



EBOOK

Overcoming 3 security tool challenges to compliance

How the connectivity cloud reduces compliance risks

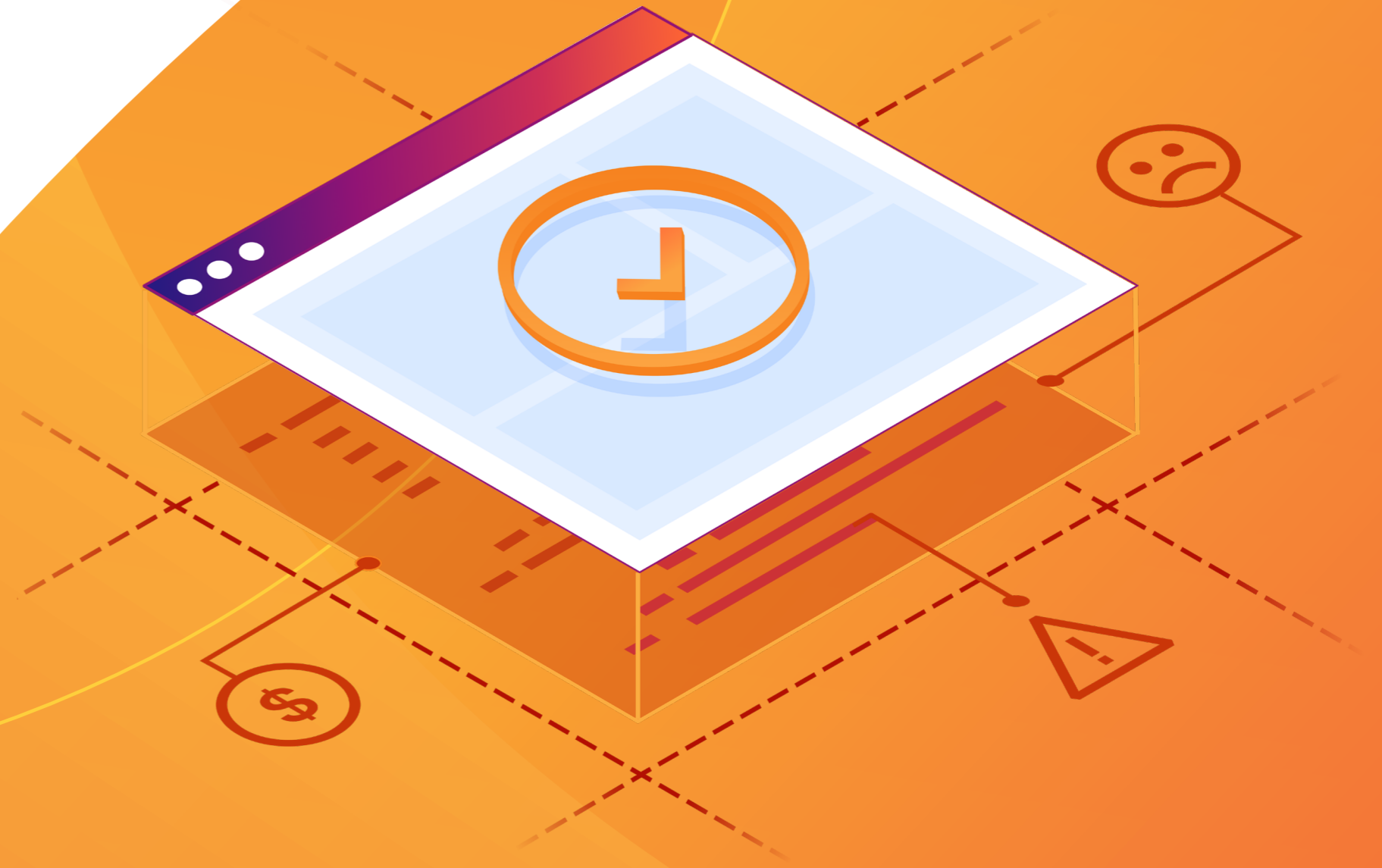


Table of Contents


[Table of contents](#) >

| | | | |
|----------|--|-----------|---|
| 3 | Compliance today | 8 | 4 must have's for streamlined compliance |
| 4 | The top 3 challenges to compliance | 9 | A new approach: The results |
| 5 | What's needed to tackle challenges? | 10 | Customer Testimonial |
| 6 | A new approach | 11 | Summary |
| 7 | A new approach: How it works | | |

Compliance today: Fewer resources, evolving regulations

From HIPAA for US healthcare organizations to the GDPR for any organization doing business in the EU or with its citizens, data compliance - or, the process that ensures organizations meet legal, regulatory, and operational data requirements - is critical.

