



skyfence
An Imperva Company

**Visibility & Control
for Cloud Apps**



www.skyfence.com

The Skyfence Cloud Gateway automates visibility and control over cloud apps. It automatically discovers cloud application use, analyzes the risks, and enforces appropriate controls for SaaS and production applications. With Skyfence, users get the apps they want and IT staff gets the control they need.

The Skyfence Advantage

- Part of the Imperva family of data center security solutions that span on-premise and cloud environments
- Comprehensive App Discovery, Analytics and Protection in one integrated solution
- Flexibility in deployment with appliances, virtual appliance, cloud-based or managed service offering
- Granular policies for mobile and endpoint devices enable access control and data protection for managed and unmanaged phones, tablets and laptops
- Built-in integration with enterprise directories, SIEM and MDM infrastructure

Solutions for Your Business

Enterprise

- App Discovery and Risk Mitigation
- Mobile & Endpoint Control
- Cloud SIEM Integration
- Privileged User Monitoring
- Cyber Threat Prevention & Credential Theft Protection

Service Providers

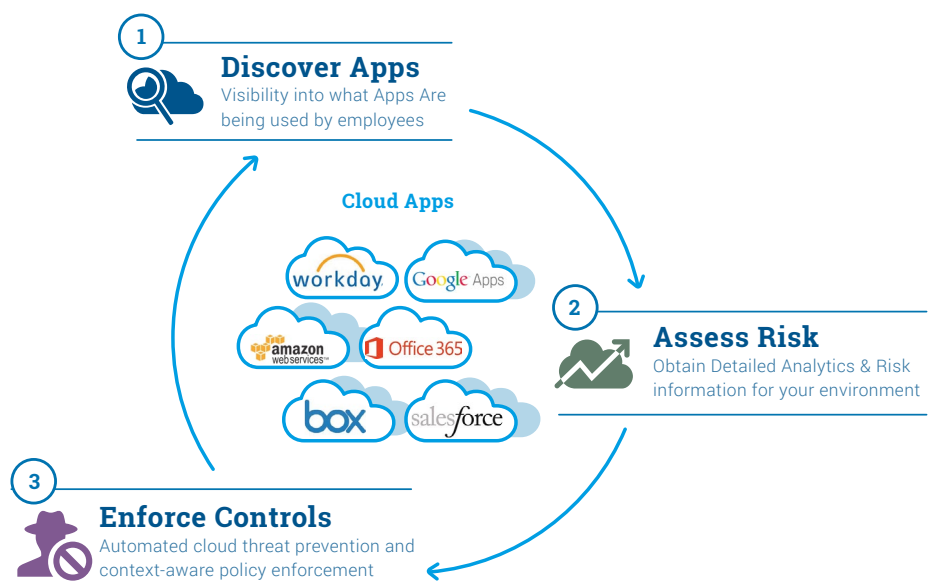
- Account Takeover
- Activity Audits



Cloud Apps Are Here to Stay

Cloud apps allow organizations to reduce costs and elastically allocate resources - but they introduce risks to their security and compliance posture. The “bring-your own” cloud app trend has created a blind spot that is not addressed by traditional perimeter and endpoint controls. IT has little or no visibility into which cloud apps are in use, who is accessing what information and who is performing privileged activities. They are unable to assess the risks associated with each cloud app and to enforce necessary policies and controls. In addition, many enterprises are deploying externally facing production applications for customers and partners which are increasingly the target of account takeover threats due to compromised or stolen credentials.

Skyfence Cloud Gateway ensures visibility and control across all users, endpoints and applications by combing behavioral analytics and anomaly detection to make cloud application use safe and productive.

