INSIGHTS | TECH BRIEF

Faster Cloud Migration, Stronger Security: SASE for a Better UX

Cloud migration is a top priority for enterprises, but traditional network security models were never designed to support cloud-based applications. Organizations still relying on VPNs, MPLS, and legacy firewalls face operational challenges, increased costs, and security blind spots. As cloud adoption grows, IT leaders must rethink how they secure and connect users to critical applications.

Secure Access Service Edge (SASE) provides a modern approach by combining network and security functions into a cloud-delivered architecture. This model eliminates outdated dependencies, allowing users to securely access cloud applications without relying on traditional data center routing. The result is a more effective security posture, cost savings, and a better experience for employees—whether they work on-premises, remotely, or from mobile devices. This tech brief will cover:

- How legacy network security models create challenges for cloud migration.
- How SASE removes these obstacles by providing direct, secure access to cloud applications.
- The business and security benefits of adopting SASE in a cloud-first IT strategy.
- A common use case that illustrates the challenges enterprises face and how SASE provides a solution.

The Challenges of Cloud Migration with Legacy Network Security

Dependence on Centralized Data Centers: Many enterprises built their security and network models around the idea that all applications and users should connect through a central data center. This approach worked when applications were hosted on-premises, but as workloads move to the cloud, backhauling traffic through data centers introduces performance issues and unnecessary complexity.

A common challenge is that remote users must connect via VPNs to reach both private cloud applications and SaaS platforms like Office 365 or ServiceNow. This results in:

WEI's Approach To Cyber Assessments:

Practical & Proactive

WEI takes a holistic, risk-based approach to cybersecurity, integrating people, processes, and technology to build a defense strategy that addresses every layer of risk. Our methodology ensures proactive, adaptable security measures tailored to your organization's unique challenges.

STRATEGIC SECURITY SERVICES

- Strategy Development & Analysis
- Maturity Assessments

SECURITY COMPETENCIES

- Cyber Security Strategy
- Cloud Security
- SIEM & SOAR Orchestration
- Policy Framework
- Incident Response
- Vulnerability Management

Learn more about WEI Cybersecurity

- Slower application performance due to unnecessary routing through the corporate network.
- Increased costs from maintaining MPLS circuits that are no longer necessary.
- Security gaps when employees bypass VPNs to access SaaS applications directly, leaving corporate policies unenforced.

Fragmented Security Tools: Enterprises often rely on multiple security solutions, including firewalls, intrusion detection systems (IDS), VPN concentrators, and CASB platforms. These tools were built for different architectures and require complex integrations to function together. Managing these disjointed systems increases administrative workload and can create coverage gaps in security policies.

Security Risks in Cloud Access: When applications move to the cloud, traditional security measures—like internal firewalls—lose effectiveness. Enterprises struggle with:

- Lack of control over data movement between SaaS applications.
- Shadow IT risks as employees use unauthorized cloud services without security oversight.
- User experience (UX) challenges, where employees drop VPN connections to avoid slow performance, bypassing security controls in the process.

A Common Use Case

A challenge in enterprise environments is managing secure access to cloud applications while maintaining strong security controls. Many organizations have built their security stack around a mix of separate firewall appliances, URL filtering solutions, and CASB platforms. As remote workforces expand and cloud applications replace on-premise software, IT leaders face:

- Increasing VPN usage leading to poor performance.
- Complex cyber management across multiple tools.
- Rising networking costs, particularly with MPLS circuits.
- Gaps in security enforcement as users bypass VPNs for direct SaaS access.

How SASE Solves Cloud Migration Security & Access Challenges: SASE was designed to address the disconnect between traditional security models and modern cloud requirements. It shifts security enforcement from data centers to a globally distributed cloud-based infrastructure, applying security controls closer to the user.

Removing Legacy Bottlenecks: With SASE, enterprises no longer need to route all traffic through a data center. Instead, users connect to the nearest SASE enforcement point, which provides:

- Direct-to-cloud access for SaaS applications without requiring VPNs.
- SD-WAN integration to optimize performance and reduce dependence on MPLS.
- Consistent security policies applied no matter where a user connects from.

