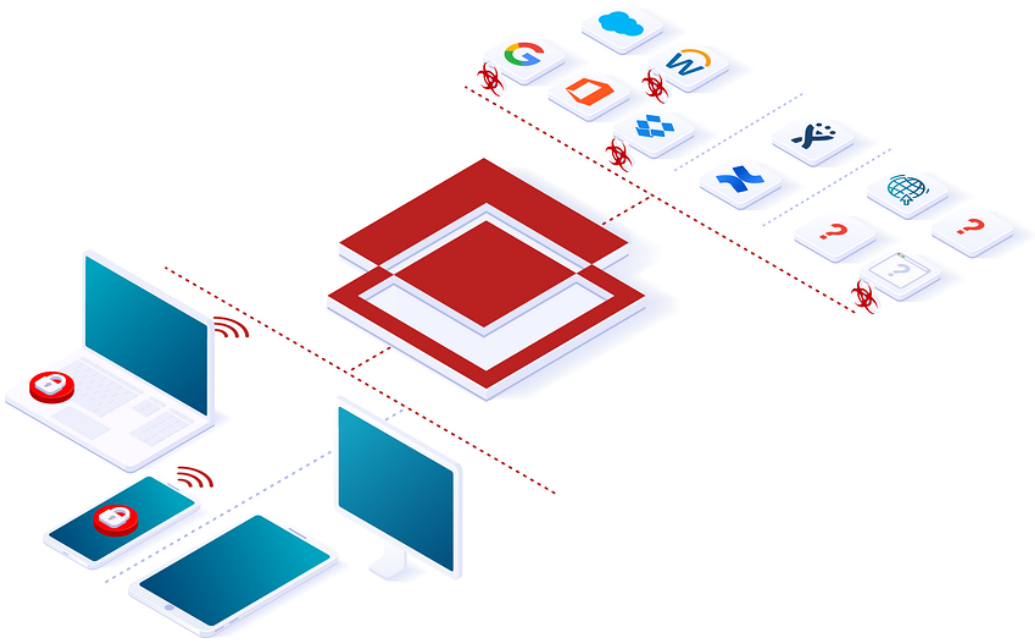
Secure Access Service Edge (SASE) with Bitglass

The security needs of modern organizations are changing. While digital transformation and cloud migration improve productivity, flexibility, and mobility, these benefits need to be balanced with the proper security controls. As data moves off premises and beyond the reach of conventional tools like firewalls, the enterprise needs to think differently to identify how best to secure it. With the proliferation of cloud computing, mobile devices, and remote work, security must be delivered for and from the cloud. Organizations need to secure access to cloud services, block threats like malware, prevent data leakage, enable secure remote work, and comply with compliance frameworks.

Legacy network security solutions built around on-premises appliances cannot support the evolving demands of cloud and mobile. Digital transformation of IT also demands transforming security to a cloud-first architecture. The Bitglass Secure Access Services Edge (SASE) is a comprehensive security solution for digital transformation.

SASE refers to the consolidation of cloud security solutions into flexible, cloud-first platforms that are designed to protect data wherever it goes. Bitglass' SASE offering comprises its Next-Gen Cloud Access Security Broker (CASB), its SmartEdge Secure Web Gateway (SWG), and its zero trust network access (ZTNA).



Next-Gen Cloud Access Security Broker

A typical enterprise may use dozens of public cloud applications such as Office 365, G Suite, Salesforce, Box, ServiceNow, and Tableau. While application providers secure their underlying infrastructure, the applications themselves are freely accessible by any user, on any device, from anywhere in the world. As a result, it is the responsibility of the organization to secure its data as it is stored and accessed on each application. When infrastructure as a service (IaaS) is used, cloud customers have an even greater responsibility for security.

Bitglass provides the Next-Generation Cloud Access Security Broker that offers end-to-end protection for data in any cloud service and any device. With support for managed apps like Office 365 and Salesforce as well as IaaS platforms like AWS and Azure, Bitglass is built to protect corporate data in real time across your officially sanctioned enterprise resources. 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.

Access Control & DLP	• Contextual access control governs data and app access by user group, device type, and location • Enforce DLP policies for data in transit (redact, DRM) and at rest (e.g. quarantine, encrypt) • Leverage prebuilt data patterns or customize your own
Identity	• Native single sign-on for authenticating users across the cloud • Native multi-factor authentication options like SMS tokens, hardware tokens, and Google Authenticator • Integrations with leading identity providers (IdPs) including Ping, Okta, and Centrify
Threat Protection	• Block known and zero-day threats with integrated behavior-based protections from CrowdStrike and Cylance • Stop threats at upload, at download, and at rest without the use of agents
Visibility	• Comprehensive activity logs detail all file, user, and app activity • Thorough visibility and reporting enable compliance and security audits • Show that regulated data patterns are safe--critical for demonstrating regulatory compliance

SmartEdge Secure Web Gateway

Users accessing the web are exposed to threats and data leakage risks. Unfortunately, “VPNing into” the corporate firewall for traffic inspection is a cumbersome bottleneck--particularly when there are remote users. On-premises solutions require the use of appliances that are expensive to maintain and are challenging to scale as organizations grow. Likewise, backhauling traffic to a cloud proxy SWG introduces a latency-inducing network hop and invades user privacy because all user content is inspected at the proxy, including login credentials.

