Cisco Tetration Application Segmentation

The Cisco Tetration™ platform using application insight and white-list based policy model, simplifies the implementation of zero-trust model. It enables effective application segmentation using consistent policy enforcement across on-premises data centers and private and public clouds.

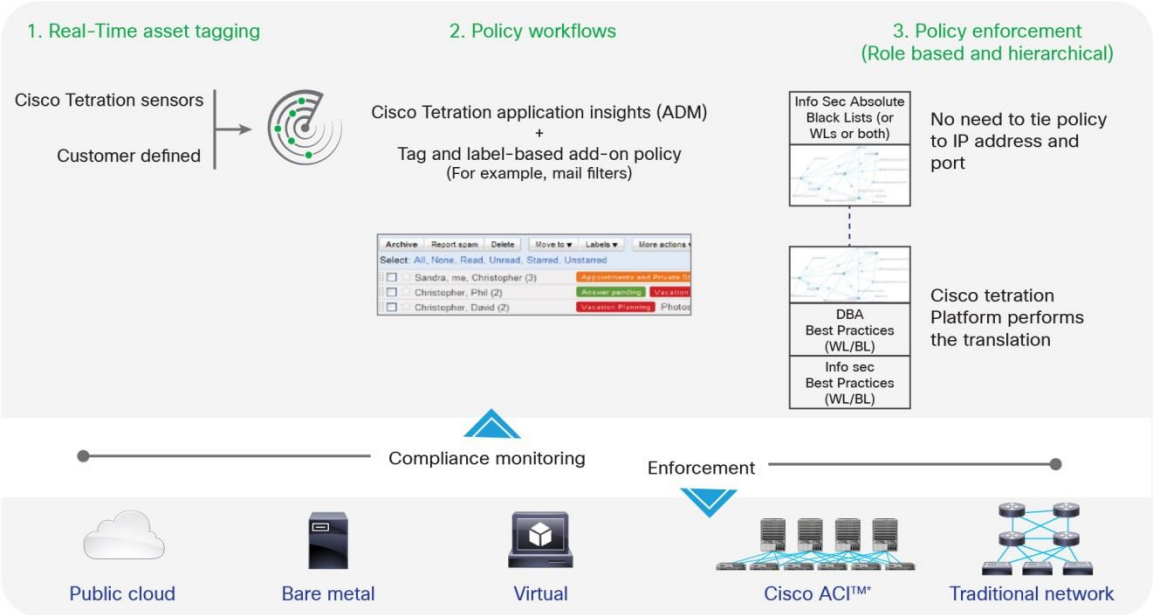
Product overview

Today, applications are the critical entities in the data center. All the infrastructure decisions are being made based on the application structure, consumption, and service delivery models. Applications are also dynamic, using virtualization, containerization, micro-services, and workload mobility technologies, with communication patterns between application components constantly changing. To provide a secure infrastructure for these dynamic applications, the traditional perimeter-based static security model is not sufficient. A whitelist-based zero-trust model needs to be implemented in the data center to better protect the applications, and the solution should offer a consistent and infrastructure-independent approach that includes support for public clouds.

The Cisco Tetration™ platform offers its application segmentation capability to address these challenges in a scalable and efficient way. This capability enables data center and security operations team to automate enforcement of highly specific application segmentation policy for their mission-critical applications running in both on-premises data centers and the public cloud. By applying a consistent policy across bare-metal, virtualized, on-premises data centers and public and private clouds, this model significantly reduces the data center surface that is vulnerable to attack. It also increases operation efficiency through automation of routine tasks associated with data center security. These tasks include discovering and defining application segments, collaboratively defining policies to align with broader organizational business policies, and securing these segments through automated policy enforcement. This platform also automatically identifies application behavior deviations and invokes appropriate workflows for policy updates.

Three unique functions enable application segmentation in the Cisco Tetration platform: asset tagging, application workspaces, and one-click policy enforcement (Figure 1). Segmentation efficiency is increased through automation and analytics. Analytics-based insights enable an administrator to gain a unique perspective on the data center's operations and serve as a catalyst to increase efficiency.

