White Paper

Leveraging Cloud Security to Weather Threatening Storms

How to Defend Your Perimeter from Today's Outsized Threats

Table of Contents

Executive Summary

While threats to network and information security have existed since the dawn of the information age, the complexity and scale of attacks have exploded in recent years, presenting enterprises with daunting challenges as they struggle to defend an increasingly vulnerable perimeter. With cyber crime now more lucrative, and far less risky, than the illegal drug trafficking trade, it is hardly surprising that the level of criminal talent devoted to the Internet has risen tremendously.[1] Consequently, threat levels and attack impact have skyrocketed. For example, in just a few years, Distributed Denial-of-Service (DDoS) attacks have jumped in size from dozens to hundreds of gigabits per second — a result of increasingly sophisticated malware and growing zombie armies.

Unfortunately, traditional perimeter defense solutions have not kept pace with the rapid growth in risk. While enterprises currently have an arsenal of threat-specific tools at their disposal, these rigid, centralized defenses do not provide the flexibility or scale necessary to combat the outsized, adaptive threats facing today's IT infrastructure.

Cloud-based security services offer an innovative approach to helping organizations address the limitations of traditional perimeter solutions by adding a globally distributed layer of defense. This instantaneously scalable layer is designed to deliver a level of protection that is orders of magnitude greater than any centralized defense.

In addition, cloud security solutions offer unprecedented flexibility across a broad set of protective capabilities. This allows companies to leverage just-in-time defenses that help them adapt to rapidly changing risks and protect against unknowable future threats, while avoiding the costly proposition of having to correctly predict — and pay for — their security needs in advance.

This paper assesses the current cyber threat environment and discusses the use of distributed cloud services as an effective means to protect against evolving, modern-day IT threats. It takes a close look at DDoS defense in particular, and provides actionable strategies for leveraging cloud security services to provide a robust layer of defense in an increasingly threatening Internet environment.

Defending Your Perimeter

A Brave New World: Today's Outsized Threats

More new malicious code vulnerabilities were introduced in 2008 than in the previous 20 years combined. That number was surpassed again in just the first half of 2009, with a new threat signature appearing every eight seconds.[2] Such is the challenge IT organizations face today: while their businesses are relying more and more on the Internet for mission-critical communications and operations, serious security risks are proliferating and causing greater enterprise-wide impact.

In part, this is due to the reality that enterprise IT infrastructure has become increasingly complex and difficult to secure. The enterprise perimeter grows increasingly porous as organizations migrate from desktop to Web and mobile Web. Moreover, in the race to take full advantage of the Web's potential, security is often neglected.

Security firm Sophos estimates that a new Web page is infected every 3.6 seconds.[3] Today's highly complex Web environments and unending rapid application development cycles result in the continual introduction of new security flaws — many of which are severe. According to the Web Application Security Consortium, more than 87% of Web applications currently carry a vulnerability classified as high risk or worse.[4]

Attackers are quick to take advantage. Sitting behind these open vulnerabilities is a wealth of valuable assets and business-critical operations. Whether through business disruption, data theft, or system compromise, today's exploiters enjoy lucrative rewards at businesses' expense. Estimates put the business cost of cyber crime at $1 trillion in 2008 alone.[5] Low risk and even lower barriers to entry add to the attraction, resulting in a flourishing shadow underground that includes growing number of well-organized crime rings.

These criminals also leverage an increasingly powerful arsenal of tools. Botnets have become one of their most potent weapons, enabling attackers to control large armies of zombie machines with little effort. This magnifies and multiplies the size of possible attacks. In 2007, a crippling, month-long attack launched against the Estonian government and other commercial entities was found to have been the work of a single, disgruntled student.

