WHITE PAPER

SASE:

Optimizing the financial enterprise for a distributed, cloud-first world

LUMEN®

Sudden changes with lasting impact

The past several years have marked a period of intense change for the financial services industry. Spurred by the global pandemic, trends toward online or app-based mobile banking accelerated. At the same time, new entrants into the field coming from the FinTech arena increased competition with more traditional financial institutions. As all that played out, the cybersecurity threat increased across the economy. Financial institutions provide key targets for bad actors because of the obvious concentration of financial assets, but also because of the wealth of information they hold about their customers.

Many financial institutions have a physical asset to leverage in this competitive environment – the branch. And technology approaches such as Secure Access Services Edge (SASE) bring new ways to secure these distributed assets.

LUMEN®

Leveraging the branch

Many customers still identify the branch as the place for certain kinds of transactions such as obtaining loans or opening accounts. For small businesses, a local physical presence may provide stickier relationships than a virtual one. And for all customers, the physical branch is likely the only tangible manifestation of an institution's brand that the customer will experience. So, the physical branch still has great value. However, all these customers will expect the same level of convenience and customization in the experience as they get in a digital world.

That places a priority on digitizing, automating, and personalizing as much of the customer experience in the branch as possible. Think of cameras with facial recognition capability, or Wi-Fi beacons that recognize when a customer's phone enters the branch. Personalized concierge service can begin immediately in that environment.

Financial services firms have been making strides at protecting the core of their IT resources because they had to. Securing the branches is just as urgent, but it is a different challenge. Routing all transactions and digital interactions through centralized core infrastructure to secure them is not efficient for the institution and latency issues could frustrate employees and customers.

The evolving and expanding threat landscape

Security has always been a daunting challenge, but as IT models have become more distributed institutions 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 band- aids, hair pinning 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.

Since the start of the pandemic, ransomware attacks have increased by nearly 500 percent,[1] and the average payment to unlock corporate resources climbed an astounding 78 percent to $541,010.[2] With a prosecution rate of just 0.05 percent,[3] 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 multi- million-dollar rewards for any leads.[4] 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.[5]

1. Infosecurity Magazine: Ransomware Attacks Grew by 485% in 2020
2. Palo Alto Networks: Ransomware Payments Hit New Records in 2021 as Dark Web Leaks Climbed
3. U.S. Congressional Record: CREC-2022-03-28
4. Bleeping Computer: US targets DarkSide ransomware and its rebrands with $10 million reward
5. Bleeping Computer: Conti ransomware shuts down operation, rebrands into smaller units

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.[6] With an everevolving threat landscape, an increasingly distributed IT model, and opportunistic bad actors, that's no surprise. The challenge for financial institutions and other enterprises lies in enabling that security while reducing complexity and simplifying visibility and management.

The average enterprise has more than 400 applications deployed today across on-prem, cloud and SaaS.[7] 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,[8] but more than half of IT experts admit they're unsure of how well those tools even work.[9]

The average enterprise has more than 400 applications deployed today across on-prem, cloud and SaaS

Bank branches and other parts of the financial services industry are the very definition of a distributed business model. Yet, new technologies deployed in the branch to improve the customer experience create new attack vectors. Securing those new technologies cannot add to the IT burden of these small branches with little to no IT support.

6. Quadrant Strategies: Global trend report 4th industrial revolution
7. McAfee: Every company is a software company today
8. ZDNet: The more cybersecurity tools an enterprise deploys, the less effective their defense is
9. Help Net Security: 53% of enterprises have no idea if their security tools are working

LUMEN®

Enabling branch upgrades 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: (uCPE), that is already incorporated into Lumen's edge compute architecture. This reduces costs to the customer by allowing for additional virtual network functions and applications, simplifying deployment for all parties.

- **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 cloud-native 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.

- **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.

- **Centralized management for simplified orchestration and increased visibility:** A SASE model allows IT teams to centrally set policies via cloud-based 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 2020.10 It's evident that SASE is the preferred networking framework for a distributed, cloud-first world.

How the Lumen Platform enables SASE

A platform modeled on 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 ~400,000 route miles of fiber and ~150,000 on-net fiber locations and serves 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.

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

LUMEN®

An integrated, cloud-native architecture

The Lumen Platform 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

The Lumen Platform 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. The platform 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®, the Lumen Platform 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 with the Lumen Platform.

Simple, flexible management

The Lumen Platform simplifies network and security management with converged capabilities from market leaders. Through the platform's online marketplace businesses can design, price, purchase and deploy software-defined network infrastructure and information security capabilities. The Lumen Platform 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, the Lumen Platform enables organizations to reduce complexity while maintaining the level of control they prefer.

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

LUMEN®

Summary

Increased competition, rising customer expectations and an evolving and expanding threat landscape are pressuring financial institutions to find new leverage in their branch infrastructure. New ways of serving customers through technology-enabled personalized approaches enhance the branch's utility as a differentiator. However, these upgrades must be secured without adding complexity to the branch's IT infrastructure.

SASE simplifies security by allowing that software to be served as a service through edge compute facilities. The branch manager doesn't need to buy a lot of hardware, find places to put it, and sign lots of new service contracts for support. It can all be centrally managed by a provider. This allows increased visibility across the IT environment so that patterns – especially those indicating coordinated attacks – can be identified centrally and early. Because SASE is a framework in which multiple technologies must be integrated, a provider such as Lumen can choose the best-inclass components tailored to a given institution's needs.

The Lumen Platform, modeled on 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 latency-sensitive, data-rich needs of next-gen applications and emerging technologies.

Learn more

About Lumen's SASE capabilities at lumen.com/financial-services.

* 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. All third-party company and product or service names referenced in this article are for identification purposes only and do not imply endorsement or affiliation with Lumen. This document represents Lumen products and offerings as of the date of issue.

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

LUMEN®