CLOUDFLARE

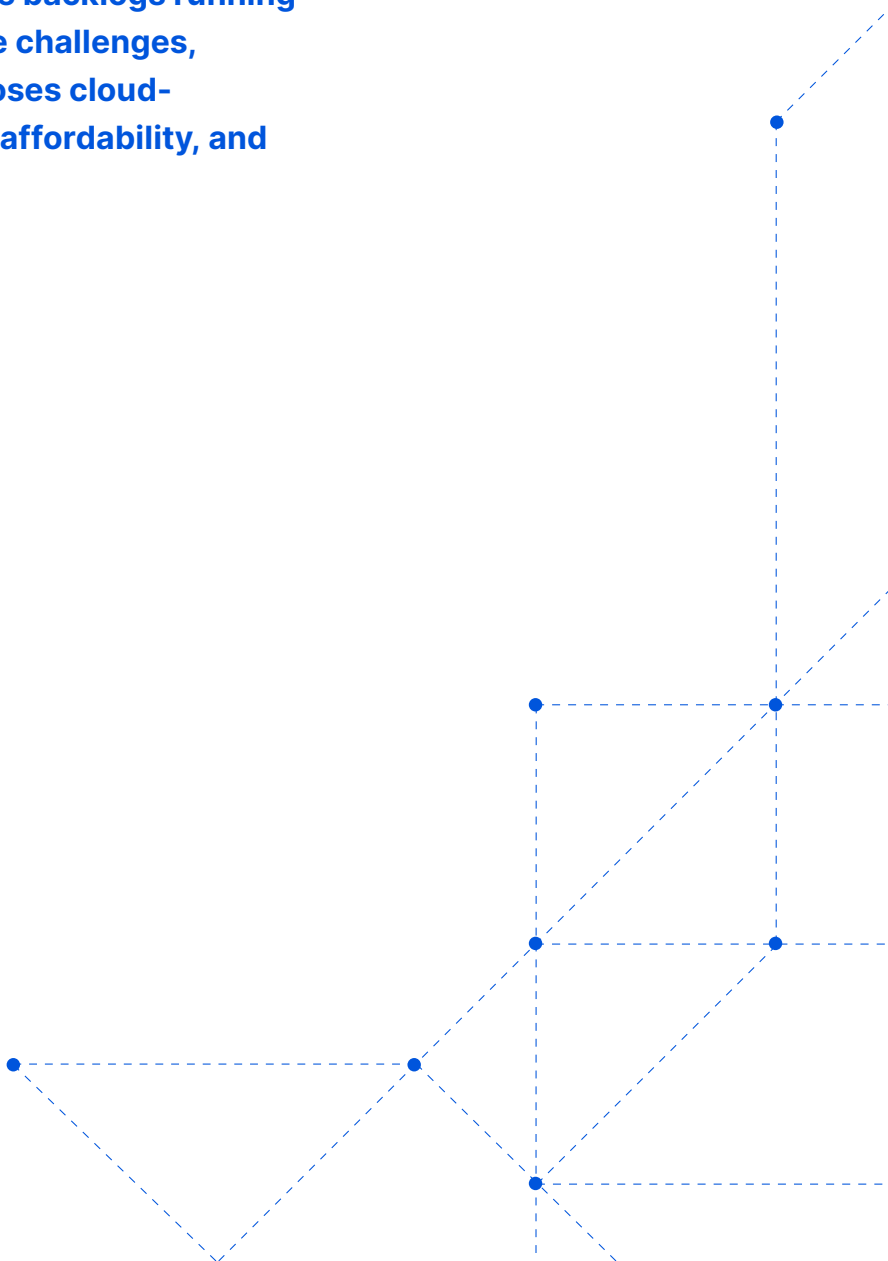
WHITEPAPER

The Death of Network Hardware Appliances

Why the time to break free from network hardware is now

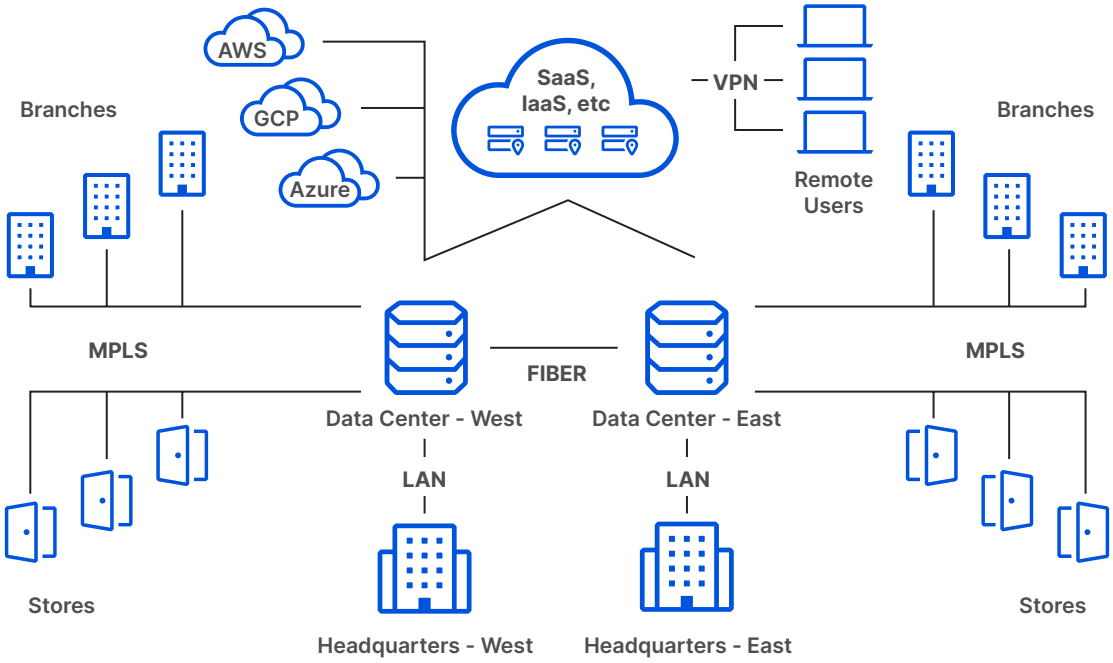
Executive Summary

While storage and compute have moved to the cloud, many networking functions remain on-premises, creating capacity limitations, high total cost of ownership, support challenges, and security gaps. Organizations are struggling to ensure adequate capacity and effective security with hybrid work becoming the norm. Many transformation projects have stalled because of hardware backlogs running well over a year. This paper outlines those challenges, quantifies their consequences, and proposes cloud-based solutions for improving the speed, affordability, and security of hybrid cloud infrastructure.



Introduction

Cloud migration has proven to be an effective strategy for reducing infrastructure costs, improving the availability of data and applications, and increasing operational agility. However, this migration rarely happens in one fell swoop. Many large organizations find themselves with a complex mixture of multi-cloud and on-premise infrastructure:



This type of hybrid infrastructure is not necessarily a bad thing, but it does introduce complications. Specifically, it creates situations where various networking functions — such DDoS mitigation, load balancing, firewall, and VPN — remain on-premise.

