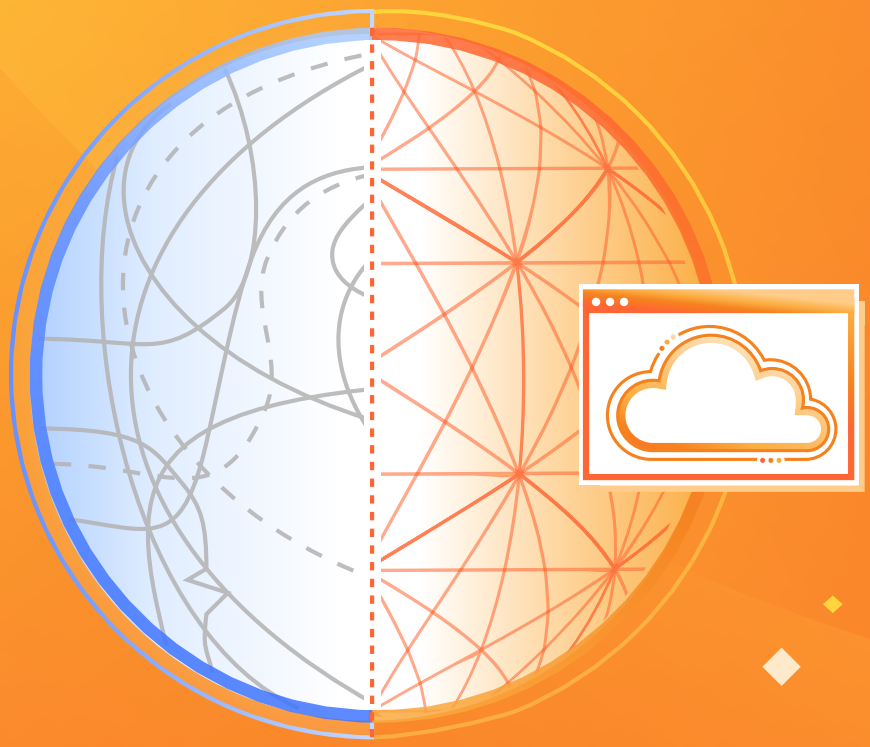
CLOUDFLARE

WHITEPAPER

Developing a strategy for your network modernization



Content

Legacy networking: A hurdle for digital modernization

Agility is crucial to excel in a world where business conditions can turn on a dime. But agility is not simply a matter of leadership and decision making. Agility also depends on organization capability to execute change. Systems must be established in a manner to flex and adapt without breaking down. The business must be able to realign to accommodate new revenue models, support new applications, and connect people around the world.

Agility is one of the primary desired outcomes for digital modernization projects, as organizations retool for competitive advantage. This is especially true when considering the state of the traditional enterprise network, which plays a critical role in delivering communications and enabling collaboration. The enterprise network has remained stubbornly resistant to change, and for good reason. It was designed to withstand shocks to the system, and change comes at great cost and effort.

Sometimes changes can be anticipated, because they happen over time, such as the effects of the cloud on the data center. With networking, exogenous market forces are driving rapid, sometimes overnight change. For example, the pandemic delivered painful lessons on just how difficult it was for some companies to rapidly add capacity for remote work, to maintain employee productivity, and to manage costs in light of how much budget was being consumed by idle networking in empty offices.

Throughout these hardships, it also became apparent that some companies were not only able to adapt, but also thrive. It wasn't solely a matter of management's ability to deliver the right business decisions, but also the capabilities of the business to transform and execute. For the CIO, it is necessary to develop strategies to deal with change, retool to support future needs in and make IT the accelerant rather than the retardant for change.

With massive investments in on-prem networking, modernization is no simple decision. To fully realize the benefits of network modernization, it's necessary to examine what must be achieved in order to define what must change.

Understanding the journey

When you consider the best practices for network design over the years, it's for good reason why so much complexity exists. For decades, organizations built out and fortified their networks, with layers upon layers of new technology. With every generation of network design, and every new innovation, the network became more complicated. The opportunity for seeking simplicity was not available, and often the addition of new technology made speed, resilience and security even more complicated.

