CLOUDFLARE

BUYER'S GUIDE

The buyer's guide for application services

Considerations for six common application delivery and security initiatives

Table of contents

How to use this guide

Applications touch almost every part of an organization, from internal productivity tools to customer-facing platforms. This guide is designed to help CISOs and CIOs remove the complexity of modernizing their application infrastructure around performance, security, and observability while improving organizational agility and continuity.

What does "application modernization" entail?

"Application modernization" typically encompasses a wide range of strategic improvements that can be made to application infrastructure, security, and performance. Within the scope of this guide, we use this term to refer to the process of updating and transforming existing software applications (and their underlying infrastructure) to better align with an organization's current and future needs.

This process can be broken down into three approaches (which may be applied concurrently or in a different order than the one laid out here):

- **Rehost ("lift and shift"):** Migrate application and application infrastructure "as-is" to the cloud (or vice versa), with no code changes to the underlying application.

- **Replatform (modify for hybrid and multi-cloud):** Optimize application infrastructure (e.g., with containers, serverless, or managed services) for multi-cloud and hybrid environments.

- **Refactor (build AI services, applications, and APIs):** Transform and build new application architecture to use modern technologies (e.g., AI, serverless, and microservice architectures) and reduce tech debt.

The use cases outlined in this guide are designed for application performance and security, which fall under one or more of the above approaches. As you begin — or continue — your modernization journey, consider which of these approaches feels the most applicable to your current priorities.

Who is this guide for?

The **buyer's guide to application services** is primarily designed for:

CISOs

responsible for improving cyber threat resilience, strengthening overall security posture, and reducing breach costs

CIOs

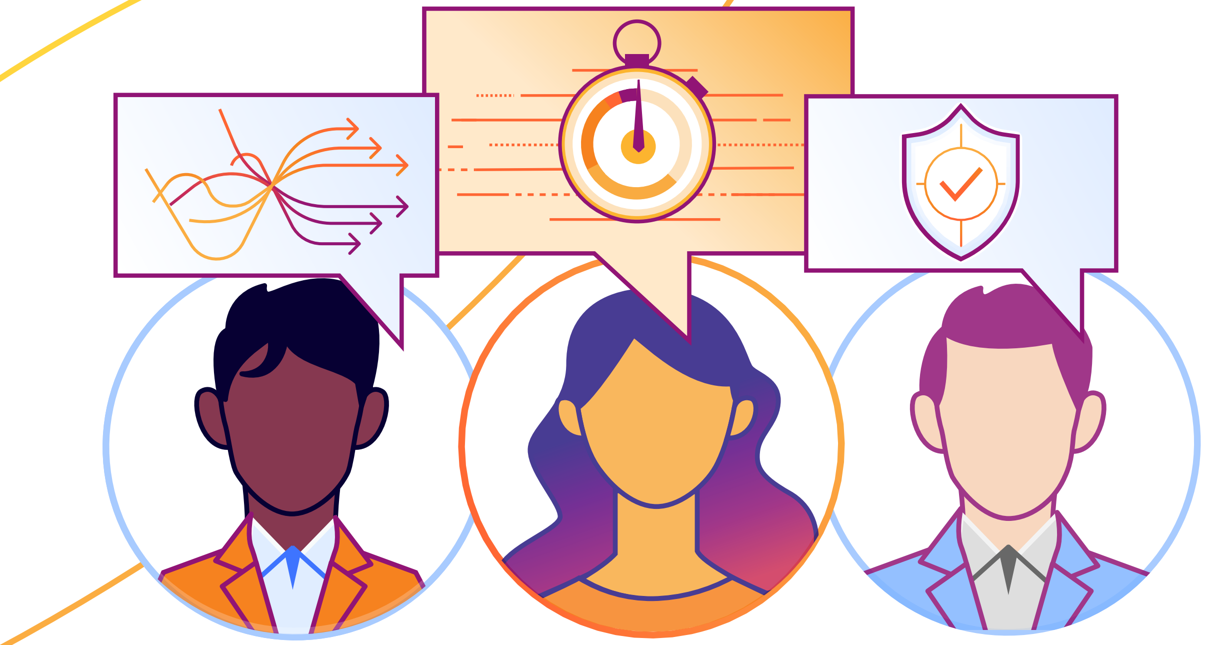
responsible for aligning system and data management portfolios with business priorities and top-level objectives

What can you use this guide for?

□ **Determining the top use cases for application performance and security.** Identify your top use cases for application security and performance. Map them to your chosen application modernization approaches. This will highlight key architectural qualities and service components to look for in a service provider.

□ **Evaluating core service components of application security and performance services.** Understand the core components of a robust, integrated application security and performance suite — *before* you start shopping around.

□ **Planning strategic conversations with vendors.** Use the sample questions at the end of this ebook to kick off conversations with application service vendors.



