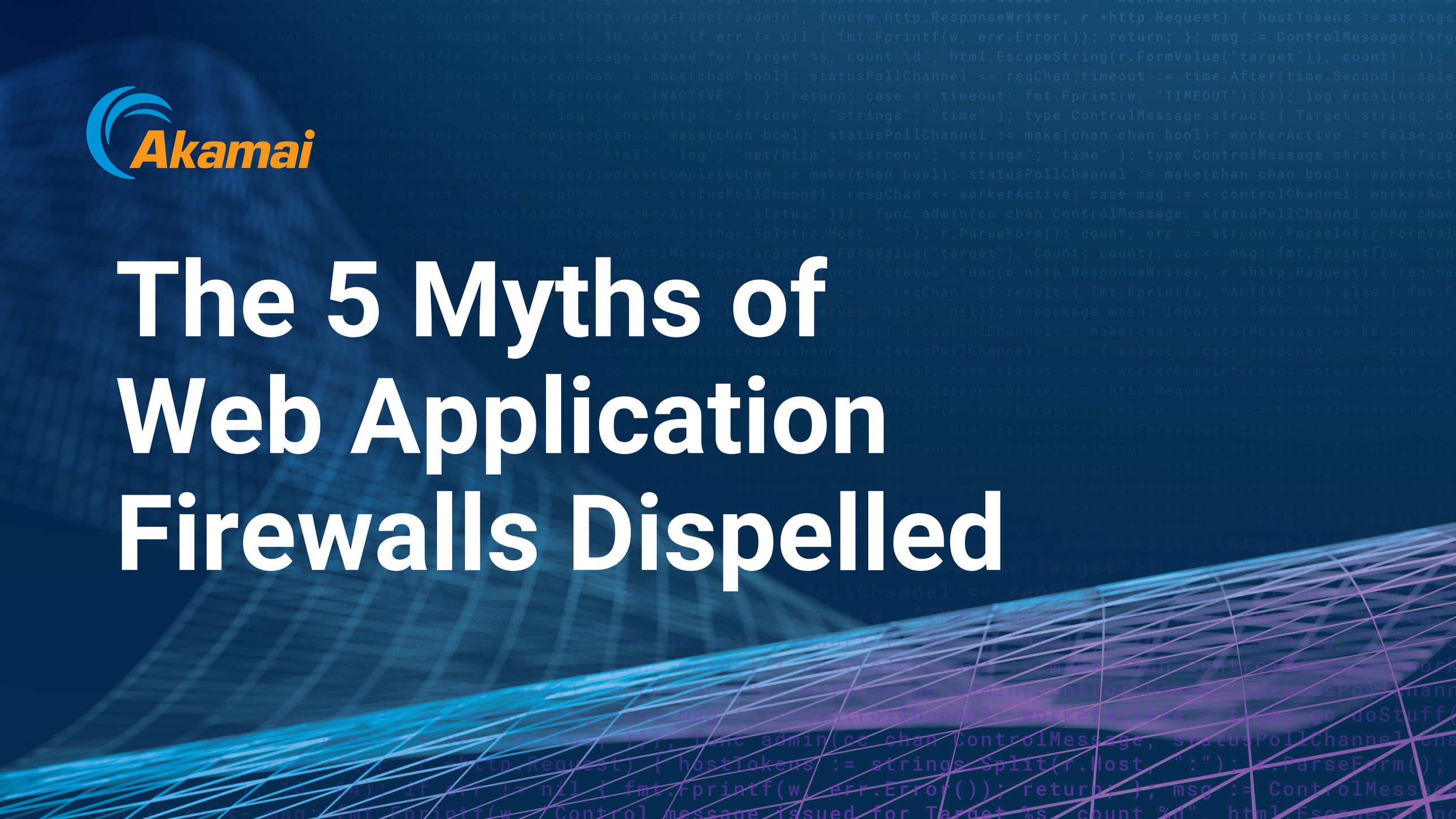

Akamai
The 5 Myths of Web Application Firewalls Dispelled

For organizations conducting mission-critical business online, the web application firewall (WAF) should be the first line of defense to keep malicious traffic out, while allowing legitimate traffic to pass through. WAF technology has been available for many years, and the original definition of WAF is far too simplistic for its evolved and modern uses. This leaves many business leaders and security professionals holding on to outdated perceptions and myths.

These myths can lead organizations to underestimate and underutilize the power of the WAF that is likely already in their stack – opening the door to attackers and increased operational risk. The need for comprehensive digital security of WAF technology continues to grow. To improve security postures and leverage the latest in WAF technology protections, we need to first address the most common myths.

