Copper River

bitglass

TOTAL CLOUD SECURITY

SECURE ACCESS SERVICE EDGE SOLUTIONS (SASE)

LEVERAGED FOR SUCCESS

- Elevated Partnership Status
- Expert-Level Certified Engineers
- Extensive Platform Specific Experience & Knowledge
- Gained Efficiencies from Strategic Distributor Relationships
- Secure Supply Chain
- Flexible Onsite Availability
- Best Practice Project Management and Engineering Methodologies

NETWORK INFRASTRUCTURE SERVICES

- Architecture Design & Deployment
- Cyber Defense Infrastructure
- Modernization / Optimization
- Assessment / Compliance
- Migration / Refresh
- Customized Engineering Block Schedules

PROVEN PAST PERFORMANCE

- Enterprise
- K-12 and Higher Education
- Service Provider
- State and Local Government

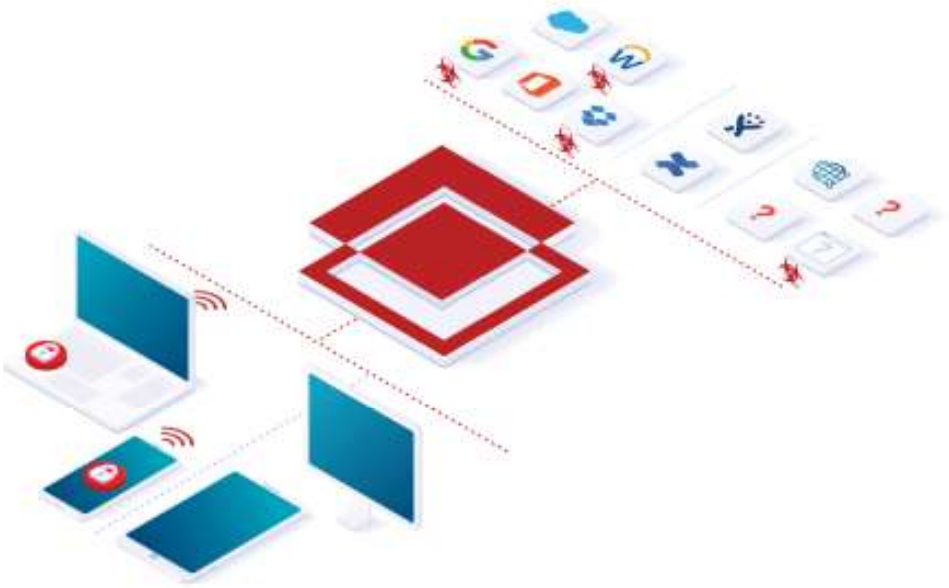
EXTEND CONSISTENT SECURITY TO ALL ENTERPRISE RESOURCES: ANY APP | ANY DEVICE | ANY NETWORK

Copper River has partnered with Bitglass to deliver The Bitglass Secure Access Service Edge (SASE), delivering the most comprehensive, FedRAMP certified security solution for digital transformation available in the market today. SASE refers to the consolidation of cloud security solutions into flexible, cloud-first platforms that are designed to protect data wherever it goes.

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.

Bitglass' Total Cloud Security Platform is designed to secure any interaction between any app, device, web destination, on-premises resource, or infrastructure. As organizations migrate to the cloud, enable BYOD policies, and shift to remote work, Bitglass delivers the granular data and threat protection policies that they need. Bitglass' secure access service edge (SASE) offering integrates its multi-mode cloud access security broker (CASB), its SmartEdge Secure Web Gateway (SWG), and its zero trust network access (ZTNA).



Bitglass' Total Cloud Security Platform

MULTI-MODE 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 a multi-mode 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 & DATA LOSS PREVENTION	• 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)
THREAT PROTECTION	• Block known and zero-day threats with integrated AV engines from CrowdStrike, Bitdefender, and Cylance • Stop threats at upload, at download, and at rest without the use of agents
VISABILITY	• Comprehensive activity logs detail all file, user, and app activity • Thorough visibility and reporting demonstrate regulatory compliance and enable security audits • Exportable logs power integrations with third-party tools like Splunk for deep visibility and analytics

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. Automated certificate management occurs directly on each endpoint, with the SmartEdge agent as the CA.

ACCESS CONTROL & DATA LOSS PREVENTION	• 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 across the cloud • Native multi-factor authentication options like SMS tokens, hardware tokens, and Google Authenticator • Integrations with leading identity providers (IdPs) including Duo, 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 defends against drive-by downloads
VISABILITY	• 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 (perfect for BYOD) and an agent-based option for thick client apps such as SSH and remote desktops. With Bitglass, users are given contextual access to specific on-premises resources rather than indiscriminate access to everything on the network. DLP and ATP policies can be automatically enforced in real time in order to stop leakage and malware, respectively.

ACCESS CONTROL & DATA LOSS PREVENTION	• 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 Duo, Ping, Okta, and Centrify
THREAT PROTECTION	• Block known and zero-day threats with integrated AV engines from CrowdStrike, Bitdefender, and Cylance • Stop threats at upload, at download, and at rest without the use of agents
VISABILITY	• Bitglass' comprehensive activity logs detail all file, user, and app activity • Thorough visibility and reporting enable audit • Show that regulated data patterns are safe--critical for demonstrating regulatory compliancelike Splunk for deep visibility and analytics

ABOUT COPPER RIVER INFORMATION TECHNOLOGY

Since our inception, Copper River Information Technology continues to transform the way our clients do business. As a Federally Recognized Alaskan Tribal Disadvantaged Business, owned by the Native Village of Eyak (NVE), we deliver high-performance IT solutions and services based on our unique advantage of holding elite-level partnerships with today's most innovative technology manufacturers. We combine these impressive product portfolios with our extraordinary engineering, design and professional services expertise to craft a complete, end-to-end technology solution unique to our clients' needs. Some of the innovative solutions and services we offer enable Cyber Security, Data Center & Cloud Architectures, Enterprise Networks and Mobility.

AT A GLANCE

- Federally Recognized, Alaskan Tribal Owned Disadvantaged Business
- Founded in 2006
- ISO 9001:2008 Certified
- SBA 8(a) Graduated | 2015

CONTRACT ROSTER

- Federal Vehicle
  - NASA SEWP V (Prime Group C&D)
- State, Local & Education Vehicles
  - Virginia Higher Education Procurement Consortium (VHEPC)
  - Maryland Department of Information Technology (DoIT)
  - Maryland Education Enterprise Consortium (MEEC)
  - Virginia Information Technologies Agency (VITA)

Market Leading SASE Solution

Bitglass & Copper River

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 resources with or without using agents

TOTAL CLOUD SECURITY

Copper River | bitglass

FedRAMP Certified

COPPER RIVER INFORMATION TECHNOLOGY
4501 Singer Court, Suite 300, Chantilly, VA 20151 | 1577 C Street, Suite 300, Anchorage, AK 99501
703.234.9000 | www.CopperRiverIT.com