Bitglass provides the world’s only on-device secure web gateway. Traffic is decrypted and inspected directly 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 thorough web security. Threat URLs and unmanaged applications are blocked before they can be visited, and employee access to content is controlled by variables like category, destination trustworthiness, user group, device type, and location. With its patented Trapdoor Proxy, Bitglass holds the only technology capable of delivering an on-device SWG.

Access Control & DLP	• Control access to content by user group, device type, and location, as well as destination category and trust rating • Scan all uploads to the web for sensitive data and automatically halt uploads as needed • Use a pre-built library of hundreds of data patterns or build custom criteria
Identity	• Native single sign-on for authenticating users accessing the web • Native multi-factor authentication options like SMS tokens, hardware tokens, and Google Authenticator • Integrations with leading identity providers (IdPs) including Ping, Okta, and Centrify
Threat Protection	• Prevent users from accessing destinations known to house malware • Scan all files downloaded from the web for infection • Prevent dormant malware already on users’ devices from calling out to command and control IPs • Remote Browser Isolation for added protection
Visibility	• Log all web browsing activity • Thorough visibility and reporting enables audit • Show that regulated data patterns are safe and that users aren’t accessing dangerous content-- critical for demonstrating regulatory compliance

Bitglass Zero Trust Network Access

While the vast majority of organizations have migrated to the cloud and embraced SaaS apps to some extent, most still have on-premises applications, as well. These internal apps typically house highly sensitive information that must only be accessed in a secure fashion by authorized parties. Some organizations achieve this through the use of VPN, but having users VPN into the network gives them full access to everything therein and violates the core principles of zero trust. Instead, users should be given secure access to specific applications only.

Bitglass offers a unique, powerful approach to ZTNA with an agentless option for browser apps, and an agent-based option for thick client apps such as SSH and Remote Desktops.

Access Control & DLP	• Contextual access control governs data and app access by user group, device type, and location • Enforce DLP policies for data in transit (redact, DRM) and at rest (e.g. quarantine, encrypt) • Leverage prebuilt data patterns or customize your own
Identity	• Native single sign-on for authenticating users • Native multi-factor authentication options like SMS tokens, hardware tokens, and Google Authenticator • Integrations with leading identity providers (IdPs), including Ping, Okta, and Centrify
Threat Protection	• Block known and zero-day threats with integrated behavior-based protections from CrowdStrike and Cylance • Stop threats at upload, at download, and at rest without the use of agents
Visibility	• Bitglass' comprehensive activity logs detail all file, user, and app activity • Thorough visibility and reporting enables audit • Show that regulated data patterns are safe--critical for demonstrating regulatory compliance

Uptime & Scalability

Bitglass SASE is built on a fabric deployed globally on the public cloud, at over 200 points of presence. The Bitglass Polyscale datacenter architecture automatically scales with load to maximize performance and uptime. Bitglass has delivered 99.99% uptime since 2014 as measured and published independently by Solarwinds/Pingdom. Additionally, users report faster access to critical business applications via the Bitglass proxy.
Learn more about the **Bitglass SASE fabric here.**

Uptime

99.99%

Since 2014

Summary

Legacy network security solutions built around on-premises appliances cannot support the evolving demands of cloud and mobile. Digital transformation of IT also demands transforming security to a cloud-first architecture. The Bitglass Secure Access Services Edge (SASE) is a comprehensive security solution for digital transformation. The following table summarizes the capabilities of the Bitglass SASE solution.

Capability	CASB	SWG
Identity Management Integrated with all leading IdP. Native IdP with MFA. Contextual session controls.	✓	✓
Contextual Access Control Policies based on user, device, access method, and location.	✓	✓
Shadow IT Reporting Identify the unmanaged apps that employees are using.	✓	
API Controls Visibility and control for data at rest within cloud applications.	✓	
Cloud Encryption Full-strength file-level and field-level encryption adds an extra layer of security for sensitive information.	✓	
URL Filtering URL classification and filtering in order to identify and block threatening and unproductive websites.		✓
Threat Protection Detects and remediates known and zero-day malware through behavior-based threat detection.	✓	✓
Data Protection Secures sensitive data in transit using advanced techniques.	✓	✓
Cloud Managed Unified policy management and reporting platform	✓	✓
Visibility Logging and audit of every interaction	✓	✓
Zero Trust Network Access Secure access to on-premises applications without using agents	✓	

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