WHITE PAPER

SASE

Optimizing the enterprise for a distributed, cloud-first world

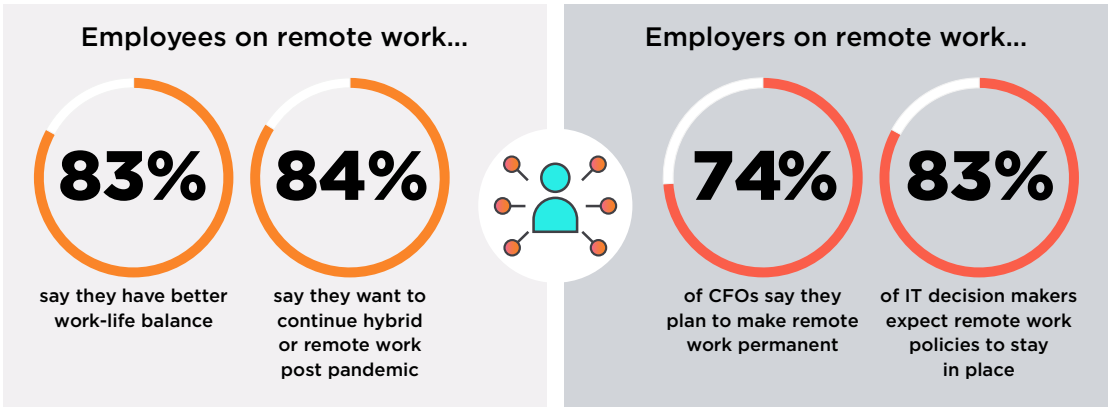
LUMEN®

Sudden changes with lasting impact

The past several years have marked a period of intense change. Spurred by the global pandemic and exacerbated by a number of knock-on effects including evolving employee-employer dynamics, challenging economic conditions, and increasing geo-political instability, organizations have faced unprecedented demands on the business and supporting IT operations. These sudden shifts have left a lasting impact best summarized by three trends that are likely to persist for years to come: the adoption of hybrid work models, an evolving and expanding threat landscape, and the proliferation of next-generation data flows fueled by emerging apps as businesses seek a competitive edge.

The adoption of hybrid work models

The global pandemic has proven that the antiquated management philosophy that connected successful work to hours spent in the physical office environment is incorrect. As companies have experienced a surge in output from their teams over the last several years, and employees and employers have realized the benefits of flexible work, it's evident that remote and hybrid work is here to stay.



For the majority of knowledge and task workers, the pandemic represented a great reset as they re-evaluated their idea of work and the relationship they have with their employers. Remote work affords them greater productivity and flexibility in their jobs — 83 percent feel they have a better work-life balance.[1] They're less stressed and can get their work done faster as a result, and many aren't willing to give up those gains — 84 percent of employees want to continue hybrid or remote work post pandemic, with some even willing to take a pay cut to do so.[2]

Employers too have realized quantifiable benefits of hybrid work through lower real estate costs, reduced turnover, better disaster preparedness, and increased progress towards their energy consumption and carbon emissions goals. It's also afforded new opportunities in a highly competitive labor market by freeing companies from the constraints of hiring within proximity of an office, opening doors to new skills, capabilities and pools of talent anywhere. Recognizing these impacts, 74 percent of CFOs say they plan to make remote work a permanent part of their workforce- and costmanagement plans,[3] and 83 percent of IT decision makers expect remote work policies to stay in place.[4]

While industry chatter lingers about the value of having employees return to office full-time, it's clear that employees greatly favor flexible work policies. Organizations that value performance over place and adopt hybrid work have an advantage in attracting and retaining the best talent, empowering their people to decide how and where they do their best work to drive success.

> "Organizations that value performance over place and adopt hybrid work have an advantage."