Illicit botnets can be harnessed to make money in any number of ways:

- **Stealing passwords, credit card numbers or other sensitive data.** Stolen account information earns anywhere from $10 to $1000 per account, depending on the country and the type of data. When security researchers at UC Santa Barbara seized control of the Torpig botnet for 10 days, they recovered enough stolen bank account information to earn them an estimated $8.3 million.[6]

- **Launching DDoS attacks.** While some distributed denial-of-service (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. In 2008, cyber criminals earned an estimated $20 million from DDoS attacks.[7]

- **Protecting phishing and other criminal sites with fast flux technology.** Botnet masters can earn anywhere from $1000 to $2000 per month for each site hosted.[8]

- **Sending spam, distributing malware, engaging in click fraud**, or renting out the bot network to do any of these types of activities. Worldwide, spam will cost businesses roughly $130 billion, according to Ferris Research.[9]

Those who lack the skills to create their own zombie army can either purchase the malware needed, or simply purchase a botnet itself, for as little as pennies per bot.[10] In fact, as financial rewards have propelled a sharp rise in cyber crime, a sophisticated black market has evolved, with vendors each marketing their own specialized skill set. There are malware authors who sell their code and subscription-based support, botnet owners who rent out the services of their zombie army, money launderers who monetize stolen account information, and even escrow services that guarantee financial transactions between parties.[11]

Now, botnets are growing ever larger and more resilient. As many as 34 million computers in the United States may currently be part of a botnet, a 50% increase over last year.[12] Conficker, the largest known zombie army, was first identified in late 2008 and acquired between 3 and 6 million machines within just a few months.

This ominous trend indicates that the number and severity of cyber attacks will continue to increase at an alarming rate. Recent, well-publicized attacks have targeted all types of organizations, from financial firms to government organizations to many of the biggest names on the Web. The threats are growing exponentially — and getting more insidious with each iteration.

Traditional Approaches to Perimeter Security are No Longer Sufficient

Considering the difficult threat environment, ensuring enterprise perimeter security is a greater challenge than ever before. From Web site defacement to data breaches, service interruptions to network infection, organizations constantly face a host of potentially crippling threats. Organizations typically rely on a number of different point solutions — such as firewalls, intrusion prevention systems, and network scanning solutions — to defend their perimeter. Unfortunately, these traditional, centralized approaches to security often fall short when it comes to meeting modern enterprise security needs. Traditional defenses alone are unlikely to provide the flexibility or scale necessary to defend against today's outsized and massively distributed threats.

Traditional perimeter defense systems also tend to be rigid. They focus on protecting the enterprise from specific types of attack, often creating bottlenecks that open doors to other types of attacks in the process. Successfully integrating these systems often takes significant time and may require re-architecting core infrastructure. This means you need to decide in advance which protections you need most, since protecting against all known vulnerabilities is cost prohibitive. But if you don't guess correctly, your business pays the price.

Moreover, as the magnitude of potential threats increases, centralized defenses typically fail to scale to the level necessary to secure the enterprise. For example, provisioning a site to handle a DDoS attack that drives traffic levels to hundreds of times normal volume is simply impossible with a centralized infrastructure.

Cloud-Based Perimeter Security – Turning a Threat into an Asset

More and more frequently, mission-critical assets are being made available over the Web, hosted on cloud services, and accessed via mobile devices. In this dynamic and distributed environment, the conventional "defend the fort" mentality no longer provides a sufficient security paradigm. Instead, to mitigate today's pervasive and evolving threats, enterprises need to embrace the distributed nature of the Internet cloud, using its scale and flexibility to their advantage when implementing a defense-in-depth strategy.

Defense-in-depth means deploying overlapping layers of security that employ a diverse set of tactics to protect against threats. Cloud-based security provides a critical layer within this approach, helping to overcome limitations inherent in more rigid, traditional perimeter defense solutions. As with other cloud computing services, cloud-based security solutions offer cost-effective, on-demand capabilities that reduce IT planning and maintenance overhead.