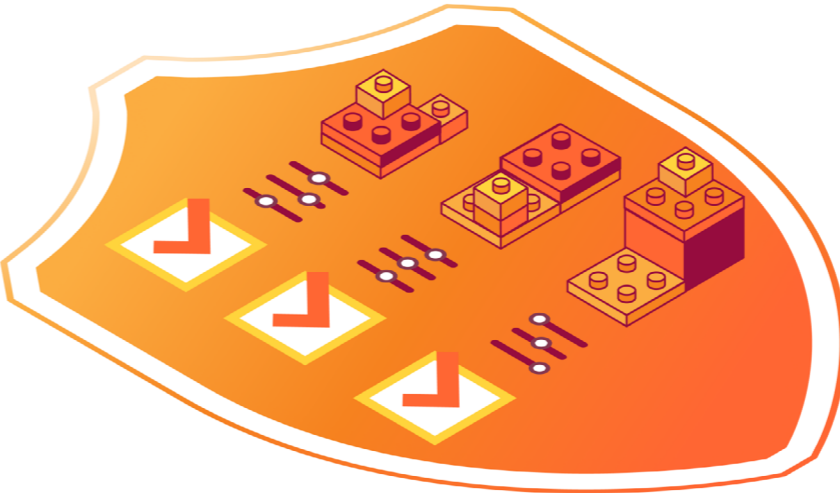
Yet in many cases, compliance leaders have fewer resources than ever, facing:



Smaller budgets **Reduced headcounts** **Rising costs**

Compliance teams aim to ensure their organizations meet the requirements of table stakes regulatory frameworks like the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and more. But today, they are doing so in a digital environment in which IT teams have lost control.

Digital modernization, the rise of remote and hybrid work, AI experimentation, result in a larger attack surface leaving IT leaders struggling to keep up . Meanwhile, legacy compliance solutions and approaches are being strained to the breaking point.



53%
of organizations say technical privacy roles are understaffed

The top 3 compliance challenges of existing security approaches

As their digital environments have changed, security and compliance leaders have been forced to cobble together a combination of legacy tools and point solutions, supplemented by manual processes to combine disparate tracking and auditing systems. But this approach leads them straight up against these three challenges:



1. Runaway costs

Compliance teams must pay for and maintain multiple siloed tools (which may or may not integrate) for data security, sovereignty, and privacy, driving up costs.



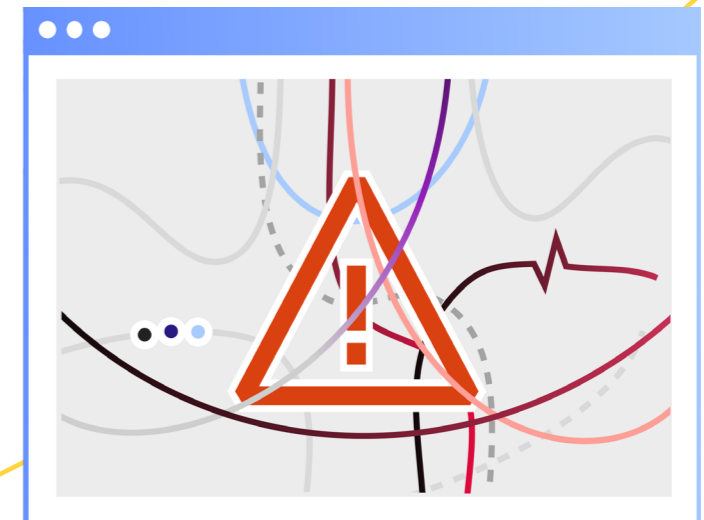
2. High risk

With so many disparate toolsets, manual processes are required to combine logs in order to meet auditing requirements. This slows down processes, results in errors, and wastes significant time and effort.



