Cisco Secure Workload

Reduce your attack surface and protect the applications that power your business

Applications are the lifeblood of business. They connect organizations with their customers, employees, supply chains, partners, and even generate revenue. But the proliferation and dynamic nature of modern applications have led to unprecedented security challenges.

Today’s applications are distributed. They’re deployed both on-premises and in the cloud, or across multiple clouds, and critical workloads are no longer tidily kept in the data center where they can be protected by a perimeter firewall. In some ways, the traditional concept of the perimeter is largely a thing of the past. To respond to this application-centric and hybrid multicloud world, you need a security solution that is closer to the application and agnostic of the underlying infrastructure, allowing you to protect what matters most–your applications and data.

Cisco® Secure Workload protects applications by seamlessly delivering zero trust microsegmentation across any workload, environment, or location from a single console. Zero trust microsegmentation prevents lateral movement by enforcing a distributed firewall policy or “microperimeter” at every workload and applying least privilege access to each. Cisco Secure Workload is one solution for your entire application environment, whether applications are deployed on baremetal servers, virtual machines, or containers. It is flexible and infrastructure agnostic, with agent and agentless capabilities, protecting workloads in the data center and across leading public cloud providers including AWS, Azure, and GCP.

Benefits

- Contain breaches and stop threats from spreading by seamlessly enforcing zero trust microsegmentation across any environment, workload, or location from one solution
- Immediately improve your security posture with deep visibility into every application workload flow and the behavioral interaction with users and devices
- Leverage powerful AI/ML-driven automation for best-practice policy recommendations that are tailored to your unique environment and applications
- Ensure compliance with a hierarchical policy model that delivers comprehensive guardrails across multiple user groups with role-based access control
- Get actionable intelligence with persona-based reporting, near real-time compliance monitoring, and Forensics alerts based on the MITRE ATT&CK framework

Consistently and accurately protect applications

Using advanced AI/ML capabilities, Secure Workload makes zero trust microsegmentation practical and achievable. The intelligence behind Secure Workload maps every application interaction and dependency and recommends policies that are tailored to your unique environment and applications.

Secure Workload enables you to:

- Test and validate zero-trust policies without impacting the application
- Automate policies for desired use cases
- Enforce policies consistently and accurately even as workloads move or change
- Use long-term historical analysis to refine and test policy changes to constantly improve your security posture
- Maintain internal compliance with a hierarchical policy model that provides comprehensive guardrails across multiple user groups with role-based access control
- Integrates with the CI/CD toolchain to write policy as code, ensuring stronger security and faster application deployment

Immediately improve your security posture

With Secure Workload you gain comprehensive visibility into every application workload communication, so you know what your applications are doing and their behavioral interaction with users and devices. Secure Workload delivers immediate benefits from the start.

Within days of deployment, you can realize stronger security by:

- Blocking insecure communications
- Cordoning virtual desktops
- Blocking unwanted app-to-app communications
- Identifying software vulnerabilities and applying virtual patching
- Shutting down all vulnerable management ports

Actionable intelligence at your fingertips

Designed for today’s complex application environment, Secure Workload is built to scale and operate at speed. Within seconds it can process millions of flows and alert you to a policy violation or potential threat. And within minutes you can enact policies to ensure it doesn’t happen again or automate the process.

Secure Workload provides:

- Real-time monitoring that identifies and alerts against unauthorized behavior, policy violations, or potential threats
- Persona-based reporting that depicts the overall security health of applications and illustrates emerging trends based on historical data
- Forensics alerts based on the MITRE ATT&CK framework
- DVR of anomalous behaviors and an auditable record