With cloud-delivered networking and security services, we are now at the forefront of the next generational change in enterprise network design. By using cloud-delivered services as an extension of the network, organizations can tackle new use cases, extend their coverage and secure applications far beyond the data center. It represents an opportunity to greatly simplify the network, because service delivery builds upon the existing network connection to the cloud provider's PoP, without breaking the connection to insert yet another appliance. The networking between the on-prem network and the cloud service remains the same, while services within the cloud service are inserted and consumed.

The problem is that not every cloud-delivered networking and security platform is built the same, and it's not always easy to see what makes one different from the other. Many have limited upside in the modernization journey. In order to understand the differences, it's necessary to map out your goals for network modernization in order to avoid replacing one source of complexity with another.

Four key network traffic paths

When evaluating the scope of your network modernization project, consider that your network covers an extensive number of touchpoints, some of which intersects the same infrastructure (for example traffic passes inbound, outbound and east-west through your core network), and some of which operates outside of it (such as your public cloud networking).

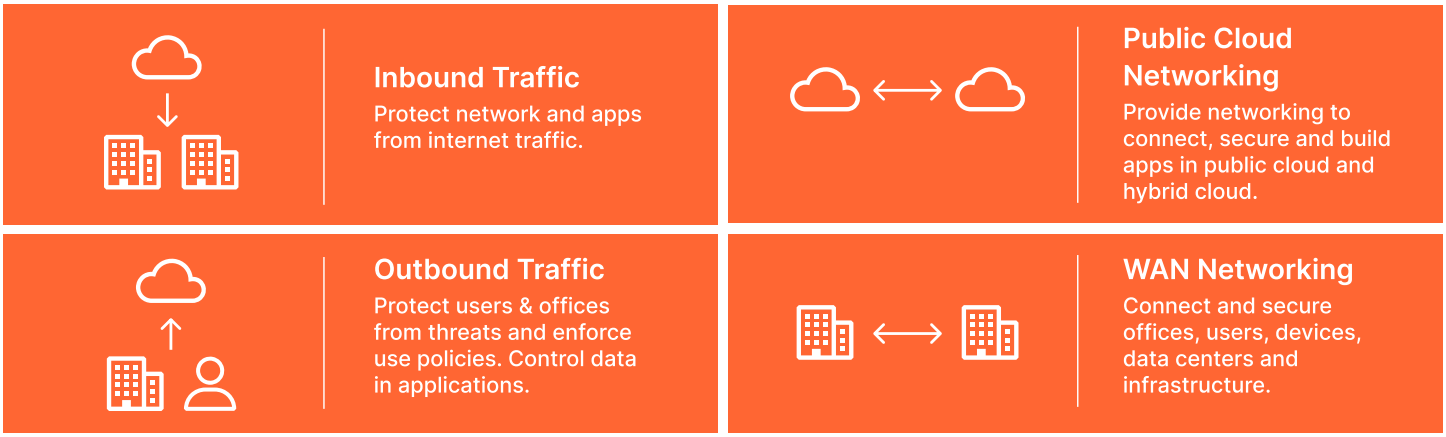
Inbound Traffic: Given that portions of the network are Internet exposed, it is necessary to maintain inbound defenses to deliver protection against attempts to incapacitate or exploit the business, while still allowing traffic from legitimate users through. Traditional perimeter defenses can be overwhelmed and require capabilities to deal with distributed denials of service.

Outbound Traffic: Connections to internet and cloud-based applications require policies that provide guardrails for safe business use such as protection against threats and data exfiltration. Given the variability in a user's location, organizations have implemented a mix of outbound protection technologies which include on-prem appliances such as firewalls (for when the user is on network), DNS resolvers as well as cloud-based proxies such as SWG and CASB (for when the user is remote).

WAN Networking: The WAN, as well as the boundaries it covers including the campus and branch, are being redesigned to support cloud-first initiatives and IoT-enabled devices. As such, the traditional network topology is undoing the backhaul to the data center in favor of direct-to-internet architectures. With the rapid advancements in networking in these areas, the insertion of security has conversely become more complex. In many cases, the internal traffic paths remain dependent on edge-deployed security appliances, impeding the organization's transformational progress.