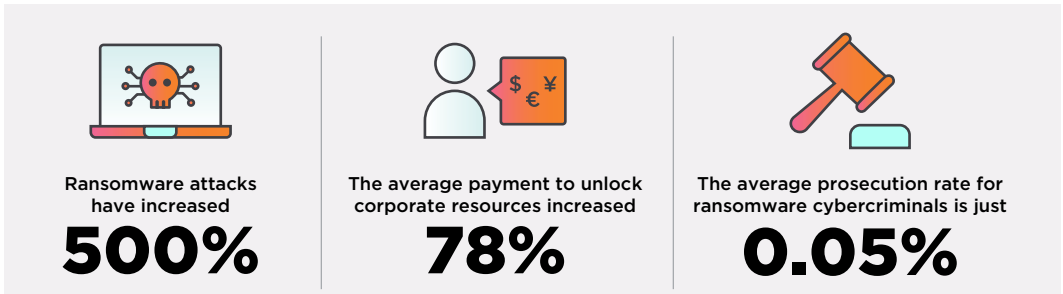
The adoption of hybrid work models

Security has always been a daunting challenge, but as IT models have become more distributed organizations have struggled to keep up and threat actors have sought to take advantage. The shift to a more distributed IT model predates the pandemic of course, as the increasing adoption of cloud, SaaS, mobility and flexible operating models slowly dispersed IT environments and expanded the attack surface of businesses. Slowly but surely, the secure perimeter with centralized control of everything — data, apps, traffic, devices, and users — was disappearing.

When the pandemic hit, that shift was dramatically accelerated. Cloud migrations that were planned over a matter of months happened in mere weeks largely in an effort to enable remote work. The collective IT miracle was that most companies were able to successfully enable their teams to work remotely, many practically overnight, and did so without breaking anything. However, many took more risks than they'd like, employing simple VPN and Bring Your Own Device solutions as bandaids, hairpinning access to public cloud, SaaS and services through the data center at the cost of user experience.

The result was predictable: remote workers turned to unapproved devices and network access to get around the poor performing VPNs. Shadow IT efforts increased as workers adopted unsupported cloud applications. Security policies played catch-up to the realities of the business while the workforce remained highly susceptible to malware, phishing, and botnet attack vectors. Bad actors were ready to pounce.

The ransomware threat has exploded over the course of the pandemic



Since the start of the pandemic, ransomware attacks have increased by nearly 500 percent,[5] and the average payment to unlock corporate resources climbed an astounding 78 percent to $541,010.[6] With a prosecution rate of just 0.05 percent,[7] cybercriminals have little incentive to rein in their activity as the risk-reward is overwhelmingly in their favor. Even those ransomware groups known for the most brazen of attacks have yet to be caught, with governments offering multimillion-dollar rewards for any leads.[8] Rather than face further scrutiny, those ransomware organizations often splinter their operations into smaller groups to continue their efforts, or rebrand as ransomware service providers to enable others while staying clear of the spotlight, demonstrating how persistent a threat ransomware will continue to be.[9]

> "Security policies are playing catch-up to the realities of the business."

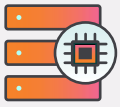
The proliferation of next-generation data flows

Corporate data flows are fundamentally changing. Emerging applications are creating new business opportunities, harnessing advances in compute power, AI, machine learning and IoT, combined with new app-driven architectures, to fuel new experiences for workers, customers and partners.

Similar to the adoption of remote work and distributed IT models, this trend began before the pandemic but has been dramatically accelerated by it. The online nature of the pandemic has led to an influx of self-serve options, increased personalization, and virtual consultations — ingredients that were needed to replace many of the in-person experiences people were unable to partake in. During the pandemic 75 percent of consumers tried a new shopping behavior, and 71 percent expect personalization from the brands they choose.[10] Virtual consultations are 38 times higher now than before the pandemic.[11] Businesses have measured the financial success of these efforts and consumers have noted the added convenience so even as in-person activities resumed, these experiences have persisted.

Businesses also increased their focus on AI, machine learning, IoT and automation to drive real-time insights and optimizations, monitoring and management, and intelligent processes across a range of industries in order to increase efficiency and resiliency and maintain their competitiveness. During the pandemic 41 percent of companies accelerated their AI strategies,[12] and automation deployments tripled with 68 percent of organizations saying they used it as part of their pandemic response.[13] Next-generation experiences in government, manufacturing, healthcare, retail, smart cities, education and logistics are fueling vast amounts of data over networks.

91% of IT decision makers say the ability to quickly acquire, analyze and act on data determines future leaders



90% of IT decision makers say that edge compute is vital to their future

The ability to move and harness data is integral. Of IT decision makers surveyed, 91 percent believe the ability to quickly acquire, analyze and act on data determines future leaders, and 90 percent say that edge compute is vital to their future and anticipate implementing edge compute services to keep pace with the expansion of IoT in the coming years.[14] This surge in operational traffic poses new security challenges including the potential for operational network threats to impact traditional IT networks and a myriad of access requirements to support partners and vendors.

