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.

Effective Security for the Multicloud Era

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

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.
- 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.
- 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.

Public Cloud Infrastructure Security
- Cisco Cloudlock
  - Protects the public cloud 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.
- 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.
- 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.

Access from Anywhere
- Public Cloud Infrastructure
- SaaS Apps
- Internet

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

Elevate Your Cloud Security with Cisco

- 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.
- Hybrid Cloud Workload Protection
  - Cisco Tetration offers holistic workload protection for multicloud data centers by enabling a zero-trust model using segmentation. This approach allows you to identify vulnerabilities and exploits faster, contain lateral movement and reduce your attack surface. Its infrastructure-agnostic approach supports both on-premises and public cloud workloads.
- Next-Generation Firewalls for the Cloud
  - Cisco’s virtual Next-Generation Firewalls and VPN capabilities help safeguard traffic and workloads that expand, contract, or shift their location over time. Flexible deployment options position protection exactly when and where needed to secure users and workloads on premise and in the cloud.
- Secure Access to the Cloud
  - Cisco Umbrella
    - Protects users anywhere and at any time they access the internet. It leverages deep threat intelligence to make employees work from cloud-based, on-premises, software-defined, or hybrid work environments.

- SaaS Apps
- Public Cloud Infrastructure
- Access from Anywhere

- OAuth-connected SaaS apps discovered
- 300,000

- 70% of branches have direct, anytime cloud access
- 84% of companies will use multiple clouds

Learn More

© 2018 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.