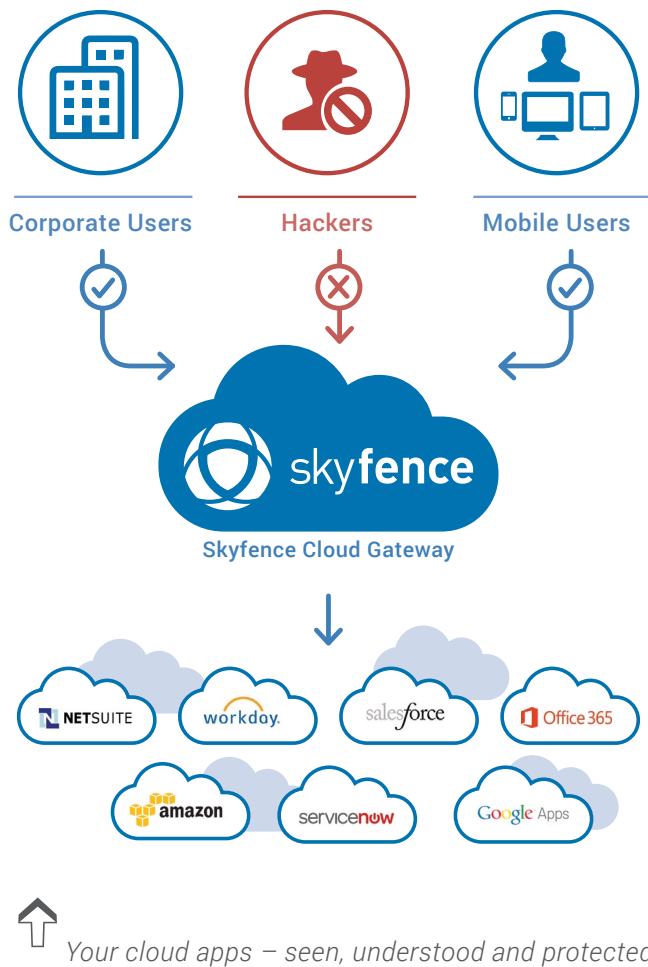


Achieving visibility and control requires an automated process for app discovery, risk assessment and policy enforcement that ensures safe and productive use of all cloud apps



See Your Cloud Apps

Skyfence Cloud Discovery automatically uncovers cloud apps by analyzing data imported from your log files. It aggregates user access scans from web-proxies and firewalls to provide global and regional views of which applications are being used and how frequently. The Cloud Discovery report provides a detailed risk profile for each app so you can determine the right policies for your organization. The process is non-intrusive and requires no agents or changes to applications.



Know Your Cloud Risk

Skyfence Cloud Analytics delivers a complete picture of cloud app risk along with the operational intelligence you need to protect data in the cloud. Skyfence provides detailed usage analytics that tell you what's happening with cloud data and users, including privileged user activity. It aggregates usage metrics across the distributed enterprise for an unlimited number of cloud apps.

Skyfence Cloud Analytics provides critical insight and intelligence into:

- **Data usage:** Who viewed or modified what, when, and how often
- **Privileged user monitoring:** Including data access, configuration and user permission modifications
- **API activity:** Cloud app and services data accessed via APIs

Skyfence Cloud Analytics has built-in adaptors that make it easy to integrate with enterprise directories and market leading SIEM solutions including Arcsight, Splunk and Q1 Labs.



Control Your Cloud Users

Skyfence Cloud Protection automatically detects and blocks threats to cloud applications and enforces policies that mitigate risk. Innovative Dynamic User and Device Fingerprinting™ technology quickly establishes detailed behavioral profiles based on the normal patterns of use for each user, department, and device. Any access that fails the fingerprint test can be configured to immediately alert, block or require two-factor identification in real-time. With the intuitive policy editor, you can quickly define customized, granular policies and enforce them across an unlimited number of cloud applications.

Skyfence Cloud Protection enables you to block or restrict cloud app usage from endpoints that are not managed by a Mobile Device Management platform. It enhances your investment in MDM and provides a cost-effective alternative to routing all remote access to cloud apps through a VPN.

Highlighted Features



App Discovery, Usage & Risk

CLOUD APP DISCOVERY

Leverage log files to automate discovery and categorization of all cloud apps

CLOUD APP RISK SCORING Define high, med & low risk based on technology, regulations and best practices

CLOUD APP USAGE SUMMARY

Includes users, activities, traffic volume and usage hours per app

ADVANCED RISK METRICS Detailed risk posture metrics that can be customized to meet your needs

DASHBOARD

Centralized dashboard for managing & analyzing App usage across distributed environments

DISCOVERY ANALYTICS

Flexible reporting, viewing, sort and filter across users, activities, apps & more

APP CATALOG & RISK UPDATES

Automatic updates to Cloud App Catalog and changes in risk properties as they are available



Activity Monitoring & Analytics

MONITORING & ANALYTICS

By user, group, location, device, action, data object, time and department

PRIVILEGED USER MONITORING

Including data access, configuration changes, permission modifications

ENTERPRISE SIEM INTEGRATION

Feed activity logs into leading SIEM solutions

DIRECTORY INTEGRATION

Use existing Active Directory or LDAP directory infrastructure

ROLE BASED ADMINISTRATION

Define permissions for editing assets, policies and system settings

ENTERPRISE REPORTING

Flexible predefined and custom reporting options



Cloud App Control & Protection

AUTOMATIC ANOMALY DETECTION

User and Device Fingerprinting™ detects insider and external threats

REAL-TIME THREAT PREVENTION

Enforce policies that alert or block account centric threats in real time

DYNAMIC ALERTS

Real-time notifications for any policy violation or activity threshold

MOBILE & ENDPOINT ACCESS CONTROL

Eliminate VPN for cloud access with policies to protect unmanaged endpoints

MDM INTEGRATION

Leverage existing MDM to identify unmanaged devices for cloud access

CUSTOM POLICIES

Visual editor for granular policies based on user, endpoint, location, data object, action, time of day and more

PRODUCTION APPLICATION PROTECTION

prevent account takeover and other account centric threats and provide detailed activity logs for data center and customer facing applications



www.skyfence.com | info@skyfence.com

© 2014 Skyfence Networks Ltd. All rights reserved. Skyfence and the Skyfence logo are trademarks of Skyfence Networks Ltd.