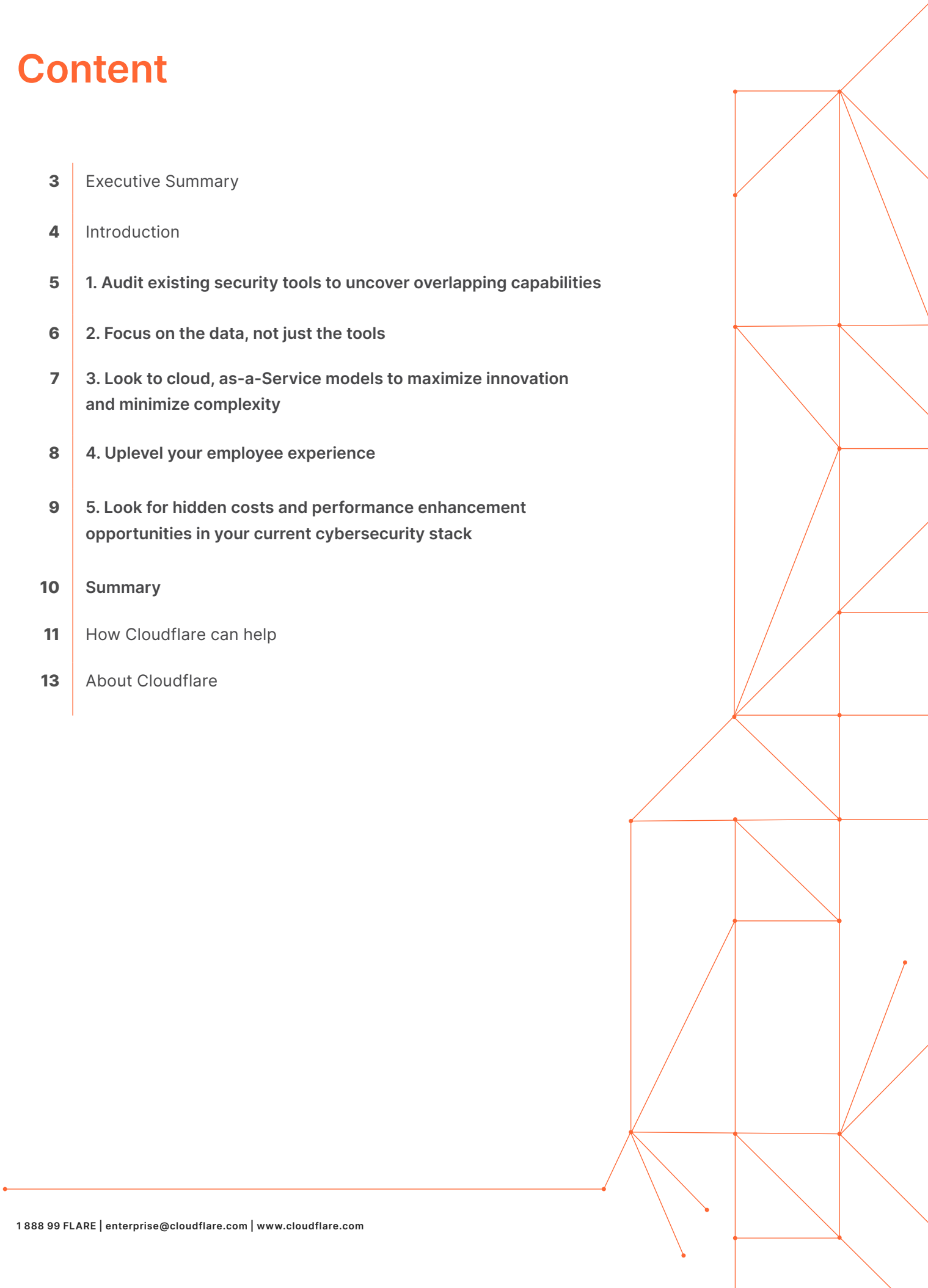
CLOUDFLARE

WHITEPAPER

Hope on the horizon: How to build a better cybersecurity posture during economic uncertainty

