

WHITEPAPER

Doing more with less

Cost-effective application security and performance strategies from 7 companies.



Content

- 3** Executive summary
 - 4** When security and IT teams have to do more with less
 - 5** Ways to cut costs in your application security practice
 - 6** Reduce costs with security vendor consolidation
 - 7** Streamline labor and infrastructure costs with automated certificate management
 - 8** Block attacks that drive up traffic costs
 - 9** Eliminate unexpected fees and costs like bandwidth, cloud, and egress fees
 - 10** Streamline application security and cut costs with Cloudflare
- 

Executive summary

Protecting web applications and APIs from bad bots, DDoS attacks, code injection, and other vulnerabilities is a critical task for organizations. However, implementing a robust security strategy can be challenging, especially when dealing with constrained budgets and limited team growth.

This paper shares real-life stories of companies that have successfully created efficiencies and cut costs in their application security strategy. By learning from these success stories, enterprises gain valuable insights into using application security practices to streamline expenses.

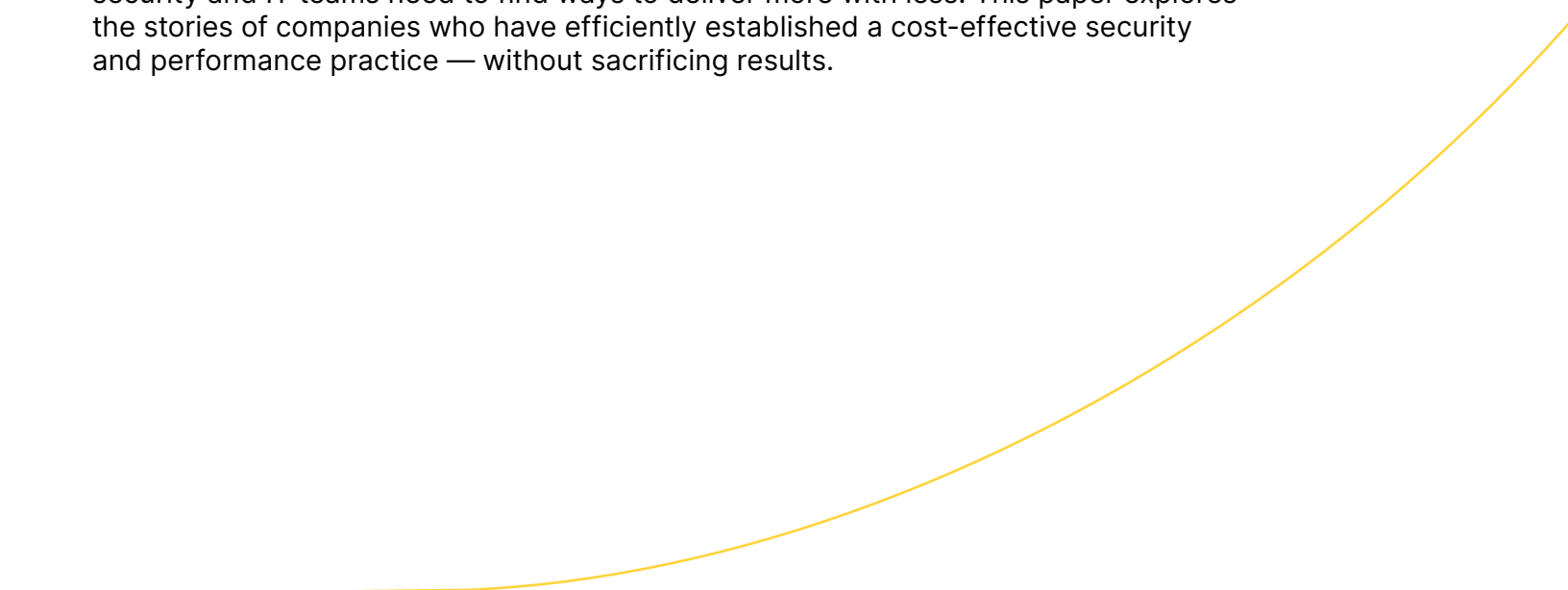
When security and IT teams have to do more with less

When organizations face budget constraints, no team is entirely immune. Whether due to broad economic uncertainty, falling sales, organizational restructuring, or a host of other reasons, security and IT teams are often forced to improve operations without hoped-for budget growth — or worse, to do so while simultaneously slashing costs.

