Cisco Multicloud Portfolio: Cloud Protect

Protect yourself across your environments

Cloud Protect solutions help you:

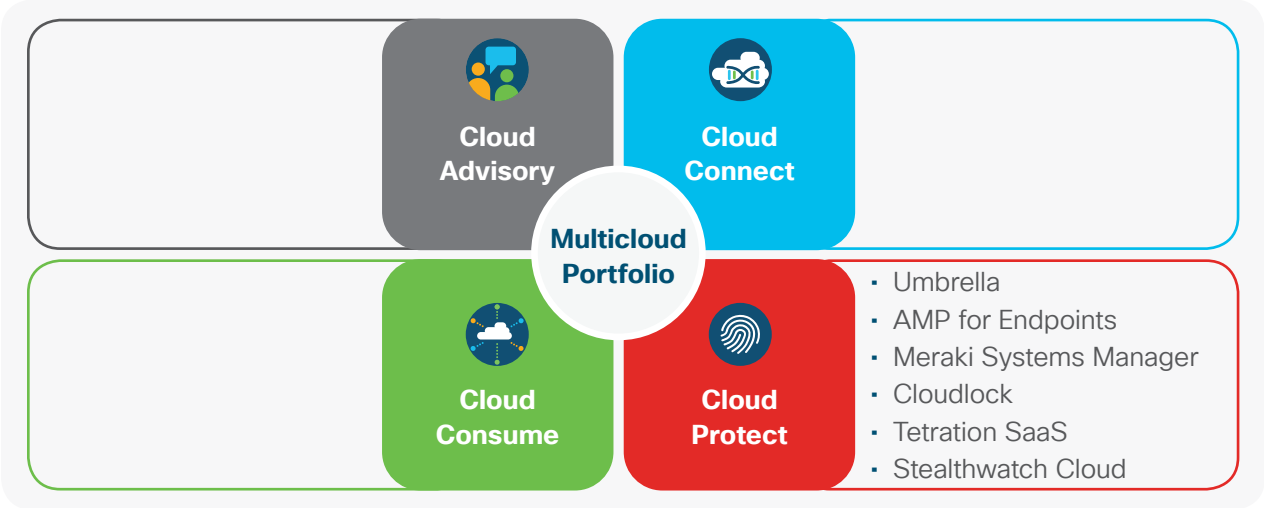
- Protect your multicloud identities, direct-to-cloud connectivity, data, and applications, including Software-as-a-Service (SaaS), by pinpointing and isolating sensitive data
- Secure cloud access for users on and off the network using a secure Internet gateway
- Enable compliance in the cloud by controlling access to the Internet and securing mobile devices, workloads, and SaaS applications
- Dynamically react to changes in endpoint posture by controlling applications, users, and services that access the cloud data via laptops and mobile devices
- Effectively identify threats and monitor user and device behavior across public clouds and on-prem networks

Benefits

- **Secure endpoints, applications, data, and workloads with a single vendor solution** across on-premises and cloud environments
- **Increase compliance** in the cloud by controlling access to the Internet and securing mobile devices, workloads, and SaaS applications
- **Increase visibility and responsiveness** by dynamically reacting to changes in endpoint posture

Elevate your expectations

The multicloud world is complex. With Cisco® Multicloud Portfolio, we make it simple: simple to connect, simple to protect, simple to consume. To explore Cloud Protect design and deployment guides, visit www.cisco.com/go/clouddesignguides.



Simplify how you protect your multicloud world

Protecting a multicloud world raises complex challenges: inconsistencies in security process and policies across private and public domains; increased security troubleshooting from misconfiguration of cloud environments due to unfamiliar and disconnected tools; new security breaches resulting from application developers opening holes in their efforts to develop and test new features; and complexity in designing and implementing a layered security model that covers multiple users, locations, applications, and cloud environments.

With Cloud Protect, you can:

- Secure users and devices connecting to cloud environments from both on and off the network
- Enable endpoint protection by ensuring the right security services are installed and configured and by constantly evaluating and dynamically taking corrective action based on changes to endpoint posture
- Secure cloud applications and data by detecting data leakages through sanctioned SaaS applications
- Discover, map, baseline, and protect applications for cloud workloads to help plan application migrations, identify deviations in application behavior, and apply security policies for enforcing fine-grain application microsegmentation
- Effectively identify threats and monitor user and device behavior across public clouds and on-prem networks

C45-740173-02 08/18