Desired business outcomes

While the pandemic posed unparalleled challenges, many companies looked at the crisis as a catalyst for transforming their organization – an opportunity to rethink their business, their work models, and the IT strategies that support them. They've sought to develop solutions to address current needs while challenging the models of the past in order to emerge even stronger. To that end, the three lasting trends described above have informed the primary business outcomes organizations are seeking to achieve today: increasing worker productivity, enabling greater security while reducing complexity, and achieving new levels of performance and agility.

Increasing worker productivity

Businesses are looking to increase worker productivity. Yes, hybrid work is here to stay, but it's not enough to just make hybrid work permissible. Organizations need to evolve the employee experience to be virtualfirst in order to maximize worker productivity and effectiveness. Whether it's interviewing and onboarding, development and training, team collaboration and support, organizations that can make the virtual versions of those the best version know that they're giving employees who are remote on any given day as good of an experience as if they were onsite, and that requires a new approach to IT.

People, devices, and the networks they access are in a state of perpetual movement. To maintain security and control, IT has to move away from force-fit access through centralized data centers. Unstable connectivity and limited bandwidth availability cannot support cloud-based application performance. A cloud-native solution is required to enable the best network performance and security.

90% of employees say they are as productive or more productive working remotely when compared to the office

Productivity increased up to **20%** for some employees working remotely each day.

When done right, hybrid work policies, combined with a supportive culture, and a secure, performant employee experience leads to substantial productivity gains. Ninety percent of employees say they are as productive or more productive working remotely when compared to the office.[15] Another study conducted demonstrated that productivity increases up to 20% for some employees working remotely each day[16] — effectively the equivalent of a six-day work week. Far from adding total hours, workers cite the elimination of their commutes or the ability to quickly switch between personal and work tasks as enabling more time to get work done.

Enabling greater security while reducing complexity

Security remains the number one pain point for IT organizations today: nine in ten IT decision makers cite application and data security as their top IT concern.[17] With an ever-evolving threat landscape, an increasingly distributed IT model, and opportunistic bad actors, that's no surprise. The challenge lies in enabling that security while reducing complexity and simplifying visibility and management.

The ever-increasing IT complexity of the average enterprise

- **400+ applications** deployed across on-prem, cloud and SaaS
- **Unmanaged devices** exacerbated by the rapid shift to remote work and supply chain issues for company-issued laptops
- **Shadow IT solution**s adopted by employees, particularly for file storage and sharing, productivity, collaboration and project management
- **New attack vectors** from IoT operational data using traditional IT networks
- Constantly changing **network technologies**
- **45 different cybersecurity-related tools**

The average enterprise has more than 400 applications deployed today across on-prem, cloud and SaaS.[18] Add to that unmanaged devices, shadow IT, new operational attack vectors, and a wide variety of constantly changing network technologies and it paints a picture of how complicated and fragmented enterprise security has become. The average enterprise deploys 45 different cybersecurity-related tools on their networks today,[19] but more than half of IT experts admit they're unsure of how well those tools even work.[20]