Legacy network hardware appliances aren't up to the task of securing and accelerating critical infrastructure in a cloud-focused world. They've always been a hassle — an expensive, often unruly, mess of equipment strung together with spider webs of cables. Once you add the cloud to the picture, security gaps, performance penalties, and additional support challenges quickly emerge.

This paper describes risks and pitfalls of maintaining network hardware in a world shifting to the cloud, and offers strategies for building a more secure and effective network.

The risks of hardware in a cloud world

Network hardware appliances span a variety of specific functions, and are used somewhat differently from organization to organization.

Common examples include:

Security

- DDoS protection
- Firewall
- Virtual private network
- Configurable policies

Performance & Reliability

- Load balancing
- Traffic acceleration/ WAN Optimization
- Packet filtering
- Traffic analytics

When this hardware is deployed on-premise, the resulting architecture generally suffers from five categories of risks: **supply chain strain, capacity limitations, high total cost of ownership, support challenges,** and **security gaps**.

The first three categories have always posed challenges to even the most sophisticated network and security teams. The other two are exacerbated by cloud migration.

Supply chain strain

Like any kind of physical product, networking hardware is vulnerable to a variety of supply chain difficulties. When material costs go up, certain materials and components are harder to obtain, or shipping providers become overburdened, networking hardware becomes more difficult to purchase and replace.