Public cloud networking: As organizations build out their applications across multiple clouds, it becomes increasingly difficult to establish and maintain networking and security configurations on a point to point basis. Setting up and managing the networking consumes time and resources — time that's better spent on project development.

Each of these traffic paths have a number of technologies that organizations implement within their network or consume from the cloud. Given that modernization projects touch traffic paths in multiple directions, it's necessary to plan for the full network modernization journey across all four directions in order to avoid making an architectural mistake that limits the attainable transformational benefits or requires multiple disparate technologies to tackle unaddressed use cases.

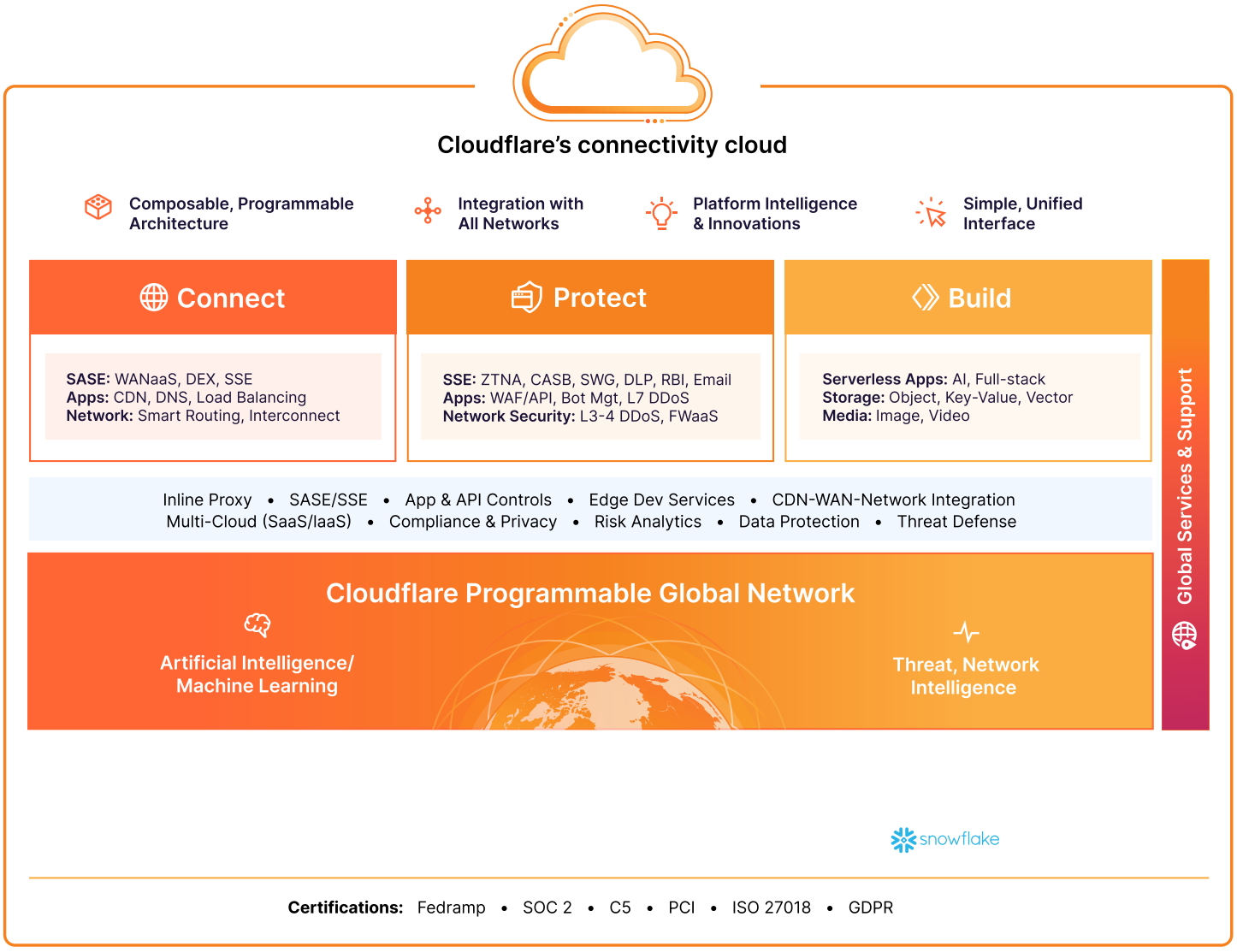


Cloudflare's connectivity cloud

Consider Cloudflare's connectivity cloud for your network modernization. It is built upon a philosophy of using a composable, programmable architecture to provide networking and security services to your users and across your cloud-enabled business infrastructure and applications. As a result, it addresses both current and future needs in your modernization journey.

With Cloudflare, you can add functionality and support new use cases by enabling services rather than inserting appliances. The connection to a Cloudflare Anycast data center remains the same, while you configure and deploy services from the unified management interface to process traffic. You can address current needs while putting the platform in place to support your future use cases and support your entire network modernization journey.

Instead of building out global infrastructure, use ours. Your organization benefits from the lightning-fast speed delivered through the Cloudflare global network. With direct connections to nearly every service provider and cloud provider, the Cloudflare network can reach 95% of the world's Internet population within approximately 50 ms.



Key use cases for network modernization

To get started, start with use cases that deliver business impact and the most meaningful benefit to your organization. These use cases are not prescribed in a particular order, as your priorities are unique to your business. What's important is to tackle near term needs while also building upon an architecture that will support your network modernization journey, no matter what path you may take.

	Modernization Projects
Branch Connectivity Reduce cost, improve the user experience	• Transition from MPLS to connectivity cloud • Transition from SD-WAN to connectivity cloud
