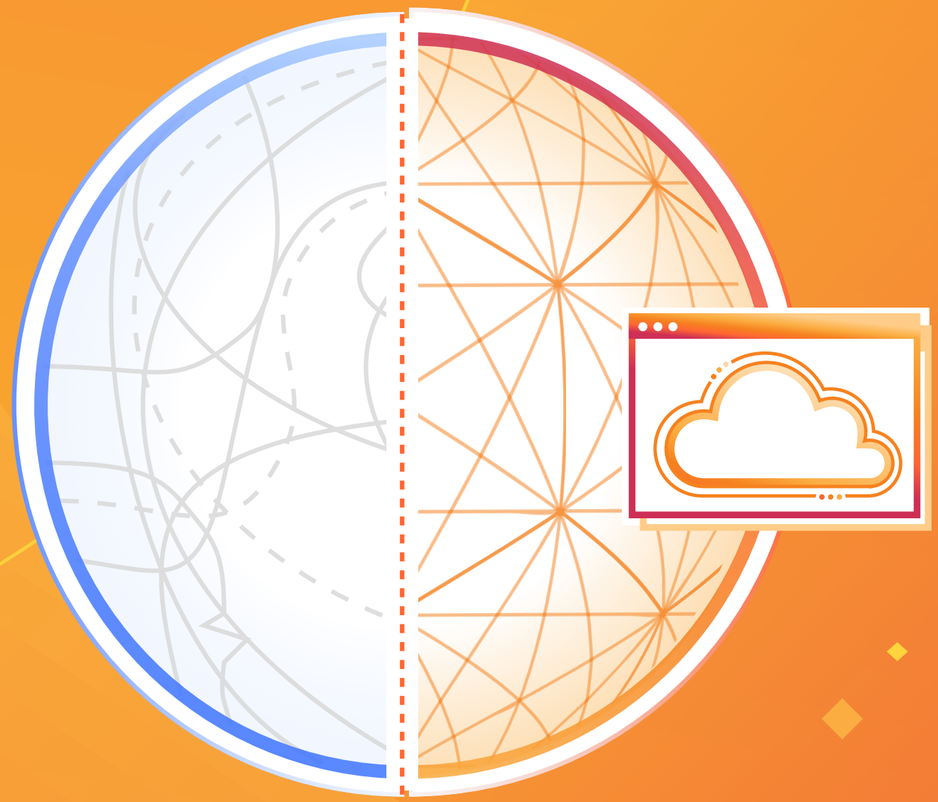
CLOUDFLARE

EBOOK

Driving down IT stack complexity

A new approach to platform consolidation



Platform consolidation is a priority and a challenge for IT and security leaders

Platform consolidation — the integration of multiple tools and infrastructure into a single, cohesive platform — is a strategic priority for security and IT leaders, driven by increasing tech stack complexity and economic challenges.

Eighty-eight percent of IT leaders are actively consolidating and optimizing their technology stacks. Generally, they do so to achieve several closely intertwined benefits:

1. More efficient operations

When more services live on fewer platforms, there are fewer integrations to troubleshoot and fewer vendor relationships to manage. In addition, fewer tools to manage simplifies visibility and means fewer tickets and fewer process steps are required to make changes.

2. Cost savings

IT budgets are increasing for most organizations, but inflation and rising costs can offset those increases — preserving pressure to reduce costs in existing services. Sunsetting legacy data platforms, consolidating vendors and optimizing cloud spending are just a few ways to save resources and fund new and more impactful innovation projects.

3. Improved security

Multiple integration points create security gaps, block visibility across the attack surface, and introduce risk. Platform consolidation is the way to get control of security and compliance and implement consistent policies from a central control point — helping avoid missed threats, reducing the need for qualified specialists, and simplifying attack response.

4. Greater focus on innovation and strategic initiatives

The easier the IT stack is to manage, the more time IT, security, and development teams have for long-term strategic projects, new technologies, and new opportunities for innovation.

Unfortunately, platform consolidation projects often struggle to meet expectations due to gaps between what platforms can do and what it should do. As a result, IT and Security team productivity slows even further, and business initiatives attempting to connect and secure the organization's technology stack fall short.

This ebook explores the reasons for these struggles, and offers suggestions about how to overcome them.

Challenges with platform complexity for the enterprise

Despite widespread interest in platform consolidation, few organizations have made as much progress as they'd like.

