Secure Access Service Edge with Bitglass

bitglass

SASE

The security needs of modern organizations are changing. As data moves off premises and beyond the reach of conventional tools like firewalls, steps must be taken to ensure that it remains safe. With the proliferation of cloud computing and mobile devices in the workforce, security must be delivered for and from the cloud. The secure access service edge (SASE) refers to the consolidation of cloud security solutions into flexible, cloud-first platforms that are designed to protect data wherever it goes. The components of Bitglass' SASE offering can be found below.

Next-Gen Cloud Access Security Broker

Bitglass is the Next-Generation Cloud Access Security Broker that offers end-to-end protection for data in any app, any device, anywhere. With support for managed apps like Office 365 and Salesforce, unmanaged apps like personal Dropbox and social media, and IaaS platforms like AWS and Azure, Bitglass is built to protect corporate data in real time across your most critical enterprise applications. Only Bitglass provides granular data protection, zero-day threat protection, robust identity and access management, and comprehensive visibility, both with and without agents. With these four pillars of CASB in place, organizations can rest assured that their data is truly safe.

SmartEdge Secure Web Gateway

Bitglass provides the only on-device secure web gateway (SWG). Network traffic is decrypted and inspected on users' devices and only security events are uploaded to the cloud. This enables the solution to preserve user privacy, eliminate latency-inducing network hops, and deliver visibility and control over corporate devices and data. Threat URLs are blocked before they can be visited, and employee access to content is controlled by URL categories and user groups. With its patented Trapdoor Proxy, Bitglass holds the only technology capable of delivering an on-device SWG.

Bitglass Zero Trust Network Access

Bitglass offers a unique, powerful approach to ZTNA. The agentless solution eliminates the need for VPN clients and software installations on endpoints by tying into organizations' single sign-on (SSO) solutions. When users authenticate via SSO in order to access custom apps hosted either on premises or on infrastructure-as-a-service (IaaS) platforms, Bitglass is inserted into the path of traffic. Once users are authenticated via SSO, their traffic is automatically, agentlessly proxied by Bitglass, enabling them to access protected apps and data. Users who are not deemed trustworthy in this way are not granted access.

Want to experience Bitglass for yourself? Request a free trial.