3. Poor user experience

Legacy on-premises security solutions create network bottlenecks that slow down app performance. This problem is intensified by data localization constraints.



What capabilities are needed to tackle these compliance challenges?



1. Write streamlined rules from a single control plane acting as a unified policy engine that provides consistent data protection and security policies across on-premises, cloud and web environments.



3. Localize data for regional compliance needs without performance challenges. Ensure your data localization needs do not disrupt your business agility with a network that can support localization requirements.



2. Apply, configure and extend consistent controls across locations, users, apps, (web, SaaS and private) and infrastructure — wherever you need. Meet regulatory concerns as soon as they are set with extendable controls.



4. Achieve successful audits with security efficacy, data visibility, analytics and reporting across your network and multi-cloud environments with a consistent set of detection and prevention policies to ensure control over data between source and destination to help adhere to compliance requirements.

A new approach: Streamlined compliance via a connectivity cloud

A connectivity cloud is a new model for securely connecting users, data, infrastructure, and apps no matter where they are located. This model not only gives organizations back control over their networks and security, it also addresses the major challenges faced by security and compliance teams.

✓ 1. Reduce Total Cost of Ownership (TCO)

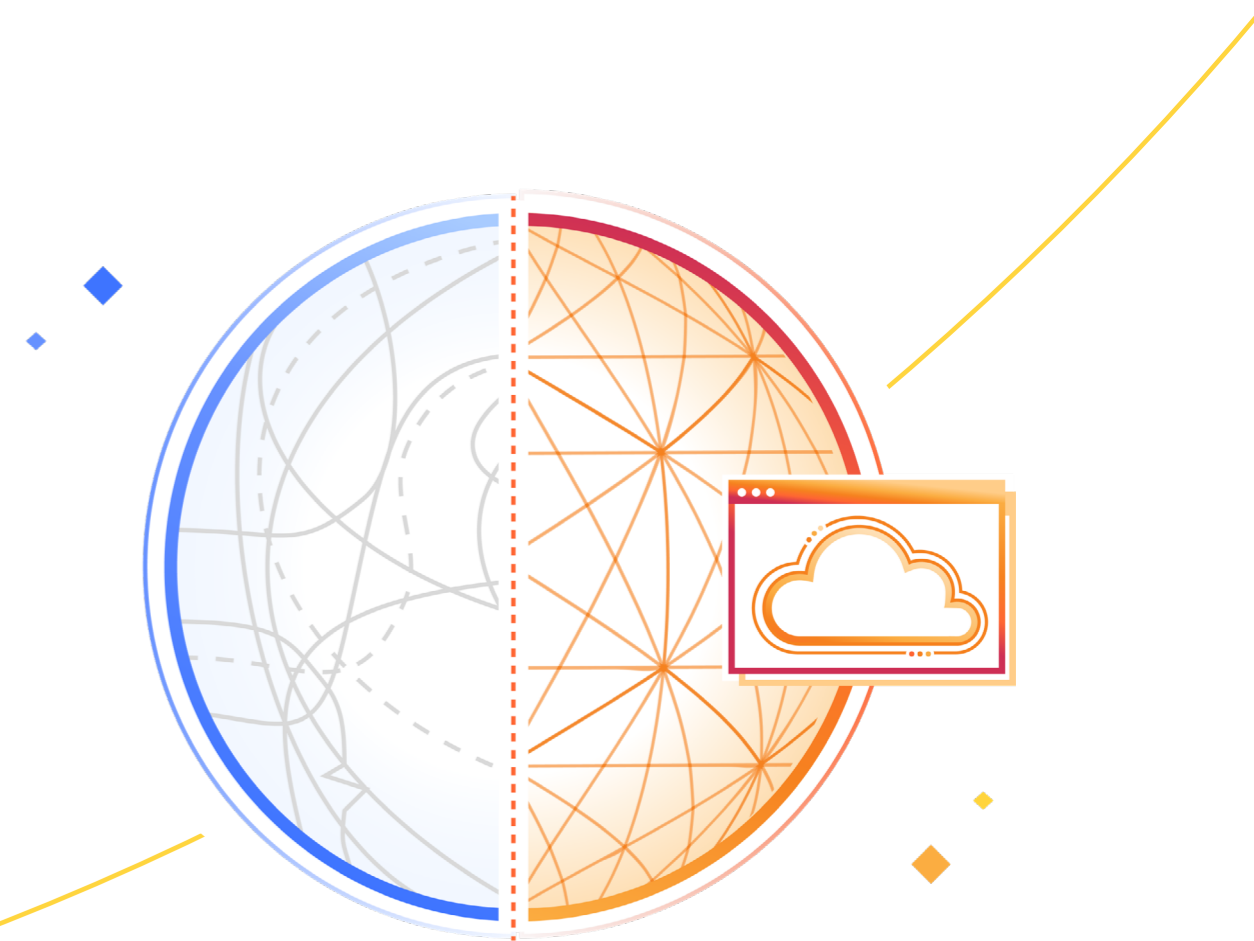
A connectivity cloud integrates all services in one platform that scales on-demand.