Six priority use cases for application services

SIX PRIORITY USE CASES FOR APPLICATION SERVICES

Modern applications enable organizations to deliver even more personalized, real-time, and intelligent user experiences — while simultaneously increasing operational efficiency and reducing risks and associated costs. But knowing where to start can be difficult, as every area for potential improvement comes with unique technical hurdles and business considerations.

To make your path to modernization easier, we've broken this out into six key application security and performance use cases:

1. **Securing against generative AI (GenAI) threats, volumetric distributed denial-of-service (DDoS) attacks, and application vulnerability exploits**
2. **Managing AI bot activity and application fraud**
3. **Managing and securing APIs** across your application and AI landscape
4. **Accelerating applications** in any environment: cloud, on-premises, and enterprise
5. **Optimizing application and AI services and reducing downtime** during high-traffic periods
6. **Maintaining data compliance** by keeping sensitive data in-region

In the sections below, we will dive deeper into each of these six initiatives, while highlighting customer wins and outlining critical architectural requirements and vendor considerations.

USE CASE #1

Vulnerability exploits, DDoS, and attack prevention

Customers expect modern applications to be secure. Maintaining a variety of application security solutions — usually with multiple integration points — can create security gaps, limit visibility across attack surfaces, and impact an organization's ability to effectively mitigate threats before they degrade the user experience.

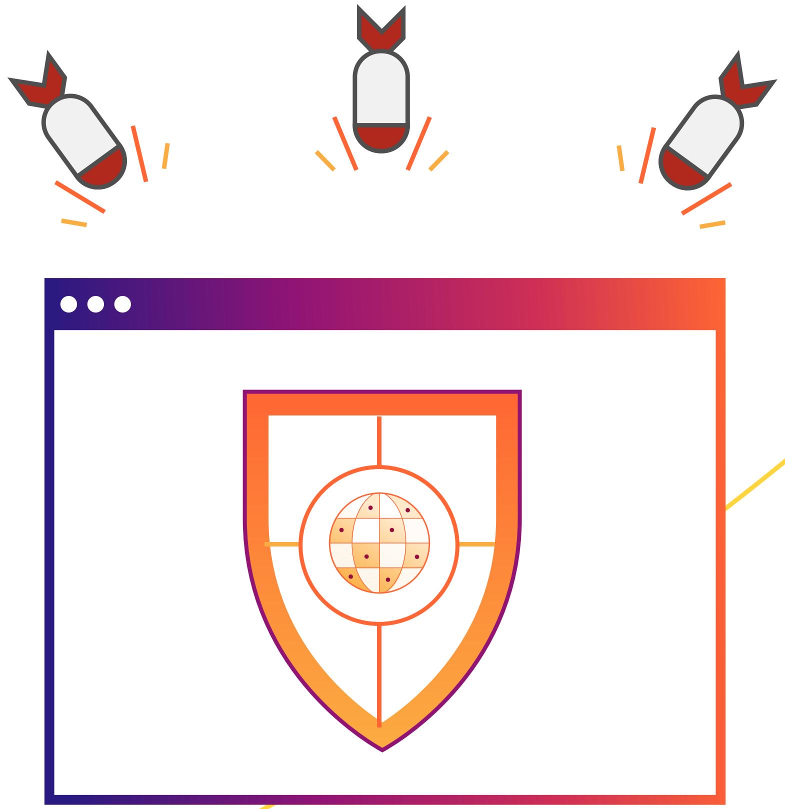
When evaluating application security solutions, look for integrated services that help automate threat detection and response, without leaving major gaps between critical services or impacting application performance and reliability.

Architectural qualities to look for:

- Easy deployment (no application architecture changes), automation (via APIs and IaC tools), and management (via a consolidated UI)
- Visibility across applications hosted in hybrid and multi-cloud environments
- Always-on mitigation
- Runtime protection
- Request and response inspection between applications and large language model (LLM) services
- Anycast networking
- Network scale and global threat intelligence
- No trade-offs between application security and performance capabilities
- No separate scrubbing centers

Quick adoption guide

- □ Always-on DDoS protection
- □ Web application firewall (WAF) with managed rulesets
- □ Rate limiting
- □ GenAI service / LLM application protection
- □ Machine learning-driven zero-day detection



CASE STUDY #1

TELUS

TELUS reduces their attack surface while improving digital experiences and eliminating legacy IT complexity

- Global communications technology company
- 19 million+ customer connections across wireline, wireless, Internet, security, entertainment, and TV services

As a company with a vast global presence, TELUS' migration from on-premises data centers to the cloud came with considerable complexity and risk. While shifting to cloud-based infrastructure offered opportunities for expansion and innovation, it also had the potential to amplify their security challenges by increasing the company's attack surface.

"We were seeing an increased number of DDoS attacks that were not mitigated," said Steve Tannock, Director of Platform at TELUS. "As a result, our team was spending lots of time on call, which was stressful and led to burnout. We needed to completely rethink how we were protecting the company."

With Cloudflare, TELUS curbed the influx of DDoS and bot attacks by implementing advanced DDoS protection and bot management. And, because Cloudflare offers these services from a single, unified connectivity cloud, the TELUS team was able to quickly consolidate their security stack as well.

"Consolidation helps us be lighter and faster," said Tannock. "We can be more responsive to issues. And at the same time, with fewer tools to manage, we're reducing our team's cognitive load."

Key results

- Saved C$11.8 million over three years by consolidating security tools
- Avoided hundreds of hours in team overtime with automated attack prevention
- Increased user satisfaction by reducing page load times by 65%

USE CASE #2

Malicious bot and fraud management prevention

AI crawlers are changing how digital content is discovered and used — sometimes without permission. Many organizations have witnessed sharp drops in organic traffic and revenue, while their content is scraped and republished elsewhere.

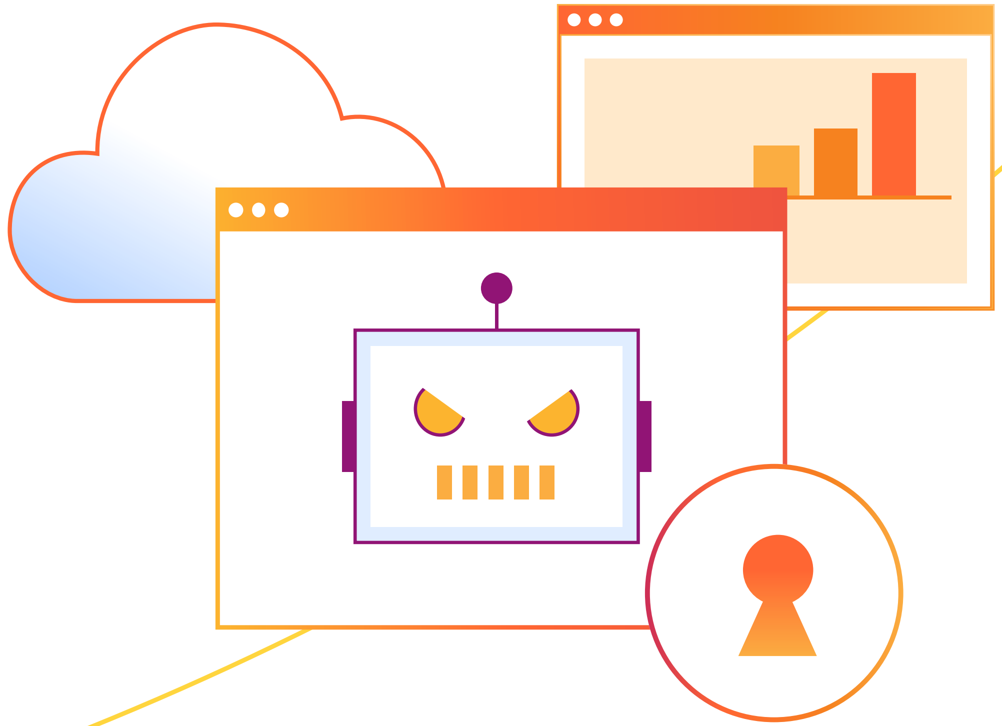
When evaluating application security solutions, look for integrated services that unify bot management across all environments and are built on robust machine learning models — for timely detection and threat responses to evolving attacks.

Architectural qualities to look for:

- Seamless bot management across web and mobile applications
- Detection and management of AI bots and AI crawlers
- Privacy-conscious bot detection
- Comprehensive protection from common bot threats: account takeover, credential / card stuffing, content scraping, inventory hoarding, AI bots that violate application policies, and more
- Integrated detection and response (both within policy engine and analytics)
- Ability to train machine learning models quickly on the largest-possible data sets
- Privacy tokens — to safely identify bots on mobile devices (without affecting personal user data)

Quick adoption guide

- □ Bot management
- □ WAF
- □ Advanced rate limiting
- □ Privacy-preserving, No CAPTCHA challenges
- □ Multiple, integrated client-side and server-side detection engines
- □ Easy-to-understand bot versus human traffic identification



CASE STUDY #2

GPC creates a cohesive security posture and improves attack visibility and mitigation

- A Fortune 200 company with over 900 ecommerce websites
- Sells a wide variety of automotive replacement parts, industrial parts, and related supplies

For Genuine Parts Company (GPC), stopping malicious bots was at the top of their to-do list. The team could not tell how many bot attacks and DDoS attacks were being prevented across 900+ ecommerce channels worldwide. Worse: they had no visibility into the total volume of attacks they were facing.

“We were paying a lot of money, but we had no visibility into our global digital footprint,” explained Damian Apone, Global Director of Governance, Risk, Compliance, and Security at GPC. “We didn’t have any information on how or when we were being attacked and we had no idea who was targeting us.”

Cloudflare helped change that. With Cloudflare Bot Management, DDoS Protection, Web Application Firewall (WAF), and Advanced Rate Limiting, GPC regained visibility into — and control over — their entire web application attack surface. This increased the agility of their security team, who could allocate internal resources toward the most serious threats while automatically tracking associated vulnerabilities and risk levels.

“Our busiest website gets approximately 2.5 billion requests a month,” said Apone. “It’s hit by approximately 57 million threats each and every month. And Cloudflare blocks all 57 million every month. I know this because Cloudflare’s security insights technology shows me exactly what’s happening across our entire digital footprint.”

Key results

- Mitigated ~450 million threats in one year
- Reduced latency and improved customer experience by blocking millions of malicious bots
- Increased internal efficiency and costs by consolidating security stack across 900+ websites

USE CASE #3

API security and management

APIs are an integral part of GenAI growth, the mobile application economy, and a standalone API economy. With this rapid growth comes new, API-specific and age-old web application security risks — whether used as a vehicle to carry out attacks or simply left unsecured. This, in turn, can cause irreparable damage to an organization, inflate operational costs, and render applications slow or inaccessible for users.

When evaluating application security solutions, look for integrated services that automatically discover, document, and secure API endpoints, while also protecting against vulnerability exploits, blocking invalid traffic, and preventing automated and sophisticated API threats.

Architectural qualities to look for:

- Automatic discovery of API and GenAI endpoints
- Schema discovery and management for customers
- Positive security model (allow valid traffic to API origin servers and block invalid traffic)
- Protection against vulnerability exploits, automated attacks, and business logic attacks on APIs

Quick adoption guide

□ WAF

□ Advanced rate limiting

□ API security with both negative and positive security models

□ DDoS and malicious bot protection

□ GenAI service / LLM application protection

CASE STUDY #3

lendingtree

LendingTree streamlines complex security infrastructure and stops malicious bots from abusing their APIs

- Online marketplace that enables consumer and business borrowers to connect with multiple lenders
- Partnered with over 400 financial institutions worldwide and 15 million+ active users

LendingTree's 15 million+ users rely on the platform to connect with hundreds of lenders and financial institutions worldwide. But malicious bots were wreaking havoc on their ability to access key services.

The bots — which abused LendingTree's APIs — cost the company a lot of money in both bandwidth and opportunity costs. However, the solution was not as simple as restricting the APIs completely, as the company's partners needed to be able to access them for current rate information.

"Our bill for a particular API service went from $10,000 a month to $75,000 practically overnight. The next month, it rose to $150,000," said John Turner, Application Security Lead at LendingTree. "My team had to spend a lot of time investigating these attacks and writing custom rules in an attempt to stop them. Because the attackers were constantly adjusting their tactics, the rules we wrote would be partially effective for only a short amount of time."

Cloudflare Bot Management gave LendingTree immediate results. Within 48 hours of enabling the solution, attacks against a particular API endpoint dropped by 70%. And, unlike previous solutions the company had tried, Cloudflare Bot Management did not impede legitimate automated traffic — so LendingTree's partners and customers saw no interruption of service on their end.

"By enabling us to deliver our products fast, securely, and reliably, Cloudflare provides us with security at the speed of business," Turner added.

Key results

- Saved $250,000 over five months by stopping API endpoint abuse
- Reduced API attacks against a frequently abused endpoint by 70%

USE CASE #4

Accelerate applications in the cloud, on-premises, and in enterprise environments

Application response delays and performance degradations are often caused by network latency or backend processing lags. By delivering applications closer to end users, organizations can ensure faster application performance and a smoother user experience.

When evaluating application performance solutions, look for integrated services that deliver content as close to end users as possible, support multi-cloud flexibility and instant failover, and scale applications and infrastructure without increasing latency, internal complexity, or cost.

Architectural qualities to look for:

- Fast DNS resolution
- Global CDN coverage with robust edge caching
- Customizable data storage with regional and global tiered caching
- Global and local traffic management
- Hybrid and multi-cloud support
- Automated, real-time monitoring of application performance
- Automated network congestion detection and response

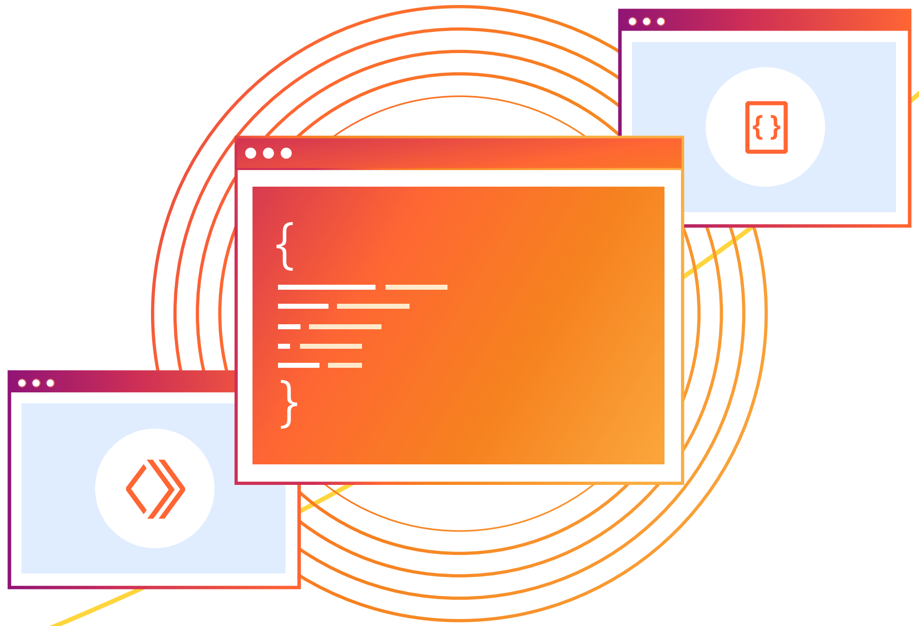
Quick adoption guide

□ DNS

□ CDN

□ Load balancing

□ Context-aware smart routing



CASE STUDY #4

Delivery Hero

Delivery Hero secures a rapidly expanding workforce while minimizing internal complexity

- Founded in Berlin in 2011
- The world's leading local delivery platform
- Global pioneer of q-commerce — online sales and logistics services that deliver goods in under one hour

For Delivery Hero, rapid growth had introduced complexities and challenges for their IT and security strategy. Keeping pace with onboarding new users and integrating new companies with different tech stacks were increasingly taxing for Delivery Hero's internal teams.

"With so many different new people and infrastructures to manage, the complexity added up," explained Wilson Tang, Director of Engineering, Platform Core Services at Delivery Hero. "That limited how efficiently we could innovate. To move quickly, we needed tools to help us get that complexity under control."

To reduce this complexity, Delivery Hero adopted Cloudflare's connectivity cloud, which helped them converge their security, performance, and developer functionalities onto Cloudflare's control plane. Some of these consolidations included securing employee access to internal resources with Zero Trust, improving security and performance across public-facing applications and websites, and streamlining the development and configuration of new applications.

"Being able to onboard new teams quickly and easily shift our new brands onto a consolidated, easily -administered platform like Cloudflare improved our efficiency and time -to -market with new products," Tang explained. "Speed of innovation is everything in the tech industry, and by simplifying operations using Cloudflare we can iterate and create service and value improvements that keep our customers from turning to our competitors."

Key results

- 90% reduction in bandwidth expenses due to improved bot security and content caching in the connectivity cloud
- Mitigated bot attacks, freeing up development teams to focus on product innovation rather than fraud prevention
- Reduced organizational complexity, speeding up employee onboarding and infrastructure configuration

USE CASE #5

Optimize applications for high-traffic periods

Applications — both internal and customer-facing — need to remain fast and available at all times. And the global uptick in AI traffic and resource-intensive AI infrastructure means that more organizations are struggling with greater latency and infrastructure costs, making applications hard to use and hindering enterprises from maintaining a competitive edge.

When evaluating application performance solutions, look for integrated services that offer load balancing, simplified traffic management, and graceful handling of traffic surges (via virtual waiting rooms) across the entire application landscape.

Architectural qualities to look for:

- Global CDN coverage with robust edge caching
- Global and local traffic management support
- Automatic, near–real-time failover
- Automatic and virtually limitless scalability
- Hybrid and multi-cloud support
- Low-latency execution at the edge
- Model deployment and load balancing across edge locations
- Granular visibility into AI prompts, token usage, application requests, responses, and more

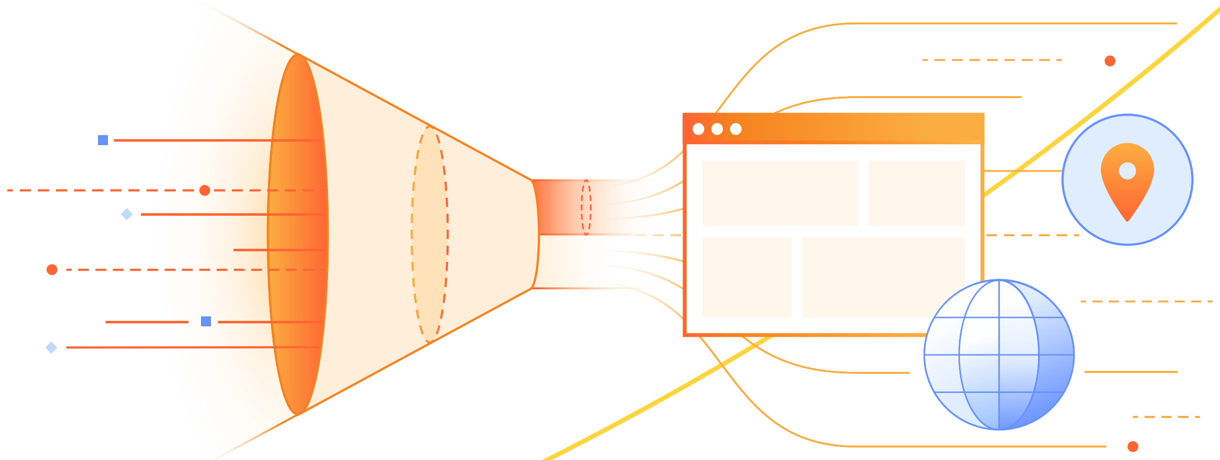
Quick adoption guide

□ CDN

□ Load balancing

□ Virtual waiting room

□ AI gateway



CASE STUDY #5

West Ham United Football Club ensures 100% availability — even during traffic surges of 10x

