

Effective Security for the Multicloud Era

Welcome to the multicloud era - SaaS apps in the cloud, public and hybrid clouds hosting infrastructure, employees and branches accessing the cloud and internet from anywhere.

SaaS Apps

Public Cloud Infrastructure

Access from Anywhere



300,000 OAuth-connected SaaS apps discovered

84% of companies will use multiple clouds



70% of branches have direct, anytime cloud access

Security must be elevated to meet the threats unique to SaaS applications and the public cloud.



Lack of Visibility

Companies don't have visibility into cloud apps being used (Shadow IT) or visibility into public cloud activity. If we don't know what people are doing, how can we protect the cloud?

Compromised Accounts

If account credentials are compromised, bad actors can access public cloud data or SaaS apps used to run business - with the risk they take down entire cloud infrastructures.

Misconfigured Settings

Misconfigurations of cloud settings can be serious. If misconfigured, anyone - attackers included - can steal public cloud data or download sensitive documents.

SaaS Apps Security



Cisco Cloudlock

Protects sanctioned apps and manages Shadow IT by discovering the full extent of SaaS apps being used, providing risk profiles, enforcing data security policies, detecting suspicious behavior and enabling healthy cloud adoption.

[Learn More](#)



Cisco Email Security

Protects the most popular SaaS app - cloud-hosted email. Cisco email security protects organizations from email threats and phishing attacks in Office 365 and GSuite.

[Learn More](#)

Public Cloud Infrastructure Security



Cisco Stealthwatch Cloud

Delivers security visibility for the public cloud to detect abnormal behavior and threat activity to quickly respond before a security incident becomes a devastating breach.

[Learn More](#)

Secure Access to the Cloud



Cisco Umbrella

Protects users anywhere and anytime they access the internet. It leverages deep threat intelligence to keep employees safe from malicious online destinations and blocks suspicious callback activities.

[Learn More](#)



SaaS Cloud Security

When users and endpoints are anti-network, anti-virus is often the only protection available. Ensuring threat efficacy, AMP for Endpoints with Threat Grid is a critical end-point device that when Tetra is turned on eliminates the need for anti-virus.

[Learn More](#)



Cloud Security Assessment Service

Helps organizations design cloud adoption strategies and architectures, and highlights current data security and user behavior issues to facilitate healthy cloud adoption.

[Learn More](#)

Elevate Your Cloud Security with Cisco

[Learn More](#)



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.