Secure Access Service Edge (SASE)

The shift to migrate data and applications to the cloud provides clear benefits such as lower cost, improved performance, and enhanced agility but also presents a set of unique challenges. Legacy architectures slow down the business, the visibility of threats becomes limited and complex ecosystems of security can be overwhelming and costly to manage. Secure Access Service Edge is a model that provides the right path for many organizations to modernize their enterprise for security, speed, growth, and cost reductions. Accenture and Palo Alto Networks have defined four ways organizations can embrace digital transformation and deliver cybersecurity success with SASE.
Moving Your Organization Confidently into the Future with Secure Access Service Edge (SASE)

Networking and security infrastructures are the backbone of technology for all organizations. Yet, business leaders all too often overlook the impact IT architecture has on their ability to drive the business, become nimble, operate seamlessly, reduce complexity, and mitigate risk.

In recent years, there has been a large shift to migrate data and applications to the cloud based on benefits such as lower cost, improved performance, and enhanced agility. However, this move from enterprise data centers to the cloud brings unique challenges:

1. **Legacy architectures slow down the business:** Existing network approaches and technologies cannot provide the performance needed for the workforce dynamics of today. Traffic patterns have changed, and the way data moves through the network does not address today’s application consumption needs. Enterprises must be able to deliver uninterrupted access for their users, wherever they may be around the globe, without sacrificing cybersecurity.

2. **Moving data and applications to the cloud limits visibility:** Securing data and applications in the cloud requires organizations to have complete visibility of risks and threats – specifically, visibility to traffic at rest, in transit, and in the cloud. With increased remote use, software-as-a-service (SaaS) applications, data in the cloud and traffic going to the public cloud, it becomes more difficult to track and to ensure consistently enforced security controls. This emphasizes the need for deeper visibility and control – and the need to introduce efficiencies to reduce operational cost.

3. **Inherent complexities can be overwhelming and costly to manage:** Enterprises are struggling to manage highly complex ecosystems, due to a plethora of security and networking tools. These complexities often result in misconfigurations and gaps in security. The lack of efficiencies tied to integrating these solutions makes it difficult and expensive to manage, with little visibility to application context and performance.

In an evolving business environment, change is inevitable

To stay competitive, organizations must decide how to respond and navigate transformations around business support systems, data centers, cyber security, remote workers, data, analytics and maturing technologies such as artificial intelligence and machine learning. While this path can be daunting, inaction is not an option. The time to move is now.

---

Cybersecurity and innovation must go hand in hand: 71 percent of executives surveyed said cybersecurity concerns are impeding digital innovation, with a full 75 percent admitting their IT spend isn’t aligned with business growth.

---

**Start with a strong foundation: SASE**

Secure Access Service Edge is a service model that provides the right path for many organizations to modernize their enterprise for security, speed, growth, and cost reductions: The SASE service model can reduce costs (by as much as 40 percent²), increase application performance and improve user experiences, while reducing complexity.

These advantages illustrate why SASE is a transformation enabler and accelerator, helping companies create new business models and platforms that can generate revenue from new products and services. It frees us from the constraints of legacy systems and enables companies to securely embrace a cloud and mobile-driven world. It also saves organizations from making a potentially fatal mistake: shifting their problems from the data center to the cloud.

Prior to the evolution of SASE technologies, organizations were forced to choose between performance, security, and cost, often having to optimize for a single factor. This ultimately hampered speed to market. Leveraging the SASE service model removes that need for compromise and allows the business to grow securely, while lowering operational cost.

**What is SASE, exactly?**

Digital transformation and adoption of mobile, cloud and edge deployment models have fundamentally changed the way traffic moves on the network, relegating the network as we know it today to true ‘legacy’ status. SASE offers all the benefits of as-a-service cloud-hosted delivery, including plug-and-play implementation, fast optimization, scalability, lower total cost of ownership, and hands-free upgrades and maintenance. Instead of considering mobile access, cloud access, and site access as separate issues, SASE puts it all into a single global solution. With this service model, businesses no longer need multiple security policies. There is one policy — for protecting against network-based threats.

