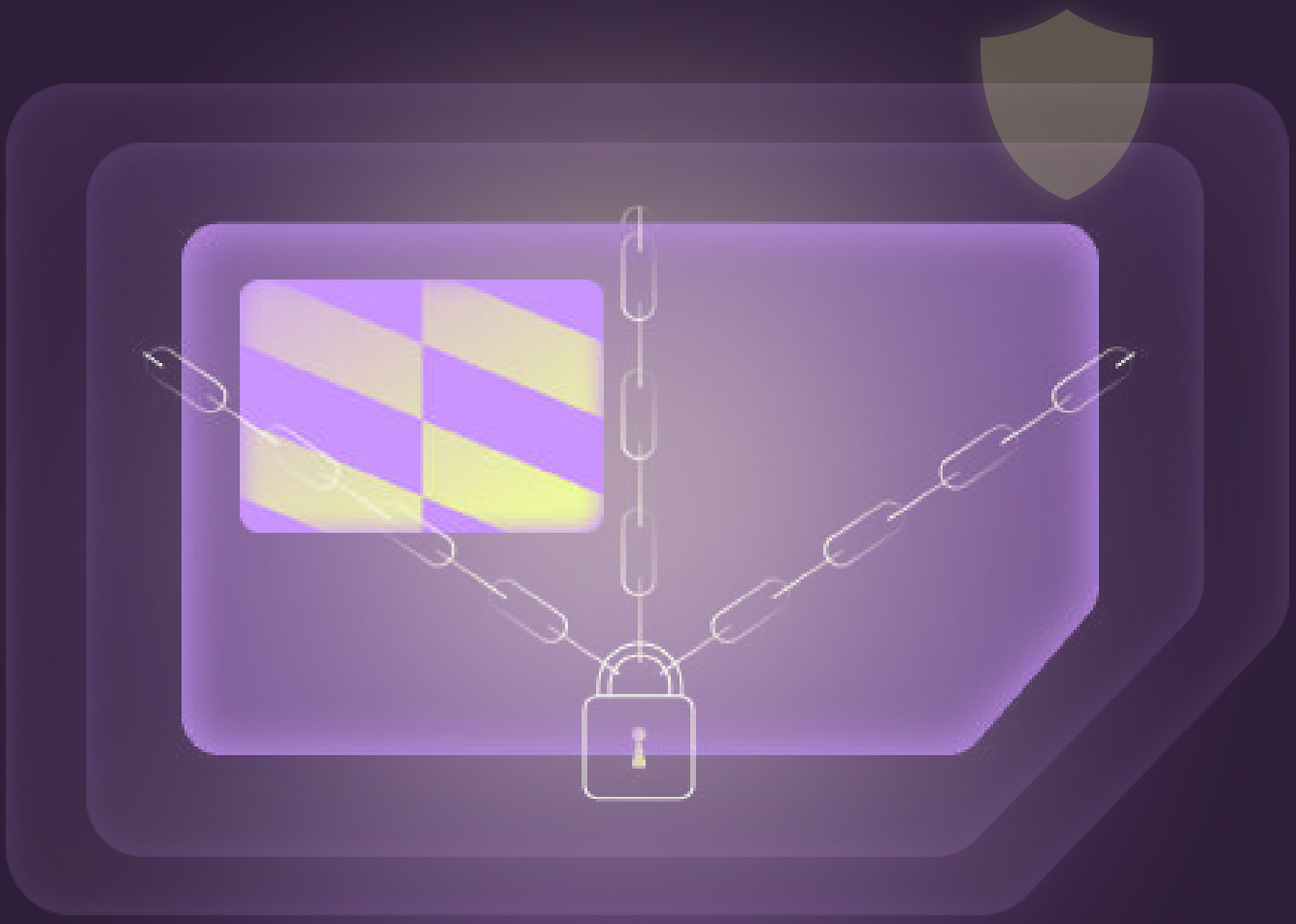
UNIBEAM

# SASE

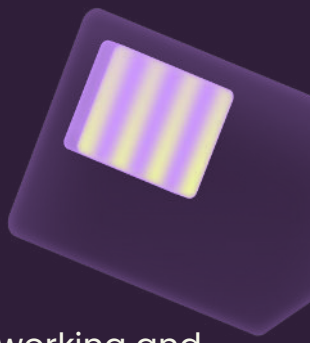
## Secure Access Service Edge

Zero Trust, Total Confidence



Traditional network security struggles to keep up with the demands of a hybrid, cloud-first world. Employees connect to apps and data from remote locations, branch offices, and personal devices, inherently creating security gaps. Perimeter-based models designed for centralized data centers leave networks vulnerable to modern threats. Attackers have evolved, too – easily bypassing passwords and multi-factor authentication (MFA). Modern enterprises need a new approach to protect their users, data, and networks in an environment where the old rules no longer apply.

**That's why we created Unibeam SASE.**



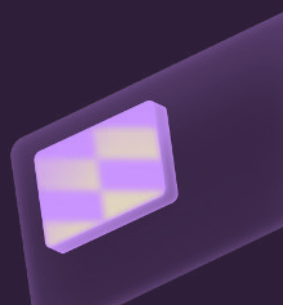
## Unibeam SASE: Security That Keeps You Productive

Unibeam's Secure Access Service Edge solution meets the changing networking and security needs of businesses like yours in a cloud-first, hybrid work world.

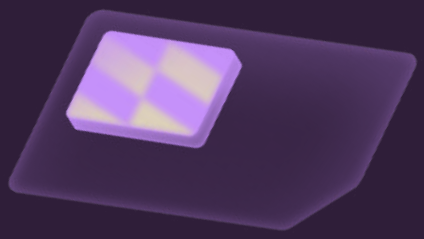
Unibeam SASE gives your team fast, secure access to whatever they need, wherever they work from. Unibeam SASE uses Unibeam's unique SIM-based authentication and Zero Trust Network Access (ZTNA) principles to extend and enhance your existing authentication systems. Whether your employees are in the office or remote, Unibeam SASE simplifies access to the company resources they need to do their jobs. At the same time, it makes your business safer, more compliant, and easier to manage.

## Why Unibeam SASE?

- → Seamless Access, Anywhere- Unibeam SASE ensures fast, secure access to resources for your employees and service providers - whether on-site, remote, or on the move.