However, application security and performance are not areas that allow for diminished results. On the security side, protecting applications gets more complicated every year. [Attacks grow larger and more complex](#) than ever before, and as organizations scale, so do their attack surfaces. By one estimation, CVE Program reported that the number of new vulnerabilities [increased by 25%](#) from 2021 to 2022, to a total of 25,059 confirmed records in 2022.

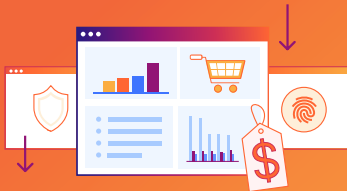
And on the performance side, consumers expect every digital experience to be fast, reliable, and personalized. Even minor slowdowns can have a significant impact on user engagement and conversions, leaving companies in the lurch if they can't meet their customers' expectations.

When facing the dual pressures of budget constraints and rising expectations, security and IT teams need to find ways to deliver more with less. This paper explores the stories of companies who have efficiently established a cost-effective security and performance practice — without sacrificing results.



Ways to cut costs in your application security practice

When it comes to protecting web applications and APIs from modern threats, the best defense is not only one that offers layered security services, but one that allows organizations to trim unnecessary expenses. To achieve this, organizations may use several key strategies, including vendor consolidation, streamlined certificate management, dedicated protection from attacks that drive up traffic costs, and egress fee reduction.



Reduce costs with security vendor consolidation



Streamline labor and infrastructure costs with automated certificate management



Block attacks that drive up traffic costs



Eliminate unexpected fees and costs like bandwidth, cloud, and egress fees



Reduce costs with security vendor consolidation

A recent survey by [Gartner](#) states that 75% of companies are exploring vendor consolidation in their security practice. By [reducing the number of vendors](#) they rely on, organizations can optimize supply chain processes and achieve greater efficiencies, which translates into decreased costs.

Chrono24, a leading online marketplace for luxury watches, reduced their reliance on multiple vendors by [consolidating with Cloudflare](#).

Before the switch, Chrono24 used a CDN solution from EdgeCast and DDoS mitigation and WAF from several other vendors. The medley of solutions performed poorly, leading to significant latency, poor security performance, and wasted vendor expenses.

After consolidating with Cloudflare's solutions — including a CDN, WAF, and DDoS mitigation — Chrono24 experienced a 67% reduction in website security and performance costs.

"Our base cost is much lower now that we've consolidated performance and security under one provider," states Sven Ferber, Director of Technology. "I estimate we're spending about one-third as much."

Vendor consolidation can be a highly effective strategy for businesses to streamline their purchasing and management expenses. Below are three quick questions you can use when looking to consolidate vendors:

1. Does your vendor offer threat protection and improve app performance?
2. Can you manage your applications and APIs from one console?
3. Can multiple teams in your organization leverage the same vendor for budget efficiency?

By following the consolidation tips above, organizations can reduce costs, simplify supply chain management, and strengthen relationships with key vendors.



Takeaways

75% of companies are exploring vendor consolidation

Chrono24 experienced a **67%** reduction in website security and IT costs after consolidating with Cloudflare

By reducing the number of vendors and consolidating services, companies can **reduce costs** and simplify supply chain management

Streamline labor and infrastructure costs with automated certificate management

Deploying security configurations across multiple domains and geo-regions can be a costly and time-consuming process for IT teams. And hidden costs can create additional headaches for the organizations they support — especially those facing budget constraints.

Often, those hidden costs are disguised in certificate management. SSL/TLS certificates make up the digital identity of a network. On average, an enterprise's web presence may require hundreds, if not thousands, of certificates. But managing these certificates can be expensive as labor and infrastructure expenses add up — not to mention the loss of revenue that may result from unexpected certificate outages.

SHOPPY, an ecommerce platform, uses [Cloudflare to automate the management of SSL certificates](#), including private key creation, protection, domain validation, issuance, renewal, and re-issuance.