Content

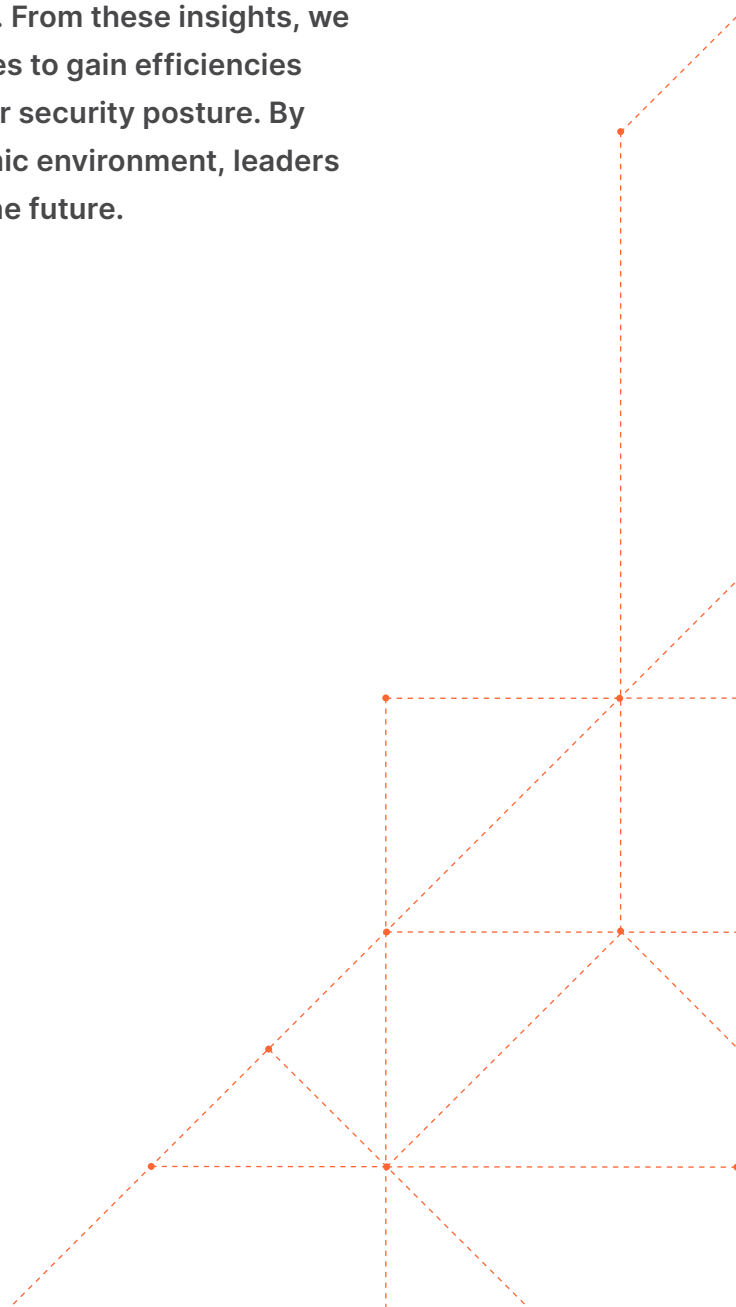


Executive Summary

Organizations are facing economic uncertainty as the outlook grows more unpredictable. This uncertainty — often exemplified by shrinking budgets — puts pressure on CIOs and technical leaders to find new paths forward.

Fortunately, leaders who strategize to weather the storm by proactively re-aligning budgets, redefining processes for efficiency, and continuing planned growth without a substantial increase in resources can still find themselves well-positioned once the uncertain times subside.

In the following sections, we will define and expand on the varying factors creating these circumstances and market conditions. From these insights, we define five steps leaders can take to find opportunities to gain efficiencies in their security practices without compromising their security posture. By aligning IT infrastructure strategy to the new economic environment, leaders can set their organizations up for success well into the future.



Introduction

Over the past few years, IT leaders have been dealing with crisis after crisis as they plan and execute their strategy. They have had to react to a global pandemic and its second-order effects, supply chain shortages, an escalating conflict in eastern Europe, and what may unfold to be a recession. In the words of Stanford economist Paul Romer, "A crisis is a terrible thing to waste" (source). Choices that CIOs made in supporting their remote workforce will have long-lasting, unintended benefits in making their workplaces attractive for supporting remote work. Similarly now, as leaders face a worsening economic outlook, choices they make about security, networking, remote access, storage, development, and infrastructure will help them emerge stronger and better positioned for secure, sustainable growth in the future.