✓ 2. Mitigate risk

A connectivity cloud offers composable controls for authentication, security, networking, and logging, all in a single dashboard.

✓ 3. Improve user experience

A connectivity cloud is location-agnostic and can efficiently connect users no matter where they are in the world.

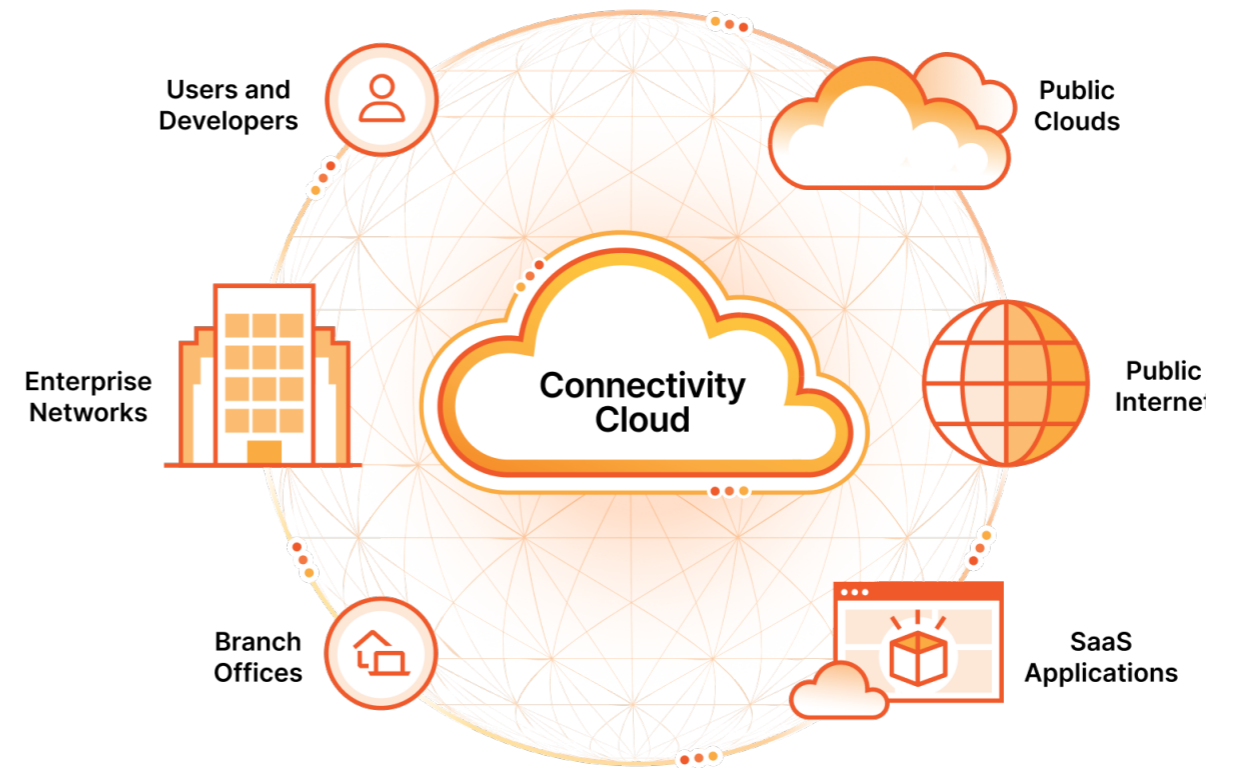
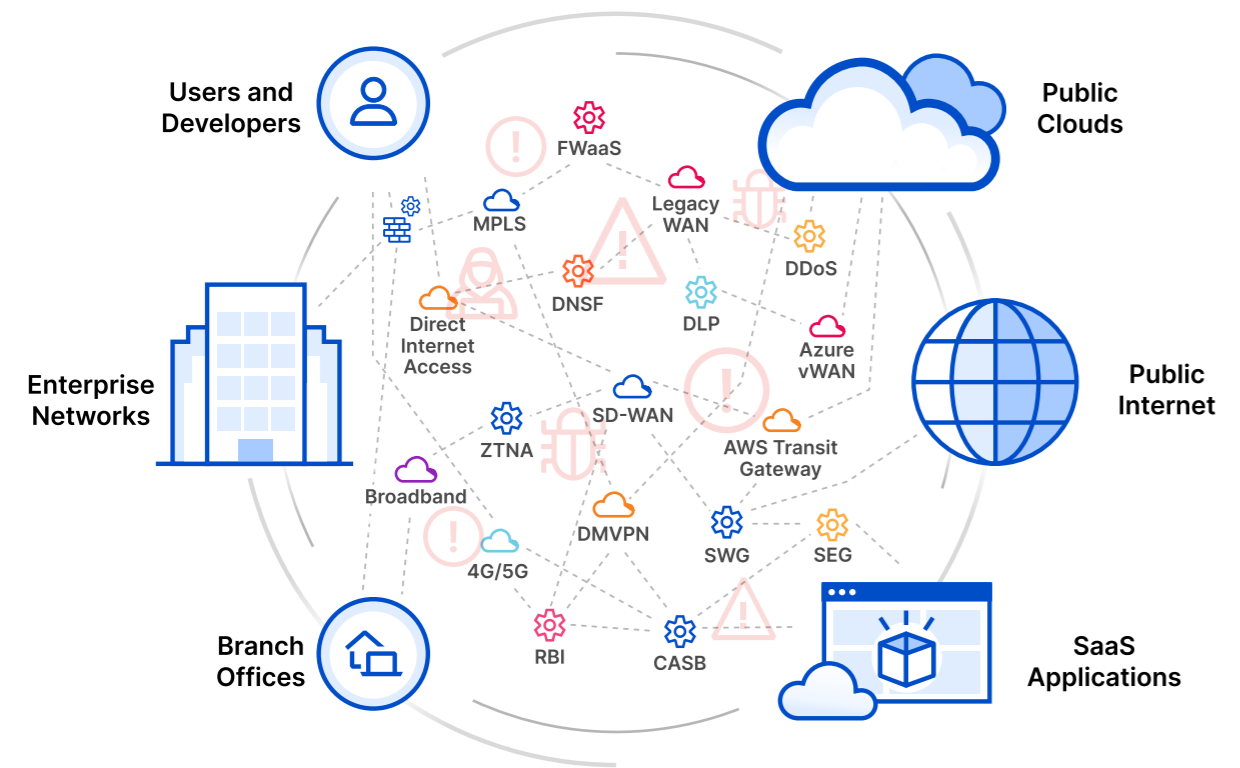


A new approach: How it works

The cloud, SaaS, Internet, and on-premises domains are intrinsically different and disconnected. Visibility and control have become harder, and the tools used to tame the complexity just add more complexity. A connectivity cloud bridges siloes instead of creating more, moving an organization...

From this:

To this:



4 must have's for streamlined compliance

1. Architected for data compliance:

Cloudflare has the largest and strongest network out of any connectivity cloud provider, with locations in hundreds of global cities. This enables compliance teams to apply, configure, and extend consistent controls across locations, users, apps, and infrastructure all over the world.



2. Unified policy engine:

The Cloudflare network has the same services available in all locations. Compliance teams can write rules once from a single control plane acting as a unified policy engine, and apply them everywhere.



