GUIDE

How to Implement Secure Access Service Edge (SASE) in 6 Steps

Combine Networking and Security Capabilities for Better Protection – Without Sacrificing Performance

“I don’t need another security tool.”

This is a common refrain from both IT and security leaders. And it makes sense when you consider that many large enterprises today have over 130 security tools.[1] This reality creates a challenge, both in managing and optimizing these siloed systems — not to mention trying to correlate them into a single risk rating.

According to Gartner and many global CISOs, the answer to this excessive proliferation is consolidation. Enterprises need tools that can be integrated to work together seamlessly, rather than deploying individual solutions that meet one-off requirements.

Gartner’s secure access service edge (SASE) framework outlines the convergence of networking and security capabilities to create an effective and secure edge. The cybersecurity concept emphasizes the need for vendor rationalization to reduce complexity while increasing visibility and ease of management.

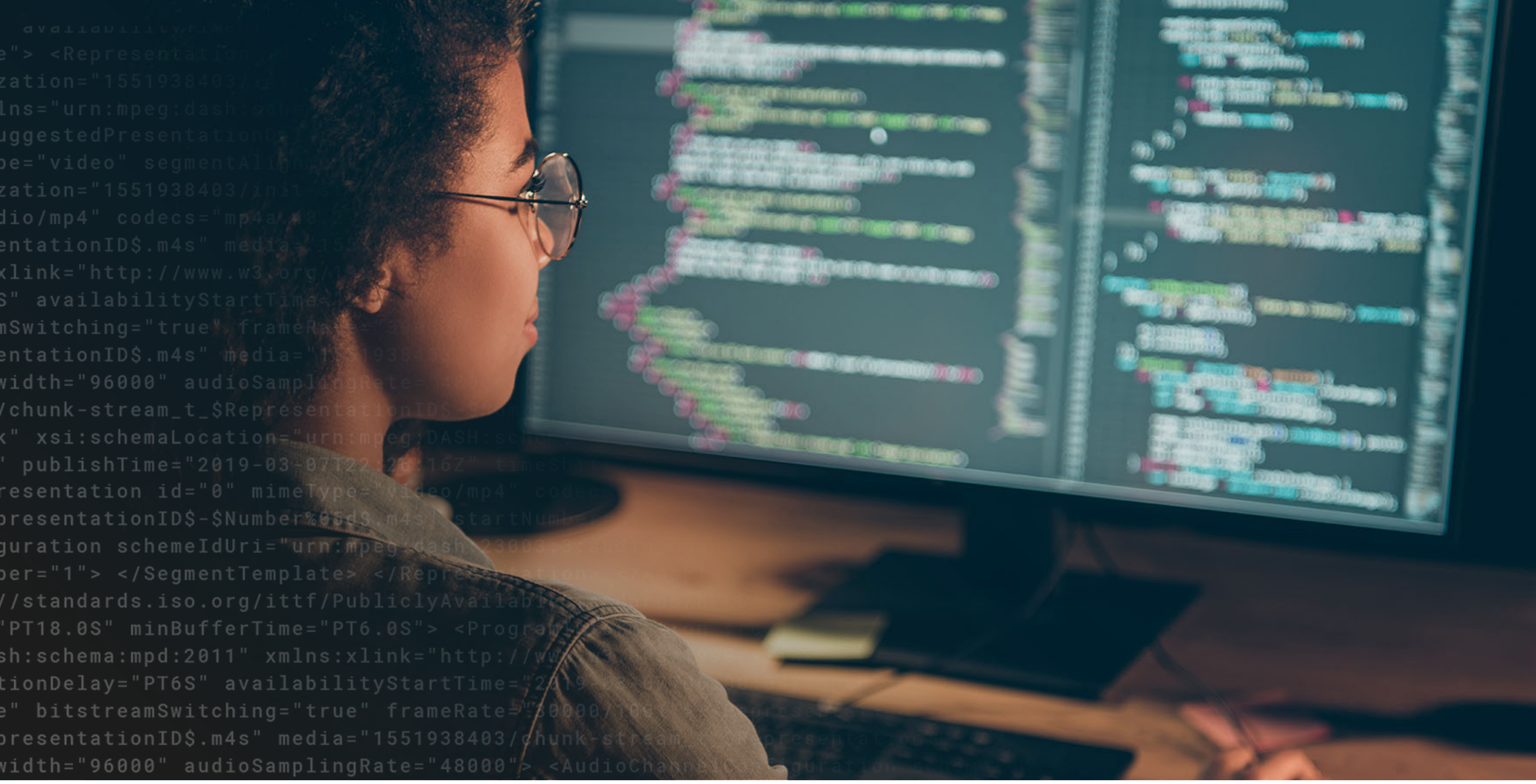
> The quantity of security products utilized does not equate to safety. In fact, these tools may be working to do the opposite. **Over 70% of CISOs admit they don’t evaluate security tools based on how effectively they reduce cyber risk.** And 36% report that their security team is sidelined by manual efforts.[2]

