aws marketplace

Security ebook Series

The value of a secure access service edge (SASE) model in protecting your cloud infrastructure

How SASE's cloud-native approach to security can protect today's highly distributed enterprise more effectively and efficiently

Pandemic-triggered change

The COVID-19 pandemic has dramatically changed the way businesses operate, and how and where employees work, accelerating the trend toward:

- **Highly distributed enterprise operations:** Multiple employees working in different locations, including corporate headquarters, remote and home offices, and in the field.
- **Remote work:** Employees doing their jobs in locations other than a company's central office.
- **Migration to the cloud:** Moving all or some of a company's digital workloads to a cloud infrastructure such as AWS.

Changing work environments, increasing challenges

The National Bureau of Economic Research reports that 20% of Americans are working from home full-time post-pandemic, up from just 5% pre-pandemic.[1] Zippia reports that in 2020 alone, due to the pandemic, 61% of businesses migrated their workloads to the cloud.[2] Growing trends in distributed workforces and remote work have sharply increased the challenges facing security teams that use traditional centralized security.

Latency

The model of users connecting to centralized data centers, services, and applications can introduce significant latency, which can introduce security risks—for example, by widening the gap between when a breach occurs and when the organization identifies the attack.

The need to transmit data across long distances

Distributed and remote employees are sharing more data—and for farther distances—than ever before. With increased distances and volume, data in transit risks exposure to multiple internet exchange points that process and route it as well as outside threats that blend into legitimate traffic.

Complex, multifaceted authentication processes

With employees working remotely, there's a good chance they're using a variety of devices—possibly on unsecured home networks—to access and share corporate data. Security teams must identify every threat vector and reduce attack surfaces to ensure bad actors can't get too far without authentication.

---

[1] "Why Working from Home Will Stick," NBER, April 2021, www.nber.org/papers/w28731.

[2] "25 Amazing Cloud Adoption Statistics [2022]: Cloud Migration, Computing, And More," Zippia.com, Dec. 19, 2022, https://www.zippia.com/advice/cloud-adoption-statistics.

What is SASE?

A secure access service edge (SASE) is a security architecture model that integrates a range of security applications and concepts—many of them already in place—to secure complex cloud implementations more effectively and more efficiently.

Why is SASE important?

SASE combines network security functions with WAN capabilities to support the dynamic secure access needs of organizations. A SASE model is designed to solve for complexities around user access, scalability, security monitoring, and shifting perimeters by bringing security to the edge and unifying security controls.

Cloud-native SASE is increasingly recognized as a highly effective, highly efficient means of addressing the challenges of supporting distributed and remote workforces and a cloud migration.

What is the “edge”?

Cloud infrastructures are decentralized by nature because they move systems outside the traditional on-premises perimeter (or boundary) between trusted (corporate) and untrusted (internet) networks, assets, and users.

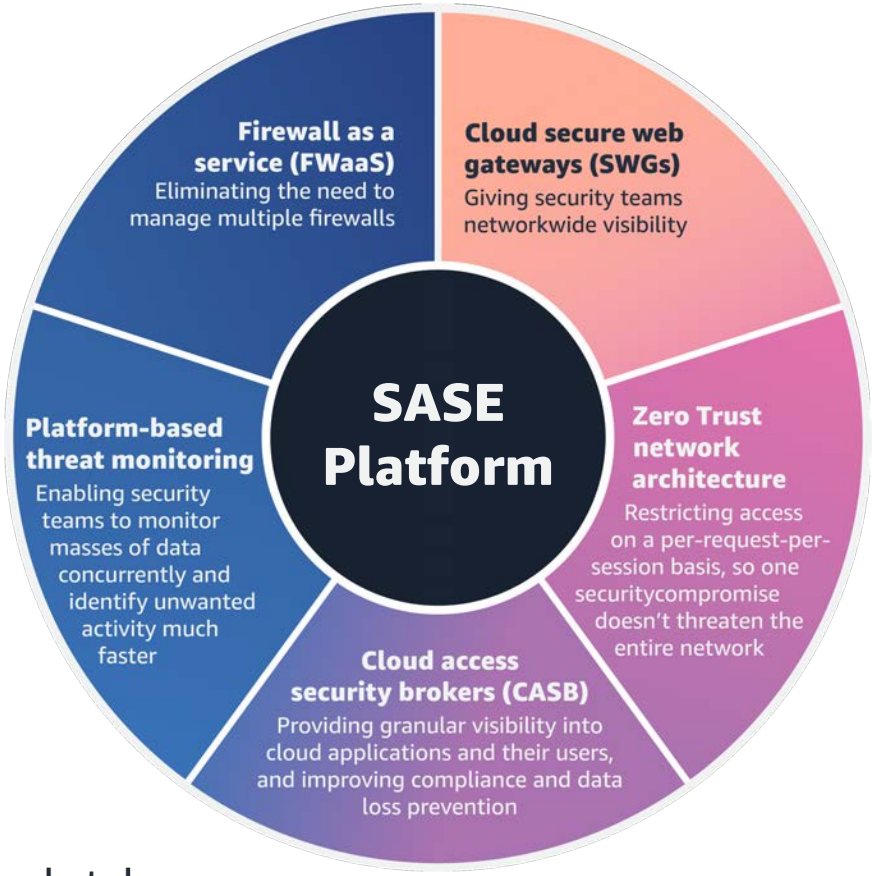
A new boundary, or “edge,” comes into play when you use a SASE model to increase visibility by creating a new perimeter that will provide insight into both cloud and on-premises activity.