3. Data sovereignty and localization without slowing performance:

Cloudflare is built to allow for data localization. Send all traffic to the nearest data center for optimum performance; meanwhile, logs are sent securely over a private network backbone to any selected region.



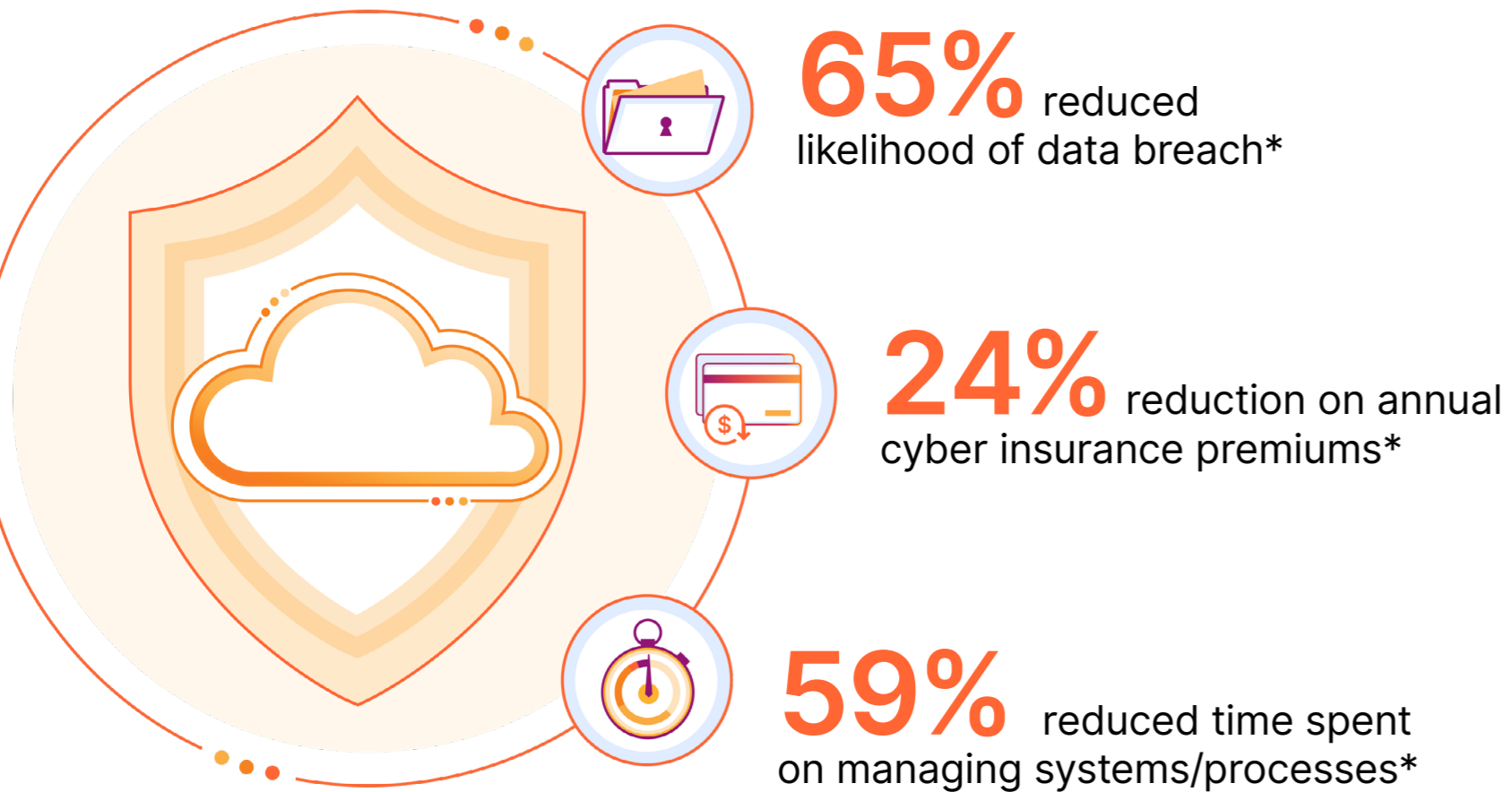
4. Satisfy audits with intelligent reporting:

Cloudflare's reporting provides detailed audit trails. Cloudflare's massive scale enables visibility into the latest threats from all over the Internet, allowing for intelligent automated detection of new attacks.