In essence, SASE is the convergence of wide area networking (WAN) and network security services like CASB, FWaaS and Zero Trust, into a single, cloud-delivered service model. As described by Gartner, it provides cloud-delivered, identity driven, any device/anywhere access by converging networking and security services into one unified, cloud-delivered solution. See Figure 1.
**Why it’s different**

SASE is different (and better) because it focuses on the user, rather than the modus operandi of legacy systems of yesterday (and, unfortunately for many, today). It does this by helping organizations become:

- **Identity-driven**: Employing a least-privileged, Zero Trust methodology and enabling the strict enforcement of access control, SASE enables interactions to be controlled within all resources, based on attributes such as application access, user and group identities and the sensitivity of all data. It makes security pervasive.

- **Cloud-based**: As a cloud-native architecture and platform, SASE embeds the agile, holistic, adaptive, self-updating and secure capabilities of cloud without the need to maintain on-premise infrastructure. It is an efficient, flexible and easily adaptable way to serve all business needs regardless of location.

- **Streamlined**: SASE includes the delivery of networking and security services for traffic directed to the internet, cloud applications and/or the data center with faster provisioning of new services. This means, for example, that SD-WAN appliances support physical network edges (i.e., branch offices) while mobile clients and clientless browser access gives users on-the-go secure access to the internet.

- **Globally distributed**: With true low-latency service to all enterprise network edges, SASE makes the theory of global work and distribution a productivity-enhancing reality.

**The Benefits**

The SASE service model offers three key benefits:

1. **Rapid transformation**: Critical business applications are increasingly SaaS and cloud-hosted, estimated to account for 80 percent of enterprise applications by 2022. In addition, networks are rapidly becoming, by necessity, perimeter-less, to give users secure access to cloud-based applications from any location. SASE eliminates the need for appliances to support separate security and networking stacks and simplifies management of the infrastructure. With cloud-based services from diverse geographical locations replacing slow, expensive MPLS networks with SASE’s SD-WAN (anticipated to increase by 168 percent over the next five years) secure network access will improve dramatically. As a result, employees can work unencumbered by network latency, securely accessing the tools and information they need.

---

With the number of devices connected to the Internet exploding – IDC forecasts up to 41.6 billion by 2025 – a prevention-based architecture with a Next Generation Firewall can simplify security and deliver consistency with complete visibility.
2. **Enhanced security**: To improve security within the enterprise, organizations must increase end-to-end visibility. The average large enterprise is trying to manage as many as 130 separate security tools, including aging and slow virtual private networks (VPNs). In this scenario, it’s easy to see that the risk can increase exponentially. SASE’s simplicity enhances security by providing visibility across the entire environment, delivering fully integrated, high performance, all-in-one security policies that eliminate gaps and redundancies.

3. **Immediate and continuing savings**: Reducing the number of vendors, tools, and technology stacks means SASE can save organizations up to 40 percent of their current WAN budgets allocated to security and network access. By laying the foundation for stronger cybersecurity, it can also provide significant operational cost and incident-avoidance ROI. SASE also provides the flexibility to easily spin up or down a remote office/branch, aligning technology and security with business cycles.

**Four keys to transformation**

Accenture has defined four ways organizations can embrace digital transformation and deliver cybersecurity success with SASE. While each is important, all four can be addressed at once or they can be approached uniquely. This flexible, step-by-step, meet-an-organization-where-it-now-stands approach helps tremendously regarding budget, leadership buy-in and laying a proven foundation for success.

1. The foundation for a digital transformation is migrating to a secure virtualized private cloud, based on a Zero Trust methodology, to further secure business assets.
2. This is followed by network consolidation and optimization to align assets with business needs.
3. Now the stage is set for secure network modernization with visibility and simplification of the network. This paves the way for automation to expand business services.
4. This is when organizations are truly ready to leverage SASE, while also gaining business agility through analytics and automation.