Not all cloud services are created equal, however. In order use the unique strengths of the cloud to their advantage, enterprises must find security solutions that leverage a highly distributed, multi-network platform — one that can deliver massive scale at the edges of the Internet and protect core origin infrastructure by deflecting attacks closer to their source. Offerings built on this type of architecture help organizations combat today's Internet threats in an innovative way that no centralized solution can offer. They provide:

- **Unmatched Scalability.** Only a large, highly distributed architecture can withstand and deflect attacks of the magnitude being observed today. The key is using a service that can scale instantaneously and on demand.

- **Flexibility and Adaptability.** By offering the ability to provision a variety of capabilities quickly and easily, without requiring changes to core infrastructure, cloud-based security solutions are designed to enable effective defenses that are adapted to each unique attack. Enterprises can employ new business logic, use targeted capabilities, and turn strategies on and off as warranted to best counteract the specific attack while maintaining availability for legitimate users.

- **Cost Efficiency.** Cloud services help enable organizations to overcome the costly problem of "guessing right" in their defense and capacity planning. Capabilities and resources are cost-effectively provisioned on demand, as needed, with a goal of ensuring that businesses have exactly the right amount provisioned at all times.

- **Superior Redundancy.** Unlike centralized architectures, a defense layer that spans a thousand-plus networks and locations is structured to offer unmatched, built-in reliability and redundancy against the Internet's many potential threats and failures.

- **Improved Performance.** Traditional defense systems typically sacrifice performance for security, but a highly distributed platform boosts response times instead, by handling requests at the edge of the Internet and counteracting attacks at their source.

- **Holistic Integration.** A successful defense-in-depth strategy requires overlapping security layers that work in concert. Cloud security services should integrate with conventional perimeter security solutions, providing additional robustness for the enterprise's existing security architecture.

- **Global Purview.** Highly distributed cloud providers have the unique vantage point of a real-time, global view of the Internet's health, enabling more proactive identification and analysis of attacks. This threat intelligence can be leveraged to bolster all layers within a security architecture, including centralized defense systems.

Cloud-based Security with Akamai

For over a decade, Akamai has been making the Internet a better, faster, and more secure place to transact business. Nearly 3,000 companies now rely on Akamai to secure and accelerate their business-critical online transactions through its EdgePlatform, the world's largest distributed computing network. Comprised of more than 50,000 servers across approximately 1,000 networks in 70 countries worldwide, the EdgePlatform currently delivers approximately one-fifth of all Web traffic at an aggregate rate ranging from 800 Gbps to over 2 Tbps.

Designed with security, resilience, and fault-tolerance at the forefront, the EdgePlatform is a proven platform for providing intelligent, scalable, edge-based defenses that protect against a broad range of attacks, whether targeted at an organization's DNS infrastructure, network layer, or Web applications. Akamai's security capabilities cover a wide gamut — including distributed Web application firewalls, a variety of authentication and access controls, PCI-certified SSL delivery, flash crowd protection, and DDoS mitigation.

This extensive and flexible set of capabilities can be leveraged as needed to adapt to different types of threats and attacks on demand. There is no infrastructure to architect or build, no months of lead time for deployment, virtually no limitations to scalability. In short, Akamai enables customers to harness the full power of the cloud to maintain their business continuity and harden their infrastructure against today's insidious cyber threats.

To better illustrate how this works, we now take a closer look at a specific class of threat: distributed denial-of-service attacks.

DDoS: A Threat of Epic Proportions

Distributed denial-of-service (DDoS) attacks are one of the most visibly disruptive forces in cyberspace today, paralyzing systems by overwhelming targeted pieces of infrastructure with floods of illegitimate traffic. The August 2009 attacks on Twitter, Facebook, and Google were particularly well-publicized, but many business and government organizations have experienced similar costly attacks — and many of them deal with DDoS on an on-going basis. The effects reverberate long past the assault itself — not only in terms of the loss of revenue, resources, and productivity from the business disruption, but also in terms of damage to brand reputation and customer trust as well.