The rise of remote work was accompanied by a boom in ransomware and sophisticated cyber threats that established new benchmarks for revenue impact, scale and sophistication (source). The evaporation of what remained of the network perimeter, coupled with historic increases in employee turnover, led to gaps in security and delays in strategic IT projects. This forced organizations to re-think not only their approach to hiring and retention, but also their approach to controlling access to their systems and machines. Though the pandemic gave rise to a dramatic increase in eCrime (source), it also opened the eyes of organizations and their boards to the urgent necessity of effective cybersecurity. The time is now for organizations to take a more strategic approach to the long game of enabling secure, productive, and available hybrid work infrastructure.

Here are five things you can do to de-risk your business on a budget and elevate your organization's ability to handle the emerging threats looming on the horizon:

1. Audit existing security tools to uncover overlapping capabilities

Organizations have a lot to gain by consolidating their security vendors. Though no single tool will ever be the "silver bullet" solution CISOs would love to have, many security operators said they believe their company is wasting money on too many tools that still don't give them an optimal defense. Supporting multiple tools from multiple vendors means your employees are spending valuable time on procurement, implementation, management, troubleshooting, and supporting a large number of disconnected systems – instead of securing your infrastructure and data. In fact, a June 2022 survey conducted at the annual RSA Conference found that "half (53%) of the responding businesses feel they have wasted more than 50% of their cybersecurity budget and still cannot remediate threats. Forty-three percent of survey respondents say their number one challenge in threat detection and remediation is an overabundance of tools, while 10% of organizations lack effective tools for remediating cybersecurity threats" (source). If you were to eliminate even just a handful of those tools, you could improve security while saving valuable employee time.

By shifting investments from capital expenditures to operational expenditures, you can also make immediate improvements to short-term cash flow and avoid getting locked into multi-year capital investments that impede business agility. One way to simplify is to reduce dependence on traditional hardware. Shifting from legacy boxes to as-a-Service solutions can help to ensure that your highest priority initiatives remain funded, even if budgets decline. Buying into the as-a-Service model also means that you benefit from the inherently faster innovation cycles of software and eliminate the unavoidable pain of frequently patching legacy hardware. Offloading patching and innovation allows your teams to focus on activities that truly differentiate your business. When facing uncertainty, strategic simplification and consolidation can help you achieve long-term success.

2. Focus on the data, not just the tools

Leadership teams should consider shifting focus to better integrate not just the tools, but also the data, across all their security toolsets to better uncover patterns and anomalies. Historically, security teams have continued to add more and more tool sets over time without considering the long term impacts of too many datasets in too many places. Oftentimes, the result is a patchwork of products with little to no interoperability and opaqueness in the data, which results in weaker insights with lower levels of accuracy by introducing opportunities for human error. Not to mention, the amount of time it may take for a team to pull multiple data sets, merge them together, and run the queries is not only wasting time, but also resources. Instead, those resources could be focused on more strategic business initiatives.

While teams may be able to find creative workarounds to solve interoperability challenges, such as manual merging of datasets or importing and exporting of CSVs, it's important to consider that, putting efficiency aside, the value of security tools lies in the data that these systems digest, create, and make available for defenders. If your data is everywhere - unclassified, not secured, and not carefully managed - it can skew what might have otherwise been impactful insights derived from such data, especially if there is data sitting in instances of shadow IT that may have been left out entirely. By consolidating toolsets and thoughtfully considering interoperability of your security stack, you have the ability to reduce human error and better secure your data. Because even if you have invested in the best tools available today, siloed data sets and shadow data sets lead to poorer insights.

In terms of efficiency, it is important to consider that in the era of Zero Trust ("never trust, always verify"), more tools means teams are also spending additional time logging in, authenticating, and gaining access to the systems before they can even begin to do their work. The less systems any given employee needs to touch saves them time and allows them to move faster. It is critically important to consider that the data within these systems, as well as how many systems they have to access to complete any given task, is ultimately what will either enable or hinder teams ability to respond, rather than react, to threats in a timely manner.

3. Look to cloud, as-a-Service models to maximize innovation and minimize complexity

Every business needs to innovate to remain competitive, but any company that isn't in the business of cybersecurity doesn't have the time, budget, or resources to keep up with the latest CVEs, attack trends, and critical patching required to keep their entire infrastructure secure. Adopting as-a-Service models, where feasible, allow leaders to benefit from continuous innovation without having to concern themselves with making trade-offs or difficult decisions around technical debt.