Unfortunately, such difficulties have been common of late, in large part due to the effects of the Covid-19 pandemic. According to Gartner Research, "Pre-pandemic, lead times of 4-6 weeks were common. Now, 200–300 days is common, and we've seen 430+ days quoted in writing to customers."

These delays stem from multiple factors:

- **Logistics difficulties:** Historical supply chain models have multiple points of failure, bare minimum workforces, and heavy reliance on technologies that may or may not be secure — challenges that have come home to roost recently. During the pandemic, many factories have shut down, shipping companies are experiencing delays, and many types of supply chain workers became harder to hire and retain. All of these challenges make it take longer to manufacture and deliver hardware. Perhaps the most challenging aspect to remember of any logistics is that it is comparable to a relay race - just because your individual organization may not be experiencing challenges doesn't mean that you won't be impacted by a broken link further up the chain.
- **Higher material costs:** Network hardware appliances rely on a variety of raw materials. Due to high demand and limited supply, prices of materials have skyrocketed, which means not only are businesses waiting longer to get what they need for their network, but they're also looking at paying significantly more for it. Unfortunately, due to these challenges, Gartner expects hardware appliance lead times to remain high through early 2023 (source).

All of these challenges have follow-on consequences. Continuing to focus on procuring, maintaining, and replacing hardware boxes means more overhead costs, more time spent on planning rather than executing, and added security concerns around securing a physical supply chain during uncertain times. Rather than focusing on logistics, lead times, procurement, and storage of hardware boxes - organizations could instead focus on meeting the needs of their customers.

Capacity limitations

It should be no surprise that by their very nature, network hardware appliances can become overburdened during unexpected traffic surges — whether that traffic is legitimate or not. But several recent trends mean reaching those limits is a more common concern.

Consider Distributed Denial of Service (DDoS) mitigation. The largest DDoS attack in history took place in November of 2021, according to Microsoft, and is claimed to have reached a maximum volume of 3.47 Tbps (source). DDoS attacks would overburden many times over the most advanced DDoS mitigation hardware boxes on the market, which typically provide a fraction of the capacity required to mitigate such attacks.

In November of 2021, the largest DDoS attack in history is claimed to have reached a maximum volume of 3.47 Tbps.

Not all organizations will attract attacks of such scale — but not all organizations can or do implement the most advanced DDoS mitigation hardware, either. A Cloudflare report found that volumetric attacks increased in 2022 Q1. In fact, attacks above 10 Mpps (million packets per second) grew by over 300% QoQ, and attacks over 100 Gbps grew by 645% QoQ (source). Not only is the sharp increase in DDoS attacks alarming, but these types of attacks would overburden many purportedly high-capacity hardware-based mitigation solutions.

Furthermore, attack volume does not take into account legitimate traffic that might reach your data center at the same time.

Should a smaller attack arrive during a high-traffic period — such as the Black Friday shopping weekend, when ecommerce daily pageviews double overnight, on average (source) — the resulting traffic surge still might be enough to push security hardware past its breaking point.

DDoS mitigation is just one example of on-premise hardware's capacity limitations.

Other examples include:

Load balancers: Individual on-premise load balancers can easily be overburdened by sudden spikes in legitimate traffic. When this happens, it can take a long time to provision and install additional hardware. The alternative is maintaining enough capacity for the worst-case scenario, but this approach requires the organization to continually run a lot of hardware at a high cost.

Virtual Private Networks (VPNs): VPN usage has become much harder to predict in advance. For many organizations, fully remote and hybrid work is the new normal, but the traditional VPN approach requires careful planning, maintenance and management, since many VPNs were not designed for continuous use by an entire organization. When too many employees use a VPN, connectivity and reliability suffer. In addition, security issues can emerge, just by nature of how VPNs were designed without any Zero Trust controls. Furthermore, if a VPN becomes overburdened, organizations may "split-tunnel" traffic so that web-bound traffic does not go through the VPN — which makes it hard to track and manage employee web activity.

When faced with these problems, one response is to buy more, newer, higher-capacity hardware. But such an approach introduces a host of other problems.

Costs of ownership

As with capacity limitations, it should come as no surprise that data center hardware is expensive. For example, the hardware required to attain approximately 100 Gbps of DDoS mitigation capacity might cost between $400,000 and $500,000 up front.

What's more, these costs are just one part of a hardware appliances' total cost of ownership.

