VENDOR PROFILE

# Akamai: Turning Enterprise Security Inside Out

Christina Richmond Duncan Brown

## IDC OPINION

Akamai is a leader in content delivery network (CDN) services. The company has built a web security portfolio that emphasizes scale, intelligence, and expertise, along with security services for cloud/internet-dependent enterprises. In addition:

- Akamai has experienced significant growth because its services address two challenging business issues. The first is maintaining uptime and preventing data loss through web services, which are essential to customer engagement and growth. The second is improving security for enterprise users that are increasingly mobile and outside of the traditional network perimeter.
- Akamai is adapting what it has done for outward-facing web applications and applying this inwardly for enterprises. This effort spans two divisions: the Web Business unit, which is focused on instant, secure access to applications and sites for all users and devices, and the new Enterprise Business unit, whose vision is to secure, optimize, and accelerate the enterprise as a service in the cloud. The business units' approach to thwarting attacks is timely and innovative, with a multipronged strategy encompassing web application firewall (WAF), DDoS mitigation, bot management, DNS, remote application access, threat protection, and branch network architectures.
- As a result of acquisitions and internal development, Akamai's portfolio of cloud security services is market leading, easy to use, and backed by high performance levels.

## IN THIS VENDOR PROFILE

This IDC Vendor Profile analyzes Akamai's security services offerings. This Vendor Profile reviews key success factors including company strategy, service strategy, service offerings, and partnerships.

## SITUATION OVERVIEW

### Company Overview

Akamai was founded in 1998 out of MIT as a better way to deliver internet content. The company has more than 230,000 servers in more than 130 countries within 3,500+ locations. The publicly traded company is headquartered in Cambridge, Massachusetts, and has offices throughout the United States, Canada, EMEA, and Asia/Pacific (APAC). The company's client list includes one-third of the Global 500, 96 of the top 100 online U.S. retailers, all branches of the U.S. military, the top 30 media and entertainment companies, 13 of the top 15 automobile manufacturers, and other high-profile companies and industries. Akamai says it can optimize web performance and availability for any web environment.

May 2017, IDC #US42558715

Akamai's solutions are organized into three divisions:

- Web, which delivers instant, secure access for "any device, anywhere" and personalized online experiences including dynamically generated rich content, with protections against applications and DDoS attacks (The platform, which distributes web content, enterprise applications, and video, sits between a company's infrastructure and the public internet. It monitors internet conditions and provides device-level detection as well as identifies, absorbs, and blocks security threats.)
- Media, which delivers high-end online experiences related to content produced by media, gaming, and software companies (Relevant capabilities include Adaptive Media Delivery, Predictive Content Delivery, Adaptive Media Player, and Media Analytics.)
- Enterprise, which facilitates remote access to internal applications, accelerates the applications, reduces bandwidth costs, and extends the internet and public clouds into private wide area networks (WANs)

Akamai's annual revenue is $2.3 billion, with approximately $400 million coming from security services.

## Company Strategy

Akamai's content delivery strategy is to be at the edge, distributing content close to end users. Similarly, Akamai addresses online threats closer to attackers instead of nearer to enterprise datacenters and web assets. This approach is enabled by Akamai's global platform, which provides visibility into attackers and their tactics before they hit enterprise infrastructures and facilitates the delivery of good traffic.

Akamai wants to make it easier for organizations to remain secure. To this end, the enterprise security solutions focus on simplifying infrastructure for chief information officers (CIOs), even as more users, applications, and data leave the traditional confines of the enterprise network and datacenter. The solutions use the same security technology and platform used by other Akamai services but focus on requests going out from an enterprise instead of requests coming into the web infrastructure. Akamai's laudable goal is to augment and extend what enterprises are currently doing with their infrastructures, allowing them over time to shrink their infrastructures as they move "outside" into cloud and service provider environments. This evolution requires a fabric to link the inside and outside, and Akamai wants to be the fabric.

The vision for the fabric is that it will contain necessary security controls such as threat protection, proxies, web gateway, and ultimately next-generation firewall. The Bloxx acquisition in 2015 is an essential part of this strategy because it brought deep packet inspection and application classification capabilities.

