With Skyhigh Secure, organizations address all of their cloud data protection requirements from a single solution. Skyhigh Secure effectively provides customers with a virtual ‘cloud edge’ that consistently and transparently enforces their security, privacy, and regulatory policies on corporate data stored in cloud services.

Skyhigh Secure supports leading cloud services across all major categories:

- **COLLABORATION**
- **CRM**
- **DEVELOPMENT**
- **ENTERPRISE RESOURCE PLANNING**
- **HR & FINANCE**
- **INFRASTRUCTURE**
- **IT MANAGEMENT**
- **PRODUCTIVITY SUITE**
- **STORAGE**

“With Skyhigh, once we had the intelligence around risks to our organization, we were able to secure corporate data without impacting business user productivity.”

Brian Lillie
Chief Information Officer
**Contextual Access Control:** Provides the ability to enforce access control policies based on user, device and location. Administrators can set policies ensuring that only users in particular groups using registered devices from specific geographic locations are allowed access to specific cloud services. This capability empowers security teams to extend the appropriate access rights and minimize risk.

**CloudFlow™ Encryption:** Applies standards-based 256-bit encryption to structured and unstructured data while maintaining the end-user functions such as sorting and searching. By owning encryption keys, companies have complete control over their data while minimizing exposure to breaches and blind subpoenas.

**Application Auditing:** Captures detailed metrics of application usage including views, updates, and downloads. Object-level reporting, dynamic anomaly thresholds, and configurable alerts provide administrators with complete and actionable intelligence for incident response.

**Direct-to-Cloud Access:** Utilizes a patent-pending cloud-based reverse proxy to secure cloud usage while allowing end users to directly access popular cloud services without requiring a device agent, VPN, or traffic backhaul. Direct access and agentless deployment accelerates utilization and preserves end-user experience.

**Cloud-to-Cloud Control:** Enables consistent enforcement of corporate policies as data moves from mobile to cloud, on-premise to cloud, and even from cloud service to cloud service. This enables IT administrators to permit the secure usage of federated cloud services while preventing data leakage to unapproved applications.

**Federated Single Sign-On (SSO):** Integrates with single sign-on solutions (such as Okta, Ping Identity, and OneLogin) to transparently redirect traffic through Skyhigh after authentication. Users benefit from securely accessing cloud services through SSO without behavior changes or device configuration.

**CloudDLP™:** Enforces compliance policies inline and offline via alerting, blocking, or encryption to prevent leakage of personally identifiable information (PII), and offers the ability to synchronize policies with existing DLP solutions. Data loss prevention protects against theft or loss and helps ensure compliance with PCI, HIPAA, and HITECH.

**Flexible Deployment Options:** Enables the deployment of Skyhigh Secure in the cloud, on premises as a virtual appliance, or in a hybrid architecture to meet specific security requirements. In a hybrid deployment, security policies for endpoints behind the firewall can be distinct from devices on public networks.

---

Access to specific cloud services can be enabled/disabled by user, device and location.

Quickly configure standard and company-specific data security policies.

To gain visibility and control over the cloud, contact Skyhigh Networks today.