One reason is natural and unavoidable: in the IT world, service deprecation and replacement simply takes time. Many organizations procure their services on multi-year contracts that can't be canceled at the drop of a hat. But even when organizations are contractually capable of consolidating certain services, they often run into obstacles like:

Compatibility issues

Every digital environment has proprietary infrastructure, multiple clouds, unique compliance needs, and other highly specific tooling, processes, and configurations. Finding consolidation platforms that work with all of those requirements can be difficult.

Misleading vendor promises

Consolidation is a common vendor promise, and many IT platforms claim to offer fully integrated services. However, many of these 'platforms' actually run different services on different infrastructure, meaning they still require time-consuming integrations to set up and maintain.

High switching costs

Turning one security or connectivity service off — and another one on — often imposes high labor costs, whether in the form of internal team time or managed services. The former approach also imposes an opportunity cost on other projects.

Organizational inertia

Certain leaders or teams is loath to change their current tech stack, no matter how inefficient it may be. From their perspective, the devil you know is better than one you don't.

A connectivity cloud makes platform consolidation easier

A connectivity cloud is a unified platform of cloud-native services that provides secure, any-to-any connectivity for an organization's entire IT environment. These services span security, networking/connectivity, and development use cases. And the underlying platform is designed with the following architectural factors:

Deep integration: A connectivity cloud is integrated natively with the Internet and with enterprise networks, offering secure, low-latency, infinitely scalable connectivity between every user, application, and infrastructure. In addition, all services can run on every server in every data center in the underlying network, and don't require manual integration to work together.

Programmability: A connectivity cloud's architecture provides limitless interoperability and customizable networking, letting it adapt to multi-cloud deployments, proprietary infrastructure, unique compliance needs, and other highly specific tooling, processes, and configurations. All layer 2-7 connectivity is fully API programmable via serverless functions that live on the same servers as every other service.

Platform intelligence: A connectivity cloud has a wide range of security and connectivity services, and analyzes extremely high volumes and varieties of traffic from all of them in order to automatically update threat and network intelligence models.

Simplicity: A connectivity cloud offers all of these services from a single pane of glass, and provides further visibility by integrating with any cloud log storage and analytics platform.

These qualities are designed to address the common challenges of platform consolidation, as the table on the next page shows:

Consolidation challenge	Connectivity cloud solution
Compatibility issues	**Programmability:** Fully programmable connectivity lets organizations customize where data lives and is decrypted, helping meet unique privacy and compliance requirements **Deep integration:** Since the connectivity cloud is natively integrated with the Internet, enterprise networks, clouds, SaaS apps, etc, it's able to work with whatever other tools the organization requires
Misleading vendor promises	**Deep integration:** Since all services live on the same infrastructure and are built to work together, implementation and integration become much more straightforward
High switching costs	**Deep integration:** Since all services are built to work together and run on the same infrastructure, they take less time to set up, and integrate out of the box **Simplicity:** Since all services are available from one pane of glass, there's less new training for the team
Organizational inertia	**Programmability:** A connectivity cloud's ability to integrate with any flavor of service and infrastructure means organizations can keep their favorite tools while using the connectivity cloud to fill in the gaps **Platform intelligence:** A connectivity cloud's massive body of cross-domain threat intelligence is an upgrade over many point solutions, which may help leaders feel more confident about switching

A connectivity cloud delivers tangible consolidation benefits

Organizations that consolidate onto a connectivity cloud tend to make significant progress in their overall consolidation goals. According to recent studies of connectivity cloud users, these organizations report:

1 Improved operational efficiency

50% improved efficiency and more resources freed up to focus on strategic projects

UP TO **75%** faster response times to security incidents, helping reduce organizational risk exposure

2 Significantly lower TCO

50% reduction in TCO of security and network investments

3 Better overall business outcomes

54% accelerated time-to-market for new innovations

Ultimately, these benefits point towards a common aim: helping IT leaders and their teams focus on strategic projects that accelerate the business in its ability to grow, scale, and beat the competition.

Next, let's see how innovative companies across industries leveraged a connectivity cloud to drive results.

Ivanti: Five vendors replaced by one connectivity cloud

Ivanti came into existence from a merger of several companies, which meant relying on a complex IT infrastructure provided by disparate vendors. “Different parts of our organization were relying on a patchwork of providers to address their respective needs,” said Andrew Ariotti, Senior Web Marketing Manager at Ivanti.