LUMEN®

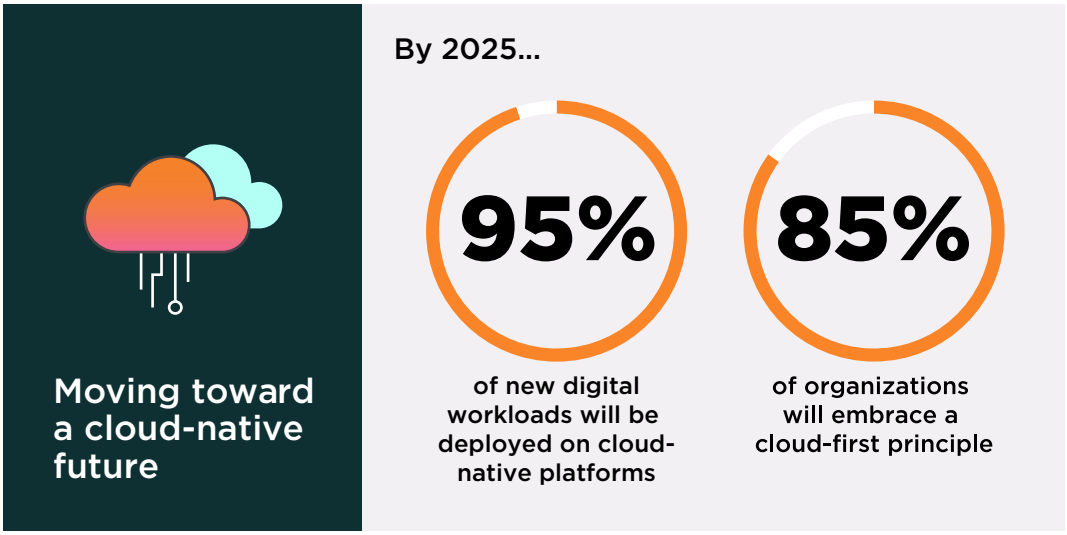
To address this, businesses are striving to enact a converged network and security approach that delivers contextual security, is simple to manage, and provides enterprise-wide visibility.

> “Businesses are striving to enact a converged network and security approach to simplify management and visibility.”

The ever-increasing IT complexity of the average enterprise

If there was one lesson every business learned from the pandemic, it was to build flexibility into operations in order to be resilient in the face of any future disruption. Agility on its own is a fine goal, but those organizations who seized on this moment to go beyond that — rethinking the future of their business and corresponding IT strategies — are taking bold steps to enable greater IT performance as well.

Performance paired with agility enables organizations to connect people, processes, applications and things; to react to changing market demands on a moment’s notice; to scale capacity on-demand; and of course to improve business resiliency and continuity to handle unpredictable events. Achieving new levels of performance and agility empowers businesses to foster new innovation, accelerate progress and increase competitiveness by developing and delivering new data-rich, latency-sensitive applications and experiences without IT operations breaking a sweat.



Today's emerging applications are tomorrow's status quo, so businesses are investing to not be left behind. Last year, spending on infrastructure as a service (IaaS) increased 41 percent making it a $90 billion market.[21] Spending on public cloud services is expected to increase more than 20 percent this year.[22] By 2025, it's estimated that more than 95 percent of new digital workloads will be deployed on cloud-native platforms, up from just 30 percent last year, and it's expected that more than 85 percent of organizations will embrace a cloud-first principle requiring the use of cloud-native architectures and technologies.[23] Greater performance and agility together are fundamental to future success.

> "Greater performance and agility together are fundamental to future success."

LUMEN®

Enabling business outcomes through SASE

Secure Access Service Edge, or SASE, is a new framework for network architecture designed to excel in a highly distributed, cloud-first world. SASE streamlines network access, improves security, boosts network performance and reduces management complexity by rolling software-defined wide area networking and security into a cloud service. Simply put, SASE enables cloud-hosted networking and security-as-a-service for any-to-any connectivity.

While SASE combines a number of network and security capabilities that secures network traffic as the sum of those functions, the SASE model can be summarized by three core attributes:

1. A cloud-native architecture for increased network performance and agility

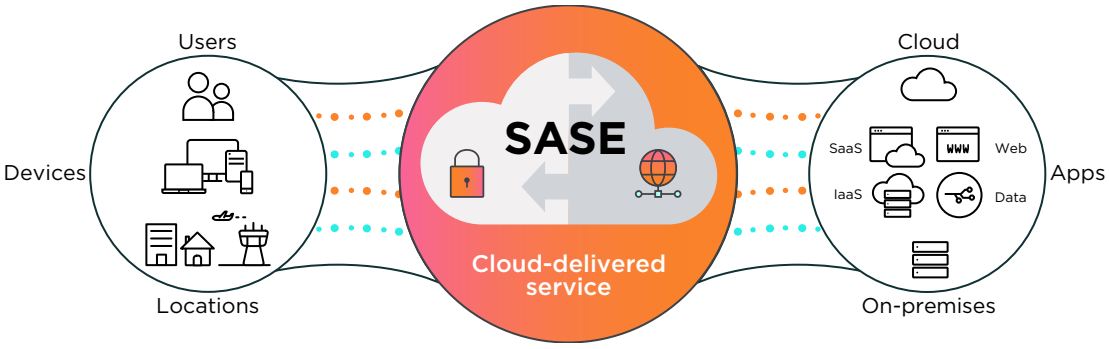
A SASE model has a flexible network topology making use of a software-defined perimeter that supports all edge types. This cloudnative architecture optimizes client-to-cloud latency by taking security to the edge, where the users and traffic are. Users have the same access experience regardless of what resources they need and where they and the resources are located, and the authentication process is simplified by applying appropriate policies for those resources based on the initial sign-in. Quality of service can be optimized so that each application gets the bandwidth and network responsiveness it needs.

