INSIGHTS | TECH BRIEF

Written By Terry Dever
WEI Solution Architect & Professional Services Engineer

Deep Dive: How SASE Redefines The Enterprise Perimeter

Today's enterprise networking environments often rely on legacy systems composed of disconnected point products. These tools, managed separately, fail to work together as a cohesive platform—an issue driven by budget constraints and the organic growth of users and perimeters over time. As a result, many organizations are left with fragmented systems that struggle to keep up with modern demands.

Whether dealing with greenfield, hybrid, or brownfield environments, enterprises face a growing need for a unified framework to address today's escalating security threats. Without proper guidance, these environments become vulnerable to the increasingly complex threat landscape.

The challenge is clear: an ever-expanding attack surface, distributed perimeters that include every user and application, remote employees, and data stored offsite in cloud or SaaS applications. Together, these factors create significant risks for data leaks—forming a "perfect storm" that complicates efforts to secure critical information.

Today, there are many security and network/Wide Area Network (WAN) transformation issues which companies are faced with, including:

Zero Trust Network Access: You might have many security point products (firewalls, URL filtering appliances, IDS/IPS appliances, etc.) and wonder if these products in your environment are built upon the five pillars of ZTNA (least privilege access, continuous trust verification, continuous security inspection, protection of all data, and protection of all applications). According to Gartner, a viable SASE product must be architected and built upon the five pillars.

Rising Costs: Rising year-over-year costs for networking and security infrastructure are a growing challenge, especially when managing multiple security appliance point products. These include firewalls, outdated URL filtering tools, explicit proxy services, WAN edge routers, IDS/IPS appliances, CASBs (cloud access security brokers), and RBI (remote browser isolation) services, among others. Each device requires ongoing upgrades, patching, and resources like power and cooling, creating significant operational overhead. Additionally, every device or service comes with its own licensing, configuration console, and maintenance needs. Many of these tools are outdated, falling short of meeting today's advanced security requirements, and adding complexity without delivering sufficient protection.

51%

of IT decision makers indicated **'security and compliance concerns'** as a top driver for digital transformation.[1]

WATCH: WEI Workshop

Security Everywhere:

How SASE Transforms Network & Security With Simplicity

CYBERSECURITY

Breaches: The looming fear of breaches/security events, issues affecting your environment, and not knowing if the products in your environment are secure or even industry compliant. Do you have best practice security recommendations configured? Do you have a product that prevents known and zero day (unknown) malware?

Client VPN: Legacy client VPNs struggle to meet the demands of today's enterprise. These outdated systems often grant unrestricted access once users connect, exposing the network to unnecessary risk. Without two-factor or device authentication, there's no assurance that connecting devices are company-certified or compliant. This creates challenges for BYOD users and contractors, such as enforcing granular access or verifying device posture before granting permissions.

Security risks escalate further when infected or non-compliant devices connect to the corporate environment, potentially spreading malware or compromising sensitive resources.

Performance is another major issue. Traditional VPN setups backhaul user traffic through a central data center, introducing latency and delays—especially for globally dispersed users. "Split tunneling" may address performance by routing Internet traffic directly while reserving the VPN for corporate resources. However, this sacrifices visibility and security for Internet-bound traffic, forcing admins to adopt additional tools for oversight and protection.

Modern VPN solutions must go beyond basic connectivity, offering device verification, granular access, and seamless user experiences—all while maintaining complete security and visibility for both corporate and Internet traffic.

Lack of Visibility: If mobile users encounter broken connectivity, intermittent jitter, delay, packet loss, or overall slowness getting to one application but not another, or latency when accessing all applications, then how and where do you triangulate the root cause? What if you want visibility into user traffic, the applications they are using, and the applications they are experiencing latency in? You also may want to identify why the latency is occurring, when it is happening, and the frequency of the reported latency.