Consider the following expenses:

- Team costs: Purchasing, operating, and maintaining hardware to defend against threats at every layer of the OSI model — and to provide the level of performance and reliability expected from modern websites and Internet applications — requires team members who are experts in every one of those networking functions. Building a team with this breadth and depth of expertise is an expensive proposition - especially during one of the tightest labor markets the world has ever seen. A 2022 ISACA survey found that out of 2,000 cybersecurity professionals that participated in the annual survey, 63% have unfilled cybersecurity positions – up 8% from the previous year (source).
- Maintenance costs: The average on-premise piece of network hardware only has a 3 to 5 year shelf-life, yet warranties for those entire periods often require extra expenditure. When you take into account the pace of technology innovation, it is inevitable that these on-premise boxes will only continue to shorten in lifespan. The alternative is unexpected — and thus unbudgeted — repairs from the original manufacturer or a third party. Hardware malfunctions can also cause data center downtime, which has an average opportunity cost of over $8,800 per minute (source).
- Replacement costs: Replacing a hardware appliance every three years requires organizations not only to repay their initial investment, but to dedicate resources to shipping and installing new hardware. Delaying these replacements often results in more frequent malfunctions — and thus additional maintenance costs.

Contrast this model with cloud-delivered networking services. They are possible to operate with a nimbler team, do not impose maintenance and shipping costs, and do not force organizations to choose between costly upgrades and an increase in malfunctions.

Hardware malfunctions can cause data center downtime, which has an average opportunity cost of over $8,800 per minute.

Support challenges

Supporting network hardware appliances is not just an expensive proposition, but also a logistical challenge. Hardware requires frequent patching in order to keep up with the latest vulnerabilities and attack tactics — a process that often relies on manual implementation, and is thus susceptible to human error.

The more hardware appliances an organization uses, the higher the chances it will eventually neglect a patch due to inattention or concerns about affecting vital systems. In a recent joint Cybersecurity Advisory, the National Security Agency (NSA), the Cybersecurity and Infrastructure Agency (CISA), and the Federal Bureau of Investigations (FBI) reported that 16 publicly known flaws in unpatched network devices have been exploited in widespread campaigns (source). The exploits impact various on-premises devices from small business routers to enterprise VPNs and potentially give the attackers the ability to manipulate network traffic and exfiltrate data out of the target networks.

Despite most of the 16 flaws listed being rated as critical, patching and remediation is no simple task. In fact, patching hardware can be so complex that an entire category of software exists to help companies keep up to date (source).

And the consequences of just one missed patch can be significant. Not only will the hardware remain vulnerable, but once a patch is released, the corresponding vulnerability becomes a higher-profile target for opportunistic attackers. Contrast this situation with cloud-based security services, in which fixing vulnerabilities and installing updates happens automatically by default, and can take as little as thirty seconds to propagate depending on the cloud provider's network speed.

Other maintenance challenges with hardware include:

- **Troubleshooting:** In a hardware-only scenario, troubleshooting often forces IT teams to go through the arduous process of unplugging load balancers, firewalls, and other on-premise appliances one at a time to discover where the problem lies.

  This process is further complicated by the concurrent use of cloud services. Hardware-reliant organizations often manage access to those services through the centralized data center and all of its individual appliances. When employees are unable to access a particular service, IT teams have an extra place to check in order to diagnose the issues. When you consider a recent report from Productiv showing that 56% of all SaaS applications fall under the category of Shadow IT – or unapproved and unmanaged applications procured without the knowledge of IT – this problem quickly grows in both scope and scale (source).
- **Physical maintenance:** When a hardware appliance does break, IT teams must physically unplug it, order a replacement, test the replacement, and re-install it — another arduous process. When considering the scale of many global enterprises, these appliances in need of attention could be halfway around the world.

Security gaps

Even if an organization had the resources required to continually provision and maintain the latest, highest-capacity on-premise hardware, the resulting infrastructure would still suffer from critical security deficiencies — especially in a world trending towards the cloud.

Consider employee access management. While VPN hardware can establish encrypted tunnels between remote employee devices and applications hosted in an internal data center, it cannot monitor and secure user activity after establishing this tunnel.

Should the employee's device become compromised by malware, or should a phishing attack compromise their VPN credentials, an attacker might be able to use that VPN access to access a wide variety of sensitive information. Both phishing and malware continue to pose serious risks and generate significant monetary gains for threat actors. In 2021, $6.9 billion was lost to cybercrime according to the FBI. Specifically, business email compromise (BEC) cost businesses $2.4 billion in losses (source).