- → Stronger Security, Smarter Defense- Built on Zero Trust and using advanced threat detection, Unibeam SASE protects against evolving cyber threats while keeping your data and users safe.
- → Integrated and Scalable- Unibeam SASE is a scalable cloud-native framework that integrates seamlessly with your existing authentication systems (Active Directory, Okta, Ping, OneLogin, and more).



# Behind the Scenes: How Does Unibeam SASE Work?



01

### One-Time User Login

Whether on-site or remote, you start by entering your username and password on your device.

02

### MFA Challenge

Once your credentials are validated, your system sends a secure, **personalized** MFA prompt to your phone using your mobile number.

03

### SIM-Based Authentication

Since your phone's SIM/eSIM and device are cryptographically bound to your account, Unibeam SASE can ensure the login request comes from your registered device.  A pop-up will appear on your mobile phone asking you to approve or deny the login attempt. You can also ignore it if it wasn't intentional.

04

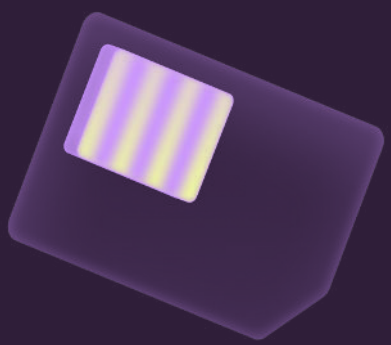
### Verification

Your phone sends your response, along with unique SIM and device identifiers, back to the Unibeam SASE cloud and immediately forwards it to **your** External MFA process. The responses are checked against what's stored in the company's Active Directory to confirm that it's really you

05

### Access Granted or Denied

Based on your response and company policies, you're either granted access or blocked. If blocked, the attempt is logged for review.



# User Login Flow with External MFA in MS Active Directory - Unibeam SASE
(Works with any Directory listing, ADD/AD as an example)