust Web presence regardless of origin server availability or Internet conditions.

EdgeComputing

Akamai's EdgeComputing service allows companies to deploy J2EE applications onto the zero-downtime EdgePlatform network, bringing unmatched performance, scalability, and reliability to Web applications. Both the presentation layer and application business logic are executed on the Akamai network, so applications that are backend-light or are based on infrequently changing data — such as product catalogs, store locators, contests and giveaways, user registration, and site search — can be run with only minimal, occasional roundtrips to an origin database, or without any origin infrastructure at all.

Akamai: Building a Better, More Secure Web

As the capabilities of cyber attackers continue to grow in scale and sophistication, enterprises need to be innovative and proactive in protecting their Web infrastructure and digital assets. Traditional, centralized security systems are no longer enough, as they lack the scalability and reach to defend a perimeter that now extends to the edges of the Internet.

For this reason, highly distributed, cloud-based protections have become a necessary layer within any defense architecture. These types of solutions help overcome the challenges posed by the inherently distributed nature of the Internet. They offer unprecedented, on-demand scalability, flexibility, and performance, as well as the power to mitigate attacks at their source, before those attacks have a chance to reach the company's core infrastructure.

Akamai has spent the last decade making the Internet a better, faster, and more secure place to transact business. With thousands of companies depending on its EdgePlatform to securely and reliably deliver an aggregate of 500 billion Web interactions each day, security is never a secondary priority at Akamai. Instead, it is comprehensively integrated into every aspect of Akamai's network and operations, from hardened servers and a self-healing architecture to the rigorous physical and operational security policies in place.[7]

Organizations looking to lock down their perimeter at the edge of the Internet can leverage Akamai's proven expertise and unique global platform through its broad array of security solutions and capabilities. These capabilities, along with Akamai's integrated, flexible, and comprehensive set of content and application services, will continue to help enterprises across all industries achieve their business goals, by delivering their mission-critical Web applications — securely, responsively, and reliably.

[1] http://projects.webappsec.org/Web-Application-Security-Statistics.

[2] http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf.

[3] http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html.

[4] http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

[5] http://www.arbornetworks.com/report. Arbor Networks Worldwide Infrastructure Security Report, Volume IV. October 2008.

[6] http://asert.arbornetworks.com/2008/11/2008-worldwide-infrastructure-security-report/. Arbor Networks Infrastructure Security Report, Volume IV, 2008.

[7] For more information, see the Akamai Information Security Management System Overview, which discusses Akamai's comprehensive network and operational security policies in greater detail.

The Akamai Difference

Akamai® provides market-leading managed services for powering rich media, dynamic transactions, and enterprise applications online. Having pioneered the content delivery market one decade ago, Akamai's services have been adopted by the world's most recognized brands across diverse industries. The alternative to centralized Web infrastructure, Akamai's global network of tens of thousands of distributed servers provides the scale, reliability, insight and performance for businesses to succeed online. Akamai has transformed the Internet into a more viable place to inform, entertain, interact, and collaborate. To experience The Akamai Difference, visit www.akamai.com.

Akamai Technologies, Inc.

U.S. Headquarters
8 Cambridge Center
Cambridge, MA 02142
Tel 617.444.3000
Fax 617.444.3001
U.S. toll-free 877.4AKAMAI
(877.425.2624)

www.akamai.com

International Offices
Unterfoehring, Germany
Paris, France
Milan, Italy
London, England
Madrid, Spain
Stockholm, Sweden
Bangalore, India
Sydney, Australia
Beijing, China
Tokyo, Japan
Seoul, Korea
Singapore

Akamai
Powering a Better Internet

©2009 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice.