CLOUDFLARE

3 challenges of securing and connecting application services

Why traditional architectures fail — and how a connectivity cloud can help

Content

Overview

Web applications and APIs are fundamental to modern business growth. In 2023, the number of businesses that maintained a web presence jumped to 71%, while another study estimated that 28% of all business activity is now conducted online.[1]

From mobile ecommerce platforms to internal productivity tools, applications (and the APIs that allow them to function) not only help deliver dynamic, personalized content to customers, but also connect global workforces, increase user productivity, and accelerate the pace at which developers can continue to innovate. As businesses scale, however, maintaining optimal application performance and security becomes increasingly important — and difficult to ensure:

- **APIs are easy to use, but hard to secure.** One study found that the cost of API insecurity (breaches due to API errors or exploits) totaled around $41-75 billion in annual losses[2]
- **Even a few seconds of latency can significantly damage the user experience, engagement, and conversion rates.** Traffic spikes, outages, and subpar application performance drive customers away; by one estimate, 88% of online users will not revisit a site after a negative experience[3]
- **Business growth is hampered by application sprawl, complexity, and vendor challenges.** As businesses scale, managing an expanding portfolio of applications — often across multiple environments and vendors — comes with rising costs, a loss of control, and greater security and IT headaches

Combating these issues — without slowing business operations — requires a more agile solution than either traditional hardware or multi-vendor, single-solution cloud services can provide. A **connectivity cloud**, one that is designed to connect and secure everything within the IT environment, can help businesses consolidate crucial application services and improve business growth.

Challenge #1: Cyber attacks are complex and costly

Web applications and APIs enable businesses to function with more flexibility, deliver premium user experiences, and innovate faster than ever — and they also represent an ever-widening attack surface. DDoS attacks, API threats, malicious bots, and zero-day vulnerabilities can compromise business operations and degrade customer trust, sometimes for good.

Attacks are bigger and more sophisticated than ever

As businesses scale their operations and customer bases, they represent an ever-increasing and lucrative target to cyber attackers across the globe:

- Application-layer attacks have spiked by as much as 80% in 2023
- In Q3 2023, Cloudflare mitigated a record-breaking 201M RPS DDoS attack
- The average cost of a data breach jumped to $4.45M — a 13% increase from 2020

Not only are attacks larger than ever before — their effect is also compounded by increasingly sophisticated tactics. Just as organizations turn to more advanced security technologies to protect their applications, infrastructure, and data from harm, modern cyber criminals also use artificial intelligence and machine learning tools in order to carry out tailored and adaptive attacks.[4]

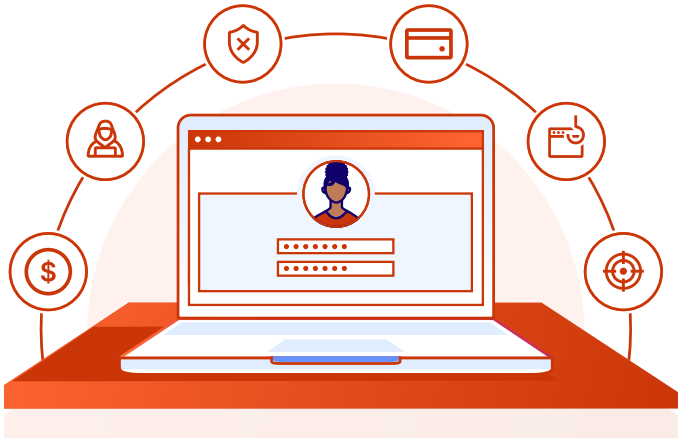
Successful attacks like these may compromise confidential user data, heavily impact revenue, brand reputation, and customer trust, and result in serious compliance fines and steep remediation costs.

The cost of API breaches is on the rise

APIs have experienced explosive growth in recent years, allowing businesses to increase their agility and pace of innovation to unprecedented levels. But the rapid increase in API development also makes it nearly impossible to detect and patch every vulnerability they contain, especially when developers and engineers fail to communicate with security teams before launch.

For businesses that lack the internal resources needed to secure their API environment, the consequences can be severe. In a recent survey, 53% of respondents experienced a data breach within their applications and networks due to compromised API tokens.[5] Experts also found that vulnerable or insecure APIs cost businesses between $41-75B in global annual losses.[6]

However, securing APIs is far from a simple process. Existing application security toolsets, including web application firewalls (WAF), DDoS mitigation, and bot management services, are not designed to defend against the specialized nature of API threats — and many still do not offer the granular controls needed to defend APIs from targeted threats.



Challenge #2: Poor application performance drives users away

Across online businesses and mobile applications, consumers expect a smooth, fast experience at all times. Unfortunately, traffic spikes, overloaded servers, and unexpected outages can all impact application availability and performance, creating a subsequent lapse in customer engagement and trust. To counteract these issues, businesses need reliable application services that can guarantee fast load times and availability, while effortlessly scaling rich, dynamic user experiences.

Latency issues drive down sales — by the billions

According to Forbes, approximately 71% of global businesses maintain some form of web presence in 2023, with an estimated 28% of all business taking place online.[7] In other words: consumers are spoiled for choice, which puts additional pressure on businesses to deliver a lightning-fast, always-available, and easy-to-use experience.

Among all performance benchmarks, latency is one of the clearest indicators of a smooth and successful online experience. Slow-loading web experiences not only frustrate customers, but often have a detrimental effect on conversion rates as well.

One report found that a staggering 40% of users will navigate away from a website if it takes longer than three seconds to load.[8] And the loss of user engagement is only growing: an estimated $2.6 billion is lost in sales every year due to lagging load times.[9]

Site unpredictability can alienate users just when businesses need them most

Today's online businesses are all too familiar with the challenges of maintaining a seamless consumer experience in the face of holiday traffic spikes and explosive growth periods.

A sudden influx of holiday shoppers can easily overwhelm ecommerce apps, fueling user frustration when shopping carts are unexpectedly emptied or product pages fail to load quickly. Or, emergency service web pages may be ill-equipped to service a large influx of users, causing extended outages right when their assistance is most critically needed.

Without sufficient traffic optimization and reliability measures in place, businesses stand to lose a significant portion of their user base. By one estimation, 61% of web users expect to find what they need on a site within the first five seconds; otherwise, they will begin to look elsewhere.[10] That's a risk many businesses can't afford to take.

Challenge #3: Application services come with scalability challenges

Protecting and accelerating web applications and APIs is critical to the success of modern businesses. As those businesses continue to grow their internal operations and customer bases, however, the focus quickly shifts from ensuring application security and performance to doing so *at scale*.

Managing complex architectures can slow business growth — and compromise control

In 2023, connecting and securing complex digital environments is a complicated process for many businesses. Critical data and applications exist across an ever-expanding combination of on-premises infrastructure, public clouds, and SaaS environments, and over 40% of security and IT teams are newly tasked with managing and securing them.[11]

But as these application portfolios grow, so does the time it takes to properly configure, secure, and maintain them. And businesses are rapidly finding themselves strapped for time and resources to do so, leading to a loss of visibility and control across their entire application landscape.

A survey conducted by Cloudflare and Forrester Consulting[12] found that this loss of control is driven by four primary factors:

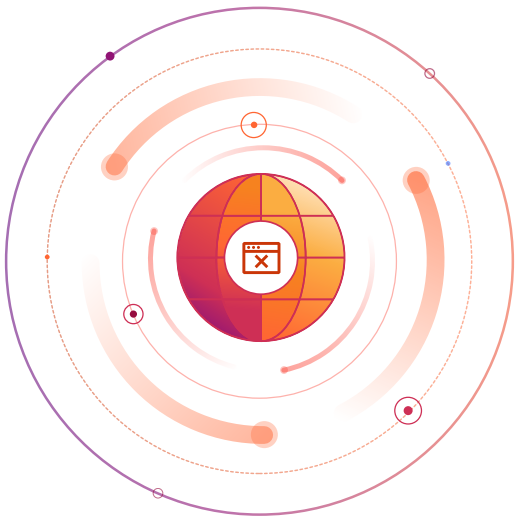
1. Organizations are responsible for a greater number of applications (66% of respondents said yes).
2. Applications live in a greater number of locations (62%).
3. Organizations have shifted operations from on-premises locations to cloud environments (54%).
4. Organizations have shifted to a remote or hybrid working model (49%).

Without the ability to control every aspect of their environment, businesses may face implementation delays, leave applications vulnerable to threats, or find it difficult to expand their operations (and competitive advantage) in an efficient manner.

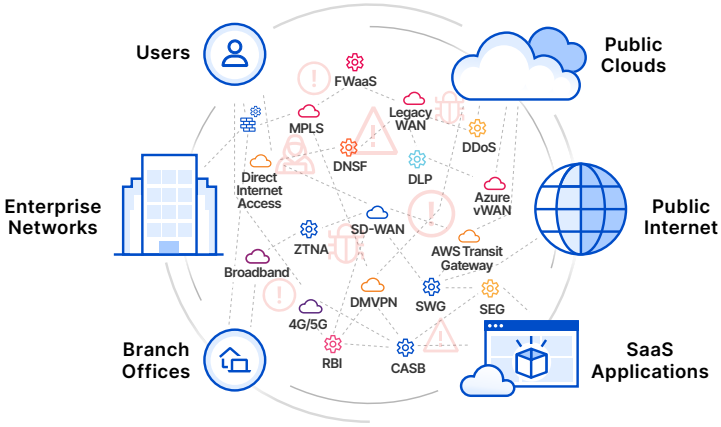
Existing application services are not designed for flexibility and business growth

Making matters worse, cloud vendors that offer consolidated application services can trap businesses into contracts that put them at a disadvantage, especially as they try to scale. Businesses may benefit from vendors' initial offerings, but get locked into inefficient pricing models for data storage or lack the flexibility to mix and match services across multiple providers.

In the face of vendor lock-in, decreased flexibility, and hampered business growth, 98% of surveyed organizations said they would find value in a cloud-native platform that offers secure, performant, "any-to-any" connectivity across their users, applications, data, devices, networks, and cloud environments.[13] Not only would such a platform help reduce businesses' overall attack surface, but over 50% of respondents said it would also help accelerate time to market and grow revenue.



Where traditional hardware and cloud solutions fall short



Optimizing web applications and APIs requires a host of dedicated services, from local and global load balancing, waiting rooms, content optimization and video streaming services, to web application firewalls (WAF), API protection, bot management and DDoS protection. But both traditional hardware and cloud-based point solutions fall short of delivering the streamlined protection and performance businesses need to ensure competitive growth, maintain customer satisfaction, manage risk effectively, protect brand reputation, and improve internal productivity.

Hardware cannot optimize and protect what lives in the cloud

On-premises hardware appliances were never designed to support the needs of cloud computing and meet modern business requirements.

These legacy solutions are expensive and clunky to scale, leading to security and performance trade-offs that can have a detrimental effect on application performance and availability, as well as the customer experience.

And this often exacerbates the burden on security and IT teams, who must handle the near-impossible task of managing and securing a complex web of hardware and virtualized appliances, hybrid and multi-cloud environments, and SaaS applications that are fundamentally incompatible with each other. Inevitably, teams are left struggling to find workarounds, meet increasingly stringent compliance requirements, and avoid introducing security vulnerabilities — without losing productivity or frustrating end users.

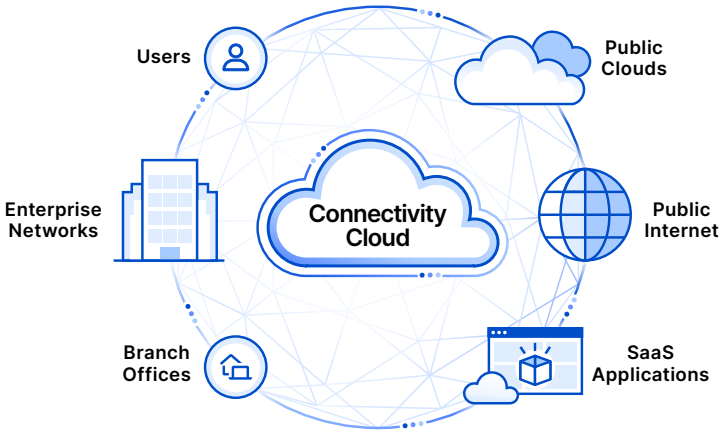
Multi-vendor cloud services introduce complexity and vendor lock-in

On the whole, cloud-based application services enable businesses to operate with more flexibility and agility, but they are not immune to performance, security, and scalability issues of their own. As business needs continue to grow — and the application landscape becomes more complex — finding a cloud vendor that excels in both web application security and performance optimizations can be challenging.

Vendors who claim to offer consolidated services may not always provide true integration “under the hood,” choosing instead to package disparate solutions that are still difficult to implement, maintain, and scale.

Today, most cloud-based solution providers tend to lock customers into their ecosystem, which makes their solutions incompatible with customers who have hybrid or multi-cloud deployments. This forces businesses to either consolidate on that one cloud vendor (often a complex and costly undertaking) or to maintain multiple application security and management stacks — an IT nightmare.

Introducing the connectivity cloud: a new way to consolidate application services



Modern businesses need to scale seamlessly without application performance and security trade-offs. And that requires a more flexible approach to application services than either hardware or cloud-based point solutions can offer.

This new approach is called a **connectivity cloud:** a unified platform of cloud-native services designed to help businesses regain control over their IT environments. Powered by an intelligent, programmable global cloud network, it offers unmatched security, performance, visibility, and reliability.

While traditional cloud providers (like AWS, GCP, and others) only offer their services to applications hosted on their cloud platforms, a connectivity cloud is built to work with any application, no matter where it is hosted.

At its core, a connectivity cloud delivers four key features:

1. **A composable and programmable architecture.** A connectivity cloud is designed for flexibility and ease of use, making it easy for businesses to manage their proprietary infrastructure, cloud systems, compliance needs, and specific configurations without damaging the user experience or management process.

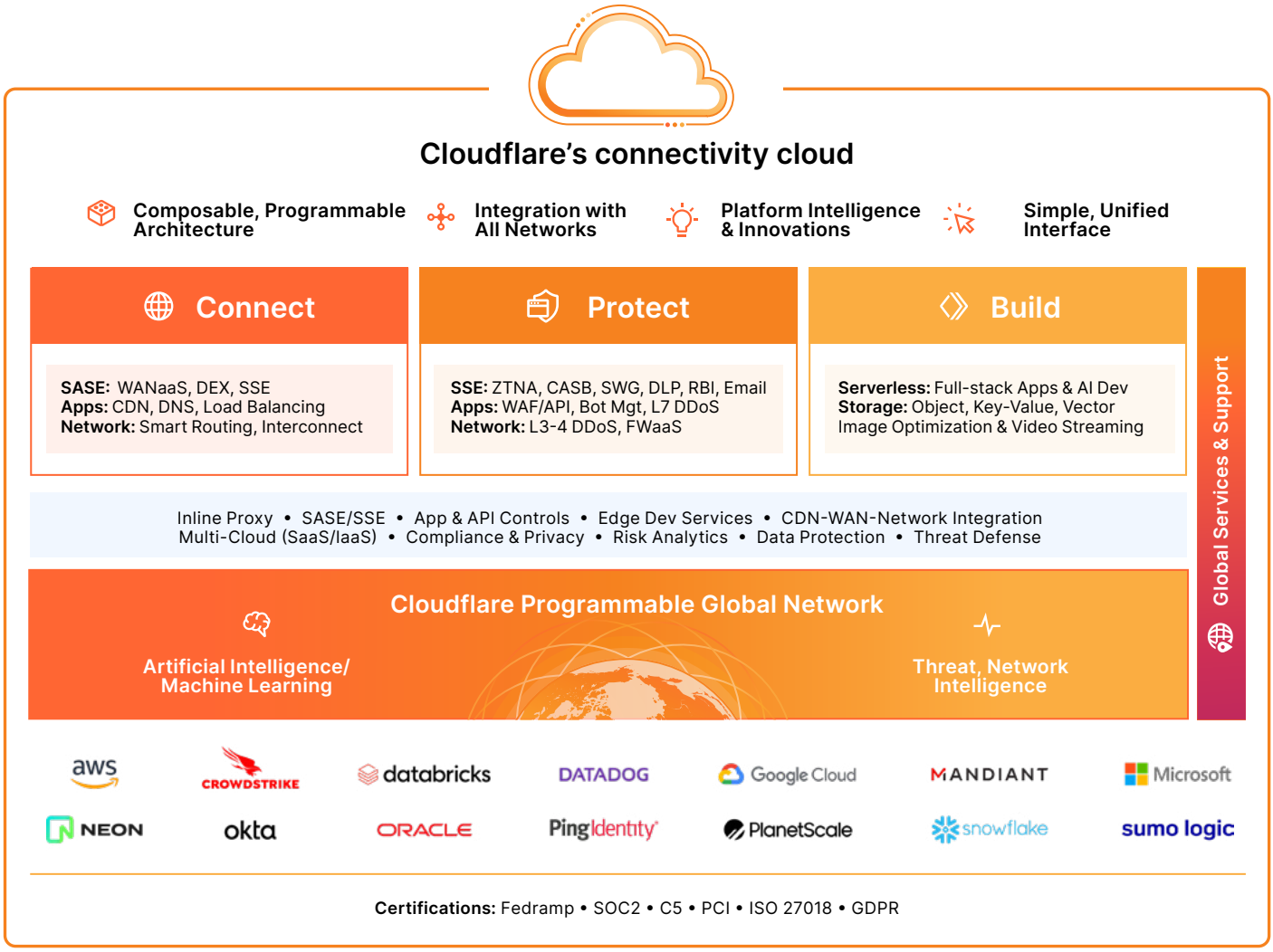
2. **Native, ubiquitous Internet integration.** A connectivity cloud natively integrates with both the Internet and enterprise networks, offering secure, low-latency, infinitely-scalable connectivity between every user, application, and infrastructure.

3. **Built-in platform intelligence and innovations.** A well-architected connectivity cloud has a wide range of services built in at a foundational level, and analyzes extremely high volumes and varieties of traffic in order to automatically update intelligence models — without creating inefficiencies or security gaps.

4. **A unified and simplified interface.** A connectivity cloud significantly reduces tool sprawl, dashboard overload, and alert fatigue by managing most of the IT environment from a single pane of glass.

Key capability	Technical benefit	Business benefit
Limitless interoperability	Orchestrate and automate services with any third-party system by building API-enabled serverless functions on the same servers	Free up internal resources and reduce costs across your organization
Customizable networking	L1-7 connectivity that is fully API-programmable to meet compliance, privacy, and sovereignty requirements	Satisfy compliance with local regulations, without sacrificing productivity or efficiency
Native Internet integration	Connect enterprise networks and resources to the Internet — with complete control from the business request source to the destination	Ensure always-available application connectivity and performance, from any location worldwide
Global network connectivity	Low latency to every Internet-connected user, application, and network infrastructure	Create better customer experiences and fuel your competitive advantage
Infinite network scalability	Scales on-demand without any customer configuration, hardware, or virtual appliances required	Effortlessly grow your business without complex configurations or hidden costs
True single-pass processing with built-in services	Security, performance, and privacy functions are built in — so connectivity is never disrupted or compromised	Improve application security, performance, and reliability without trade-offs
Platform intelligence-enabled innovation	Platform intelligence boosts visibility across all Internet paths and helps accelerate code, data, and traffic along the fastest routes	Regain control over and visibility into your environment — no matter where applications and data reside
Accelerated vendor consolidation	Consolidates vendor services, logs, and customer service capabilities and delivers them from a unified management interface	Reduce complexity and streamline application management across multiple vendors and services
Accelerated digital transformation	Fully connects your current and future networking environment across all users, applications, systems, and locations	Boost productivity, efficiency, and agility by connecting your environments, applications, and users

How Cloudflare delivers connectivity and control



Cloudflare is the world's *first* connectivity cloud. With a global network spanning over 310 cities in 120+ countries, Cloudflare is uniquely architected to provide the connectivity businesses need to deliver optimal application security and performance — without leaning on outdated solutions or opening the door to threats.

Consolidate application services with Cloudflare

Contact us

> **The experience for end users is very smooth, and using a centralized service like Cloudflare to manage application access policies makes it easier for our IT and security teams. Plus, we now have visibility into who is using each of our services, which helps us improve our security holistically."**
>
> João Pedro Gonçalves, Global Chief Information Security Officer, EQT

EQT

References

1. Forbes Advisor. “Top Website Statistics For 2023.” https://www.forbes.com/advisor/business/software/website-statistics/. Accessed October 20, 2023.
2. Tech Wire Asia. “API vulnerabilities costing businesses up to US $75 billion annually.” https://techwireasia.com/2022/06/api-vulnerabilities-costing-businesses-up-to-us75-billion-annually/. Accessed October 20, 2023.
3. Forbes Advisor.
4. McKinsey & Company. “Cybersecurity trends: Looking over the horizon.” https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon. Accessed October 23, 2023.
5. VentureBeat. “50% of orgs report experiencing data breaches due to exposed API secrets.” https://venturebeat.com/security/data-breaches-api/. Accessed October 23, 2023.
6. Tech Wire Asia. “API vulnerabilities costing businesses up to US$75 billion annually.” https://techwireasia.com/2022/06/api-vulnerabilities-costing-businesses-up-to-us75-billion-annually/. Accessed October 20, 2023.
7. Forbes Advisor. “Top Website Statistics For 2023.” https://www.forbes.com/advisor/business/software/website-statistics/. Accessed October 20, 2023.
8. Forbes Advisor.
9. Forbes Advisor.
10. Forbes Advisor.
11. Cloudflare and Forrester Consulting. “New Study Reveals Cloud Giants are Holding Businesses Captive.” https://www.cloudflare.com/press-releases/2023/new-study-reveals-cloud-giants-are-holding-businesses-captive/ Accessed October 20, 2023.
12. Cloudflare and Forrester Consulting.
13. Cloudflare and Forrester Consulting.

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

REV:BDES-5435.2024JAN10