WAN Transformation: What if, during your WAN transformation, you want a guaranteed performance increase/improved uptime for users and applications? There is an increasing need to completely transform the WAN due to expensive leased lines (MPLS specifically), while eliminating single points of failure and building in resiliency, while safeguarding against application brownout where chatty bandwidth/intensive applications can "starve" out the traffic from other applications. This causes jitter/delay/latency or even outages with little or NO visibility into the root cause, while possibly bonding WAN links together as one overlay while securing traffic as it moves east-west between networks at each branch and data center.

Staying or Going: Most companies, especially since the pandemic, have branches with expiring equipment, expiring licenses, expensive maintenance/upkeep/rent/real estate, etc. Are there branches you can "sunset"? If so, you can save on the aforementioned costs. If so, you've also increased your mobile user headcount.

Sprawling Corporate Perimeters: The traditional corporate perimeter no longer exists. With fewer employees working from the office five days a week, today's perimeter is everywhere your users are—on the road, at home, or in a hybrid workspace. Each user and device essentially becomes a corporate perimeter, requiring security for every data connection to the Internet and back to corporate systems.

Adding to this complexity are the SaaS (Software as a Service) applications housing your sensitive corporate data and intellectual property—your company's "secret sauce." These applications operate outside your direct control, raising critical questions:

- Who has access to this data?
- Where is it being shared or stored?
- Does it contain hidden malware or vulnerabilities?

Without a centralized strategy to manage these sprawling perimeters, your network risks spiraling into chaos, with critical data left exposed. Securing users, devices, and SaaS applications while minimizing latency demands a modern approach to IT security—one that addresses the reality of a boundaryless enterprise.

Global Connectivity: What if you could seamlessly interconnect your mobile users, remote branches, and data centers on a global scale while securing SaaS applications and performing DLP (Data Loss Prevention) on application traffic? Imagine having full visibility into all traffic, blocking both known and zero-day malware, and ensuring every connection—whether from a user, branch, or data center—is routed through a globally deployed service that's always local to your needs.

With a unified SASE solution, this vision becomes reality. Centralized management through a single GUI simplifies operations while delivering security, performance, and visibility—wherever your users or infrastructure are located.

Are You Asking The Tough Questions?

- List your current pain points about your network and network security. What keeps you up at night? What does the company really value and what is core to the business? What do you like and dislike about your current network and network security? What is preventing you from achieving your transformation and security goals?
- What does "ZTNA" mean to your organization? What does it mean and how does it impact YOU?
- Does your organization have a consistent security posture that can be easily implemented for all users, all mobile users, all sites, all applications everywhere?
- Then, ask yourself: Why make changes based on your business initiatives? What is the technology gap you are faced with? How do those issues map to meet or miss business goals? What is your ideal business outcome and why solve it now? What is the risk of doing nothing vs. strengthening your network and security posture ASAP?
- How can I proactively mitigate the inception and spread of zero day malware in real time at the "front door" so I can stop being reactive to the spread of malware?
- Are you drowning in log spam and have no way to figure out the alerts to focus on? Which alerts correlate together?
- Why are you considering one vendor vs. another and do they fully cover ZTNA 2.0? Do they fully mitigate zero-day malware? What is your organization doing to prevent both known and zero-day malware? And more importantly, how do you know those measures are effective? Threat actors exploit target vulnerabilities in software to execute malicious code, deploying malware and wreaking havoc.

  Most breaches go undetected, with organizations often discovering them 60 days—or more—after the fact. Silent attacks allow bad actors to remain unnoticed as they siphon off resources and disrupt operations. Essentially, these attackers are operating on your payroll without your knowledge. It's time to fix the glitch and take proactive measures to stop them. It is not a creatively packaged telco bundle.
- Why are you considering one vendor vs. another and do they fully cover ZTNA 2.0? Do they fully mitigate zero-day malware?
- How many workers do you have worldwide? Including contractors, what is the projected number 3-5 years from now? Which geographic locations do they reside in? Where will they be in the future...traveling, perhaps? How many remote workers at peak times? Do workers need to "phone home" back to your company or do they access SaaS applications directly via the Internet? How is mobile user data kept safe while the user is at home or traveling?