**Quantifying the ROI of cybersecurity**

New Accenture methodology enables organizations to make far more informed decisions about the benefits of their investments in cybersecurity. For example, when Accenture calculated the costs vs. risk reduction associated with adding user activity logging, the mitigation ROI was calculated at 356 percent. (See the graphic below for sample security risk ROI estimates).

**Prioritized Recommendation Details for Strategic Cyber Risk Management**

<table>
<thead>
<tr>
<th>Business Application</th>
<th>Control Recommendation</th>
<th>Change in P(L)</th>
<th>Risk Reduction</th>
<th>Cost to Implement</th>
<th>Mitigation ROI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Line #1 Applications</td>
<td>Add Hardware token based authentication</td>
<td>-3.77%</td>
<td>$4.7M</td>
<td>$2M</td>
<td>135%</td>
</tr>
<tr>
<td>Product Line #1 Applications</td>
<td>Add Software token based authentication</td>
<td>-1.55%</td>
<td>$1.93M</td>
<td>$500k</td>
<td>286%</td>
</tr>
<tr>
<td>Product Line #1 Applications</td>
<td>Add Biometric authentication</td>
<td>-1.55%</td>
<td>$1.93M</td>
<td>$1.5M</td>
<td>29%</td>
</tr>
<tr>
<td>Product Line #1 Applications</td>
<td>Add automatic log monitoring</td>
<td>-1.37%</td>
<td>$1.71M</td>
<td>$500k</td>
<td>242%</td>
</tr>
<tr>
<td>Product Line #1 Applications</td>
<td>Add logging of user activity</td>
<td>-0.91%</td>
<td>$1.14M</td>
<td>$250k</td>
<td>356%</td>
</tr>
</tbody>
</table>

- The table above outlines the top recommendations output from Risk Quantification
- Risk reductions are created by computing the change in P(L) that controls effect
- That change is applied to the expected loss, which is used to calculate ROI

At least 40 percent of enterprises will have explicit strategies to adopt SASE by 2024, up from less than 1 percent at year-end 2018.
How to get started
Gartner calls upon security leaders to embrace the Continuous Adaptive Risk and Trust Assessment (CARTA) strategic approach. An initial step in implementing CARTA is adopting Zero-Trust. We can help you get started by assessing the readiness of your environment to adopt a Zero Trust strategy and start your journey to enabling an easier control of users, data and devices traversing your networks. To schedule your assessment and learn how Palo Alto Networks and Accenture can help you to drive transformation in your organization, reach out to accenture@paloaltonetworks.com.

About the authors
This whitepaper was jointly developed by Palo Alto Networks and Accenture Security. Working through a strategic partnership, Palo Alto Networks and Accenture Security offer multiple solutions around and beyond SASE: Cybersecurity, Managed Security Services, Network Optimization and Transformation Services, Security Operations & Optimization Services, Compliance Strategy/Risk management, Endpoint Security and Network Transformation.

About Accenture
Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries — powered by the world’s largest network of Advanced Technology and Intelligent Operations centers. With 513,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at www.accenture.com.

About Palo Alto Networks
Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world’s greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

References:
3. https://www.idc.com/getdoc.jsp?containerId=prUS45213219#:~:text=18%20Jun%202019-,The%20Growth%20in%20Connected%20IoT%20Devices%20is%20Expected%20to%20Generate%2D3.2%20billion%20in%202025
5. https://www.bbcmag.com/breaking-news/sd-wan-market—expected—to-increase—168—percent—by—2024#:~:text=REDWOOD%20CITY%2C%20CA%20-%20%20%E2%80%94%20The%20worldwide%20market%20is%20expected%20to%20surpass%20%2431.2%20billion%20in%202024