Akamai delivers enterprise security services in three areas:

- **Enterprise application access (EAA) to address the problem of remote access.** EAA launched earlier this year based on the acquisition of Soha Systems in 2016. The service enables Akamai to simplify and improve remote and mobile access to enterprise information with cloud-based application access control. The service, which can be deployed in minutes, solves three security challenges:
  - Moves infrastructure off the public internet and eliminates inbound network port access

    - Enables an enterprise connector (a virtual machine) inside the infrastructure that only dials out and is fully managed in the cloud — eliminating inbound holes in the firewall
    - Isolates Layer 7 connectivity from users' browsers all the way back to the enterprise application, so the network is not open and users see only the applications exposed to them
- **Threat protection by making DNS safe and preventing DDoS attacks.** Akamai has built a new threat research team focused on DNS and is rolling out a cloud-based recursive DNS platform to customers and carrier partners to provide visibility on this side. Akamai already has visibility on the authoritative DNS side from its legacy business. With this approach, Akamai can improve security by preventing DNS-based data exfiltration, command and control callbacks, and access to malicious malware and phishing domains.
- **Branch acceleration.** Akamai Cloud Networking is designed to provide secure, reliable internet connectivity for branch and remote offices. Currently, the service is designed for network service and communication service providers and branch infrastructure vendors to incorporate into their offerings, covering IP-VPNs and cloud and SaaS applications. Cloud Networking services will provide:
    - SLA-backed route optimization and packet delivery
    - Caching, data deduplication, and quality-of-service optimization
    - Secure web gateway functionality with cloud-based outbound web filtering and inbound malware protection with identity integration

## *Web Security Product Strategy*

Akamai's cloud network and interconnected services provide expansive data that the company has turned into an information security and threat intelligence platform. The platform is augmented by a security operations center (SOC) and managed services function. Key web security offerings include:

- Automated WAF capability (Web Application Protector) for businesses that require protection from DDoS and compliance but don't have resident expertise or want to allocate resources elsewhere
- More robust WAF capability (Kona Site Defender) that provides automated rule updates and a managed services option
- Scalable DNS (Fast DNS) infrastructure to protect against volumetric attacks
- Network traffic routing protections (Prolexic) through scrubbing centers, where traffic is inspected by Akamai's SOC staff (Flow-based monitoring helps enterprises understand when to route traffic on and off this solution.)

The aforementioned offerings can be augmented with additional solutions:

- Client reputation to address evolving threats that result from malware, spyware, and account takeovers
- SIEM integration to ensure that the existing analytics infrastructure is valuable and reliable
- Bot management–related account takeover and, in the near future, credential abuse (This includes a means of aligning business objectives and IT/InfoSec concerns regarding bot management.)

## Partnerships

Akamai has a robust partner program. Certain strategic alliances are notable for their potential to aid Akamai's growth. In early 2017, LAC, an information security company, augmented its portfolio with

Akamai's internet-monitoring service for the purpose of protecting corporate websites. In late 2016, Akamai began training and certifying Singtel personnel to deliver professional and managed security services for web security solutions initially in Singapore and eventually in Asia/Pacific.

## FUTURE OUTLOOK

### Challenges and Opportunities

The security landscape is a highly complex mix of technologies, services, and approaches. As adoption of digital transformation and 3rd Platform technologies (cloud, big data/analytics, mobile, and social) accelerates, new challenges arise related to where data resides, how data is accessed, and who owns security. With hybrid architectures and migration to cloud, applications, data, and users increasingly are outside the chief information officer's traditional domain, yet CIOs are responsible for security, visibility, control, and compliance.

