Google Cloud

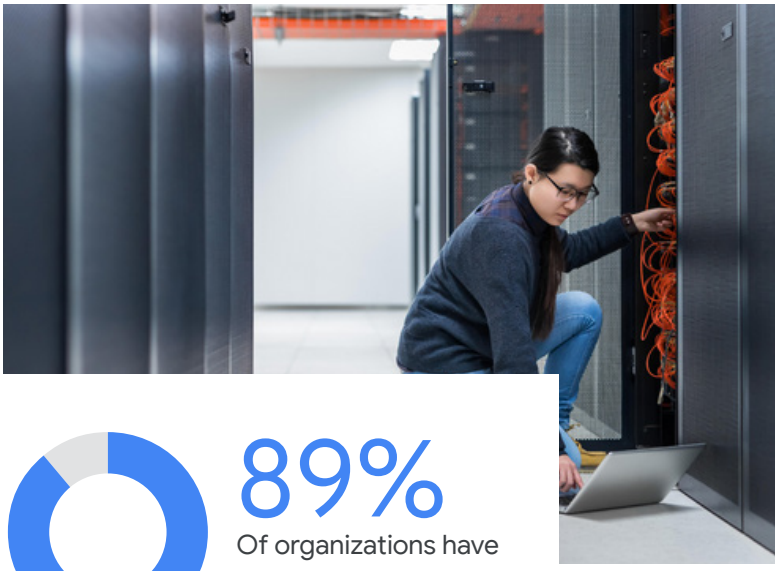
CISCO

Secure your multicloud environment with Cisco and Google Cloud

Gain end-to-end workload visibility and fortify applications against attack with modern zero trust microsegmentation.

Organizations host an increasing number of applications on multiple cloud and hybrid form factors. These environments must be maintained and updated to take advantage of their cloud-native capabilities, including scalability and flexibility, containerized microservices architectures, global availability, and improved security.

However, the complexity of the workloads and services interoperating within dynamic cloud environments creates an expanded attack surface and reduced operational visibility. Siloed teams must manage this increased complexity and reduced visibility with disparate, siloed security tools as threats become increasingly sophisticated.



89%

Of organizations have seen their attack surfaces grow in the past 2 years.[1]

Adopt a proactive cybersecurity posture quickly and seamlessly

Cisco and Google Cloud believe in a proactive approach to security. Organizations must shift to a mindset that assumes breaches will occur and implement measures to protect critical data and applications. This requires deep visibility across the hybrid or multicloud environment and dynamic implementation of zero trust at the application workload level.

Zero trust microsegmentation prevents unauthorized lateral movement by enforcing a distributed firewall policy or micro-perimeter at every workload. It applies least-privilege access, in which a user or application is given the minimum access or permissions necessary to perform their job. This ensures individual workloads remain protected even if a breach occurs or a threat is present.

Organizations need access to real-time insight into their cloud workloads across hybrid and multicloud environments to succeed in mitigating threats.

Cisco Secure Workload on Google Cloud delivers a comprehensive and scalable solution that combines Cisco's expertise in network security and workload protection with Google Cloud's cloud-native security capabilities. The Cisco Secure Workload on Google Cloud offers benefits including unparalleled visibility, granular access controls, and automated policy enforcement across both hybrid and multicloud environments.

With Cisco Secure Workload on Google Cloud, lateral movement is mitigated, critical applications are protected, and robust security posture is maintained.

[1] Cisco App Dynamics 2023

Google Cloud

CISCO

Cisco

- Flexible metadata-enriched policy definition and continuous policy updates
- Workload behavior anomaly detection and proactive software vulnerability detection
- Automated microsegmentation policy recommendations and enforcement

Google Cloud

- Scalable, fault-tolerant global infrastructure protected by a multi-layer approach to security
- Frontline threat intelligence and expertise with unmatched depth and global reach
- Cloud-native SecOps platform with advanced threat detection, investigation, and response

Together

- Comprehensive visibility across hybrid multicloud with seamless scalability
- Simplified policy management with consistent and accurate enforcement
- Proactive risk reduction and protection against known vulnerabilities

See every workload no matter where it lives

Cisco Secure Workload on Google Cloud provides visibility into every application interaction in any environment for any workload, regardless of location. Deep visibility into network communications, application dependencies, and potential risks allows proactive identification and addressing of security threats.

Securing the network within days by blocking insecure communications, identifying vulnerabilities, and shutting down vulnerable management ports.

With Cisco Secure Workload on Google Cloud, organizations microsegment critical assets and applications within weeks. This enhances security posture and ensures value at every step.

Implement zero trust microsegmentation

Simplify the complexity of securing modern application workloads with powerful AI/ML-driven automation. Cisco Secure Workload on Google Cloud streamlines the creation, testing, and implementation of zero trust microsegmentation policies, enabling organizations to achieve a robust security posture at the speed of application development.

Leverage multiple levels of automation. Receive recommended policies automatically that can be tested and validated before implementation without impacting the application, or set Cisco Secure Workload on Google Cloud to auto-configure and enforce policies based on specific criteria. Organizations are also able to manually adjust policies to fit particular use cases.

Enforce security policies at scale

Effectively enforce zero trust security policies across both hybrid and multicloud environments. Cisco Secure Workload on Google Cloud leverages a single platform to implement granular access controls and segmentation policies, mitigating the risk of lateral movement and ensuring continuous policy compliance as the cloud environment evolves.

Proactively extend microsegmentation capabilities to Kubernetes clusters to enforce security policies at the pod level. Segment containerized workloads based on labels, namespaces, or service types. Continuously monitor policy compliance and investigate, approve or reject anomalous activity in real-time, enabling complete security control.

Embrace cloud transformation and application modernization while ensuring the highest levels of security and compliance with security solutions from Cisco and Google Cloud.

Visit the Google Cloud Marketplace to learn more.