Additional Questions Worth Asking

- Least Privilege Access and Continuous Trust Verification: Can I trust users (identity by User-ID and Group-ID) and devices to access specific applications and internal or Internet-based corporate resources the entire time? Are users doing the right things while connected? How do you know? How do they know?
- How do you ensure that "X" group of users can only access "X" group of applications? Same question regarding contractor access to your organization! How do you police this?
- How is your branch network configured today? Are legacy edge appliances still in place at each location? Do branches need direct access to each other or the data center, and is that access sufficient? Bandwidth requirements, security enforcement, and traffic prioritization for critical and latency-sensitive applications must all be considered.

  If you're backhauling branch traffic through centralized data centers, you may be introducing unnecessary latency and bottlenecks. Optimizing branch connectivity requires modern solutions that balance performance, security, and efficiency.
- Can you perform micro-segmentation at the branch?
- Do remote workers need to access the branches and data centers, or just the data centers?
- How are you enforcing security when people and applications "scatter"? How do you know?
- How are you networking to and reaching applications in the data center/reaching cloud or Internet applications?
- Most organizations rely heavily on SaaS applications, but how well are they managing access and security? Are all users allowed access to every application and all the data within them, or are there controls in place? Which applications are trusted, blocked, or tolerated, and how is access restricted based on user roles?

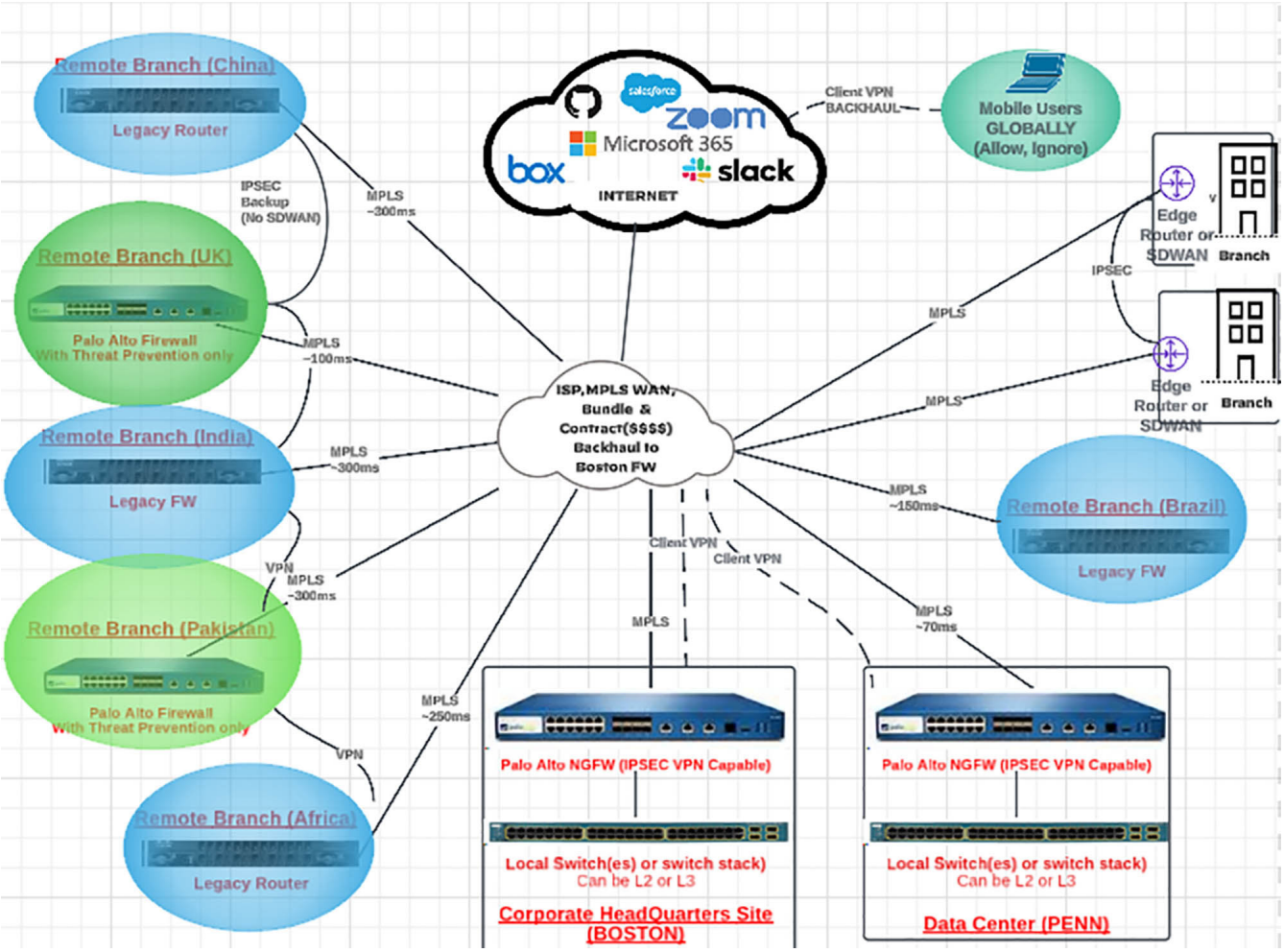
  Beyond access, there are critical questions about security and visibility. Is the application configured securely? Where is your data going, and is it being shared externally? Could it contain malware? Without proper oversight, sensitive data could be at risk of leakage or misuse. A comprehensive strategy for DLP, policy enforcement, and compliance is essential to ensure application security and safeguard sensitive information.
- For Internet or cloud-based applications—do you have per-application/per-user visibility when things go wrong intermittently?
- Are you doing SSL/TLS decryption at scale without oversubscribing your resources?
- If you want to change your security and WAN architecture, can you implement this security quickly, everywhere, at hyper-scale, cost friendly, and without oversubscription?
- When it comes to security, the cheapest solution is rarely the best. Consider the cost of a breach—your brand, reputation, and sensitive data could all be at risk. How much would you pay to protect your intellectual property, your company's "secret sauce"? The value of that protection is incalculable.