Should the employee's device become compromised by malware, or should a phishing attack compromise their VPN credentials, an attacker might be able to use that VPN access to access a wide variety of sensitive information.

Cloud services and SaaS applications further complicate security for hardware-centric infrastructure. In a hybrid cloud model, for example, an organization operates a mixture of on-premise and cloud infrastructure. The organization cannot simply send security hardware to a cloud provider. If it wishes to continue using on-premise hardware for its own data center, different parts of its infrastructure will be protected in different ways, giving security teams less visibility into and control over incoming attacks.

Cloud-based services can overcome both of these challenges by unifying data centers and cloud services under a single software-defined layer.

A detailed explanation of this approach is beyond the scope of this paper — to learn more, explore the following articles:

- What is a Zero Trust network?
- What is Secure Access Service Edge?

Cloud-based security & performance services: Advantages & challenges

Delivering network services through the cloud avoids many of the problems associated with hardware: supply chain strain, capacity limitations, costs, support challenges, and security gaps.

- **Supply chain:** Many cloud-based networking providers are designed to scale with modern, global architectures, making supply chain issues less acute.
- **Capacity:** Due to the cloud's distributed nature and software-defined nature, organizations can provision additional capacity easily as their business scales.
- **Cost:** The add-on costs of hardware are either non-existent or easier to plan for in advance. What's more, cloud services are typically classified as operating expenditures, not capital expenditures, which offers tax and accounting benefits for many businesses.
- **Support:** Logistical and resource needs are handled by the service provider. In addition, there is no chance of missing a patch, since updates occur automatically.
- **Security:** Software-defined networking services can unify different infrastructure under a single protective layer.

However, cloud networking services present their own risks if not deployed thoughtfully:

Risk	Description
Latency	Some cloud-based network functions rely on specialized cloud-based data centers — e.g. scrubbing centers for DDoS mitigation. Backhauling traffic to those data centers can add significant latency depending on its location relative to the destination server. This problem compounds when an organization uses different providers for different networking functions. When traffic must hop from provider to provider, latency can be measured in hundreds of milliseconds.
Support	When an organization uses different providers for different functions, troubleshooting remains an issue. It can be hard to tell which provider is the cause of congestion or outages.
Costs	When an organization uses different providers for different functions, the time (and thus the money) required to manage them can still be high.

To avoid these problems, consider the following strategies:

- **Look for providers that work with both cloud and on-premise infrastructure.**
  This capability allows IT and security teams to set consistent controls and monitor global traffic from a single place. It also helps to build a more resilient architecture – one where your teams can quickly pivot in response to fluctuations in market conditions.
- **Look for cloud providers offering multiple networking functions that work together.**
  This often reduces the number of network hops traffic must make, resulting in reduced latency and therefore a better end user experience. Troubleshooting network problems is also easier when you have one company to call instead of many. Also, bundling multiple functions together often results in lower costs.
- **Look for cloud providers that can perform multiple networking functions from every location in their network.**
  Providers that expand their service portfolios by acquisition do not always integrate those new services fully, which means certain functions can only be delivered through certain data centers. Consider providers who offer these functions across the entirety of their network to avoid the same problems listed above.
- **Look for cloud providers with a broad global presence.**
  This capability supports the previous one, ensuring end users are always close to the network no matter where they are. It also creates a large network surface with which to absorb DDoS traffic and conduct other networking functions that require a large capacity.