A new approach: The Results

The Cloudflare connectivity cloud streamlines compliance while minimizing risk:



The result: a simpler, customizable approach to compliance, managed from a single dashboard.

In addition, compliance leaders can rest assured that data on the Cloudflare network is secure. Cloudflare natively meets compliance requirements for:

- [PCI](#)
- GDPR
- SOC 2 Type II
- FedRAMP

For a complete list see: cloudflare.com/trust-hub

* 65% stat: IBM Cost of Breach 2022 report

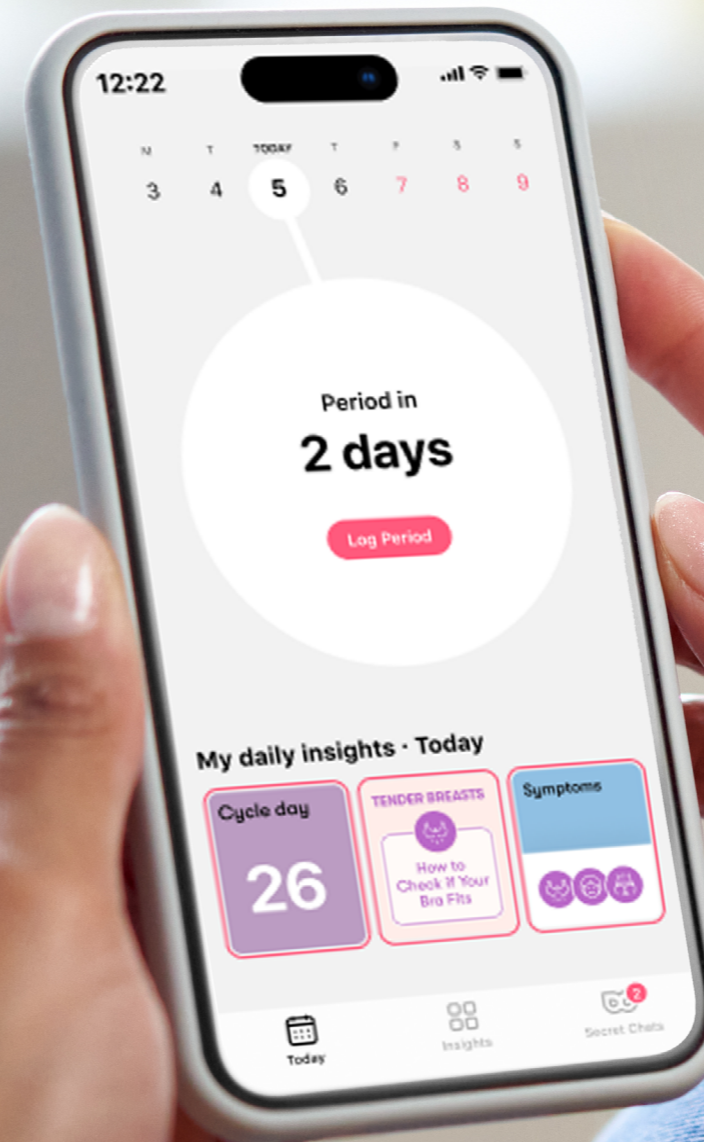
* 24% stat: 2023 Cloudflare TechValidate Survey of Cloudflare App Service Customers.

* 59% stat: 2023 Cloudflare TechValidate Survey of Cloudflare App Service Customers.



“At Flo, we firmly believe that every woman deserves the right to track their health without concern... and thanks to Cloudflare’s suite of products, we are able to offer a deeper level of protection for our users’ data.”