  Security solutions must evolve, ensuring the ability to mitigate zero-day malware. The real question isn't about price—it's about whether your current security measures can provide the peace of mind that your organization is fully protected.

Real World Examples

Let's consider two scenarios: (1) a legacy enterprise network without SASE and (2) that same network transformed with the power of SASE.

1. Legacy Network: Please see the network diagram below. This diagram is a composite of several real-life legacy networks observed over the years.



This is a complicated diagram. Simplifying it, let's go over what we see:

- **Mobile Users:** Thousands of mobile users, spanning North America, Europe, and Asia, rely on client VPN to connect to the Boston HQ and Penn data center for access to private applications and remote desktops. With average latencies ranging from 70ms (California) to 300ms (Asia), backhauling these connections causes delays. While most users are trusted employees, some are external contractors. At home, users access the Internet without restrictions, and their traffic is often ignored by administrators after connection, further complicating security and performance.

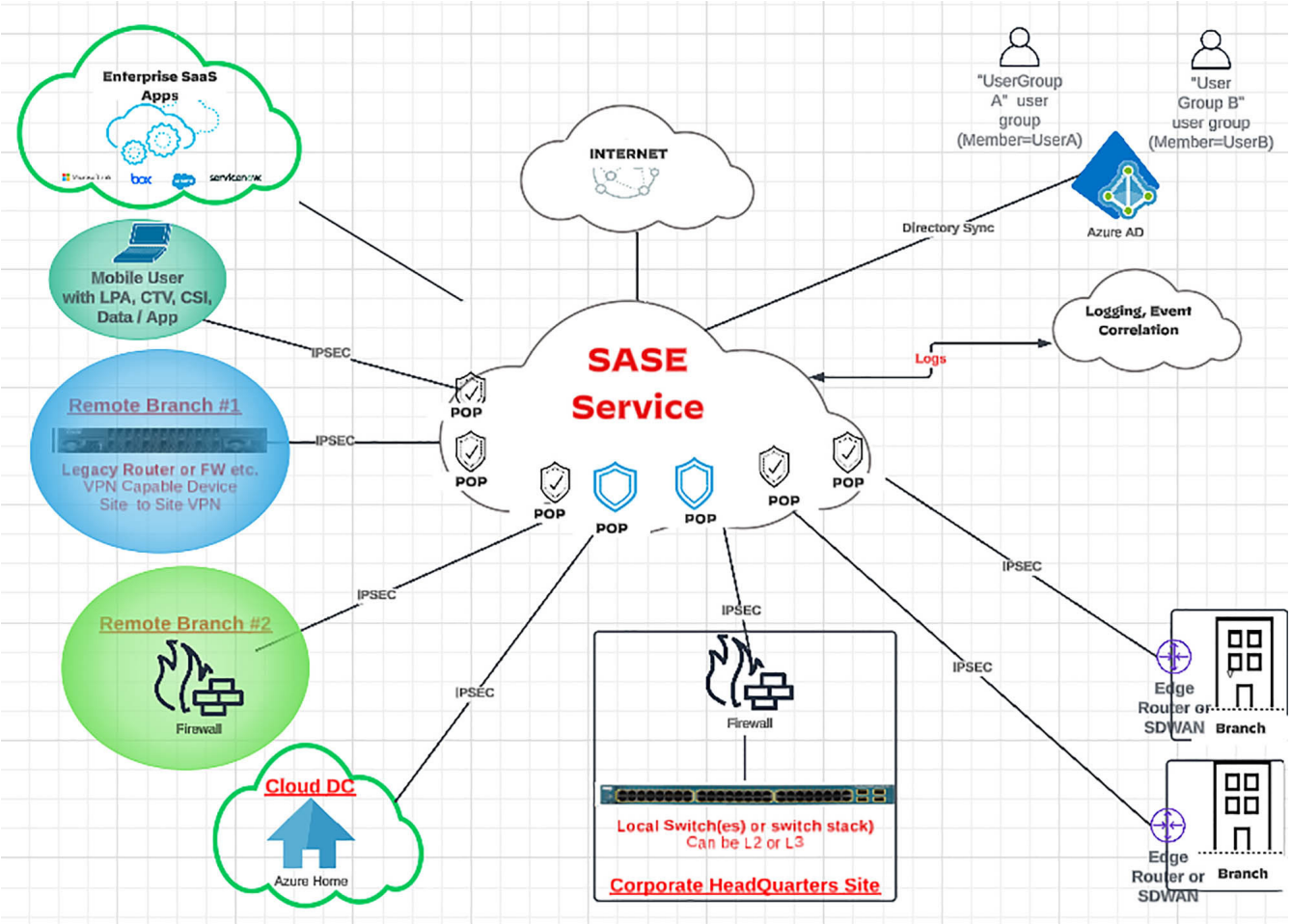
1. Legacy Network, continued:

- **Branches:** Branch users connect to the Internet via their local ISP. Two branches have NGFW (UK, Pakistan). Several branches either connect to the Internet via routers or legacy firewalls (China, India, Africa, Brazil). All branches connect back to the Boston and Penn sites via expensive MPLS connections. The global MPLS contract expires in 8 months. The company is trying to decide whether or not to keep MPLS. Several branches will be going away soon. All users at those branches will become mobile users. Branches connect to each other via site to site VPN if MPLS is down. Certain branches have full legacy SD-WAN connectivity to each other if MPLS is down, but they do not have backup connections to other branches. All branches backhaul connections to Boston and Penn sites, causing latency.
- **SaaS Applications:** All users (mobile users, branch users, Boston users, Penn servers) connect to the Internet via their local ISP. Consequently, they connect to their public SaaS applications via their local ISP as well. Most of the company's intellectual property is "housed" within these SAAS applications with no security and no visibility into who is accessing what.
- Is there next-gen L3 through L7 security? Very little in this environment.