Protect your public-facing infrastructure Extend lifetime of FW, DMZ investments	• Reduce load on network firewalls • Shift DMZ security to connectivity cloud
Simplify your corporate network Implement Zero Trust for better security and lower capital expenses	• Reduce / Eliminate the DMZ • Replace the VPN with ZTNA • Eliminate elevated trust on the LAN • Accelerate connectivity for M&A
Connect and secure your clouds Use the best of every cloud in your apps	• Build and secure apps • Leverage developer services to centralize core functions

Branch connectivity

A major component of WAN networking is to link the smaller sites, such as branch offices or stores, which depend on connecting users and devices to applications. Traditional hub & spoke architectures linked sites to the data center using expensive MPLS circuits, but with the growing need to support cloud applications, more organizations are using direct-to-internet architectures with broadband.

SD-WAN sought to make network connectivity more reliable but has an imperfect relationship with security insertion. Most SD-WAN architectures rely on heavy edge appliances and local firewalls to enforce security policy over the SD-WAN fabric and only use SSE/SASE integration for outbound traffic.

Use Cloudflare's connectivity cloud for branch connectivity and support your full migration path, whether augment or replacing legacy services. Cloudflare uses an architecture based on a 'light edge / heavy cloud' philosophy to deliver networking and security services. Facilitate site-to-site connectivity across network locations — branch offices, retail locations, or factory floors — with Cloudflare Magic WAN. It provides secure, performant connectivity and routing for your entire corporate networking, reducing cost and operation complexity. For security, Cloudflare Magic Firewall deploys seamlessly together with Magic WAN, enabling you to enforce network control policies whether North/South or East/West as traffic transits through Cloudflare's network.

Protect your public facing infrastructure

The enterprise network and the DMZ are addressable and exposed to the Internet, and require measures to stop attackers from causing harm. In a perfect world, traditional network firewalls could inspect and drop all unwanted traffic, but every firewall has finite capacities (available bandwidth, utilization / compute, session counts, etc). It's simply a matter of scale for the attacker to succeed, namely if the attacker can generate enough noise to overwhelm the company's ability to operate across different network protocol layers.