2. Contextual, identity-based policy enforcement at the edge for improved security

In a SASE model security is delivered as a service with contextual, identity-based policies being equally enforced regardless of user location or IP address. SASE uses a Zero-Trust security approach, granting least-privileged access based on the identity of the user, the type of device connecting, and the sensitivity of the application or resource being accessed as specified by security and compliance policies. No matter where or how users are connecting, and what they're attempting to connect to, enterprise-grade authentication is used. And because security is provided as a service, policies and detections can be updated and applied immediately as new threats emerge.

3. Centralized management for simplified orchestration and increased visibility

A SASE model allows IT teams to centrally set policies via cloudbased management platforms and have those policies enforced at distributed points of presence (PoPs) close to the users. The same management platforms enable comprehensive visibility and control of users, applications, and risks. As a single service, SASE reduces complexity and cost. IT has to deal with fewer vendors, less hardware requirements in branch offices and other remote locations, and fewer agents on user devices. IT teams are able to shift from managing point products to delivering policy-based solutions. Centralized access to network and security data also enables more advanced capabilities such as holistic behavior analytics and continuous risk assessments to spot threats and anomalies that otherwise wouldn't be apparent in siloed systems. Updating threat data or incorporating external intelligence feeds is also made easier because those analytics are delivered as a cloud service.

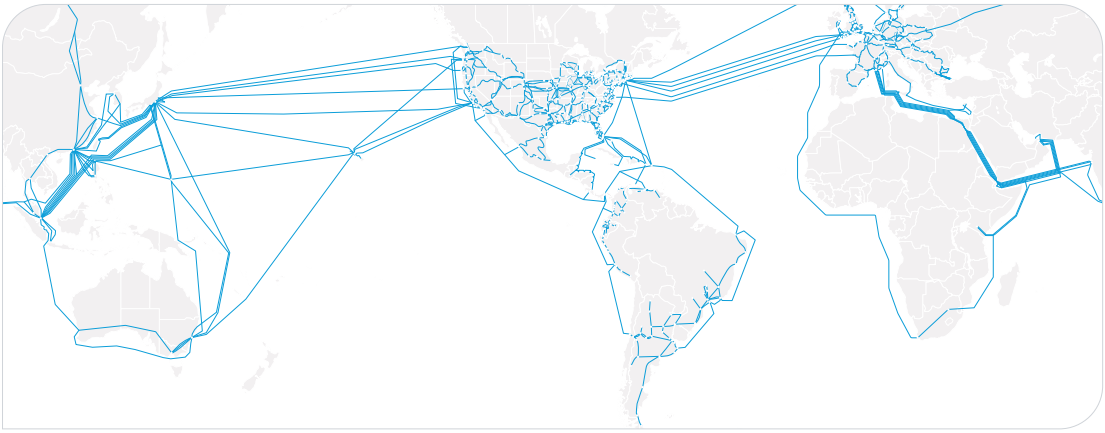


SASE gives organizations better performance and agility, flexible and consistent security, while reducing complexity to empower an effective distributed workforce. It enables business to respond faster to disruptions while minimizing their impact, and positions them to take advantage of emerging next-generation applications and experiences. Enterprises have taken notice of SASE and are racing to implement it. By 2025, at least 60 percent of enterprises will have explicit SASE strategies and adoption timelines encompassing user, branch and edge access, up from 10 percent in 2020.[24] It's evident that SASE is the preferred networking framework for a distributed, cloud-first world.

> "By 2025, at least 60 percent of enterprises will have explicit SASE strategies and adoption timelines encompassing user, branch and edge access."