Simplify and manage security from core to edge

It isn't only distributed operations and remote work that introduce serious security considerations. The ongoing worldwide migration to the cloud decentralizes the enterprise environment by moving assets and workloads from on-premises to the cloud, which reduces a security team's visibility and poses challenges in:

- **Security monitoring and detection**
- **Perimeter defense**
- **User access**
- **Scalability**

The cloud-native SASE security model addresses all these challenges with a cloud-forward approach that doesn't require a complete overhaul. Instead, a SASE model unites existing systems, including:



The bottom line: Uncomplicated, cloud-native security

The SASE approach offers significant improvements in the security of cloud infrastructures like AWS, while reducing the complexity and difficulty of security management.

Lyft drives the health of user devices and customer data protection with Duo Beyond

The Challenge

Lyft needed to streamline and secure its employees' access to user data and internal applications hosted on Amazon Web Services (AWS).

The Solution

Duo Beyond from Duo Security (Duo), available in the AWS Marketplace along with other Cisco SaaS solutions, enabled Lyft to strengthen its security capabilities by providing a centralized view and continuous monitoring of all Lyft employees' managed and unmanaged user devices. Lyft can now prevent unauthorized access to sensitive customer data—without affecting employee productivity—as well as quickly deploy risk mitigation policies.

The Results

- 50% reduction in total cost of ownership (TCO)
- Ability to automatically deploy Duo Beyond in 10 minutes
- Consolidation of multiple security projects into a single solution

"Duo Beyond has enabled us to push our Zero Trust strategy faster, allowing us to utilize client systems (ChromeOS to be specific) that were difficult and costly to support, making it very low effort to bring new services online and grant granular access control."

– Mike Johnson, CISO, Lyft

aws marketplace

Cathay Pacific gains first-class micro-segmentation with Illumio Core

The Challenge

Cathay Pacific needed to tighten internal security controls and protect applications to build on its cybersecurity program initiatives.

The Solution

Cathay Pacific uses Illumio Core for precise protection of critical applications, enabling Zero Trust control against the spread of potential attacks.

The Results

The combination of Illumio Core and Illumio Endpoint allows Cathay Pacific to demonstrate to regulators and auditors a trusted Zero Trust network.

- 3,000+ servers and ~600 applications protected—both on-premises and in AWS
- <3 months implementation time vs. 12-18 months at the network-based level
- Visibility for cross-team collaboration

> "The first thing we were excited about was being able to map dependencies between applications. There are lots of tools that say they do it, but none of them do it particularly well. Illumio was the first one we saw that really made that easy."

– Kerry Peirse, General Manager Infrastructure, Operations, and Security, Cathay Pacific

aws marketplace

Getting Started

How to protect your distributed workforce beyond the edge

Recent research shows that 26% of US employees work remotely, as of 2022[3], and that while 94% of companies use cloud services, cloud adoption still grew in 2022.[4]

Cloud migration is game changer when it comes to network architectures and supporting the new era of distributed workforces and remote work. Outdated security strategies and systems can't keep up with modern threats, and remote employees can be specifically vulnerable to cyberattacks.

You've seen two examples of how a SASE model helps organizations improve cybersecurity while enabling employees to securely access internal assets. Find more examples and solutions from AWS Marketplace to address your modern security needs.

[3] "25 Trending Remote Work Statistics [2022]: Facts, Trends, And Projections," Zippia.com, Oct. 16, 2022, https://www.zippia.com/advice/remote-work-statistics.

[4] "25 Amazing Cloud Adoption Statistics [2022]: Cloud Migration, Computing, And More," Zippia.com, Dec. 19, 2022, https://www.zippia.com/advice/cloud-adoption-statistics.

