

AKAMAI SOLUTION BROCHURE

CLOUD SECURITY SOLUTIONS

FAST » RELIABLE » SECURE.



Threat >

The number and size of cyberattacks are increasing rapidly

Website availability and rapid performance are critical factors in determining the success or failure of many organizations today. The Internet, however, is inherently insecure, and an escalating number of firms are falling prey to downtime and data-theft attacks. A combination of technological, economic and political factors are fuelling an explosion in cybercrime, meaning access to a robust, scalable security solution is more important than ever to ensure online business continuity.

Technology has bought complex, highly distributed attacks to the masses via highly accessible, sophisticated toolsets and 'attack-for-hire' services — equipping novice and experienced cybercriminals with the capability to bring down and exploit global websites for a fraction of the traditional cost.

Digital espionage tactics are now a popular method for holding companies to financial ransom, as typified by a wave of recent activities from the DD4BC (DDoS for bitcoin) group. Their Distributed Denial-of-Service (DDoS) campaigns threaten to render targeted websites inaccessible unless a payment (anonymous via bitcoin) is made. In the absence of a highly scalable security solution, victims often pay, knowing that further downtime could result in huge online revenue losses, additional technical support costs and significant brand damage. Akamai's 2015 Q1 State of the Internet report quantified these trends, stating that the number of DDoS attacks across its network, which carries 15-30% of all web traffic, have doubled since Q1 2014.

From a political standpoint, a rise in state-sponsored hacktivism, as seen against a major online gaming platform towards the end of 2014, is providing an unprecedented investment in skills, techniques and capabilities, making it even harder to defend valuable assets in an already evolving threat landscape.

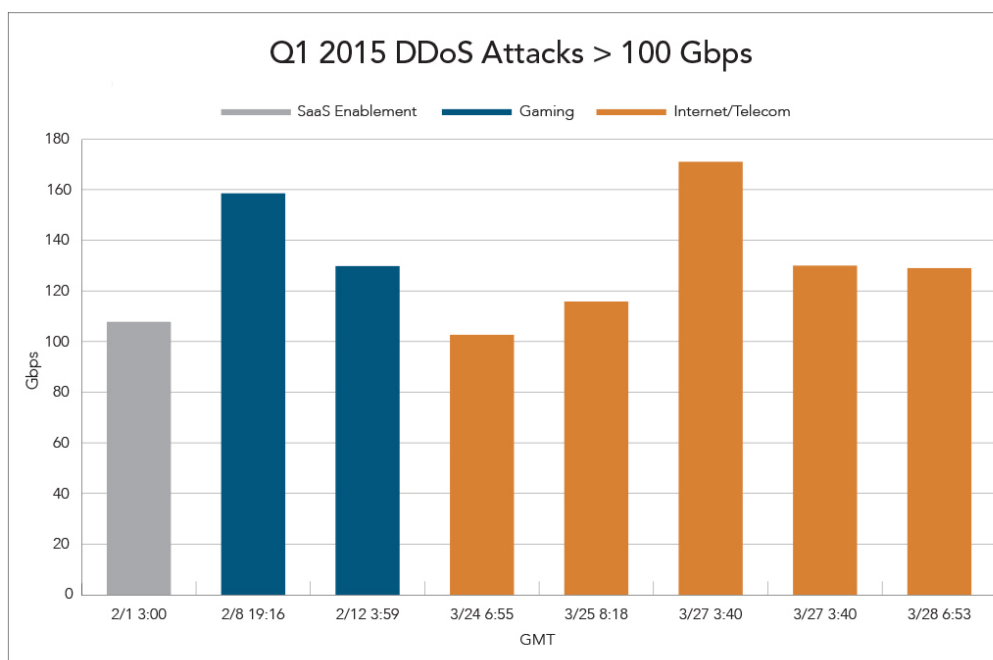


Figure1: Q1 2015 saw eight mega attacks against Akamai customers, with the largest peaking at nearly 170 Gbps

“ According to a 2014 survey done by the Ponemon Institute, the average cost of web application attacks is over \$3M per year and less than 40% of surveyed individuals consider a WAF part of their security solutions.

< Response

Introducing Akamai Cloud Security Solutions

Akamai makes online business fast, reliable and secure. We earned our global reputation by building the world's fastest and largest cloud-enabled delivery platform, which is backed by the most scalable, distributed security solution available. Our platform carries up to 30% of global web traffic, giving us an unrivalled window into the security exploits that are taking place in real time. We use this intelligence to continually enhance our security offerings to ensure that as security threats change, our ability to stop them doesn't. For example, we had already developed and deployed patches across our defenses to secure Akamai customers against the Heartbleed vulnerability prior to it being known about publicly. Our network of over 180,000 acceleration and security servers, located in over 100 countries across the world, gives us the unique advantage of stopping web application and DDoS attacks at the Internet edge. In fact, in the majority of cases we can block an attack within one network hop of the attackers themselves, ensuring that malicious traffic stays as far away from your data center as possible.

Our 24/7 global security teams, enabling an instant extension of your security team, support our comprehensive solutions. With full access to their vast knowledge, experience and data-derived intelligence, you will have the best possible chance of mitigating the growing array of attacks. We successfully defend against thousands of online exploit attempts every day, where the average volumetric attack is between 5-10 Gbps (with a peak of 321Gbps in 2014), ensuring our technical team's skill base is always relevant, distributed and effective

We are passionate about ensuring that your applications are always safe, available and fast. As a result, we have made it possible to have the best available web security, with a guarantee of no negative impact on page load times and performance. Akamai Cloud Security Solutions help you avoid data theft and downtime by extending the security perimeter to the remote edges of the Internet, inside the user's ISP, where enterprises do not have control today.

