

Cheat Sheet: What is SASE and Why Should I Care?

SASE—which stands for “Secure Access Service Edge” and is pronounced “sassy”—is no less than a transformation of traditional security architecture. Companies that adopt SASE may be less likely to be breached than those that don’t. They’re also more likely to remain safe in an environment where most employees are working and accessing customer data from home. If you’re a business leader who’s focused on evading the financial consequences and reputational damage that come from enduring a data breach, you should definitely care about SASE.

Why Switch Away from “Normal” Security Architecture?

Traditional security architecture often follows what’s known as a “defense in depth” model. At the center, you have your corporate data center or server room. This comprises storage for all your customer data, employee data, and protected intellectual property, and also comprises the physical hardware for your private network—all the switches and cabling, for example.

In this traditional model, you assume that most if not all of your trusted users are sitting down at a desk that’s physically located inside a building you own, using a computer that’s physically connected to the data center inside your building. As such, you tend to ignore the people who are logged into your network. Your focus is on preventing unauthorized parties outside your network from either logging in and stealing your files or dropping malware that can encrypt or exfiltrate data automatically.

To this end, you surround your network core with physical and software protections—network TAPS than can extract and monitor network traffic, IDS/IPS software, firewalls, malware protection, and more.

Here’s the thing: none of this architecture really takes mobile phones, the cloud, or remote work into account. Although it can be modified in order to adapt to the presence of these variables, it’s really beginning to creak. Administrators are basically in the position of adding a new solution as a patch on each new security issue—DDoS, ransomware, phishing, etc. Better to rip down the edifice and start over.

Fixing Traditional Security with SASE

Right now, the central corporate data center is present mostly as an inconvenience to employees. Most application are delivered through the public cloud, with the average enterprise now using approximately **288 SaaS apps**. If you make your users VPN into your corporate data center before accessing these apps, you put a massive brake on their productivity without adding much to their security. Many users will rebel—almost **half of employees** decide not to use VPNs before accessing corporate data via SaaS.

Therefore, SASE kills two birds with one stone:

- Aggregates all security tools into a single public cloud dashboard
- Places security in the cloud, allowing SASE to monitor all users without causing latency

In addition, SASE adds security technologies that traditional “defense in depth” architectures may omit—Zero-Trust security, Firewall as a Service (FWaaS), and Cloud Access Security Brokers (CASB).