AWS Marketplace

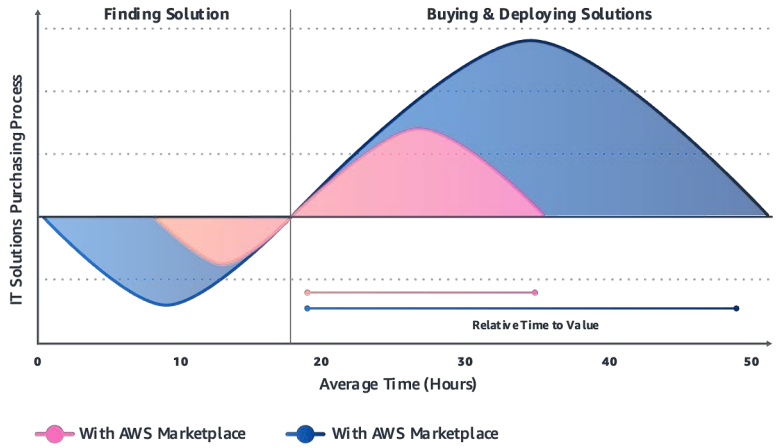
Simplify the procurement, provisioning, and governance of third-party software, services, and data.

Why use AWS Marketplace?

AWS Marketplace is a curated digital catalog that simplifies software discovery, procurement, provisioning, and management. With AWS Marketplace, customers can also utilize features that speed up production evaluation, improve governance and cost transparency, and enhance control over software spend. AWS Marketplace offers third-party solutions across software, data, and machine learning tools that enable builders to find, test, and deploy solutions to expedite innovation.

Explore and deploy solutions

IT decision-makers (ITDMs) cut their time in half using AWS Marketplace compared to other sources.



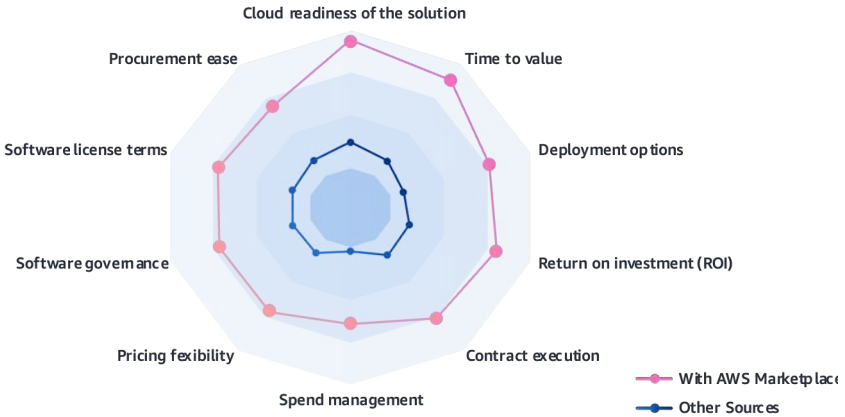
AWS Marketplace benefits

Customers can launch pre-configured solutions in just a few clicks in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a global team of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources needed to streamline migration journeys to AWS.

Make more satisfying purchases

ITDMs feel 2.4x better about purchasing using AWS Marketplace compared to other sources.



* Amazon Web Services (AWS) Marketplace surveyed 500 ITDMs and influencers across the US to understand software usage, purchasing, consumption models, and compared savings.

Getting Started

AWS Marketplace Security Solutions

Helping buyers, sellers, and consulting partners reach favorable agreements, cut down negation time, and reduce sales cycles by 49%

Innovative AWS Marketplace features enable you to reduce software purchasing inefficiencies with cloud-based procurement. One way is through AWS Marketplace seller private offers, which enable you to receive product pricing and terms that are not publicly available from sellers in a centralized portal.

To help govern purchasing, you can establish Private Marketplaces to control which products users in your AWS account can purchase from AWS Marketplace. This can help ensure that products purchased comply with your organization's internal policies.

You can also purchase software solutions in AWS Marketplace directly from Consulting Partners who have industry expertise and can offer specialized support. Many consulting Partners offer both software and professional services on AWS Marketplace to provide you with comprehensive solutions via a fast and friction-free purchasing experience.

> "AWS Marketplace makes it easier to do business with our vendors in everything from simplifying our licensing to streamlining billing to accelerating procurements. This has alleviated a major operations burden and given us time back to focus on more innovative tasks."
>
> – Stephen Pearson,
> Head of IT Vendor Management,
> Agero

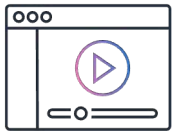
AWS Marketplace

Discover security products to meet your business needs

Discover security products and resources to meet your business needs:

Learn More | Product Overview Video

Learn More | Demo

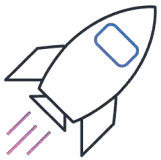


Future-proof your security with Secure Access Service Edge (SASE)

Webinar | Whitepaper

How to build a secure access service edge (SASE) model in AWS

1-Minute Webinar



Find, buy, deploy, and govern software solutions on AWS Marketplace

Visit AWS Marketplace

Get connected with a solution architect that can share best practices and help solve unique challenges

Get in touch with an AWS Expert