Unfortunately, with an estimated 190,000 DDoS assaults carried out in 2008, the attacks are occurring more frequently than ever, and on much larger scales.[13] According to Arbor Networks, the largest DDoS attacks have grown 100-fold in seven years, from 400 Mbps in 2001 to 40 Gbps in 2007.[14]

On July 4, 2009, the U.S. government faced an assault that was yet another order of magnitude larger, as Akamai handled attack traffic in excess of 200 Gbps on behalf of its government customers under siege. About one-fourth of the sites targeted by the attack were being delivered by the Akamai platform, which means the total capacity of this particular botnet could have easily exceeded half a Tbps (500 Gbps) of attack power.

These sobering numbers illustrate the ferocity of attacks made possible by modern-day botnets and amplification techniques. The July 4th assault came from over 300,000 different IP

Customer Case Study: Largest Cyber Attack in U.S. Government History

Akamai provides 100% site availability across all customers

On July 4, 2009, the U.S. government faced the largest cyber attack in its history. In total, the attack lasted more than a week and targeted 48 government and commercial sites in the U.S. and South Korea. Attack traffic at the top affected site reached a peak of 124 Gbps, nearly 600 times its normal traffic levels, and equivalent to the capacity of 2,500 Web servers and 12 OC-192 circuits.

Akamai detected elevated traffic levels early in the first wave of attack and notified customers. Akamai quickly identified attack sources and implemented countermeasures within a few hours, including blocking and quarantining traffic from Korean IP addresses, and providing uninterrupted site availability and attack traffic absorption. Despite the unprecedented intensity of the attack, all of Akamai's customers were able to withstand the attacks without disruption. Unfortunately, targeted sites that did not use Akamai were not so lucky, with most of them being shut down for as long as two days, and disrupted for much of the week.

Attack statistics:

- 200 Gbps aggregate attack traffic
- 1 million hits per second
- 308,000 attack IPs
- 64 billion log lines (13 TB of data)
- Offloaded 99.9% of origin bandwidth

addresses, hitting multiple sites with attack traffic more than 100 times normal levels. One targeted government site received eight years' worth of traffic in less than one day.

DDoS attacks are challenging to defend against, not only because of their magnitude, but also because of the variety of attacks they bring to bear. There is no silver bullet response; the best approach is a multi-layered one that depends on the precise nature of a specific attack. Is the attack coming from a small set of IPs or a specific region of the world? Is it a direct or reflective attack? Which component of the infrastructure is being targeted? What kind of amplification techniques are used, if any? What layer or protocol vulnerability is being exploited? Is it a simple brute-force, resource-draining attack, or does it take a more evasive, sophisticated approach? The diversity and scale of DDoS attacks make them virtually impossible to defend against with traditional, centralized solutions; a cloud-based defense is critical.

Strategies for DDoS Mitigation

While every DDoS attack requires its own specific analysis and plan of action, there are a number of overarching strategies that can help. As with network security in general, effective protection against DDoS requires a defense-in-depth approach using a combination of security capabilities. Here we illustrate several different ways to minimize the risk and impact of DDoS attacks on enterprise infrastructure, each discussed in further depth below.

- Offload origin server functionality to a scalable cloud service
- Cloak origin servers from the Internet
- Protect and obfuscate DNS services
- Implement a robust failover plan
- Leverage customized edge techniques
- Defend the application layer

Origin Offload

Offloading centralized origin infrastructure functions to a highly distributed cloud platform provides an important initial layer of DDoS protection by boosting the overall scalability and robustness of that infrastructure so that it can handle the large spikes in traffic associated with DDoS attacks. The more that can be offloaded to the cloud, the more scalable and robust the resulting infrastructure is.

With Akamai, customers are able to leverage over 50,000 globally distributed servers on demand, with automated capacity provisioning designed to seamlessly handle traffic spikes. In addition to cacheable Web content, Akamai's intelligent EdgePlatform can offload delivery of protected content, resource-intensive SSL content, and many types of dynamic content — including entire applications, for example, through Akamai's EdgeComputing capabilities.