How Cloudflare can help

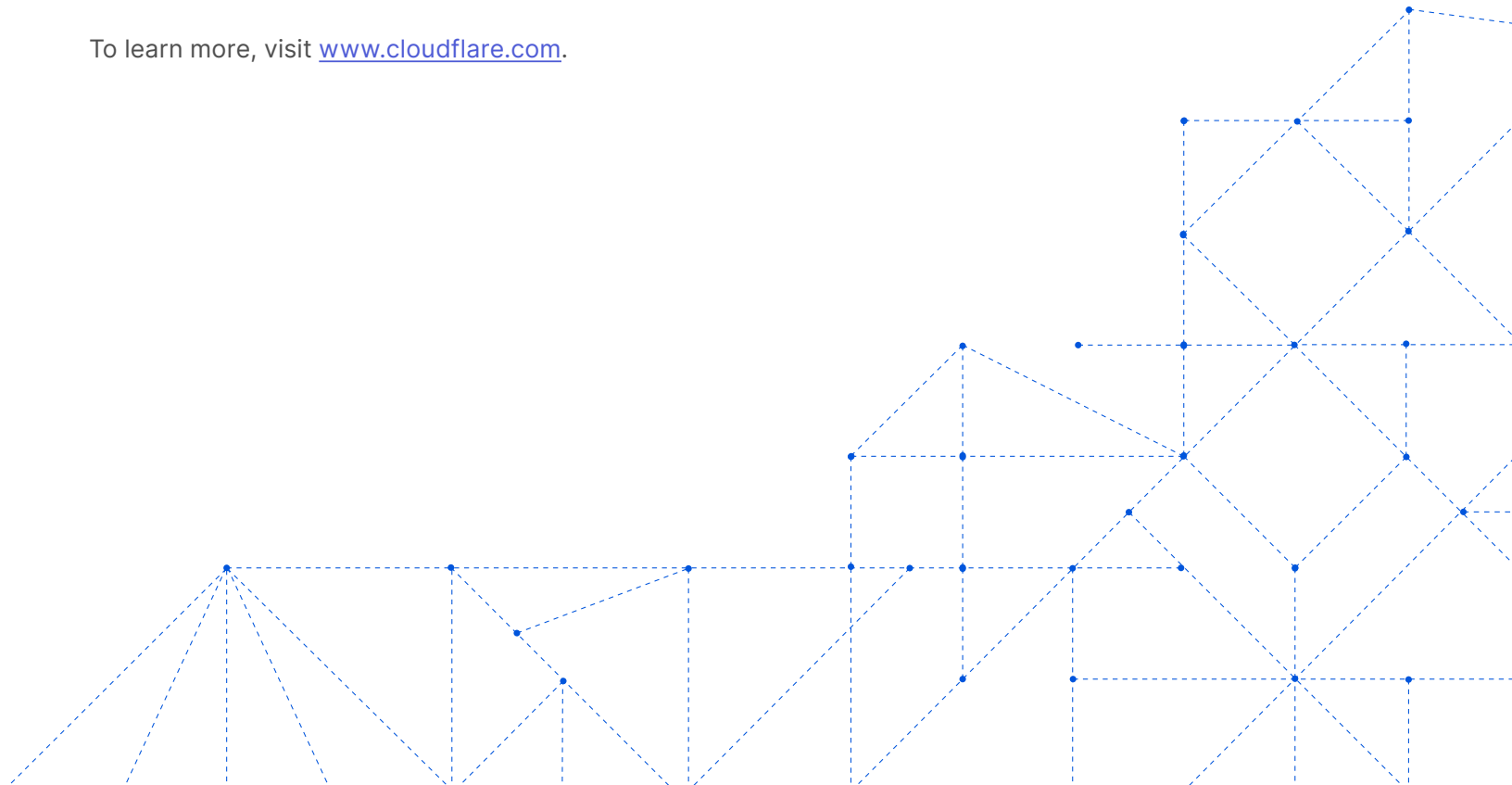
How can organizations accelerate their network transformation, without waiting on hardware to arrive and without sinking more money into boxes that will only last them a handful of years? With Cloudflare.

Cloudflare has built a global cloud platform that delivers a broad range of services — making organizations more secure, enhancing the performance of their applications, and eliminating the cost and complexity of managing individual network hardware. This platform serves as a scalable, easy-to-use, unified control plane to deliver security, performance, and reliability across on-premise, hybrid, cloud, and software-as-a-service (SaaS) applications.

Crucially, every data center in Cloudflare's 270+ city global network can deliver every one of these services, reducing the latency that can complicate cloud implementations. Streamline your network stack, accelerate transformation, and arm your network for what comes next.

To learn more, visit www.cloudflare.com.

> "Dropbox recently became a 'virtual first' organization. We've been exploring how this business strategy impacts our security approach and network architecture. We appreciate Cloudflare's support in helping us and other remote-first organizations like ours learn how to adapt to this 'new normal."
>
> Konstantin Sinichkin
> **Engineering Manager, Dropbox**



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

REV:BDES-3313.2022JUN10