It's not just traffic volume. Accepting inbound traffic opens the attack surface to unauthenticated / pre-authenticated traffic. Flaws in applications and operating systems can be exploited by an attacker that does not even have an account on the system. Credential stuffing, the use of plugging in known username/passwords from other breaches, also poses a major source of risk. By applying Zero Trust principles to applications in the DMZ, organizations can reduce exposure to the Internet, and eliminate it when possible.

Organizations can improve their network protection by applying defense-in-depth principles to absorb malicious traffic upstream from the organization's public-facing infrastructure. Cloudflare Magic Transit with built-in Magic Firewall, deployed through the Cloudflare Anycast network, acts as the front door to the organization, filtering out malicious and unnecessary traffic and delivering only clean inbound traffic.

When network firewalls perform DDoS mitigation on an appliance, it still has to process the connection before it can drop it. With Cloudflare, our network broadcasts the customer's prefix, thus drawing the traffic that would otherwise be destined for the perimeter firewall. By virtue of Anycast, we are effectively absorbing the DDoS attack by distributing load across all of our data centers. Members of the botnet see the closest Anycast PoP, which processes the traffic in accordance with Magic Transit and Magic Firewall policies.

Simplify your corporate network

Simplification drives a number of modernization benefits. IT teams can make the network more reliable if their design had fewer components to break, and more secure by taking a Zero Trust deny-all approach towards access privileges.

To simplify your network, consider:

Migrating from the DMZ

Network DMZs are an operational headache as they are particularly sensitive to zero day exploitation. It doesn't require internal network access for an attacker to communicate with the servers in the DMZ, and thus organizations have to remain vigilant to prevent exploitation and abuse.

However, while DMZs played an important role in the past, are they needed today? The DMZ as a network construct is diminishing in importance, because there are alternative ways to build and host applications.

- For public facing apps, there are economic and technical benefits to move workloads to the public cloud.
- With SaaS, many types of public-facing and private applications do not need to run on customer managed infrastructure at all.

As such, it's pragmatic from a security and a network design point of view to start thinking of how to reduce or eliminate the need for a DMZ. Not only does it make sense from an operational point of view, but it also greatly simplifies the architecture by eliminating the network infrastructure, such as the firewall, WAF, and load balancers that support it.

What about private apps that are placed in the DMZ to extend access to employees, partners, and contractors? It would be more secure to isolate them in a private network and extend access to employees and partners using Zero Trust Network Access (ZTNA).

With ZTNA, you effectively reduce the attack surface by eliminating inbound network traffic to the application. ZTNA uses contextual, brokered access to resources through Cloudflare's connectivity cloud, thus shutting down the need to open ports in the network firewall while providing the security team with full visibility on who has access to what resource.

Replacing VPN with ZTNA

The days of using VPNs to access applications are dwindling. It's impractical from a network design point of view to tether users over a very long tunnel to access the internet and cloud. It's also a major security risk to put users (and potentially compromised endpoints) on the network with a VPN.

Application access is also not the sole function of a VPN. There are scenarios where organizations need broader network connectivity with an endpoint, such as with endpoint administration and server-initiated communications. These use cases traditionally leverage the VPN's network connectivity in both directions, and stumped early ZTNA products on the market. Without an alternative, organizations ran ZTNA and VPN side by side.

To modernize the network infrastructure, organizations can consolidate the functions with ZTNA from Cloudflare. That's because with Cloudflare, organizations can support both classic ZTNA use cases along with server-initiated and bidirectional traffic. These functions help organizations collapse their application access needs by eliminating VPN, and furthers security improvements and simplicity.

Eliminating elevated trust on the LAN

With hybrid work, there are fewer and fewer differences between the way one works while at the office compared to any other location. In fact, this is especially true when users are frequently working on public untrusted networks found in coffee shops and shared workspaces.

In some ways, the open public network is the embodiment of Zero Trust — nobody has privileged access and nobody or no thing is trustworthy. If it can work in principle in a shared workspace, the home office, and the coffee shop, why can't trust be eliminated within the enterprise network as well?