Why Akamai Cloud Security Services

- Over 17 years of security experience.
- World's largest cloud security platform with over 33 Tbps of network bandwidth at the Internet edge.
- Six globally distributed scrubbing centers and 180,000 security devices across 100+ countries and 1,200+ networks.
- Up to 30% of web traffic traverses the Akamai network, providing unmatched threat intelligence and insight.
- 2 Petabytes of constantly refreshed attack data continually analysed for new threats on our Hadoop-driven data platform.
- Option of always on vs. on-demand solutions.
- Defences located within one hop of over 90% of cyberattackers across the world.
- Flexible services that can be customized to business requirements.
- 24/7 security operations center (SOC) over 100 security professionals worldwide.
- Very low false positives due to application profiling and system intelligence.

The strongest response to every cyberthreat

Akamai offers a comprehensive range of stand-alone or integrated solutions to meet your business requirements. The world's top 10 banks, the top 30 media companies and the top 60 e-commerce sites all trust Akamai to provide a robust cyber defense against web-based threats. The solutions are designed specifically to protect three key elements of your web and IT infrastructure: DNS, web applications and full datacenter.

Domain Name Service Protection

DNS is a critical and often overlooked component of the web infrastructure availability and performance. Many organizations rely on a handful of DNS servers, leaving them vulnerable to data center outages as well as DDoS attacks and system outages. This, along with the traffic amplification qualities of DNS responses, makes DNS servers popular targets for cybercriminals. Akamai's fast DNS solution improves domain name resolution times, adds massive scale to defend against volumetric based attacks, and protects against forgery and manipulation attempts. It can be implemented as a primary or secondary DNS service, replacing or augmenting existing DNS infrastructure as needed.

- High Availability —thousands of DNS servers in hundreds of points of presence worldwide.
- 100% uptime service level agreement (SLA).
- Fast Responses — The globally distributed Anycast network accelerates DNS resolutions for users, connecting to your sites and applications from anywhere in the world.
- Defense Against DDoS Attacks — Average utilization of the DNS network is less than 1%, meaning we have huge spare capacity to protect against the largest DDoS attacks.

Website Protection

Protect your valuable websites as far away from your infrastructure as possible with our proxy-based, highly distributed edge security. This always-on HTTP and HTTPS Web Application Firewall and DDoS solution defends against the largest and most sophisticated attempts to steal your data and take your services offline. The Kona suite of products utilizes Akamai's Intelligent Platform™ to ensure your customers are always receiving the best possible online experience, even when under attack. Benefit from our ability to respond rapidly to new and evolving threats and reap the business benefits of extremely low false positives and negatives.

- Shortest time to detect and mitigate due to always-on, accurate service.
- Highly accurate Kona Rule Set.
- Guarantee of no site performance degradation.
- API control and rule management.
- PCI compliant SSL network and key management.
- Origin defense by cloaking web infrastructure and reducing vulnerability.
- Fully managed or self-service options.
- Integrated solution for both your WAF and DDoS protection.

Supplementary offerings:

- **Site Shield** - Completely shield your servers from the public Internet by sending all traffic to and from the Akamai network with a dedicated leased line from your environment.
- **Client Reputation** – Behavioral analytics to accurately predict the likelihood of malicious activity of incoming requests based on source IP addresses. Assigned risk scores predict the probability of web attacks, Denial-of-Service attacks, scanning and web scraping. We rate the hundreds of millions of unique IPs seen on our network every month, giving you the availability to customize your mitigation response for each attack category.

Why Akamai Cloud Security Services

- Reduced exposure to technical support costs
- Origin server request offload, enabling reduced data center resources
- Reduced CAPEX expenditure
- Reduce hardware and bandwidth resource planning through access to the massive scale of the Akamai platform
- Potential to improve website performance

Datacenter Protection

For complete data center DDoS mitigation, we also offer the world's leading DDoS scrubbing solution to ensure continuous uptime of all of your IP-based applications. Use Border Gateway Protocol (BGP) to route network and application traffic through Akamai's global scrubbing centers.

With an ever-growing capacity of over 2.3 Tbps of dedicated attack bandwidth, we have the scale to defend against the Internet's largest volumetric attacks. Prolexic Routed comes with an industry-leading Time-to-Mitigate service level agreement (SLA) and can effectively help organizations block all DDoS attacks 24/7/365. With six scrubbing centers across the Americas, Europe and Australasia, we can always defend close to the source and guarantee that we have the bandwidth and resilience to ensure uptime and minimize latency.

Gain full access to our Akamai SOC staff to inspect traffic and respond accordingly in real time to varying attack characteristics. It's well known that attack vectors often change during an attack, and our proactive monitoring and over 20 defense technologies enable us to customize the response accordingly. All clean traffic will be forwarded securely on to your environment via GRE tunnel or a dedicated leased line for optimum performance. Return traffic continues on to the user without having to go back via our scrubbing centers.

- Wide scope of protection – All ports and protocols covered.
- Peace of mind with our leading Time-to-Mitigate (TTM) SLA.
- Full access to our 24/7 SOC team for customized attack mitigation and post-attack forensics.
- Visibility - Web-based portal for a real-time view into what's happening to your traffic (e.g., application traffic, downloadable logs, reports and ticketing systems)
- Always-on or On-demand fully monitored options.

For more information

Learn more about Akamai's Cloud Security Services and how they can protect your business from the increasing risk of cyberattacks by contacting [1 877 425 2832](tel:18774252832), info@akamai.com or visit www.akamai.com



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

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