Security service providers can differentiate themselves first and foremost by simplifying the complex mix to make it more easily digestible for CIOs and other enterprise decision makers and decision influencers. Further, threat intelligence should be a decisive factor in the selection of vendors that offer security products and services. Threat intelligence, however, is evolving rapidly with the use of artificial intelligence and machine learning, and buyers may be confused about types of threat intelligence, what to buy, how to apply the intelligence, how to prioritize the threats, and how to prevent or mitigate threats. Market-leading service providers will offer:

- Complementary consulting services that provide customizable opportunities for customers to plan and enable their security journeys
- Flexible consumption models that match customer preferences for integrating a service provider's expertise, processes, and technology
- Cloud management capabilities that enable seamless hybrid implementations
- Pricing models that align with customer preferences
- Advanced detection and analytics capabilities, including advanced detection and response capabilities, threat intelligence, and big data, for infrastructure and endpoints
- Robust customer support, including incident response and forensics, to assist with recovery from breaches
- Managed security services, supported by security operations centers that have advanced methods of acquiring and retaining security talent

The CAGR for the security services market is 8%, and the CAGR for the threat intelligence services market is 11.3%. Given these forecasts, there is significant opportunity for vendors and enterprises of all sizes. By engaging a vendor like Akamai, enterprises can implement security with a breach prevention emphasis that leverages cloud-based solutions, threat intelligence, and threat mitigation.

Meanwhile, other challenges persist:

- Integrating threat intelligence into a business is a complex endeavor. Organizations must navigate their own technologies as well as those proposed by vendors, and they struggle with defining roles, responsibilities, communications, and processes.

- Education must continue with board members and executives regarding the threat landscape, security strategies, threat intelligence options, detection and response options, integration, budgeting, and staffing.
- A shortage of security talent is a continuing problem, although service providers may have an advantage over enterprises in attracting and retaining staff because they can offer flexible career paths, cross-training, and rapid advancement. Enterprises are increasingly outsourcing security tasks because of the difficulties associated with staffing.

## ESSENTIAL GUIDANCE

### Advice for Akamai

IDC believes that Akamai is exceptionally well positioned to continue its growth in security services. The company's innovative methods of protecting websites, infrastructures, and applications represent an important advancement in the delivery of security services.

To support its continuing growth, Akamai should:

- Develop a customer journey story specific to targeted companies and verticals. A big part of this effort should be education about security basics and essentials, including services, technologies, expertise, and "what's next" to ensure cadence and encourage motion toward adoption. Akamai and its partners should be able to provide a wealth of security insights, recommendations, and use cases that can be used in an educational endeavor.
- Promote the "turning the enterprise inside out" message because it is fresh and spot on. This concept can give CIOs a framework for security education and business case development.
- Become a thought leader with respect to outcome-based customer engagements. The market is heading this way, and Akamai has an opportunity to position itself as a market leader and innovator.

Akamai's core strength in network optimization and traffic analysis is increasingly being turned toward the company's security proposition. The logical extension of this is the "cloaking" of an organization's entire network, where access to and from the public internet is brokered by Akamai. Indeed, the company is already offering elements of this to selected clients. In this regard, Akamai is competing with SDN and segmentation approaches to compete directly with Unisys Stealth as well as VMware, Cisco, and Juniper. This "segmentation as a service" could be a precious nugget of differentiation as well as being attractive to companies under constant probes and attacks.

## LEARN MORE

### Related Research

- *Worldwide Specialized Threat Analysis and Protection Forecast, 2016-2020: Enterprises Modernize Security Infrastructure* (IDC #US42068916, December 2016)
- *Worldwide Web Security Forecast, 2016-2020: Extending Protection to Cloud Resources* (IDC #US41964816, December 2016)
- *Worldwide Endpoint Security Forecast, 2016-2020* (IDC #US41825816, October 2016)
- *Market Analysis Perspective: Worldwide Managed Security Services, 2016* (IDC #US41727516, September 2016)

- *Market Analysis Perspective: Worldwide Security Services, 2016 - Security Services Grow Up* (IDC #US41816616, September 2016)
- *Worldwide Threat Intelligence Security Services Forecast, 2016-2020: Strength in Numbers* (IDC #US41053415, March 2016)
- *IDC's Worldwide Security Services Taxonomy, 2016* (IDC #US41053315, March 2016)

## About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

## Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

---