Figure 1. Cisco Tetration application segmentation

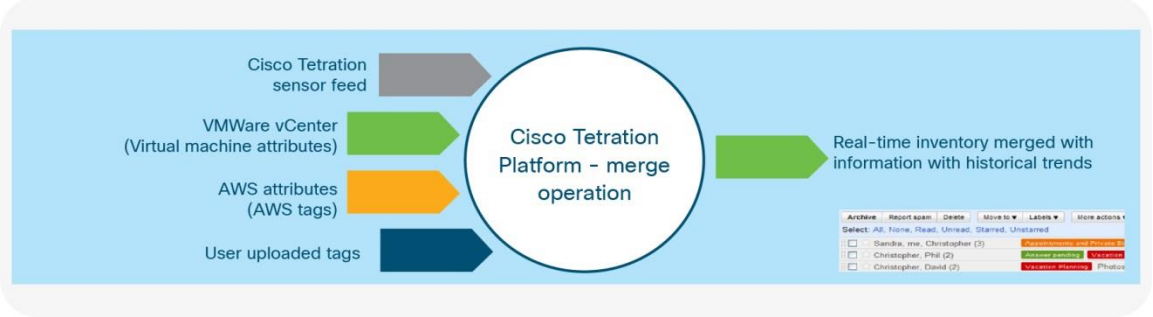


Real-time asset tagging

Asset tagging allows customers to annotate additional information to characterize the telemetry data and the workload (Figure 2). With this feature, identifying the resources to be included in application segmentation is as easy as searching the Internet. Using a robust vocabulary of keywords and judiciously using Boolean operations, an administrator can define policies governing specific workload characteristics: for example, a policy specifying that production database servers should not communicate with the Internet.

Each workload can have multiple tags (up to 32) that can add organizational and operational semantics to the identity of the asset. These tags can be imported from external systems—for example, a Configuration Management Database (CMDB) imported through an API—or they can be uploaded through a web user interface.

Figure 2. Associating business context using real-time asset tagging



The asset can be referred to by these tags, and complex queries can be constructed using these tags as references. The click-through drill-down analysis responds to tags in addition to the network identity. This capability allows the platform to respond easily to queries that do not assume IT-level expertise, thereby increasing the appeal of the Cisco Tetration platform to stakeholders such as business analysts and data scientists in addition to IT administrators.

Application workspaces

The challenge in creating a data center security framework is to develop a final policy set that can be enforced across a large number of workloads in a heterogeneous environment. Policy definition using traditional infrastructure and tools is a time-consuming, manual process and does not meet the dynamic requirements of modern applications. It results in a policy set that is static and insufficient to secure modern applications, with policy skewed to the needs of one application at the expense of the specific interests of others.

The Cisco Tetration platform uses modern big data technologies to offer organizations familiar features such as workflows and workspaces. Application workspaces enable collaboration across organizational boundaries without sacrificing specific interests. Multiple resource pools are isolated from one another using these workspaces and scopes. An application segmentation policy can span multiple workspaces.

A workspace is a collection of topology views, asset inventories, and policies that is saved as a snapshot and supports version control. Version control enables rollback to restore the workspace to a previously validated snapshot. Multiple workspaces can be owned by a single tenant and can be included in workflows that mirror the organization's structure and processes. Workspaces can be shared within a tenant and can be orchestrated in a workflow. The workflow accelerates the evolution of the data center's security framework, which includes the policy, inventory, and topology from the discovery stage to the final commit stage. Using this approach, application segmentation policy includes the whitelist policy generated as part of Cisco Tetration application insight, and it also includes other predefined policies from higher-level entities such as security operations. The Cisco Tetration platform then normalizes this policy based on the priority and hierarchy before enforcing it.