Now, let's briefly dive into the issues with this network:

- Many different types of WAN edge devices at each branch. This is a cobbled WAN with no consistent WAN backup link strategy. Admins manage each device one by one, causing inconsistent security policies and complications leading to human error. When branches reach other branches (moving East-West), they do so mostly without firewall enforcement, meaning that a malware outbreak will be allowed to happen.
- Branches and mobile users backhaul connections to Boston and Penn. This causes network-wide latency.
- Branch WAN edge devices do not have the capability to route applications over specific links or apply QOS (quality of service) or any other type of priority based on mission critical or latency sensitive applications
- Branches connect to each other via MPLS. MPLS is an expensive legacy WAN technology. Further, branches could be connecting to each other using both MPLS links and Internet links, bonding both links together. Thus, there are expensive WAN links and very little security.
- Mobile users are allowed to connect to any resource on the Internet, to any branch and to any SaaS application. This is "allow and ignore". This is a security breach waiting to happen!
- Each branch, data center, HQ, user desktop is a perimeter. Perimeters expanding out of control. There is no inline security inspection.
- If there is intermittent latency when accessing a SAAS application, it can be impossible to triangulate the root cause due to lack of user and application visibility.
- There is a long overdue, dire need for WAN transformation and ubiquitous next-gen L3 through L7 security with SaaS security and ZTNA 2.0

2. The Same Network Transformed With SASE: This is the same network as above transformed with SASE. Please see the network diagram below.



- **Site-to-site VPN and WAN Transformation with SD-WAN:** Backhauling site-to-site traffic is eliminated completely as all site-to-site traffic traverses the SASE service. Combining multiple WAN "underlay" links (ex. Internet and MPLS links, secondary and tertiary Internet links) as primary and secondary "overlay" paths while prioritizing mission critical and latency sensitive applications. Eventually, admins can remove expensive WAN links, replacing them with more cost effective links. All site-to-site WAN traffic traverses the FWaaS feature of the SASE service, preventing East-West malware outbreaks.
- **Mobile User Transformation:** The SASE service is local to each mobile user within their geographic region. This eliminates backhauling of mobile user connections to a regional HQ. Mobile user desktops are posture checked to ensure that they are trusted devices with software updated to certain patch levels, etc. Mobile users are authenticated, via a central user database, then challenged with "two-factor" authentication. Mobile user traffic to branches/data centers/Internet traverses the FWaaS, keeping mobile user traffic secured. Mobile users are segmented such that certain user groups can access certain applications while other user groups can access other applications but not applications used by another user group, etc.

2. The Same Network Transformed With SASE, continued:

- **ZTNA 2.0** provides advanced security features, including least privilege access, continuous trust verification, continuous security inspection, and protection for all data and applications across any protocol. Key components may include zero-day malware Prevention, FWaaS, SWG, Explicit Proxy (optional, depending on the vendor), CASB, and support for both client and clientless VPNs. While some features like Explicit Proxy are not mandatory for SASE, they are valuable additions.
- **Scalable SSL/TLS Decryption:** For your environment, globally, without risk of oversubscription!
- **Operational Efficacy, via One Management Console:** Your environment GLOBALLY and local everywhere. Elastic, scalable, redundant, and five 9s uptime.
- **Visibility with DEM:** To help organizations monitor and improve application and user experience with the ability to triage packet loss, jitter, delay and latency for each user accessing each application while traversing the SASE service by monitoring each application session, testing performance and collecting data to be used to triage issues.
- **SaaS Security with CASB and DLP:** Protection of SaaS applications from cyber threats/application posture/identity based application security/data governance. Sanctioning certain applications. Blacklisting unsanctioned applications. Tolerating certain applications. Inspection for data at rest, data in motion (upload/download), remediation of misconfigured security settings in sanctioned applications via continuous monitoring. Detailed application use analytics and visibility. Enforcement of who gets access to what data. DLP (data loss prevention) to prevent intellectual property from being accessed by unauthorized users/data discovery/who owns the data and policy for that data, who will get in trouble if that data is leaked? How is the data classified?
- **Security for All Applications:** Safeguarding all applications (not just web-based or DNS based applications) used across the enterprise, including modern cloud-native applications, legacy private applications and SaaS applications. This includes applications using dynamic ports and applications that leverage server-initiated connections.

