4 CRITICAL CRITERIA
for Financial Institutions Evaluating DDoS Mitigation Providers

The world will never forget the series of Distributed Denial of Service (DDoS) attacks on American banks in 2012 and 2013. Cybercriminals continue to evolve their tactics with ever-growing attack sizes and new attack methods. This dynamic and constantly changing threatscape has sparked an increased demand for mitigation services, resulting in an influx of service providers entering the marketplace. However, because many of these services reside in the cloud it is often difficult for financial institutions to assess, evaluate and differentiate DDoS mitigation service providers from one another.

How can you ensure the DDoS mitigation service provider you use can deliver on the promise of blocking the Internet's largest and most sophisticated attacks?

Given Akamai's practical experience in proven mitigation approaches — which stop 40 to 50 attacks per week — we present these four critical criteria to help you evaluate a provider's threat intelligence, experience, mitigation capabilities and capacity.

"Cybersecurity is no longer just an issue for the IT department; it needs to be engaged at the very highest levels of corporate management."

– FDIC Chairman, Martin Gruenberg

1. **Threat Intelligence.** The more you know about DDoS attacks, the more proactively you can manage your DDoS defense strategy. Your mitigation service provider should deliver you with comprehensive threat intelligence on a regular basis, compiled by a dedicated research team of DDoS security experts. Akamai's State of the Internet Report provides financial institutions with an informed view into online connectivity and cybersecurity trends and metrics including Internet connection speeds, broadband adoption, mobile usage, outages, cyber-attacks and threats.

2. **Front-Line Experience.** Nothing beats first-hand experience when you're talking about defeating determined cyber hacktivist groups. These attackers not only challenge a provider's mitigation capabilities for its customers, but they also compel the provider to protect itself against the most malicious forms of cyberattacks. Akamai has proven front-line experience. For example, during the infamous campaign of large-scale DDoS attacks conducted in 2012 and 2013 against U.S. financial institutions; a leading financial services firm, with approximately 10M customers, suffered a massive attack that went from 0 to 30 Gbps in seconds. Akamai offloaded 100% of the attack and protected the bank so that there was no impact, and the bank was able to maintain superior performance.

3. **Mitigation Capabilities.** Regardless of the size of your financial institution, you need a DDoS mitigation provider with a robust capability set to defend against all types of current and emerging attack vectors, including the largest size of attack possible on the Internet. The fact is that DDoS attackers have used the same highly sophisticated toolkits to take down both the world's largest banks and small community credit unions. With proven capabilities across all types of network environments, whether BGP (border gateway protocol) route advertisement changes, proxy or DNS-based redirection, or hybrid solutions, Akamai has the experience and expertise to architect the right solution for your environment.

4. **Mitigation Capacity.** Mitigation capacity is a key differentiator among DDoS mitigation service providers. The objective of all DDoS attacks is to exhaust your resources (bandwidth, memory and CPU for all devices that process traffic) to create a network or system outage and take down your online presence or applications. Akamai's Intelligent Platform™ is made up of a distributed network of servers and intelligent software delivering over 2 trillion interactions daily and over $1 trillion worth of financial transactions every year. Our globally distributed mitigation network provides the redundancy necessary to scale up to effectively defend against even the largest and most destructive attacks.

"Cloud-based security solutions in particular will play a large role in helping banks secure themselves against volumetric DDoS attacks."

– Rik Turner, Senior Analyst, Financial Services Technology OVUM

Let Akamai protect your asset management, brokerage, payments, financial exchanges, banking and insurance business in today's hyperconnected world.

Akamai FASTER FORWARD

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

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 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.