We saw 9.93 billion web application attacks in Q3 2023

Daily attacks during Q3 2023 peaked at approximately 327 million

Source: Akamai Threat Research

Myth 1

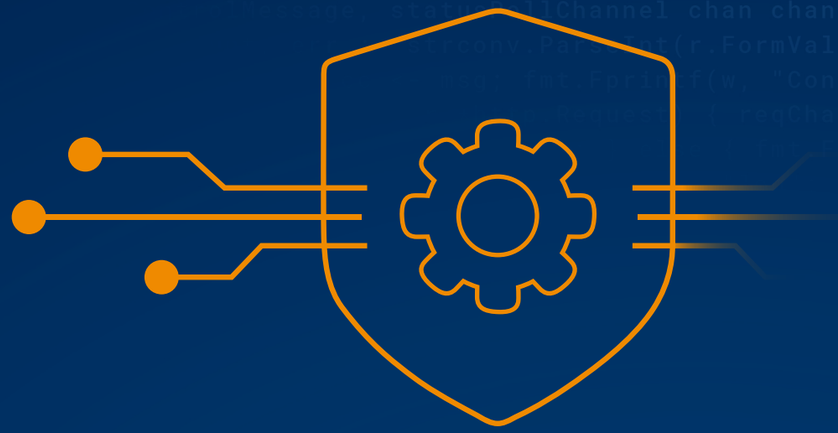
WAFs need constant manual updates to stay effective

While it is true that the latest updates provide the latest protections, there are a few myths surrounding this statement that require clarification. Many organizations today have insufficient resources or security expertise to continuously update and tune WAF rules. The business impact of automated and adaptive updates is more than just time saved and ease of use — it is also reduced risk. When we looked at businesses that chose to manually update, over 77% were five or more versions behind in ruleset updates. Akamai continuously and automatically pushes WAF updates — saving your organization time, resource investment, and unnecessary risk.

Myth 2

WAFs just gate traffic

A legacy WAF sat in the middle of the traffic between users and a web application inspecting HTTP traffic against a defined list of rules. At Akamai, our solution innovated fast and furiously beyond the traditional WAF to provide more capabilities and protections, including DDoS mitigation, API security, bot mitigation, malware detection, sensitive data discovery, and performance acceleration. And with the release of App & API Protector, your WAF security solution is now bundled with even more customer-loved technologies including Site Shield, mPulse Lite, EdgeWorkers, Image & Video Manager, API Acceleration, and more. Akamai's execution of a WAF solution is a many-in-one technology that gives security professionals complete visibility and controls for across-estate security protections.



Myth 3

WAFs drive defender alert fatigue

Ask any frontline defender, and you'll hear firsthand how security teams are strained and overwhelmed by the sheer volume of alerts and triggers they are required to investigate, especially those generated by WAF defenses. Solving this problem is exactly why Akamai developed our Adaptive Security Engine, the core technology powering Akamai's WAF solution. With Adaptive Security Engine, your organization has modern protection made possible by combining machine learning, real-time security intelligence, advanced automation, and insights from more than 400 Akamai threat researchers. Built to protect entire web applications and API estates, Adaptive Security Engine is unique because it learns traffic and attack patterns specific to each customer, analyzes the characteristics of every request in real time, and uses that knowledge to intercept and adapt to future threats. By relying on Adaptive Security Engine, defenders can say goodbye to alert fatigue while saving valuable time and reducing the level of effort to keep applications and APIs protected.

Adaptive Security Engine tuning recommendations have been shown to reduce false positives by

5x

Myth 4

More customizable WAF rules deliver more security

More rules can mean more setup, more testing, and more analysis. While more rules don't always mean improved security, fewer rules don't always mean improved security either. If you are the security pro that believes more equals more, then don't worry. Our WAF comes with unlimited custom rules – and our proactive, adaptive rule updates are delivered no matter how many you have. With automatic updates and automated self-tuning, your team can efficiently and effectively verify WAF configuration at scale across your entire digital estate. Want to add a new rule? Evaluation mode lets you evaluate the impact of new and modified rules on live traffic – seeing real-time effects in the customer portal dashboards. This shadow-mode style of testing ensures your new rule protects exactly as expected at deployment.

Myth 5

WAFs only get in a developer's way

Developers drive customer-recognized value for modern organizations. If security gets in the way, innovation slows, release cycles are delayed, and speed to value decreases. Yet at the same time, untested releases could create devastating security outcomes that halt business operations. At Akamai, we are advocates for security pros and developers. We believe WAF defenses – those that protect apps and APIs and more – can enable a culture of DevSecOps to drive speed, agility, and collaboration. That's why all of our WAF features can be managed via an open AppSec API or Terraform that allows your team to automate the onboarding of applications and APIs as well as the management of security configurations. And when you need a bit of help, Akamai TechDocs provides modern, interactive, and intuitive features specifically designed for developers.

How Akamai can help

With rapidly expanding attack surfaces and continuously evolving threats, combined with highly motivated attackers, defenders need visibility beyond traditional WAF protections. Akamai App & API Protector is a single solution that brings together many security technologies including web application firewall, bot mitigation, API security, and DDoS protection. With App & API Protector, security protections are continually and automatically updated, with customized policy recommendations implemented with a single click. Adaptive Security Engine, the technology at the core of App & API Protector, provides modern protection by combining machine learning, real-time security intelligence, advanced automation, and insights from more than 400 threat researchers.

Start a free trial or learn how Akamai protects your most critical web-facing assets to reduce risk – and operational friction – for your organization.

| Published 01/24