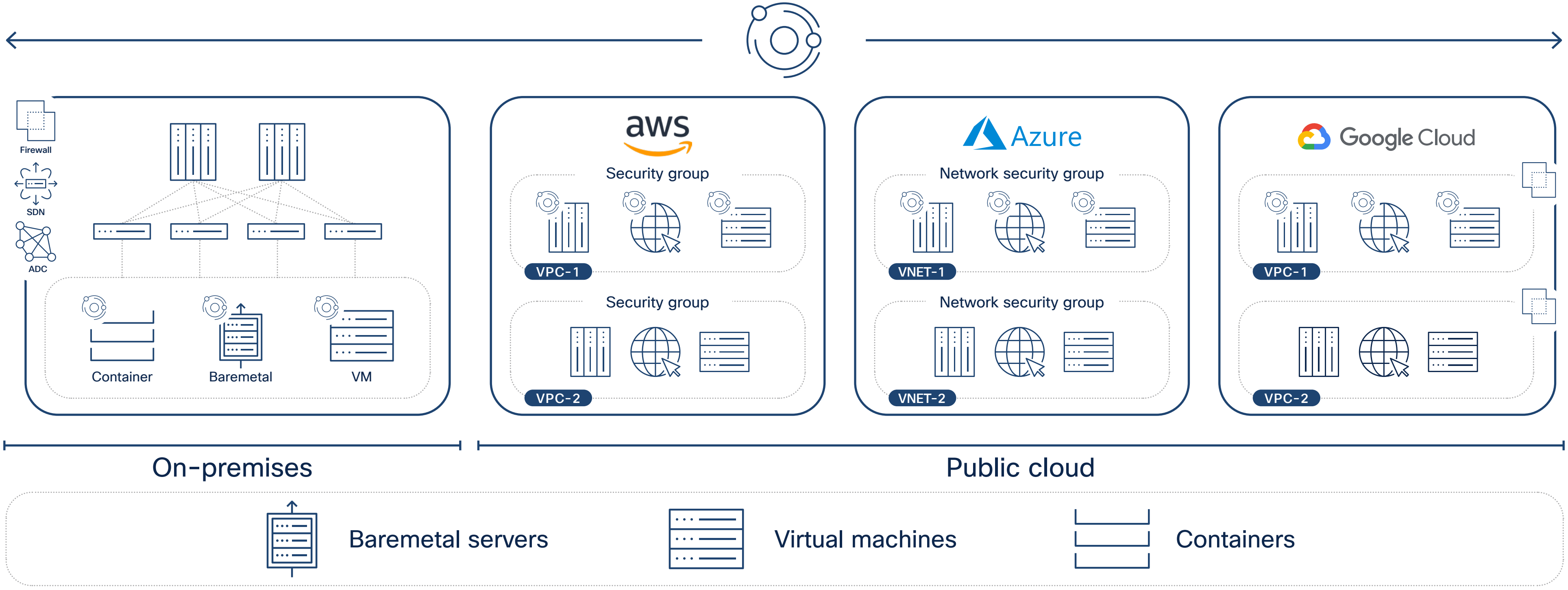
One solution to safeguard applications, reduce risk, and maintain compliance

With comprehensive visibility into every workload interaction and powerful AI/ML-driven automation, Secure Workload reduces the attack surface by preventing lateral movement, identifies workload behavior anomalies, helps rapidly remediate threats, and continuously monitors compliance.

Secure Workload enables you to:

- Maintain business operations even when threats are present
- Rapidly respond to changes in your environment
- Reduce application downtime
- Quickly onboard new applications without friction

Protect applications anywhere with Secure Workload



Defense in depth: Secure Firewall and Identity Services Engine

Cisco Secure Workload natively integrates with Cisco Secure Firewall to unify control points, provide defense in depth, and enable an agentless approach in desired on-premises scenarios. The integration gives customers the granular control to discover, enforce, and automate select policies on a specific firewall or set of firewalls through Secure Workload. Additionally, Secure Workload and Secure Firewall can seamlessly share threat intelligence and ensure that the right SNORT signature is applied to protect against a known vulnerability without breaking the application. Secure Workload also natively integrates with Cisco Identity Services Engine's ISE Passive ID, ingesting user, group, and other attributes from the customer's Active Directory and/or Azure Directory. This provides rich contextual information to enable endpoint identity-aware visibility and policy enforcement.

Stronger security now and into the future

Secure Workload safeguards critical application workloads without compromising agility. It is a strategic solution that delivers immediate returns through stronger security from the start and high-value business benefits into the future. With Secure Workload you can protect your business from breaches and advanced threats, which also protects your customer's data—increasing their trust and confidence in your brand. As a key enabler for many regulatory compliance initiatives, it eases the cost and scope of these efforts. And once in place, Secure Workload easily supports the onboarding of new business applications and processes, providing faster and more secure application development and deployment.

Secure Workload is offered as a SaaS and on-premises appliance - choose what's right for you.

Learn more: cisco.com/go/secureworkload