Akamai's massive network has been proven to help customers successfully withstand DDoS storms that have driven traffic levels to hundreds of times higher than normal. Moreover, the EdgePlatform's intelligent load balancing and routing systems help ensure that the attack traffic does not degrade performance for legitimate end user requests — for any of Akamai's customers.

Beyond simply absorbing attack traffic, by being the customer front line and taking the "first hit", Akamai's network provides an inherent layer of protection for the customer origin servers. Attack traffic is dealt with at the edges of the Internet and kept away from the core infrastructure. Akamai's hardened servers are architected to accept and forward only valid, well-formed HTTP/S requests to the origin. In addition to protecting the origin and preserving business continuity, this approach also buys time to trace and analyze the attack in order to determine the most effective countermeasures to deploy.

The distributed EdgePlatform's fault-tolerant, high availability design also enables Akamai's customers to successfully withstand many different types of failures, beyond DDoS attacks — whether they occur at the machine, data center, or network level. Wide-scale Internet outages are not uncommon, and have numerous causes, including BGP failures (accidental or malicious), power outages, cable cuts, and natural disasters, to name a few. By delivering content from its distributed servers that are close to end users, Akamai avoids these Internet failures and trouble spots, serving content quickly and reliably. And for dynamic content that must be generated at the customer origin server, the EdgePlatform leverages Akamai's SureRoute technology to divert traffic around major Internet problems that otherwise cut off connectivity.

Origin Cloaking

One way to further protect a site's core origin servers is to hide it from the public Internet. With Akamai's SiteShield service, for example, all end user requests are filtered through Akamai's distributed SiteShield servers. Because the servers in this trusted group are the only ones that can communicate directly with the origin server, SiteShield effectively obfuscates the customer origin infrastructure from many malicious actors.

By cloaking the origin — locking it down to communicate only with Akamai servers, SiteShield mitigates risks associated with network-layer threats that would directly target the origin server. This includes not only resource exhaustion attacks, such as Slowloris and SYN floods, but also TCP and SSL protocol exploits like the TearDrop and Christmas Tree attacks that use malformed packets to cause denial of service. SiteShield is transparent to the end user — legitimate requests are fulfilled by the Akamai network, communicating with the origin as needed.

DNS Protection

DNS (Domain Name System) protection is another important layer of defense. DNS infrastructure is critical to site operations — it translates Web hostnames into the actual IP addresses necessary to find a site. Yet DNS infrastructure is often the weakest link in an organization's Web architecture. Many enterprises rely on just two or three DNS servers, making them highly vulnerable to DDoS attacks as well as other types of failures.

Akamai's Enhanced DNS (eDNS) service provides protection and scalability for customer systems by resolving end user DNS requests through Akamai's globally distributed, security-hardened DNS infrastructure. In effect, eDNS obfuscates the customer's primary DNS servers, hiding them from attack, while providing highly scalable and fault-tolerant DNS services. By leveraging Akamai's highly scalable and fault-tolerant platform, eDNS mitigates risks ranging from cache poisoning to denial-of-service attacks that target DNS infrastructure.

Robust Failover

While Akamai's massive EdgePlatform provides a strong layer of protection by absorbing DDoS traffic, more sophisticated DDoS attacks can still overwhelm a site's application server or database. A robust failover plan can minimize the negative business impact of such a situation. Directing visitors to a virtual waiting room or an alternate site with reduced functionality, for example, can keep them engaged while reducing backend load.

This can be accomplished in a number of different ways. Akamai's User Prioritization feature, for example, monitors application server health and throttles incoming load when necessary, redirecting excess users to alternate cached content. This prevents a complete site failure by preserving origin server health. Users redirected to alternative content are more likely to stay on the site and eventually complete their transaction than users who experience a site crash.

If the origin server does go down, Akamai's Site Failover service offers multiple options for business continuity. Users can be served a customized failover page or cached content, or be directed to an alternate site, which may be hosted on Akamai's globally distributed, high-availability NetStorage solution. Again, keeping visitors engaged minimizes the revenue loss and the damage to brand reputation otherwise associated with denial of service.

