

# Enable secure work from anywhere with Barracuda's cloud-native SASE platform

The way we work has fundamentally changed over the last several years. Working from the office is common once again as companies have adopted a part-time home-office model. In many businesses, employees have grown accustomed to working remotely 2-3 days per week. That means that most meetings these days are online, with offices seeing up to 70% more traffic than just a couple of years ago. IT departments—traditionally understaffed and constantly under attack—face the additional challenge of delivering a work-from-anywhere experience that keeps workers both productive and secure.

## Work-from-anywhere security

Supporting WFA requires security that works whether users are working from the corporate office, their home office, or while they are traveling. Each of these locations poses challenges and requires consistent security levels for complete protection. Implementing these additional levels of security can be challenging, especially for businesses with limited financial and personnel resources.

## Secure private access to any application no matter where it's hosted

Today, users on any device expect secure and reliable access to any app, hosted in any cloud or on-premises. Existing SASE and zero-trust solutions, which were designed and optimized for secure access to cloud-based resources only, are often hard to set up and manage and fall short on usability in the real world.

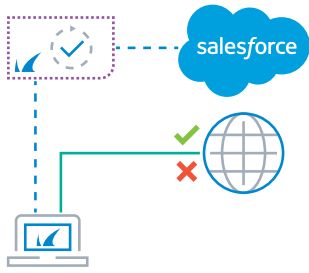
Because they are optimized for web-based SaaS solutions, setting up application support for non-web apps hosted in any cloud or on-premises is often a daunting task and sometimes not possible at all.

## Easy to acquire, deploy, and manage

Traditional SASE solutions were designed with large enterprises in mind. They are expensive, complicated to configure, and time-consuming to set up. Because they are delivered entirely by the cloud, they require all traffic to be backhauled to the service, even if SaaS traffic just gets redirected to the service provider. Newly emerging, often consumer-grade ZTNA solutions lack important SASE components and back-end security prowess, thus requiring a second or even third vendor for client security and branch connectivity.

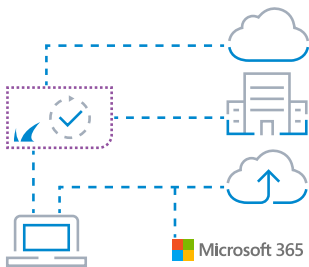


## How Barracuda SecureEdge enables secure work from anywhere



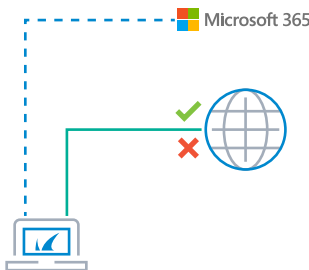
### Secure Internet Access (SIA)

Secure web-gateway functionality of the SecureEdge service extended to the endpoint with the SecureEdge Agent providing Secure Internet Access (SIA). The Agent blocks known forbidden or unwanted web categories without further inspection. There is no reason to send this type of traffic to the cloud for inspection when it can be blocked immediately at the endpoint. This could be content that conflicts with regulatory or corporate compliance or websites that are known to be malicious. This even includes “outgoing calls” of malicious software that is already on the device and trying to phone home. Access to “known good” SaaS apps is allowed by default, without being sent to the cloud service for security inspection. Customers have full control by enabling or disabling access via the 100+ URL filter categories and thousands of application definitions.



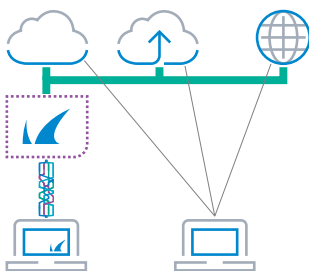
### Cloud-delivered security

Full security inspection is applied for applications and websites that are neither known good nor known bad or that the IT department just requires full inspection of for compliance purposes. Traffic to and from these destinations is automatically sent to the SecureEdge Service for full next-generation security inspection, including IPS, deep SSL Inspection, and Advanced Threat Protection via the Barracuda BATP cloud.



### Secure access to private and SaaS apps

The Barracuda SecureEdge Service and the SecureEdge Access Agent provide secure access to any private or SaaS application regardless of where they are hosted, following the zero-trust principles. Zero Trust Network Access (ZTNA) provides users with the least privileged access to business applications, minimizing business risk. Barracuda SecureEdge Zero Trust Security establishes unparalleled access control across users and devices without the performance pitfalls of a traditional VPN. It provides remote, conditional, and contextual access to resources, and reduces over-privileged access and associated third-party risks.



### VIP treatment on shared lines, better application performance

Connecting to corporate resources often suffers from limitations caused by shared lossy internet broadband lines. Last-mile optimization for application traffic via SecureEdge optimizes the end-user experience by reducing packet loss and carving out a greater slice of available bandwidth of shared lines, improving the quality of voice and video calls. The underlying technology to remediate packet loss is based on random linear network codes (RLNC), a new algorithmic coding scheme that reacts much quicker to losses and remediates these on the fly, thereby requiring fewer retransmissions and reducing overhead on the devices.



### All devices, any platform

The SecureEdge Access Agent is available for all desktop and mobile platforms, providing consistent security and ZTNA functionality. Best of all: licensing is user based and covers up to 5 devices per user.

## Secure users, sites, and things – and connect to any app

Barracuda SecureEdge is a single-vendor SASE platform addressing the needs of today's businesses to provide enterprise-class security and application access for any type of organization.

## Summary

Barracuda SecureEdge is a single-vendor SASE platform that combines cloud-delivered security for branches, endpoints, and zero-trust application access to any application, no matter where it is hosted, where it is accessed from and for any device whatsoever. Built-in automation, smart defaults, and interoperability of the components all ensure that it is easy to acquire, deploy, and manage, while providing security and an optimal application experience for the end user.

## Cloud-delivered security and networking

