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 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.

**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.

**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.

**SaaS Cloud Security**
Cisco Umbrella
Provides security for SaaS apps, which can often offer the only endpoint protection available when users work from outside of their organization’s internal network.

**Hybrid Cloud Workload Protection**
Cisco Tetration
Offers comprehensive visibility, control and security capabilities for hybrid cloud environments. It delivers zero trust, secure access and dynamic segmentation to help defend and control hybrid 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.

**Cloud Security Assessment Service**
Helps and supports organizations to plan, architect and implement advanced defense mechanisms to ward off cyber threats and secure cloud adoption.

**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**
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.