- Based at East London's London Stadium
- Founded in 1895

For years, West Ham United F.C. has brought in the English Premier League's third-highest average matchday attendance — around 58,000 supporters per game — and has enjoyed a strong international support base that depends on the West Ham website for game updates. Every match brings up to a 10x spike in visitor traffic, driven in part by the club's massive social media following and a Premier League blackout on televised Saturday matches.

This created problems for fans, who became impatient while waiting for the site to load or recover from frequent outages.

"West Ham supporters are a passionate bunch and they don't wait for a slow page to load," explains Richard Ravenhill, Technical Director at West Ham sponsor, Skye Cloud. "The website is also a hub for the club's revenue-generating activities: their YouTube videos and the official sites for West Ham tickets, merchandise, and memorabilia. If the fans can't get to those portals, they can't support the club financially — which is obviously bad news."

After a performance and security review of their website and web host, West Ham was ready for change. That change took the form of Skye Cloud, the bespoke cloud and private UK hosting provider — who quickly moved West Ham's portals onto the Cloudflare network to improve the core security and availability of their website and mobile applications.

"The Cloudflare network delivers all web content to the West Ham fanbase," says Mo Ali, Director of IT at West Ham. "Because we can offload that traffic, Cloudflare radically reduces the number of hits we take. In one 24-hour matchday peak, the West Ham site received 11.5 million requests — and Cloudflare handled over 93% of them."

Key results

- Absorbed 10x traffic surges to maintain 100% uptime
- Eliminated lost merchandise and ticket revenue due to site outages and poor load times

USE CASE #6

Maintain data compliance and keep sensitive data in-region

Keeping up with ever-changing compliance and regulatory requirements can be tough — especially given modern organizations' expanding application and API portfolios. But the penalty for failing to maintain compliance is severe, from costly fines to increased risk for organizations and users alike.

Look for services that help maintain data compliance while integrating robust security capabilities, so sensitive data is stored in-region and secured against corruption, compromise, and attacks. Modern application security solutions must address requirements across multiple overlapping, new, and evolving frameworks, from regional data sovereignty laws, like the General Data Protection Regulation (GDPR), to sector-specific regulations.

Architectural qualities to look for:

- Geographic data residency controls (with specification of where data is stored and processed)
- Regional access control and logging
- Regionalized encryption of data with jurisdiction-specific key storage
- Data leak prevention on origin servers to block transmission of sensitive data
- Prompt engineering defenses for user-facing LLMs to prevent injection attacks and data exfiltration
- Malicious third-party script and connection detection and alerting to identify supply chain attacks and data breaches
- Compliance policy updates that can be deployed globally while respecting regional variation

Quick adoption guide

- □ WAF with sensitive data detection
- □ Data localization functionality
- □ Data loss prevention for web applications and APIs
- □ Web application supply chain security
- □ LLM security
- □ AI gateway, firewall, and audit capabilities

Key compliance standards and associated technical controls

Regulation / Standard	Key requirements	Technical controls	
GDPR and regional data sovereignty laws	Data must remain in approved regions	• Data localization controls • Geofencing capabilities	• Edge computing with regional processing
DORA 2025	ICT risk management, resilience testing, and incident reporting	• Zero trust architecture • Automated incident response	• DDoS protection • Resilience testing tools
EU AI Act 2025	Risk-based controls, transparency, and data governance	• Edge AI processing infrastructure • Rate limiting for AI API calls • Audit logging of AI interactions	• Content filtering for AI outputs • Regional compute controls • Security for AI model endpoints
HIPAA / HITECH	PHI protection and breach notifications	• Encryption • Audit logging	• Access controls
PCI DSS 4.0	Cardholder data protection	• Tokenization • Vulnerability scanning	• Network segmentation
ISO 27001	Information security management	• Risk assessment tools • Continuous monitoring	• Security policy enforcement
NIST Cybersecurity Framework 2.0	Comprehensive security guidance	• Defense-in-depth architecture • Continuous monitoring	• Identity management
Cross-regulation requirements	Audit capabilities and data protection	Comprehensive logging • Data loss prevention (DLP) • API security governance • Encryption management • Compliance analytics dashboards	

CASE STUDY #6

Doctolib

Doctolib ensures secure, reliable health services while meeting evolving data compliance standards

- Founded in France in 2013
- Europe's fastest-growing ehealth service provider
- Enables 390,000+ healthcare providers to serve 90 million patients across France, Germany, and Italy

Doctolib is Europe's fastest-growing ehealth service — and as such, is tasked with securing large volumes of sensitive patient and employee information across a broad range of SaaS applications. This information, by its very nature, is also subject to stringent GDPR requirements for data protection.