It's also important to consider that some security services charge overage fees for surpassing traffic limitations and some will charge bandwidth fees. Consider taking a hard look at what your organization is paying on a monthly or annual basis to understand if you are paying more than you realize. If you are, you can take that opportunity to seek out other solutions that do not charge overages to help you not only save money, but also have a more predictable spend over the long term, which allows your team to better plan for the future.

Cloud-delivered services of this nature also allow your organization the room to grow and shrink as needed, without having to commit to racks of expensive hardware and all the pain of lifecycle management that comes with it. In times of uncertainty, businesses have to remain agile and responsive to changing market conditions. When cashflow is a concern, the ability to minimize costs or eliminate them altogether is a strategic advantage that can mean the difference between barely surviving and thriving – regardless of market conditions.

4. Uplevel your employee experience

According to Forbes, "Our survey found that complex, multi-step login processes are frustrating workers, wasting their time, hindering productivity and prompting them to give up on essential work-related tasks...In the ultimate irony, nearly 40% of workers said they had procrastinated, delegated or completely skipped setting up new work security apps because of burdensome login processes. That's like protecting your home with the strongest, tallest, most secure gate money can buy—fortified with laser-breathing dragons—only to leave it unlocked at night." Not only is it inefficient and hard for defenders to track which tool houses which function, but too many dashboards and too many places where data sits can create major security risks and visibility gaps for any organization. Companies who want to stay ahead of cybersecurity threats must consider that every single click and keystroke takes valuable time, energy, and focus away from responding to critical events. In order to create a better, more streamlined employee experience, it is critical for leadership to take a hard look at how many tools defenders need to use in order to do their job effectively as well as what can be eliminated or consolidated to cut down on the time it takes a defender to respond, not just react, to a critical security event.

When it comes to non-technical employees or employees not in defender roles, it is also important to consider that as remote workers look to accelerate their personal productivity, they may turn to shadow IT or workaround methods. While Zero Trust controls have provided a promising path forward for building more secure organizations, especially in a remote environment, there is no denying that not all Zero Trust approaches are created equal. The more complex it is for an employee to get access to what they need, the more likely it is that they will find a way to circumvent security controls rather than abide by them. Leaders should seek to understand not just the effectiveness of security products, but also take into consideration ease-of-use, because ignoring employee experience increases overall organizational risk.

5. Look for security services that don't compromise on network performance

It's not just about the tools, but how you configure and manage the tools that can make all of the difference. Consider having your teams do an audit of current configurations and customizations to uncover opportunities that may help enhance performance. If improved performance isn't possible, consider seeking out solutions that are built for performance from the ground up – as performance-as-an-afterthought rarely achieves the goals leaders hope to attain. When it comes to network performance, it is important to keep in mind that a poor architecture cannot be out-coded. Similar to how the blueprints of a building have limited opportunity for re-design once the foundation has been built, networks must be designed from the ground up for ultimate performance.

Leveraging the power of a global edge network that processes and handles data closest to the source will give organizations a strategic advantage both today and in the future. According to MIT Technology Review, "Processing volumes of data can lead to performance issues. In response, many organizations are turning to edge computing, which processes data close to the source to enable fast and real-time analysis and response, while maintaining privacy and security requirements" (source). By strategically choosing solutions that are already building upon the architectures of tomorrow, you can give your teams the strategic advantage of better network performance without sacrificing the critical elements of privacy and security.