- **Zero-Trust Security**

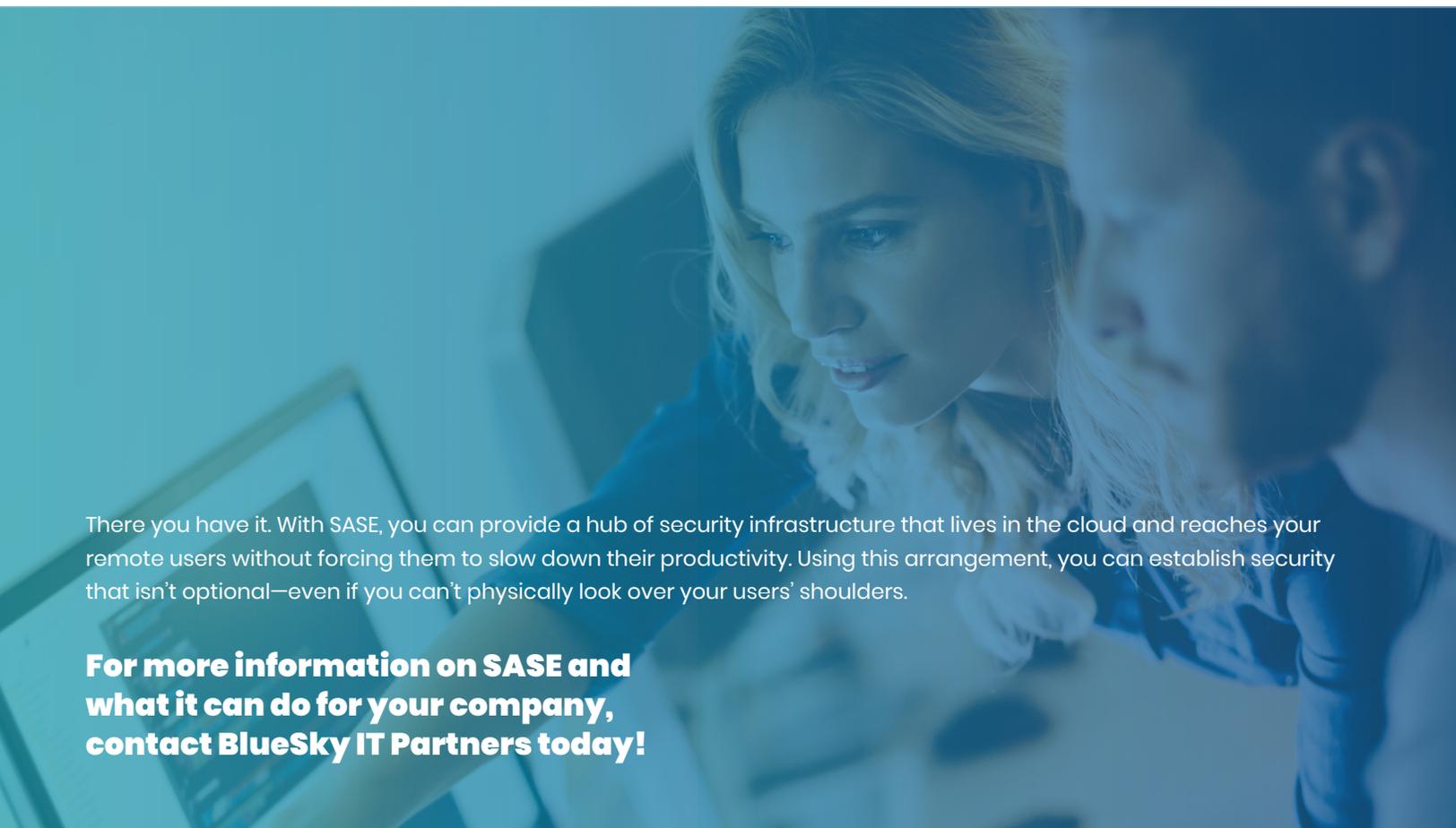
This technology is also a collection of technologies, all designed to operate under the assumption no user—whether they’re logged in or not—can be assumed not to be a malicious actor. Since credential theft and ID spoofing are two of the most common forms of attack, Zero-Trust incorporates technologies such as micro-segmentation, multi-factor authentication, and device fingerprinting to constantly validate user identities. At the end of the day, attackers are unable to perform reconnaissance on your network—and logged-in users can’t even see resources that they aren’t supposed to have access to.

- **Firewall as a Service**

Firewalls were originally delivered as physical appliances that were plugged into enterprise data centers—but this approach can no longer scale. You can’t install a hardware firewall at a remote worker’s house, for instance, nor can you install supporting applications such as IDS/IPS, threat-prevention, or URL filtering. It’s also prohibitive to backhaul user traffic to the central data center for inspection by these services. Instead, FWaaS aggregates these services together and places them in the cloud, allowing you to secure remote users at the network edge.

- **Cloud Access Security Brokers**

One weakness of the SaaS model is that users are forced to depend on the reliability of their SaaS provider as far as security is concerned. You, the user, can only make sure that no one steals your password. The provider handles everything else. With a CASB, however, you can add an extra layer of security to SaaS, PaaS, and IaaS environments. Typically, these services provide additional access controls and prevent users from accessing cloud data using unsafe devices.



There you have it. With SASE, you can provide a hub of security infrastructure that lives in the cloud and reaches your remote users without forcing them to slow down their productivity. Using this arrangement, you can establish security that isn’t optional—even if you can’t physically look over your users’ shoulders.

For more information on SASE and what it can do for your company, contact BlueSky IT Partners today!