CLOUDFLARE

Solution Brief

# Say bye to the box

Ditch your legacy appliances for agile, scalable as-a-service application security

## The problem with security appliances

Hardware security appliances are ill-matched to meet sophisticated, modern application attacks. Appliances are expensive to maintain and manage, require downtime, and unequipped to deal with traffic spikes stemming from attacks or high demand. Organizations must purchase new hardware every 3-7 years to keep pace with throughput needs as technology advances and enterprises scale. And when hardware undergoes upgrades or maintenance, security services will need to go offline, resulting in protection gaps. Appliances must also be right-sized to handle expected peak demand – leaving them either underutilized or unable to handle traffic over the expected levels, leaving applications defenseless.

Switching to cloud-based security not only helps organizations streamline their infrastructure and operations, but can lead to significant cost savings by eliminating hardware refreshes, reducing vendor sprawl, and cutting down on data center overhead.

### The Cloudflare difference

Cloudflare's global network of edge servers reduces latency and improve website performance and security. Cloudflare offers a range of security features to help protect against a variety of web-based attacks, including DDoS protection, a web application firewall (WAF), and bot protection. Our cloud-native architecture means we are well-equipped to keep up with emerging threats – for example, as soon as our team of engineers release a new WAF rule for our managed rules, Cloudflare users will get those protections in production in 10-15 seconds. Cloudflare is a one-stop shop for consolidated security and performance: our single pane of glass solution for performance and security will help security teams identify and respond quickly to incidents.

#### Scalable and easy to use

Cloudflare lets organizations consume resources on an as-needed basis, and can absorb large DDoS attacks without impacting performance.

Cloudflare enables faster, automatic threat investigations and incident responses, while minimizing manual configuration and management.

#### Fast protections for emerging attacks

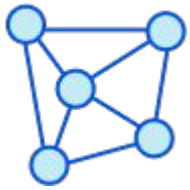
Backed by threat intelligence from a vast global network, Cloudflare's cloud-native security stack helps organizations meet these attacks head-on, without needing to wait for new security patches or appliance updates.

#### Cost effective

Cloudflare reduces valuable engineering hours spent on configuration and management so you can focus on your highest-priority initiatives.

We enable efficient growth so you only pay for the resources you need when you need them instead of paying hardware costs upfront.

## Why is scalability so important to security?



Cloudflare allows users to draw on resources as needed to respond to traffic spikes during peak times, such as during a DDoS attack or a launch of a high-demand product. We also have unmetered DDoS and Rate Limiting solutions so that you don't have to worry about being hit with surge prices or struggle to allocate resources to defend your applications.

Our network can absorb even the largest DDoS attacks so your business can stay online.

## See the comparison: Security appliance vendors vs Cloudflare

| | Legacy security appliances | Cloudflare application security |
|---|---|---|
| **Hardware costs** | Hardware costs, including refreshes and data center overhead costs. | No hardware costs. |
| **Engineering hours** | Engineering costs can be high with many hours spent on complex scripting and maintenance overhead, including hardware and software lifecycle management. | Easy-to-use product means less engineering hours spent managing one vendor, which can free engineers up for higher-impact projects. |
| **Security** | Application security from appliance vendors:<br>• Can be robust and customizable, but not very agile<br>• Downtime for maintenance means applications are left unprotected<br>• Unable to absorb or respond to the largest DDoS attacks on the Internet or handle peak traffic demands | Security benefits of Cloudflare compared to appliance vendors:<br>• Reduction of over 50% to the mean time to detect attacks<br>• Our scale and global network allow us to quickly react to threats and detect 30%-40% more intrusion attempts<br>• We typically reduce the mean time to remediate of such attacks by over 90% |
| **Accounting impacts** | Appliances are capital expenses:<br>• Require upfront acquisition costs and then can be depreciated over years.<br>• Enterprises need to acquire hardware to service peak requirements, but they will be under utilized during all other times. | Operational expenses eliminate capital expenditures and depreciation:<br>• Cloudflare's accounting benefits are more immediate<br>• Cloudflare's operational expenditure model means customers can easily scale their environment to meet their specific needs without the upfront costs |
| **Implementation time** | • Hardware lead times (lengthened by supply chain issues)<br>• Lengthy setup process<br>• Often must script central management so configurations can be deployed consistently across all devices | • Easy to centrally manage your security across all of your domains.<br>• Cloudflare provides at least a 10X faster time to value compared to appliance vendors, even once the hardware is delivered and in place |