The Benefits of SASE

The goal of integrating these networking (performance) and security (protection) capabilities, ideally in one vendor platform, is to help organizations address changes like the move to cloud applications and a distributed and mobile workforce. Here are some of the key benefits of transitioning to a SASE architecture:

- **Enable New Digital Business Scenarios** for users, devices, applications, data, and services located outside the corporate enterprise
- **Improve Security** by delivering security controls as close to the user as possible, making it harder for attackers to discover and exploit corporate resources
- **Improve Global Scale and Operational Resilience** with low-latency access to users, devices, and services
- **Reduce Vendor Management Complexity and Costs** by consolidating vendors to increase visibility and ease of management
- **Enable Zero Trust** using a multitude of threat and contextual signals to establish trust and ensure secure access to internal resources and the internet
- **Increase Effectiveness of Network and Network Security Staff** by reducing friction to secure the network without degrading performance

> “Having one vendor for endpoints, one for network/incident response, and one for the edge is a great start, providing the most return on investment.
>
> **Steve Winterfeld**
> Sr. Director, Security Technology and Strategy, Akamai



How to Implement SASE in 6 Steps

1. Define your edge

Depending on your architecture, you may still need network infrastructure, but most enterprises are moving to edge compute. Companies may be organized around thin or heavy branches, others will be cloud native or heavy cloud. Regardless, you need to define the edge and what you want to move to. Some services may still need to be delivered locally (SD-WAN), but the trend is to move to mature SASE offerings with services hosted on the edge. How you view your boundaries will determine which tools you need for your strategy.