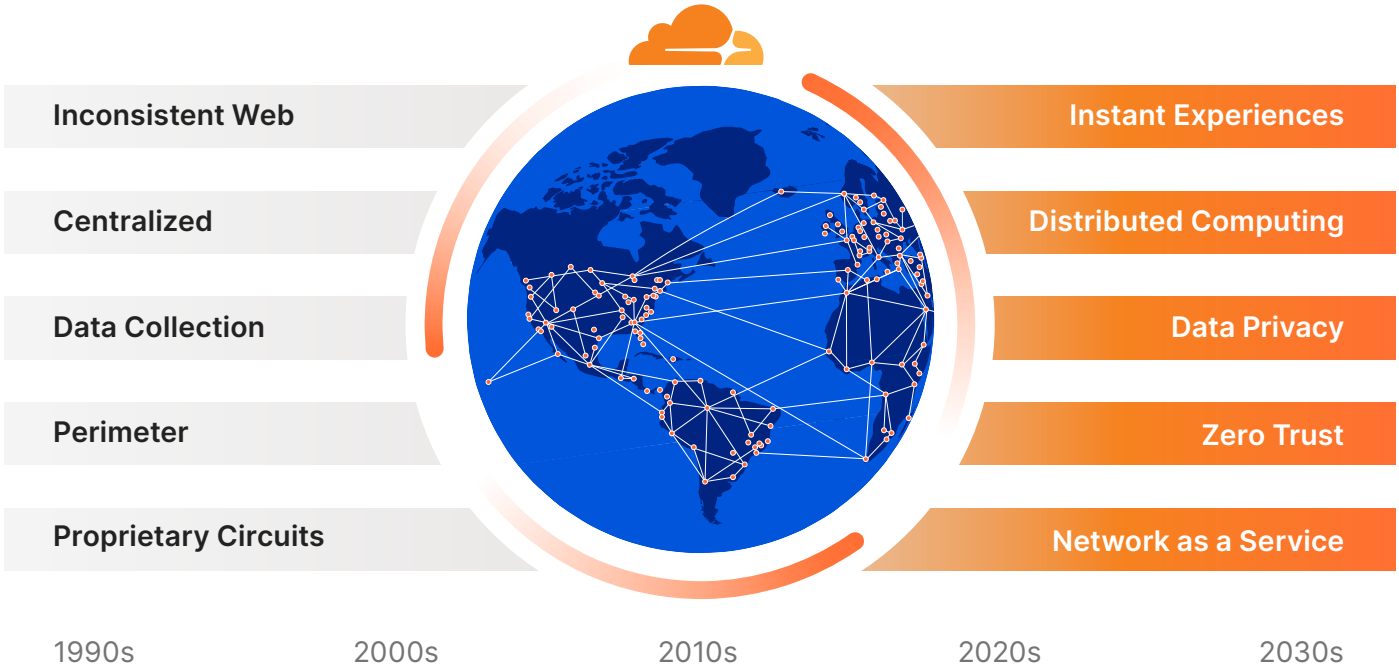
In summary, the steps you can take to build a better cybersecurity posture during uncertain times are:

1. **Audit existing security tools to uncover overlapping capabilities**
   - Consolidate overlapping tools
   - Shift investments from CapEx to OpEx
2. **Focus on the data, not just the tools**
   - Interoperability of tools leads to better, more accurate datasets
   - More accurate datasets and reporting lead to better insights, which are critical to achieving business goals
3. **Look to cloud, as-a-Service models to maximize innovation and minimize complexity**
   - If you aren't in the business of cybersecurity, you have much to gain from offloading patching, maintaining, and upgrading to as-a-Service offerings
   - Cloud and as-a-Service models offer the flexibility you need to be agile in a fluctuating economic environment
4. **Uplevel your employee experience**
   - Too many tools in too many places can create security blind spots and employee frustration - consolidating and simplifying will help to optimize their experience
   - Optimizing for employee ease-of-use will help with employee retention and deter them from turning to shadow IT to get their work done
5. **Look for hidden costs and performance enhancement opportunities in your current cybersecurity stack**
   - Audit existing tools to uncover opportunities to optimize performance, but keep in mind that you can't optimize a poor architecture
   - Adopting tools that are built on global scale closest to where you anticipate your customers are located will enable your organization to deliver a superior, secure customer experience

How Cloudflare can help

Cloudflare launched in 2010, during the aftermath of the 2008 economic crisis, to lead the transformation from on-premise infrastructure to the cloud. We engineered Cloudflare's platform with an audacious goal: to help build a better Internet. Cloudflare's suite of products protect and accelerate anything connected to the Internet without adding hardware, installing software, or changing a line of code.

Internet properties powered by Cloudflare have all web traffic routed through our intelligent global network, which gets smarter with every request. We help our customers work smarter, build better, run faster and grow securely. Today, Cloudflare protects and accelerates millions of Internet properties.



Control

Gain the power of an integrated global network that delivers comprehensive connectivity, security and compute while leaving you in control of policies.