This complexity caused inefficiency across the IT organization, and made it difficult for the company to achieve three important goals:

1. Optimize page load times of the marketing website and related web assets
2. Protect web assets from potential DDoS attacks
3. Apply custom reverse proxy rules to allow routing traffic to different origin servers

To overcome all of this complexity, Ivanti used a connectivity cloud for DNS, content delivery, and search engine optimization. The company **streamlined security workflows** and **protected access to apps, infrastructure, users and data** across the organization — all without impeding performance.

Having a connectivity cloud “serves as a reverse proxy with POPs all around the world greatly enhances the robustness, performance, and security of our web assets,” Ariotti remarked.

Ivanti’s website is now faster and more secure. And a faster site improves a user’s experience, making them more likely to use the product again or refer it to others.

> “Different parts of our organization were relying on a patchwork of providers to address their respective needs. We chose [a connectivity cloud] because it offered a comprehensive, cost-effective solution that checked all of our boxes.”
>
> Andrew Ariotti
> Senior Web Marketing Manager
> Ivanti

Mindbody: Replacing seven legacy tools with a single solution for cloud and on-prem

Mindbody, a software provider for fitness and wellness companies, deployed many security and performance solutions from different vendors across their on-premises and cloud-based infrastructure, including multiple CDNs, WAFs, and a bot mitigation service. However, managing all of these individual point solutions proved complex, and provided limited visibility and protection across on-prem and cloud-based environments.

“We had a diversity of products, all of which had different interfaces and different capabilities used in different platforms across different things,” said Eric Pierce, Senior Manager Cybersecurity at Mindbody. “It was really hard to manage and monitor that many disparate solutions and different environments.”

Using a connectivity cloud helped the company block cyber threats with an **easy-to-use, powerful security architecture** that unified solutions and environments, protected users, and provided seamless visibility and control.

> “We’ve been able to replicate all the functionality that we had previously with a variety of tools and consolidate it into one, which just makes everything easier.”
>
> **Adelyn Fears**
> **Security Engineer**
> Mindbody

mindbody

Applied Systems: Accelerated digital transformation and platform consolidation

Applied Systems builds SaaS solutions for the insurance industry. The company safeguards large volumes of sensitive data, but struggled to align myriad security solutions, which overburdened security and IT teams with endless tasks and no clear path forward.

“We had various components from different security vendors like Zscaler and Cisco and different networking paths to our data centers,” said Chief Information Security Officer Tanner Randolph. “Over the past few years, we’ve really focused on consolidating around a unified security and networking stack.”

In 2022, Applied Systems began consolidating large swaths of security and networking functionalities using a connectivity cloud’s programmable, composable architecture.

The ability to connect, protect, and build—across an entire IT environment—provided the company with **unified security controls** across web, cloud, and private app environments.

> “My teams can focus on driving business forward. I don’t know of a lot of security teams that can say that...”
>
> **Tanner Randolph**
> CISO

APPLIED

Connect, protect, and build with Cloudflare's connectivity cloud

Cloudflare provides an intelligent platform comprising programmable, cloud-native services that are integrated, future-proof, and designed for seamless integration with global scale. It meets the connectivity cloud requirements organizations need to meet their consolidation goals:

- **Composable, programmable architecture:** Services are all cloud native and interoperable with each other in every network location. Layer 2-7 connectivity is fully programmable.
- **Integration with all networks:** Built on a network spanning 310+ cities in 120+ countries, and which connects directly to over 13,000 other networks (including every major ISP, cloud provider, and enterprise).
- **Platform intelligence:** Serving over 50 million HTTP requests per second on average, and blocking hundreds of billions of threats every day.
- **Simple, unified interface:** One unified management interface spanning every security use case, network connectivity, and development.

Consolidating onto the Cloudflare connectivity cloud can significantly reduce TCO by 50% or more. This reduction is achieved through modernizing infrastructure, merging various point solutions into one, and cutting down on management overhead. Significantly, organizations attain cost efficiency without compromising on security or performance. Beyond the financial advantages, consolidation also enhances agility and accelerates the time-to-market for new innovations by up to 54%, driving top-line growth.

See why the most successful enterprise companies choose Cloudflare for platform consolidation.

Talk to our experts.

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

REV:PMM-Q12024-Platform Consolidation eBook 2024