Cisco Secure Workload Platform

Comprehensive workload security for a multicloud datacenter

What is a data center? You are free to ponder that, but by all means you do not want your data center security to be defined by the infrastructure you pick. Today's data centers consist of a hybrid multicloud infrastructure using baremetal, virtualized, and container-based workloads or anywhere in-between.

As everything revolves around software today, applications running on your infrastructure are the crown jewels, these are dynamic—these are constantly evolving. One of the key challenges is how do I provide a secure infrastructure for applications without compromising agility. Even today, the majority of data centers are designed with traditional perimeter-only security, which is insufficient. In some ways, there is no more perimeter. To respond to this app-centric world, you need a solution that can bring security closer to the applications using a "new firewall" that surrounds each and every workload, allowing you to protect what matters most to you—your applications and your data.

The **Cisco Secure Workload platform** (formerly Tetration) (Figure 1) addresses these requirements **by securing your environments using firewalls at the workload level across your entire infrastructure**, whether applications are deployed on bare-metal servers, virtual machines, or containers. The platform provides policy management capabilities to implement

Benefits

- Uses behavior-based application insight to automate zero trust policy.
- Minimizes lateral movement using microsegmentation to enable a secure zero-trust model.
- Identifies anomalies faster by using process-behavior deviations.
- Reduces the attack surface within the data center by quickly identifying common vulnerabilities and exposures.

a zero-trust model using allow/block policies, it also proactively identifies workload behavior anomalies and reduces the attack surface by actively identifying vulnerabilities and exposures.

> "Cisco's Tetration Analytics [Secure Workload] has provided us unprecedented visibility into our network and applications and is enabling us to migrate from a legacy policy model to a significantly more secure policy model driven by ACI."
>
> Healthcare customer

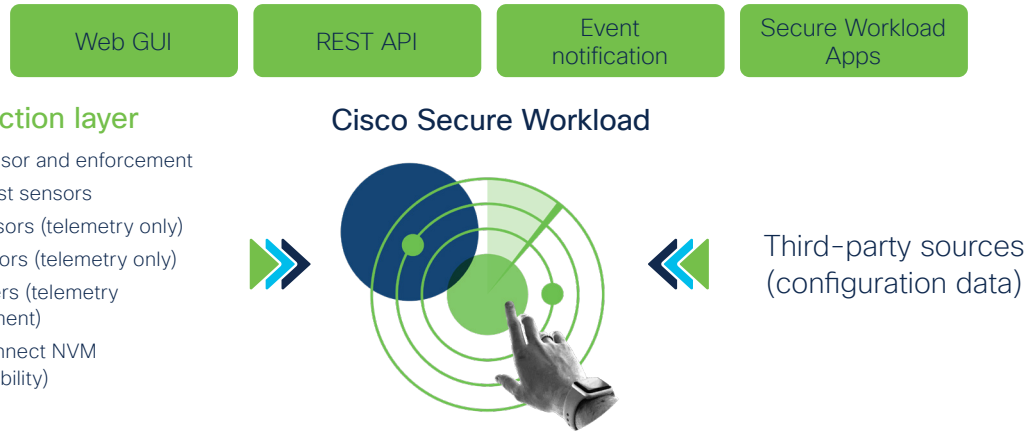


Figure 1. Cisco Secure Workload platform architecture

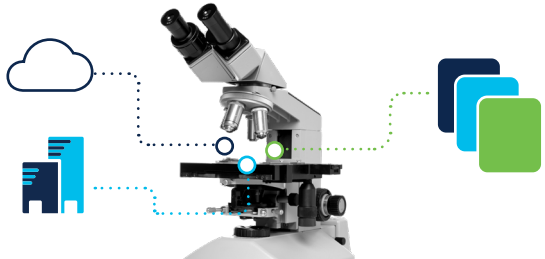
Make informed security decisions for your workloads

Cisco Secure Workload helps you to **deliver zero-trust application security, reduce risk, and maintain compliance**. With Secure Workload, you can:

- **Implement a zero-trust based model:** By using advanced algorithms, Cisco Secure Workload generates a granular segmentation policy for each application. It provides the ability to merge business policy requirements with policies that are generated based on application behavior. This normalization and hierarchical merging of policies helps ensure that administrators with reduced scope cannot override higher level business policy intentions

- **Contain lateral movement using microsegmentation:** The platform provides consistent microsegmentation through workload operating system capabilities across the multicloud infrastructure. Because policy is enforced on the workload itself, Cisco Secure Workload supports virtualized, bare-metal, and container-based environments in unison. This approach ensures that policy moves along with the workload, even when an application component migrates from a bare-metal server to a virtualized environment
- **Identify workload behavior deviation:** Behavior of the workloads can be determined by baselining the processes that are running on the server and identifying any deviations in behavior from those baselines. In Cisco Secure Workload, algorithms are available to match the behavior deviations to malware execution patterns, enabling faster detection.
- **Detect vulnerabilities associated with software packages:** The Cisco Secure Workload platform also identifes installed software packages, package versions, patch level, and publisher. Using this information, it checks whether any of the software packages have known information-security vulnerabilities listed in the CVE database. When a vulnerability is detected, you can find complete details, including the severity and impact score, identify all servers that have the same version of the package installed, and define policies with specific actions, such as quarantining a host when servers have packages with certain vulnerabilities.
- **Compliance and auditability:** The platform monitors application components for policy compliance. It can detect any segmentation policy compliance deviations in minutes and trigger a notification. In addition, enforcement policies are updated automatically to accommodate certain application-behavior changes.
- **Cisco SecureX integration:** Cisco SecureX is a highly integrated security platform that makes it easy to establish coverage across your security portfolio. The SecureX platform is included with Secure Workload and every Cisco security product. SecureX integrates Secure Workload security features to unify and extend visibility and protection across network, endpoint, cloud, and applications to accelerate threat response and realize desired outcomes.

The Cisco Secure Workload platform is unlike any other in the industry. It offers a turnkey approach for microsegmentation, minimizing the time and effort required to build a more secure environment for applications and reduces the risk of exposure.



> "Cisco Tetration [Secure Workload] enabled BBVA's teams to make decisions rapidly based on insights from Tetration [Secure Workload]. Frankly, it is the glue between the needs of my departments and stakeholders."
>
> BBVA

Put Cisco expertise to work to accelerate success

Cisco provides professional and support services to help organizations get the most value. Cisco Services experts help integrate Cisco Secure Workload into your data center and cloud environment, define use cases based on business objectives, tune and validate policies and compliance. Cisco Solution Support provides hardware, software, and solution-level technical support.

For more information

For more information about the Cisco Secure Workload platform, please visit www.cisco.com/go/SecureWorkload.