Eliminating trust does not require advancing the network design, but rather simplifies it. Instead of creating elevated access for authenticated users and using network policies to open connections to resources, it's far more secure to presume the entire network is untrustworthy. With the expression of security through SASE, organizations can get the access to the applications they need, with the appropriate security to make it safe, without requiring any presumption of trust on the network itself. Zero Trust isn't about adding trust to the network, it's removing it until we reach a better, more secure state without the explicit and excessive permissions from the past.

Accelerating connectivity for M&A activity

Organizations use M&As as a tool to acquire access to business resources and capabilities that were not otherwise immediately available. To capitalize upon the opportunity, organizations must execute quickly to make the combined company better than the sum of its parts. However, IT is not often capable of moving quickly, because the applications and underlying network infrastructure of two organizations rarely mesh together easily.

To accelerate connectivity for M&As, organizations can approach access to applications as a separate task from network integration. The timetable for designing a converged network architecture can stretch into years, but application access does not have to be dependent upon such a distant milestone.

That's because the situation on day 1 is effectively a Zero Trust use case, where trusted users on untrusted networks still need access to applications. Extend access using Cloudflare One, which provides the means to enable connectivity for M&As without being conditional on converged network access.

Connect and secure your clouds

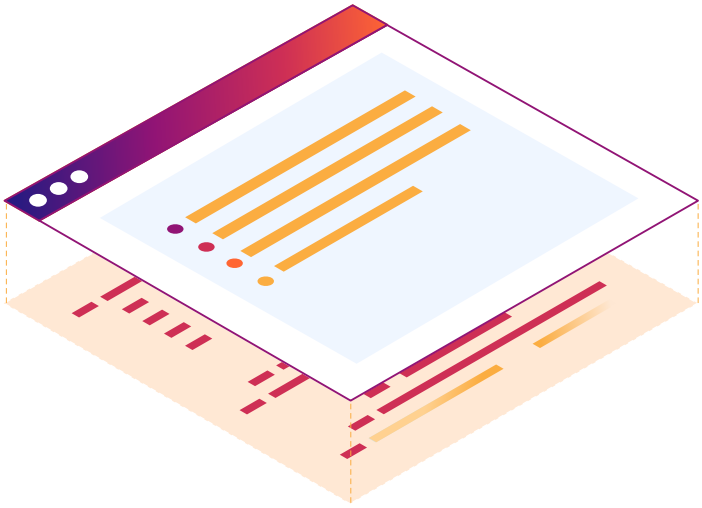
As cloud development evolves, the components in one cloud will be beneficial for being repurposed within another. Just as every organization will become multi-cloud over time, every organization will need to manage public cloud networking over time. Application development tends to be tribal in nature, with DevOps in different parts of the organization preferring the tools with which they are most familiar. Developing organizational capabilities to manage the connectivity across clouds, however, is complex as the work spans toolsets built upon entirely different frameworks.

Another aspect of multi-cloud complexity is the realm of hybrid cloud. Hybrid cloud mix on-prem private cloud with virtual private clouds. These networks are sometimes built with dedicated networking, like AWS Direct Connect, which can be costly and limited to only one cloud. As organizations build multi-cloud applications, they do not necessarily want to incur the costs of dedicated networking for each cloud.

Instead of building networking and security directly from one application to another, use Cloudflare to orchestrate and connect public cloud networking services. We believe that Cloudflare's connectivity cloud plays an ideal role in such an architecture, being ideally situated as a transit for traffic passing between clouds through the extensive Cloudflare network. With the addition of public cloud networking management capabilities, now customers can orchestrate the set up of workload connectivity through Cloudflare as well.

Our public cloud networking extends beyond just the orchestration of the underlying plumbing. Our architecture goes one step further by delivering developer services, which are available for building and integrating with multi cloud applications. The developer platform provides a rich ecosystem of foundational technology built on open source and open standards. You can choose to use all elements of the developer platform or only those you choose, without being constrained to the particular services in a given cloud.

Next steps



To take the next steps in your network modernization journey, contact Cloudflare and let us help you develop a strategy. We have worked closely with thousands of customers as they transitioned their architecture to Cloudflare's connectivity cloud.

For more information,
visit http://www.cloudflare.com

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

REV:BDES-5483.2024JAN30