—Roman Bugaev, Chief Technology Officer, [Flo Health](#)

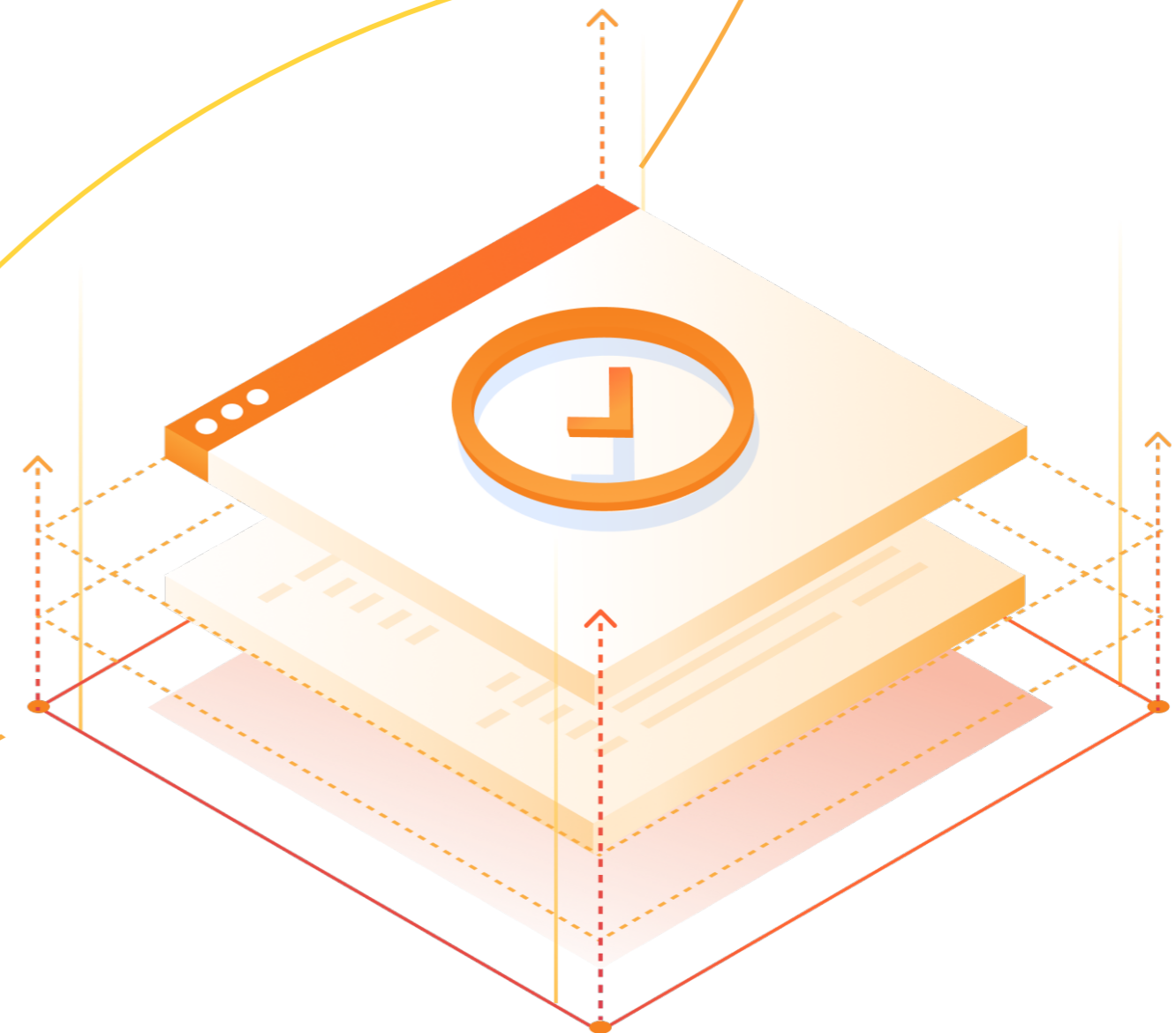


Summary

Compliance leaders need a new approach to overcome today's challenges for meeting regulatory requirements.

Legacy security solutions for regulatory compliance are expensive, inefficient, and slow. The use of a complete platform designed for compliance no matter where data is located — a connectivity cloud — can help compliance leaders overcome and eliminate these challenges.

The Cloudflare connectivity cloud helps organizations streamline compliance with composable controls for enforcing policies and localizing data. Cloudflare allows compliance teams to address data compliance without slowing innovation or performance while reducing total cost of ownership (TCO).





Learn more

**about how to use the connectivity cloud
to meet your data compliance needs**

© 2024 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.

Call: 1 888 99 FLARE
Email: enterprise@cloudflare.com
Visit: cloudflare.com