To be competitive in today's fast-moving digital economy, organizations need to make their business applications available through websites and APIs. This need is fostering a rapid and increased deployment of web applications, APIs, API-driven mobile apps, IoT devices, and other public-facing applications. All of these use cases increase complexity and risk, and broaden the attack surface.

They also raise the stakes.

Vulnerability exploits like SQL injection, malicious file execution, and cross-site scripting can diminish or even cripple a website's performance. More insidiously, they can forward application logic to a database. Once there, malicious actors can use it to compromise and exfiltrate corporate data.

For protection against this evolving threat landscape, many enterprises deploy web application firewalls (WAFs).

Deploying Cloud-Based WAFs for Protection Against a Wide Range of Threats

Unlike traditional firewalls, which only provide server-to-server protection, WAFs sit between web clients and servers. They’re designed to inspect HTTP traffic before it reaches your application.

WAFs are available as both on-premises appliances and cloud-based services. However, trends indicate that enterprises, where feasible, are migrating to cloud-based WAFs.

According to Gartner, "By 2023, more than 30% of public-facing web applications and APIs will be protected by cloud web application and API protection (WAAP) services that combine distributed denial of service (DDoS) protection, bot mitigation, API protection and WAFs. This is an increase from fewer than 10% today."

Cloud-based WAFs typically offer greater scale and flexibility than appliances located in a data center. Generally, they have broad visibility into Internet traffic and can quickly identify emerging threats and adapt protections accordingly.
Protecting Websites and Web Apps from Downtime and Data Theft

Akamai’s enterprise-grade WAF solution, Kona Site Defender, leverages an always-on, multilayered tool set to protect websites and APIs against sophisticated DDoS, web application, and direct-to-origin attacks.

Deployed across the world's largest cloud delivery platform – more than 260,000 servers in 131 countries – Kona Site Defender authenticates valid traffic at the edge. It can stop attacks at unmatched scale.

This kind of performance protection is designed to enable customers to deliver optimal end-user experiences – even while under attack. Moreover, it allows organizations to aggressively innovate their web and mobile offerings, without many of the security distractions that impede speed to market.

**Kona Site Defender Features:**

**Global Cloud Platform**
Built on the world’s largest cloud delivery platform, Kona Site Defender is designed to stop attacks at the edge, before they can reach your applications.

**DDoS Protection**
Kona Site Defender minimizes potential downtime, even as it defends your applications from the largest DDoS attacks.

**Web Application Firewall**
Protects you from application-layer threats with an automated and highly customizable rule set.

**API Protection**
API-centric protections against DDoS and parameter-based attacks, with the ability to configure protections and report on security events on a per-API basis.

**Rule Updates**
With unmatched visibility into the latest attacks, Akamai continuously and transparently updates security rule sets, leaving you in control of activation.

**Virtual Patches**
Customizable rules let you provide a virtual patch to quickly secure applications or tailor protection for your website traffic.

**100% Availability and Uptime**
A highly resilient, self-healing platform comes with a 100% uptime SLA, and site failover to keep your website up – even if your servers go down.

**SureRoute**
Mitigates network issues outside of your control to improve performance and availability, and provide users with an optimal route to your website.

**Improved Performance**
Caching, advanced offload capabilities, and TCP optimization are designed to improve website performance for users even through the largest attacks.

**Management APIs**
Integrate security controls into your software development and delivery pipeline.

**Advanced Web Security Analytics**
Helps maintain optimal security configuration tailored to your specific business needs.
Access the Complete Report, Courtesy of Akamai

The 2019 Gartner Critical Capabilities for Cloud Web Application Firewall Services report contains valuable information for security leaders who are considering WAF protections for their web and mobile applications. It includes key findings, recommendations, strategic planning assumptions, and more.

The report also includes Gartner’s 1–5 rating for each included vendor’s ability to deliver 11 WAF critical capabilities. Gartner weighed each of these capabilities in terms of relative importance to arrive at use case scores.

In the full report, you can see every vendor’s score for each critical capability. You’ll also be able to read detailed explanations of each vendor’s ability to deliver on the five critical capabilities that Gartner deems most important when evaluating WAF Services. This report is available today, courtesy of Akamai.

Get the Gartner Critical Capabilities for Cloud Web Application Firewall Services report now.
Download Report.

1. 2019 Gartner Critical Capabilities for Cloud Web Application Firewall Services report

Gartner Research, Critical Capabilities for Cloud Web Application Firewall Services, October 29, 2019, Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur, John Watts

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone—and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 12/19.