Flexibility

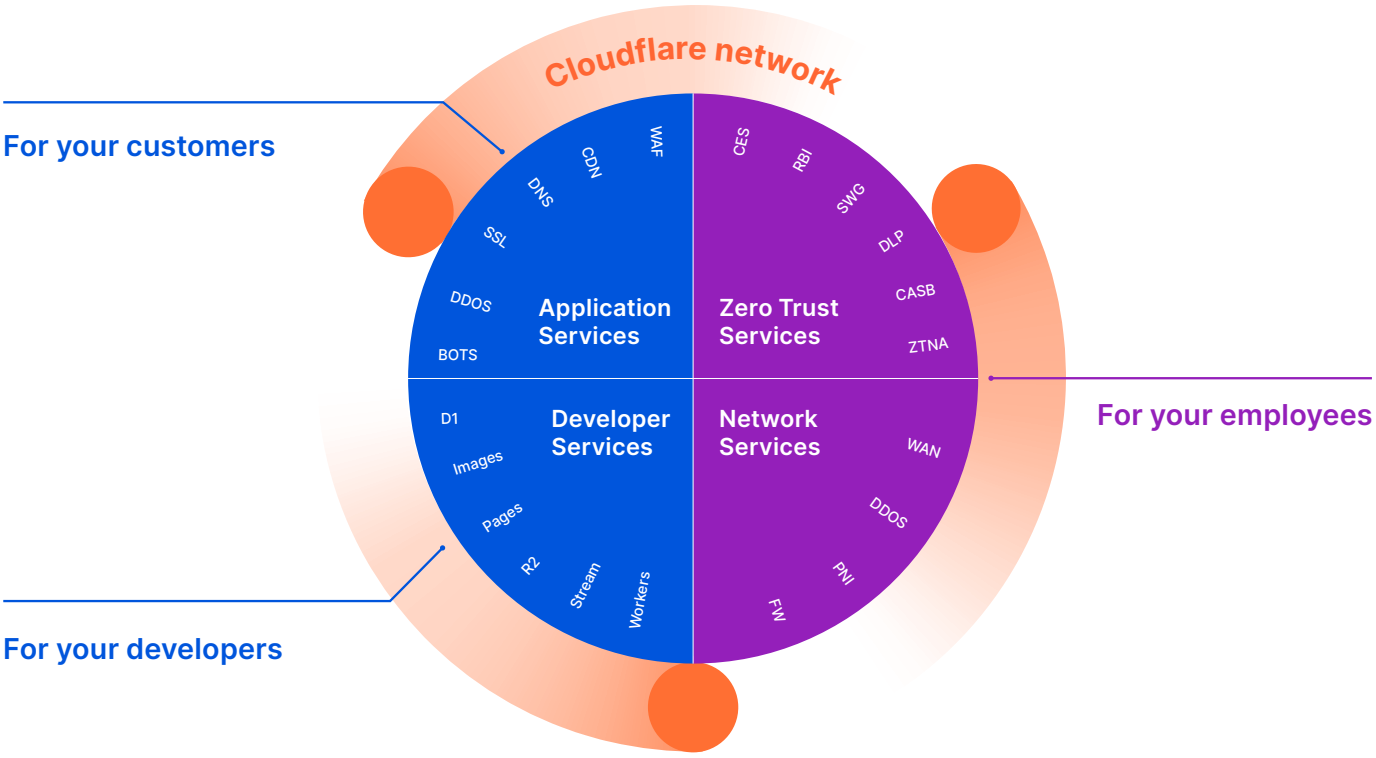
Cloud-native services mean no up-front CapEx investment is required. Easily increase or decrease usage to align with business fluctuations.

Predictability

Predictable billing – with no unexpected costs such as unbounded egress fees. No need to spend CapEx now for hardware delivered next year.

The Cloudflare global network makes everything you connect to the Internet secure, private, fast, and reliable.