To help meet these goals, Doctolib turned to Cloudflare. Cloudflare's Data Localization Service (DLS) became central to the company's compliance strategy, enabling them to prove to customers and regulators that protected patient data never leaves the European Union (EU). DLS helps ensure that non-EU providers and third parties do not gain access to sensitive information, and that critical metadata — including logs and IP addresses — is only accessible by Doctolib-authorized users.

"DLS is invaluable for us because it allows us to use Cloudflare while remaining compliant," explained Cédric Voisin, Doctolib's CISO. "And no one else in Europe has Cloudflare's capabilities and ability to handle the massive amount of traffic we have."

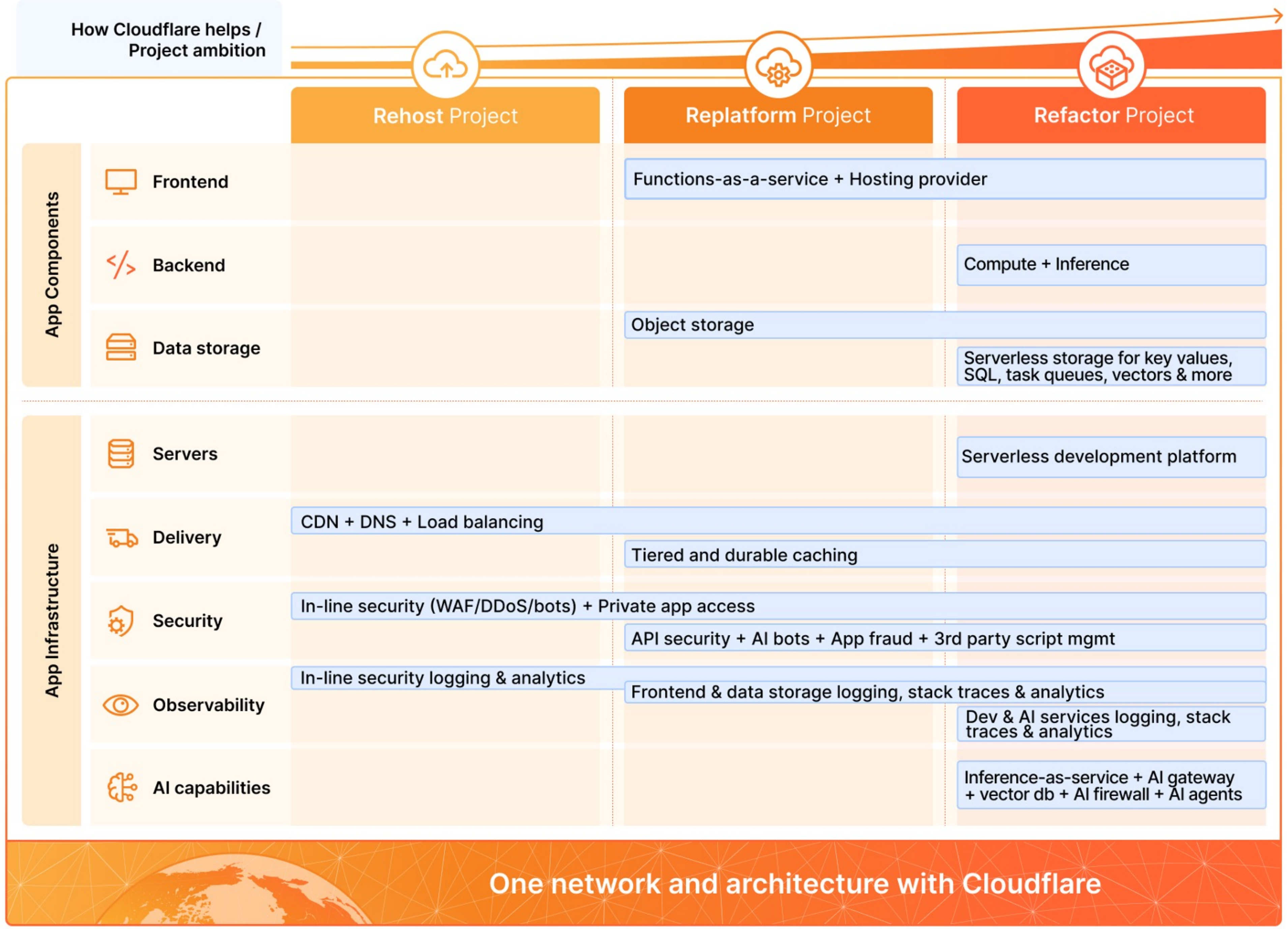
Key results

- Meets evolving GDPR compliance requirements through patient data localization and data security
- Improves data visibility and reduces risk of data exfiltration
- Maintains robust Zero Trust security via access controls and device validation

Starting vendor assessments

After developing a thorough understanding of your organization's needs and prioritized use cases, look for a vendor that can meet you wherever you are on your journey to application modernization.