Initially, SHOPPY used a free certificate management tool that provided them with unreliable certificates and short validity periods. As a result, SHOPPY had to hire additional employees to oversee the certification management and renewal process.

With Cloudflare SSL for SaaS, SHOPPY entrusts the certificate management process to Cloudflare, requiring only one internal employee to maintain the entire process.

"The use of Cloudflare products has cut costs by 60% in operation and maintenance alone," says founder and CTO Yuanming Chen.

Ineffective certificate management practices can also impact revenue due to expired certificates. LendingTree, an online lending marketplace, uses [Cloudflare's TLS certificates to save money and prevent outages](#).

"We have thousands of different properties. At that scale, it was only a matter of time before we'd miss renewing a certificate," Application Security Lead John Turner says. "Using Cloudflare's TLS certificates, which automatically renew, we save about \$50,000 a year, both in administrative costs and lost revenue from outages due to expired certificates."

Building in an effective certificate management system can also help reallocate resources appropriately. Founded in Germany, mogenius, an [automated platform that deploys cloud-based applications, automates their certificate management practices with Cloudflare](#) — enabling the company to spend more time developing their core business.

"Managing everything that Cloudflare does for us in-house would take up at least 20% of our time," Jan Lepsky, co-founder and CPO, reports. **"With Cloudflare, we can focus on optimizing cloud development and deployment pipelines for our customers."**

Offloading certificate management is crucial for enterprises looking to avoid hidden costs and ensure smooth business operations. Inefficient, manual, or patchwork certification practices lead to high labor and infrastructure expenses, lost revenue due to expired certificate disruption, and wasteful resource allocation.

By implementing certificate management with features like SSL for SaaS or TLS certifications, enterprises can save significant costs and improve their bottom line.



Takeaways

Using Cloudflare SSL for SaaS, SHOPPY cut operational and maintenance costs by 60%

Cloudflare TLS helps LendingTree save \$50,000 a year in administrative costs and lost revenue

Cloudflare enables mogenius to automate their certificate management practices — freeing up 20% of their time to focus on their core business

Block attacks that drive up traffic costs

As API use grows, so does the surface area for attacks. Malicious bots, DDoS attacks, and other threats can compromise applications and APIs — and executives and technical leaders are uniquely aware of the significant impact those attacks can have on their businesses.

By one estimate, API insecurity has been found to cost businesses [up to \\$75 billion annually](#).

These attacks result in credential stuffing and DDoS attacks, and can not only disrupt service for legitimate users, but force organizations to cover the costs of traffic surges caused by attack traffic.

LendingTree was spending significant amounts of money with a previous security vendor who charged them surge pricing during DDoS attacks. This model not only incurred massive overage costs, but ended up blocking legitimate traffic.

“Whenever we ran a new TV spot or a new social media campaign, requests would spike beyond the arbitrary limit that our vendor had us specify, which meant the vendor would interpret the spike as a DDoS attack and block legitimate traffic,” Application Security Leader John Turner recalls. **“Not only did we lose those potential customers, but we also lost the money that we spent to get them to our site, and our vendor would bill us for the ‘DDoS protection’.”**

To solve these inefficiencies, LendingTree turned to Cloudflare Bot Management and Rate Limiting features. **Within 48 hours, an attack on a particular API endpoint dropped by 70%, and in less than five months, LendingTree saved \$250,000 by stopping API endpoint abuse.**

When an online gaming holding company, Flutter Entertainment, realized that almost 70-90% of their traffic was malicious, they needed a solution to filter and block bad bots. After implementing Cloudflare Bot Management, **Flutter decreased their malicious traffic by 90%, saving more than 2 million pounds every year.**

Using bot management and DDoS protection, organizations can prevent attacks and API abuse and reduce attack-related expenditures. When exploring security vendors, organizations should look for vendors that:

- Use machine learning to set rate limits based on observed traffic data
- Goes beyond geography and IP location based rate limits because modern attacks can get around IP limits easily
- Ensure developers route all web application and public API traffic through a WAF and an API gateway
- Integrate DDoS, WAF, and API gateway tools for more layered threat defense
- Reduce latency by ensuring that protections are in place where the enterprise serve their traffic
- Offer unmetered DDoS mitigation to eliminate paying overage fees

Implementing the right vendor/security strategy can result in savings of thousands, if not millions, of dollars a year.