Targeted Edge Techniques

One of the core strengths of a highly distributed cloud-based architecture is the ability to quickly and flexibly deploy targeted defense capabilities at the edge of the Internet, cutting attacks off close to their source in a highly scalable way. Because DDoS attacks are so varied in nature, there is no one-size-fits-all mitigation strategy, so the ability to turn capabilities on and off or reconfigure them on-the-fly greatly increases the effectiveness and cost-efficiency of such a security control.

Akamai's intelligent EdgePlatform offers a tremendous range of capabilities that can be tailored to the specific characteristics of each situation. Metadata-driven features enable quick, flexible deployment across Akamai's global platform, so that multi-faceted mitigation strategies can evolve in real time in response to an attack.

Potential edge-based countermeasures include:

- Blocking or redirecting requests based on characteristics like originating geographic location, or query string patterns, and IP address (blacklists and whitelists)
- Authorizing, denying, or redirecting traffic based on characteristics such as user-agent (e.g. browser) or language
- 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 at the DNS or HTTP level

The specific defense capabilities employed will vary depending on the nature of the attack as well as the business requirements for the site or application being attacked — and may change as the attack, or its analysis, advances. By having the flexibility to deploy the defense strategies best-suited to a given scenario, businesses are able to respond more efficiently and effectively, saving money and minimizing damages. And by deploying the defenses at the edges of the Internet, companies are able to maintain the performance, scalability, and fault-tolerance they need. By leveraging these capabilities through a cloud-based service provider, businesses benefit from lower operational costs and far fewer planning headaches.

Customer Case Study: Worm Attack

Novel technique thwarts never-ending worm attack

A leading anti-virus company saw its Internet infrastructure under constant assault from a worm-based denial-of-service attack. Absorbing the continual attack was costly — and it drained significant infrastructure resources.

After careful analysis and testing, Akamai determined that the worm did not respond correctly to certain types of HTTP application layer responses. This enabled Akamai to implement a solution that successfully filtered out worm based traffic at low cost, while still allowing valid request traffic to be served normally. Denying effects on target at the edge server resulted in enormous cost savings for this customer while maintaining 100% site uptime.

Application-Layer Defenses

As attacks become more sophisticated, they are bypassing traditional firewalls and attacking the Web application layer instead — leveraging ports 80 and 443, which are typically left unrestricted in firewalls to accommodate HTTP and HTTPS traffic, respectively. According to Symantec, more than 60% of Internet vulnerabilities identified in 2008 affected Web applications.[15] Techniques such as cross-site scripting (XSS), buffer overflow exploits, and SQL injection are used to execute highly disruptive application-layer attacks.

Counteracting this threat requires security defenses that can understand and analyze Web traffic payloads. Akamai delivers this type of protection through its Web Application Firewall (WAF) service. Running at the edges of the Internet on Akamai's globally distributed platform, WAF detects and flags or blocks malicious traffic though configurable rules for protocol checking, input validation, bot and Trojan identification, and SQL leakage detection.

Unique in its highly distributed architecture, WAF differentiates itself from centralized deep-inspection firewalls as it offers both unprecedented, on-demand scalability as well as the ability to deflect 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 may prove an easy target for attackers. As such, it works well, both as a stand-alone service, or in conjunction with existing application-layer protections — leveraging the Akamai platform to enhance the robustness and scalability of those centralized systems.

Note that while WAF automatically protects against many common and dangerous Web-level attacks, like cross-site scripting and SQL injection, application-layer attack traffic can be difficult to distinguish from legitimate traffic, as it masquerades as normal-looking Web application requests. In these cases, human analysis is generally necessary to identify common traits in the attack traffic, in order to identify the best strategy for mitigation. Akamai's WAF service and other edge protection capabilities can then be selectively configured to counteract the specific attack, in addition to automatically mitigating against other known application vulnerabilities.