How Lumen enables SASE

SASE is only as good as its underlying infrastructure. For a highly distributed world, businesses need an adaptive network that connects work resources without compromise. Lumen operates one of the largest, most connected and most deeply peered networks in the world with ~500,000 route miles of fiber and ~190,000 on-net fiber locations and servers customers in more than 60 countries. It's one of the most connected networks to hybrid cloud, with dynamic connectivity to more than 2,200 public and private data centers and seamless access to all of the top cloud providers. And the Lumen network excels at the edge, with more than 60 edge node deployments and a dense metro IP network of PoPs to supercharge compute-intensive application experiences. In fact, the Lumen network is designed to deliver 5ms or less of latency covering 97% of U.S. business demand.



Lumen provides a cloud-based network and security experience modeled on SASE attributes that is fully converged, centrally controlled, and flexibly managed. Lumen is specifically designed to enable highly secure, highly performant any-to-any connectivity from traditional workloads to the latency-sensitive, data-rich needs of next-gen applications and emerging technologies. It does that through the following:

An integrated, cloud-native architecture

Lumen features an integrated, cloud-native architecture that combines Lumen's metro edge presence, cloud connectivity, underlying network assets, and market-leading SD-WAN and security partners to deliver a simplified, high-performing application experience. By abstracting away network complexities and managing resources as a service, organizations can optimize workloads by executing them in the most suitable venues, and scale on demand to enable greater organizational agility and help deliver greater performance where and when its needed.

Secure any-to-any connectivity

Lumen combines expansive threat intelligence, connected cloud data centers, and leading security partner capabilities to provide secure access to work resources from virtually anywhere, on any device, at any time. Lumen enables granular access control policies by user role, device, permissions, behavior, identity and application with enforcement at the edge, simplifying access for workers while also securing app, API, and IoT data flows. And through Black Lotus Labs, Lumen benefits from more than 200 billion NetFlow sessions, 1 billion DNS queries, and 2.3 million unique threats, all monitored every day, often surfacing malicious activity before other companies can spot it. Black Lotus Labs® provides unparalleled insight into the behavior of bad actors — intelligence that is shared across Lumen's backbone.

Simple, flexible management

Lumen simplifies network and security management with converged capabilities from market leaders. Using the Lumen online marketplace businesses can design, price, purchase and deploy software-defined network infrastructure and information security capabilities. Lumen also unites orchestration and management providing a centralized point of control and visibility into security operations and network traffic. With a variety of flexible management options to choose from, Lumen enables organizations to reduce complexity while maintaining the level of control they prefer.

Taken as a whole, Lumen delivers a high-performance, deeply managed service experience that enables SASE attributes to help organizations achieve their desired business outcomes.

> "SASE is only as good as its underlying infrastructure — an adaptive network that connects work resources without compromise."

LUMEN®

Lumen in action

Enabling hybrid work

The challenge

A global semiconductor business depends on its design engineers, located across 40 locations. The company's engineers work collaboratively on chip designs across different locations, using a remote access solution which is heavily dependent on good network performance to function well. The company was using more than 60 vendors around the world to connect its employees and secure work, but as the company grew, that complexity ground operations to a standstill. Different vendors had different service levels, and when there was a problem there were too many vendors involved to identify the issues needing remediation. Hard outages occurred frequently and there was no immediate failover. Inevitably, it had an impact on the business as engineers couldn't do their work. The company sought a new approach to enabling secure hybrid work.

The solution

Lumen began with a relatively modest proof-of-concept, delivering connectivity to four sites with mixed business use cases in different locations with agreed upon SLAs, all based on a SASE model. When that project was successful, Lumen deployed the solution companywide, implementing an integrated software-defined approach that abstracted away network complexity, and a Zero-Trust approach for secure remote access to sensitive resources. Lumen centrally defined security policies and managed operations.

The outcomes

The company realized immediate benefits. Engineers enjoyed improved performance and consistent network speed allowing them to complete their work. The flexible network approach virtually eliminated downtime, enabling multiple failover states for any connectivity or resource issues. And through Lumen, the IT team now had a simplified way to manage operations and gain visibility across the network. While reliability was the key need, the solution also provided better scalability, management, and security for hybrid work.