Flutter™

Takeaways

API insecurity has been found to cost businesses [up to \\$75 billion annually](#)

Implementing the right application security tools can result in **savings of thousands, if not millions, of dollars per year**

With DDoS protection LendingTree saw a particular API attack drop by 70% within 48 hours, and saved \$250,000 in less than five months by stopping attacks

Cloudflare Bot Management helped Flutter decrease its malicious traffic by 90% and save more than 2 million pounds every year

Eliminate unexpected fees and costs like bandwidth, cloud, and egress fees

Many security services are dependent on the cloud, and many cloud providers charge enterprises for storage and computing. Additionally, they often require enterprises to pay data egress fees, which are expenses associated with transferring data from storage.

Egress fees are calculated according to multiple factors, such as customer tier, subscription type, and volume of data transferred. For these reasons, these fees tend to be difficult to forecast — which can take a toll on organizations when they start to add up. In fact, IDC [estimates that egress charges account](#) for at least 6% of cloud storage costs.

With this in mind, PagesJaunes, a European digital directory and local search service, [decided to implement the Cloudflare CDN to help cut down on bandwidth fees](#) and improve their cache and DNS management.

“We quickly noticed that the traffic absorbed by the Cloudflare CDN meant that our infrastructure was less stressed and more resilient,” insists Loïc Troquet, Head of Architecture, Performance and Security. **“70% of the bandwidth no longer needed to be serviced by Solocal’s infrastructure.”**

And bandwidth savings results in cost savings. After adopting Cloudflare’s CDN, DNS, WAF, and DDoS mitigation services, online learning and study tool Quizlet [saved over 10 TB of total bandwidth every day](#) and cut Google Cloud Services network egress bill by more than 50%.

Implementing application security strategies and practices can eliminate unexpected egress fees.



PagesJaunes

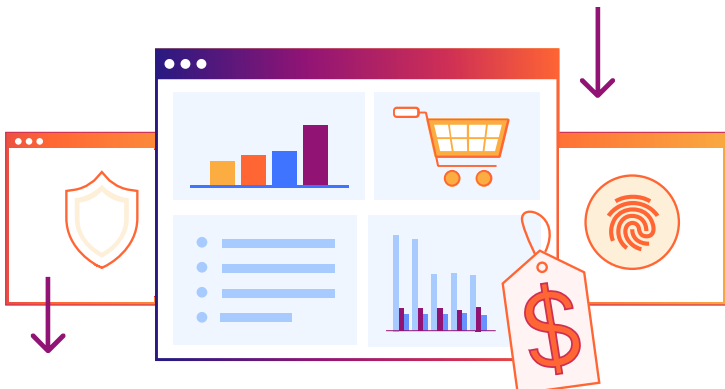
Quizlet

Takeaways

Implementing application security strategies such as choosing the right CDN vendor can eliminate unexpected egress fees

With the Cloudflare CDN, PagesJaunes reduced their bandwidth by 70%

Quizlet used Cloudflare **to save over 10 TB of total bandwidth every day** and cut Google Cloud Services network egress bill by more than 50%, resulting in thousands of dollars saved every month



Streamline application security and cut costs with Cloudflare

With Cloudflare, organizations can build in application security strategies to increase efficiency and streamline expenses. Cloudflare's integrated application security portfolio brings together best-in-class unmetered DDoS protection, a web application firewall that stops the most advanced attacks, proactive API security, bot management backed by threat intelligence, and advanced client-side attack detection.WS

Interested?

Contact Cloudflare today



© 2023 Cloudflare Inc. All rights reserved.
The Cloudflare logo is a trademark of Cloudflare. All other
company and product names may be trademarks of the
respective companies with which they are associated.

1 888 99 FLARE | enterprise@cloudflare.com | [Cloudflare.com](https://cloudflare.com)

REV:BDES-4764.2023OCT23