Customer Case Study: Adaptive Search Query Attack

Botnet attack thwarted with use of multiple, targeted strategies

Using quick deployment and a multi-layered approach, Akamai enabled a major Internet search vendor to successfully withstand a sophisticated assault of botnet-driven attack traffic consisting of an adaptive set of uncacheable search queries. The first layer of the approach consisted of Akamai automatically blocking requests from the top-offending IP addresses. This deflected approximately 85% of the initial wave of attack without any end user impact or service disruption, buying time for further attack analysis.

A second defensive component leveraged Akamai's highly scalable network to identify and block a set of bad queries. In this case, the set included variations containing different URL-encoded portions to generate greater variety and avoid detection. These bad queries were completely offloaded from the search engine's servers, freeing them to handle legitimate requests. Akamai's platform handled "bad" queries with a custom error page, informing any affected legitimate users about the situation to further minimize end user impact.

In addition, the search vendor protected its origin servers with SiteShield to prevent the botnet from making any direct, resource-draining connections. As a result, the search engine successfully rebuffed the attack with minimal end user impact, as Akamai absorbed attack traffic peaking at over 280,000 hits per second on behalf of its customer.

Conclusion

As the size and sophistication of Internet threats continue to multiply, businesses need to be more vigilant than ever in protecting their digital infrastructure and assets. Effective security requires a defense-in-depth approach that augments traditional, centralized protections with a cloud-based outer ring of defense to provide the scalability and flexibility that the current caliber of threats demands.

Distributed denial-of-service attacks are but one example of the insidious and outsized threats organizations face today, but they highlight the limitations of conventional, centralized perimeter defense solutions and emphasize the clear advantages that cloud-based security can offer, in terms of scalability, flexibility, capacity planning, and cost. In this brave new world, the Internet cloud is the enterprise perimeter, and robust enterprise security requires embracing the cloud rather than retreating from it; distributed threats demand distributed protections. However, in order to benefit from the unique strengths of cloud-based security, organizations must be careful to choose a trusted provider offering proven, scalable, cross-network solutions.

Many of the most valuable name brands in the world, both commercial and government, are secured and accelerated on the Akamai platform. Akamai has proven experience being able to weather some of the worst DDoS incidents in the history of the internet. The availability of both the Akamai platform, and the customer content we carry, is critical to our mission and our success, which is why our core competency focuses on being the best in the world at running a secure, high-performance, massively distributed computing infrastructure with 100% availability.

Security is comprehensively integrated into every aspect of Akamai's network and operations, from its hardened servers and fault-tolerant architecture to the rigorous physical and operational security policies it enforces.[16] These security controls are designed to protect not only Akamai, but the Internet at large — and the thousands of companies that depend on Akamai's EdgePlatform to securely and reliably deliver an aggregate of 500 billion Web interactions each day.

With its unmatched global purview, massively distributed network, and flexible set of protective capabilities running across a proven, secure, and highly fault-tolerant platform, Akamai is uniquely able to help enterprises harness the power of the Internet cloud to efficiently and effectively secure their perimeter and defend it against today's evolving, wide-scale threats.

[1] http://www.symantec.com/about/news/release/article.jsp?prid=20090910_01.

[2] http://gcn.com/articles/2009/08/31/security-threats-invasion-of-botnets.aspx.

[3] http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jul-2009-na-wpus.pdf.

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

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

[6] http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf.

[7] http://www.viruslist.com/en/analysis?pubid=204792068.

[8] http://www.viruslist.com/en/analysis?pubid=204792068.

[9] http://www.ferris.com/2009/01/28/cost-of-spam-is-flattening-our-2009-predictions/.

[10] Symantec Global Internet Security Threat Report: Trends for 2008.
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

[11] http://www.fstc.org/docs/articles/messaglabs_online_shadow_economy.pdf.

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

[13] http://www.viruslist.com/en/analysis?pubid=204792068.

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

[15] Symantec Global Internet Security Threat Report: Trends for 2008.
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

[16] For more information, see 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