- **Secure** your websites, APIs, and Internet applications
- **Protect** corporate networks, employees, and devices
- **Write** and **deploy** code that runs on the network edge

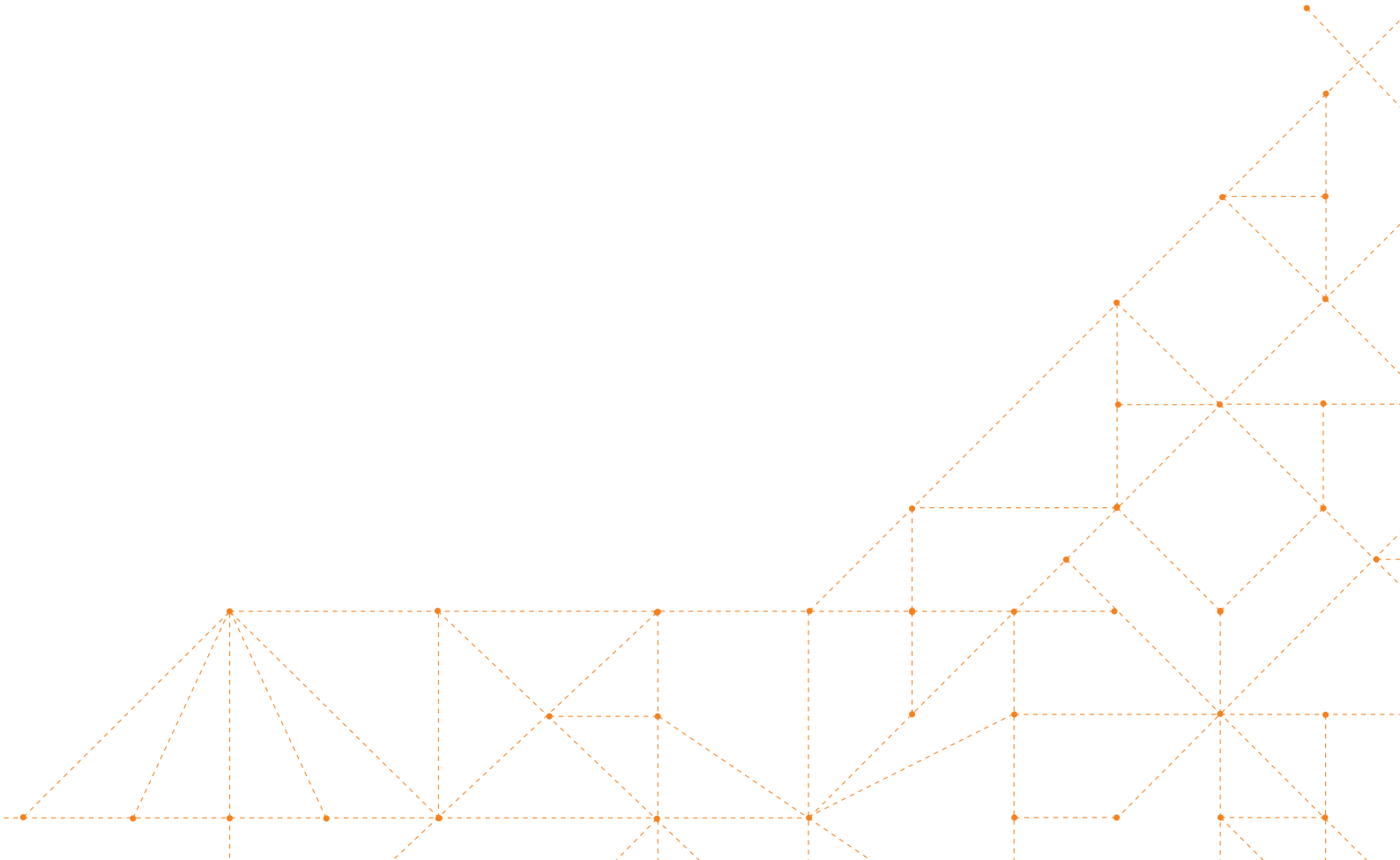


About Cloudflare

Cloudflare launched in 2010 to lead the transformation from on-premise infrastructure to the cloud. We built Cloudflare's platform from the ground up with a full understanding of our audacious plan: to help build a better Internet. Cloudflare's suite of products protect and accelerate any Internet application online without adding hardware, installing software, or changing a line of code.

Internet properties powered by Cloudflare have all web traffic routed through its intelligent global network, which gets smarter with every request. We help our customers work smarter, build better, run faster and grow securely. Today, Cloudflare protects and accelerates millions of Internet properties.

To learn more, visit www.cloudflare.com



CLOUDFLARE

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

REV:BDES-4327.2023MAR10