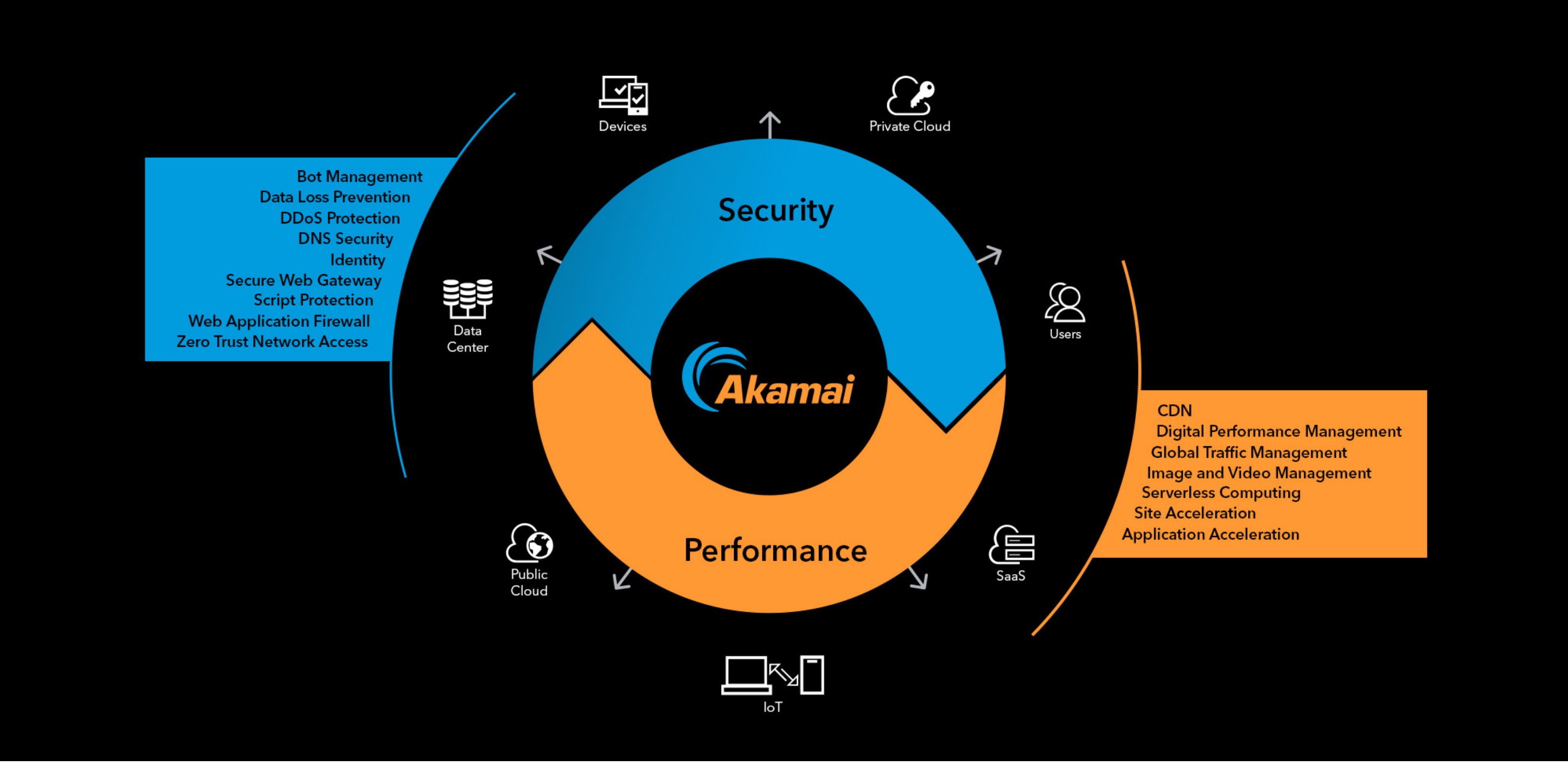
2. Determine which capabilities are critical

It is important to note that SASE doesn't present one standard set of tools but rather a framework on how to think about defending the edge. Every organization will need to assess which specific capabilities they need for both network as a service (NaaS) and network security as a service (NSaaS). Gartner's SASE framework lists a number of different capabilities, but that list is not comprehensive. For example, some newer threats require the addition of tools to protect JavaScript environments that are now facing skimmer attacks by groups like Magecart.

Additionally, if you want to build a unified edge strategy for both employees and customers, a CDN is the natural foundation networking platform. On the next page is a sample of a tailored set of capabilities from Akamai.

> Instead of the security perimeter being entombed in a box at the data center edge, the perimeter is now everywhere an enterprise needs it to be – a dynamically created, policy-based secure access service edge.
>
> **Gartner**
> The Future of Network Security Is in the Cloud; 30 August 2019; Lawrence Orans, Joe Skorupa, Neil MacDonald

Akamai Cloud-Delivered SASE



Bot Management
Data Loss Prevention
DDoS Protection
DNS Security
Identity
Secure Web Gateway
Script Protection
Web Application Firewall
Zero Trust Network Access

CDN
Digital Performance Management
Global Traffic Management
Image and Video Management
Serverless Computing
Site Acceleration
Application Acceleration

3. Conduct a gap analysis

After you have defined what you are protecting and which tools you want to integrate, it is time to conduct a gap analysis to determine where you are mature and where you will need to invest to accomplish your strategy. As part of the gap analysis, look at what features are critical for your business model. This will depend on how you enable your workforce and service your customers. This is a good time to review compliance and audit findings to see where you have mandated requirements. Finally, it is worth considering using external consultants to get a fresh perspective.

