Barracuda
Your journey, secured.

Barracuda CloudGen Access

Increase security, productivity, flexibility

A hybrid workforce, accelerated cloud migration, and SaaS adoption have expanded security perimeters and attack surfaces. As a result, the implicit trust security model is no longer suitable for modern cybersecurity threats.

Zero Trust ensures data and resources are inaccessible by default, and access is only be granted by identifying and authenticating every user, device, and request.

Barracuda CloudGen Access is an innovative Zero Trust Access solution that provides secure access to applications and data from any device and location. CloudGen Access continuously verifies that only the right person, with the right device, and the right permissions can access company data or apps, or any infrastructure.

Ensure conditional, application-specific access

CloudGen Access grants least privileged access to authorized apps without exposing your private network. Even authenticated users won't be able to scan or sweep the internal network, since they will only be able to observe apps and servers that are explicitly granted access to. Barracuda helps enforce granular policy controls and only routes your data through your infrastructure, not ours.

Protect users and data from web threats

Securing traffic to and from the web is critical, but not all web security solutions are designed for the era of cloud-connected services, remote workers, and widely-distributed networks. Barracuda CloudGen Access combines robust content filtering, granular policy enforcement and reporting, simple centralized management, and real-time threat intelligence to protect your users, your organization, and your brand.

Prevent access from rogue devices

CloudGen Access requires a valid and cryptographically secure device certificate, stored in the devices' TPM or SEP modules, to identify a valid device before the user can authenticate on your network. These certificates enable the concept of device identity and require the combination of user and device identity to be paired for remote users or machines to be able to access your internal resources.

Easy to deploy and manage

Easily onboard managed and unmanaged devices without MDM dependency. Gain visibility and control over access to corporate applications for employees, contractors, and partners with unmatched speed. Manage, track, and verify the who, what, and when of privileged access in one product.

Secure SaaS applications

Secure access to SaaS applications with certificate-based authentication, which prevents advanced MFA bypass attacks, and mitigate breach risk for your employees and contractors. Enforce granular access policies and gain valuable insights and full visibility into your SaaS resource access flows, to mitigate security and compliance risks.

Secure third-party access

Mitigate the risks associated with third-party access to your business with Zero Trust. Replace cumbersome technologies, like VPN and jump server, with CloudGen Access, to enable secure, reliable and fast access to authorized apps and workloads in your network from any device, network, and location. Enforce continuous device identity and security posture checks.

Solution Features

- Software-defined perimeter (SDP)
- Mobile first, BYOD first
- Identity-driven access and app segmentation
- Remediation engine (NAC)
- RBAC and ABAC-based global policy engine
- High-performance connectivity
- Scalability across cloud and hybrid infrastructures
- Streamlined one-click user provisioning
- Data plane belongs to the customer
- No dependency on MDM
- Compatible with all apps, from legacy to SAML/https on any infrastructure
- Web Security
  - Content filtering
  - Flexible policies
- Eliminate latency via local inspection
- Protect against phishing and blocks threats at device level
- Single-Sign-On integrations
  - Azure AD
  - Okta
  - Ping Identity
  - Google Suite
  - SAML
  - OpenID Connect (OIDC)

Technical Specs

CloudGen Access App

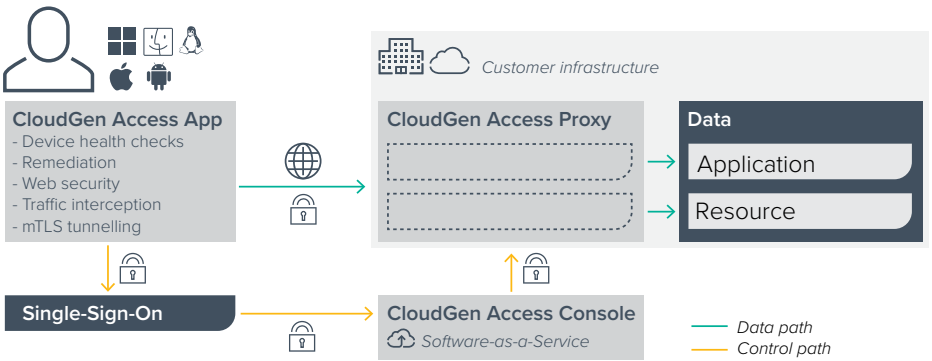
- Self-provisioning (onboarding)
- Consistent look and feel across platforms
- Integrated web security
- Integrated identity and device health check
- Self-service remediations
- Traffic interception
- mTSL tunneling for proxy access
- Very low battery consumption
- Small memory footprint
- Available for
  - Windows
  - macOS
  - iOS
  - Android
  - Chrome OS
  - Linux

CloudGen Access Proxy

- Extremely easy set up: automated, single parameter deployment
- Listens to requests, checks permissions and proxies accordingly
- Enforces authentication and authorization
- Available for
  - Barracuda CloudGen Firewall
  - Docker
  - Kubernetes (including AKS and GKE)
  - Virtual appliance
  - Amazon Web Services
  - Microsoft Azure
  - Bare metal

CloudGen Access Console

- Configuration of proxies
- Configuration of access policies
- Web security and visibility
- Security events
- Supported policies:
  - Block jailbroken devices
  - Require screen lock
  - Require firewall
  - Require antivirus
  - Require OS updates
  - Require re-authentication
  - Require CloudGen Access app updates
  - Require disk encryption



Barracuda
Your journey, secured.