LUMEN®

Simplifying network and security management with Lumen

The challenge

A growing cloud-based online consumer goods company expanded sales to six branded retail locations and large ecommerce and social venues. The expansion required the seamless integration of in-store and online shopping experiences supporting customer discounts and automated checkout, among other services. In order to always be up-to-date in their meetings, the mobile account team also required secure access to customer data and site updates. The addition of these requirements meant that maintaining application performance, segmenting users, and managing highly distributed secure access became a daunting challenge for a limited IT staff.

The solution

Lumen architected and deployed a SASE-based solution supporting secure internet, broadband, and LTE access to retail locations, cloud applications, and remote staff. Lumen edge devices were deployed at the headquarters and stores for improved application performance and traffic segmentation. Using Lumen, IT teams centrally defined security policies and Lumen then provided pro-managed monitoring and maintenance of the entire solution to help alleviate pressure on the IT team.

The outcomes

The Lumen solution enabled secure, performant application access, allowing distributed sales and retail staff to stay productive. The mobile account team gained secure access from any device. Meanwhile IT benefited from centralized management of network and security policies, and the ability to segment customer and internal application experiences to help ensure consistent quality of service.

Increasing network performance and agility with Lumen

The challenge

A regional healthcare system made up of two hospitals, 20 partner clinics, and a professional campus with partner services relies on one private data center storing personal health information which is shared with multiple cloud-hosted applications. During the pandemic, in order to minimize patient impact on hospitals while maintaining optimal patient care, the healthcare system needed to greatly increase remote access to its electronic medical records application and accommodate significantly higher telemedicine consultations. Doing so required a new network and security approach to improve application performance, securely share compliant patient information, all while ensuring up-to-date accuracy.

The solution

Lumen architected and deployed a SASE-based solution integrating and simplifying the secure, high-performance delivery of medical record applications containing sensitive patient information. The solution combined Lumen private and dedicated internet connections to segment data center traffic and share uninterrupted transport of critical data between hospital and campus environments. Patient data collected across devices and diagnostics is privately shared while maintaining uninterrupted delivery, with Lumen network storage keeping patient data secure at the edge and regular snapshots reducing the risk from any potential breach. Broadband and LTE mobile user traffic was secured and prioritized using ZeroTrust Network Access to Lumen's secure cloud gateway providing IT with end-to-end visibility and policy control. Lumen enabled centralized policy management with Lumen managing the monitoring and maintenance of the entire solution. Application performance was improved by scrubbing traffic closer to the data source at the service edge and cloud gateways for mobile and remote users.

The outcomes

The Lumen solution enabled the hospitals to rapidly offload nonpandemic-related patients to partner clinics and telemedicine services. Healthcare providers and patients benefited from secure and performant experiences, including clear telemedicine sessions and secure sharing of personal health information across devices, users and locations.

LUMEN®

Summary

The adoption of hybrid work models, an evolving and expanding threat landscape, and the proliferation of next-generation data flows is driving businesses to implement solutions that increase worker productivity, enable greater security while reducing IT complexity, and unlock new levels of performance and agility.

Forward-thinking organizations are approaching these objectives not just as a response to the challenge of the pandemic, but as an opportunity to rethink their business, their work models, and the IT strategies that support them in order to foster new innovation and increase competitiveness in the long run. It's not just about security. It's about performance and agility — accelerating today's and tomorrow's applications in the most appropriate locations in order to realize the best experience possible.

Lumen enables SASE attributes, empowers organizations to achieve those outcomes with highly secure, highly performant any-to-any connectivity to handle both today's workloads and the latencysensitive, data-rich needs of next-gen applications and emerging technologies.

Endnotes

1. Citrix and OnePoll
2. Owl Labs
3. Gartner
4. Quadrant Strategies
5. Infosecurity Magazine
6. Palo Alto Networks
7. U.S. Congressional Record
8. Bleeping Computer
9. Bleeping Computer
10. McKinsey
11. McKinsey
12. World Economic Forum
13. Citrix and OnePoll
14. Owl Labs
15. Gartner
16. Quadrant Strategies
17. Infosecurity Magazine
18. Palo Alto Networks
19. U.S. Congressional Record
20. Bleeping Computer
21. Bleeping Computer
22. McKinsey
23. McKinsey
24. World Economic Forum

* This content is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen products and offerings as of the date of issue.

866-352-0291 | lumen.com | info@lumen.com

LUMEN®