4. Define your technical debt

While you may have the networking and security systems you need for your strategy, it is important to analyze the maturity and effectiveness of those systems. Some tools might have been purchased to solve a specific issue, but haven't been optimized to fully make use of capabilities or integrated with other systems. Other tools may be customized and locked into out-of-date versions or simply behind in updates. Issues like this can contribute to "security debt"– buildup of application and infrastructure vulnerabilities in a company's IT environment that can increase the odds of a breach. One of the primary causes for this security debt is limited resources, like one engineer being responsible for maintaining multiple, disparate systems.

One in three system breaches is caused by unpatched systems.[3]

5. Plan out the phases for your transition to SASE

For most companies, the transition to SASE will be a multiphase journey. It may include moving away from individual point solutions as they age out. It is important to review your gap analysis and consider which risks need to be prioritized first. For example, if your DNS infrastructure or JavaScript environment is not protected, that is the right place to start. If you have an established program and are looking to mature it, there are some natural areas to focus on first.

- Gartner recommends that Zero Trust Network Access (ZTNA) should be the starting place for SASE implementation, as it allows for application-level access versus full network access. In the long term, it is a better approach for a distributed workforce and is the next-generation framework to focus on reducing lateral movement, security risk, and known vulnerabilities. ZTNA solutions can provide security where it is needed to meet the needs of modern business – at the edge. A CDN delivery model for ZTNA further extends protection across the core, to the cloud, and to the edge.

- The next recommended phase for most companies is a secure web gateway (SWG) and cloud access security broker (CASB). This brings up a natural challenge, as there are no SASE providers that offer all of the solutions mentioned, so it is important to look at vendors with a broad set of capabilities and integrated partners to meet your strategic goals. A SWG that is cloud based and integrated into the edge provides a better option than trying to adapt a legacy system. Look for SWGs that include capabilities like data loss prevention (DLP) and sandboxing.

- Finally, these solutions should be built on foundational capabilities like web application and API protection as a service (WAAPaaS), DNS security, and DDoS protections. While many organizations have these capabilities today, they are likely not on a single platform, which introduces complexity. Finding a platform that can support these capabilities along with ZTNA and SWG helps reduce complexity and cost.

> By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.
>
> **Gartner**
> Hype Cycle for Enterprise Networking, 2020; 8 July 2020; Andrew Lerner, Danellie Young

6. Get buy-in from key stakeholders

When building out a business case for the budget, focus on the fact that consolidating vendors with SASE reduces both complexity and cost. Additionally, having an industry-analyst-supported model like SASE provides validation, proven resources, and specialists to consult with – all of which should give the board more confidence in your security strategy.

Take these six steps to develop an integrated performance and security strategy. Then partner with Akamai – one of a small number of vendors named by Gartner as offering a SASE platform – to discuss and initiate implementation. Extend protection across your core, to the cloud, and out to the edge, minimizing risk while enabling future evolutions in business strategies that leverage the cloud with SASE.

Learn more about how to get started at akamai.com/SASE.

Sources:

1. https://biztechmagazine.com/article/2019/03/rsa-2019-most-organizations-use-too-many-cybersecurity-tools
2. https://panaseer.com/reports-papers/report/visibility-in-cybersecurity/
3. https://www.zdnet.com/google-amp/article/cybersecurity-one-in-three-breaches-are-caused-by-unpatched-vulnerabilities/