While traditional vendor "side-by-side" comparisons are still valuable, too often they steer toward feature checklists, which are tough to objectively conduct in a market that itself is moving so quickly. To better support your path to modernization, use the conversation guides below to jumpstart discussions with vendors based on your current goals and key stakeholders.



How Cloudflare helps / Project ambition

Rehost Project

Replatform Project

Refactor Project

App Components

Frontend

Functions-as-a-service + Hosting provider

Backend

Compute + Inference

Data storage

Object storage

Serverless storage for key values, SQL, task queues, vectors & more

App Infrastructure

Servers

Serverless development platform

Delivery

CDN + DNS + Load balancing

Tiered and durable caching

Security

In-line security (WAF/DDoS/bots) + Private app access

API security + AI bots + App fraud + 3rd party script mgmt

Observability

In-line security logging & analytics

Frontend & data storage logging, stack traces & analytics

Dev & AI services logging, stack traces & analytics

AI capabilities

Inference-as-service + AI gateway + vector db + AI firewall + AI agents

One network and architecture with Cloudflare

Conversation starters for CISOs

For application security

Key priorities:

- Protecting organizational data from data breaches
- Complying with global, regional, and industry standards
- Improving resiliency and maintaining 100% uptime

What to ask your application security vendor:

- Given the rise of AI-driven threats, how do you adapt your services to address new attack vectors?
- How do you discover shadow APIs and shadow AI?
- What disaster recovery and incident response support do you offer for modern cloud applications?
- How do you approach application security in the context of a hybrid or multi-cloud environment?
- How do you balance security priorities with the priorities of software development teams?

For application performance

Key priorities:

- Improving resilience and maintaining 100% uptime
- Increasing overall business agility

What to ask your application performance provider:

- How have you reduced application latency and downtime — so that it doesn't affect internal productivity, business continuity, or end user experience?
- How do you support critical user journeys that depend on optimal application performance?
- What time and resource savings have you seen for customers that implement your application performance services?
- How would you quantify the cost of productivity gains customers have seen from your services?

Conversation starters for CIOs

For application security

Key priorities:

- Reducing attack surface
- Increasing business agility and meeting modernization benchmarks
- Improving resiliency and maintaining 100% uptime

What to ask your application security vendor:

- How do you discover shadow AI and shadow APIs?
- Tell us more about your experiences with balancing security and performance while migrating applications to the cloud. How have you solved for these challenges?
- How do you think about security in the context of a hybrid or multi-cloud environment?
- What is your approach to ensuring 100% uptime for your customers? How do you balance this approach while keeping security friction low for developers and IT teams?
- Given the rise of AI-driven threats, how do you adapt your services to address new attack vectors?
- What disaster recovery and incident response support do you offer for modern cloud applications?

For application performance

Key priorities:

- Improving user experience and internal productivity
- Accelerating application modernization
- Reducing total cost of ownership (TCO)

What to ask your application performance provider:

- How do you measure the impact of application performance on the end-user experience?
- What are the biggest application performance challenges that you solve for? How do you counteract application latency and downtime?
- How do you help ensure 100% application uptime without overburdening developers and IT teams?
- In what ways do you optimize performance for on-premises, cloud-native, and microservices-based applications?
- Can you ensure a consistent and positive user experience in the event of traffic surges and service outages?
- How do you help customers balance capital expenditure (CapEx) versus operating expense (OpEx)?
- With the increasing data demands of modern applications, how are you lowering egress fees while helping customers maintain a positive user experience?

Cloudflare for application services

Cloudflare's connectivity cloud facilitates the modernization of both legacy applications and new, cloud-native applications by offering a unified platform with programmable cloud-native services to connect and protect all applications and APIs.

With Cloudflare, organizations can modernize applications faster, more securely, and at a lower cost — while ensuring a seamless user experience and avoiding the complexity of traditional multi-vendor solutions.

The Cloudflare difference

Application security	Application performance
✓ Origin-agnostic platform with centralized control and visibility ✓ Speedy mitigation powered by threat intelligence and machine learning-based detections ✓ Developer-oriented infrastructure with IaC integrations and an API-first platform ✓ Ability to address complex web application and API security issues	✓ Cloud-native platform positioned to scale with business ✓ Architecture built for speed, security, and agility ✓ Unified, self-managed, and easy-to-use interface ✓ Global reach ✓ Compliant with data regulations and location-specific requirements

Get started with Cloudflare

To learn more about how Cloudflare helps organizations meet their application modernization goals

Talk to an expert

This document is for informational purposes only and is the property of Cloudflare. This document does not create any commitments or assurances from Cloudflare or its affiliates to you. You are responsible for making your own independent assessment of the information in this document. The information in this document is subject to change and does not purport to be all inclusive or to contain all the information that you may need. The responsibilities and liabilities of Cloudflare to its customers are controlled by separate agreements, and this document is not part of, nor does it modify, any agreement between Cloudflare and its customers. Cloudflare services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com