Stronger Security Model for Cloud Applications: SASE brings together multiple security technologies into a single framework, reducing complexity while improving control over cloud applications. These include:

- Zero Trust Network Access (ZTNA): Ensures users and devices are verified before being granted access.
- Cloud Access Security Broker (CASB): Monitors and controls data movement in SaaS applications.
- Firewall-as-a-Service (FWaaS) & Secure Web Gateway (SWG): Inspects traffic at cloud enforcement points, blocking threats before they reach the user.

Optimizing Access for Hybrid and Remote Workforces: A modern security model should support users wherever they are. SASE enables this by:

- Providing secure access without requiring VPNs, reducing friction for employees.
- Applying security controls to all traffic, even when users connect directly to SaaS applications.
- Ensuring reliable performance by routing traffic through optimized cloud enforcement points instead of forcing backhaul to the data center.

Many enterprises are transitioning to SASE to address these challenges. By implementing a cloud-delivered security model, organizations have:

- Eliminated reliance on VPNs, improving both security and user experience.
- Consolidated security tools, reducing the number of separate platforms IT needed to manage.
- Lowered networking costs by reducing MPLS usage and adopting a cloud-first security model.
- Achieved consistent security enforcement, even for remote users accessing cloud applications directly.

Business & Security Benefits of SASE for Cloud Migration

Better Experience for End Users: Employees benefit from improved performance and easier access to applications. Since security policies are enforced in the cloud, users don't have to remember when to connect to a VPN or worry about slow application performance.

Faster Adoption of Cloud Applications: By removing the need for data center-based security enforcement, SASE allows organizations to migrate workloads to the cloud without disrupting access or security. Users connect securely to applications regardless of where they are hosted.

Stronger Security with Simplified Management: Instead of managing multiple security tools separately, SASE unifies them into a single platform. This provides:

- A consistent security policy across all cloud and on-prem applications.
- A centralized point of control, reducing operational burden.
- The ability to enforce Zero Trust security models without adding complexity.

Cost Savings: SASE eliminates the need for expensive networking infrastructure, including:

- MPLS circuits that are no longer necessary.
- Redundant VPN concentrators.
- Standalone CASB and firewall solutions.

Next Steps: How WEI Can Help

WEI has extensive experience helping organizations transition from fragmented, on-premises security frameworks to modern, cloud-first architectures. Our cybersecurity solution architects work closely with IT leaders to assess their current environment, identify security gaps, and design a tailored SASE strategy that aligns with business objectives. WEI's approach includes:

- **Performance & User Experience Optimization:** Our experts ensure that security enforcement does not create bottlenecks for end users, allowing for faster, more reliable access to cloud applications.
- **Security & Network Architecture Assessments:** We analyze your existing security stack, VPN usage, and cloud access strategy to identify inefficiencies and risks.
- **Custom SASE Design & Implementation:** Our team develops a plan for deploying SASE in a way that integrates with existing cloud migration initiatives.
- **Zero Trust & Cloud Security Integration:** We ensure that your organization enforces consistent access policies across cloud and on-premise environments using Zero Trust principles.
- **Cost Optimization & Vendor Consolidation:** Many enterprises struggle with multiple security tools that don't integrate well. WEI helps consolidate disparate security functions into a unified SASE framework—reducing costs while improving security oversight.

Get Started with WEI

WEI's cybersecurity architects have worked with enterprises across various industries to modernize their security infrastructure while maintaining compliance with industry regulations. We understand the operational, financial, and security challenges involved in cloud migration, and we provide hands-on support throughout the entire transition.

If your organization is evaluating cloud migration or struggling with outdated security models, WEI can help you navigate the complexities of SASE adoption. Contact our team today to schedule a security assessment and discuss how a cloud-delivered security framework can support your business objectives.

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.