Help Is Here With WEI

SASE offers a unified service that addresses multiple network and security challenges. Key features include:

- **FWaaS:** Secures traffic for mobile users, branches, and data centers across all destinations (e.g., branch-to-branch, branch-to-Internet, mobile user-to-data center). It prevents both known and unknown malware outbreaks.
- **SD-WAN Integration:** Ensures optimal application prioritization and seamless WAN transformation.
- **CASB and SaaS Security with DLP:** Protects sensitive data in SaaS applications while providing full visibility into all traffic.
- **Digital Experience Management (DEM):** Offers real-time traffic monitoring to ensure a high-quality user experience.

This single, cloud-delivered service can replace multiple appliances and point products. With ZTNA 2.0 built in, it delivers scalable, global security and is easily managed through a single GUI. SASE unifies your security perimeter, transforming your network while addressing and preventing security issues on a global scale.

SASE transitions your network from legacy technologies of the 1990s through the early 2020s to a cutting-edge, ZTNA 2.0-enabled framework. It's the evolution of "Networking and Security 2.0," designed to achieve WAN transformation and enterprise-grade security—not just connectivity.

However, simply establishing access to a SASE service is not enough. Many network and security engineers mistakenly stop after setting up basic connectivity and a few firewall rules, considering the job done. This approach is wrong. Connectivity is merely the starting point of your journey to fully leveraging ZTNA 2.0.

Leveraging the "Service Edge": Deploying the "Secure Access" part of SASE is just the beginning—you've reached base camp, but the summit still awaits. To truly protect your network, you must maximize the "Service Edge" functionality of SASE, which safeguards data, assets, applications, and services (DAAS). Achieving full protection requires systematically consuming and integrating the Service Edge features necessary for your environment.

Remember, trust itself is a vulnerability. Protecting your enterprise requires ongoing effort and continuous improvement.

Don't Overlook SaaS Security and DLP: One critical component of ZTNA 2.0 is securing users, applications, and data. Ignoring SaaS security or delaying DLP implementation is a mistake. Properly deployed, these features will protect your environment without causing interruptions. To achieve ZTNA 2.0, leverage all available tools to secure your users and their data.

Consider SASE With WEI

If your organization is facing challenges like geographically dispersed mobile users, inconsistent security postures, or expanding attack surfaces, it's time to consider SASE. For companies relying on a lenient "allow and ignore" approach to user traffic but wanting stricter authentication, posture checks, and tighter mobile security, SASE provides a robust solution. It also addresses the need for secure yet limited access for contractors, ensuring external users only access what they need without compromising the broader network.

Organizations with multiple branches, data centers, and HQ locations that backhaul traffic can benefit from SASE's WAN transformation capabilities, including micro-segmentation for east-west security across the WAN. Whether your business is experiencing rapid growth in users and locations or sporadic, elastic growth, SASE's scalability supports your evolving needs. Even as offices downsize and mobile users increase, SASE ensures application security remains a priority.

Talk to WEI today

For organizations without a consistent security posture or strategy across their environments, SASE offers a way to standardize protections and secure SaaS applications with complete visibility into user and application traffic. It is also ideal for organizations struggling to manage an expanding attack surface or striving to adopt a ZTNA 2.0 security posture. With SASE, these challenges are no longer roadblocks but opportunities to modernize and secure your network.

Contact the WEI cybersecurity team to learn more about SASE and why it could make sense for your business operations.

Sources:

1. IDG Research commissioned by WEI, January 2021.

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.