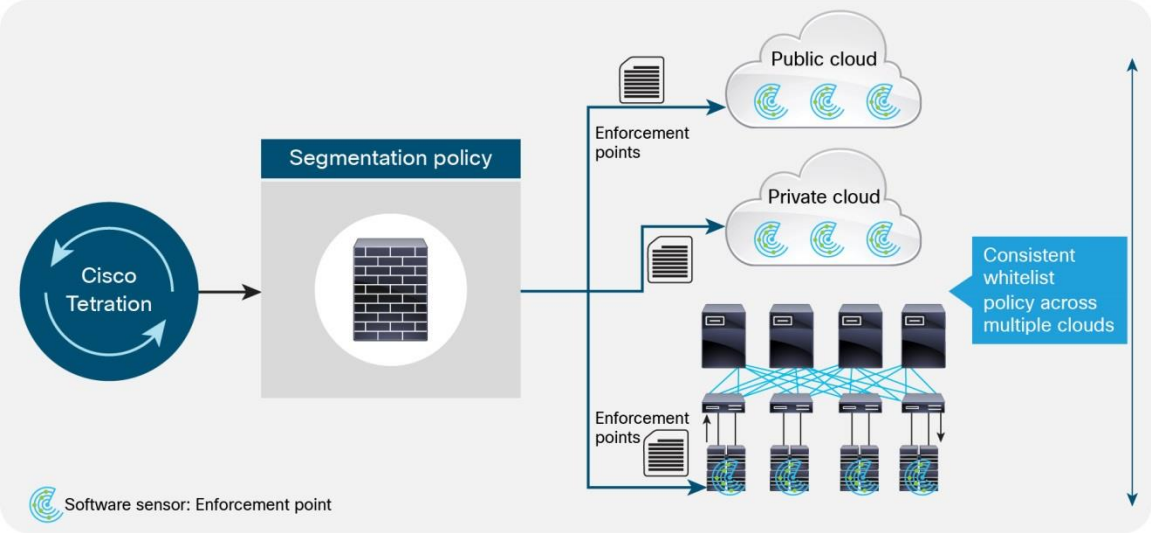
Policy enforcement and compliance

The Cisco Tetration platform allows you to merge the absolute policy, which may be part of the corporate policy, with the automated segmentation policy generated through application workspaces. After the policy set governing the application segmentation is committed, an administrator can trigger its enforcement with a single click.

Automated policy enforcement is performed through the Cisco Tetration Analytics™ software sensors running on the workload itself. The software sensors orchestrate the stateful policy enforcement using operating system capabilities such as ipsets and iptables in the case of Linux servers, and the Microsoft Windows advanced firewall in the case of Microsoft Windows servers. With this approach, effective application segmentation can be achieved across hybrid data center infrastructure (on premises and in the public cloud).

In addition, in a virtualized environment, this mechanism helps ensure that application segmentation policy moves with the workload, allowing you to increase application mobility without having to be concerned with infrastructure-specific segmentation policy. As the application dependencies and communication patterns evolve, the platform updates policy automatically (Figure 3).

Figure 3. Policy enforcement



Features and benefits

Table 1 lists that main features and benefits of Cisco Tetration application segmentation.

Table 1. Main features

Feature	Description
Zero-day readiness	**Plug zero-day vulnerabilities.** Policy from the Cisco Tetration platform allows only the required traffic, blocking everything else. This approach prevents a persistent threat from entering or searching for additional vulnerabilities on day zero.
Distributed deployment architecture	**Deploy a scalable deployment architecture for heterogeneous workloads distributed across a hybrid data center.** Application segmentation is achieved through deployment of two main components: software sensors as policy enforcement points and the Cisco Tetration platform. Sensors are installed on the workload, which can be a bare-metal system or a virtual machine. The back-end Cisco Tetration platform enforces the policy through software sensors. The platform comes with a large data store that supports workflows that scale to multiple tenants and roles and helps manage the lifecycle of millions of policies across thousands of applications.
Real-time asset tagging	**Eliminate time-consuming manual creation of lists of resources to segment applications. Define application segmentation default and absolute policies using the asset tags.** Real-time asset tagging allows you to associate rich business context with the servers. Administrators can then identify these resources just by using the tags. They can also pre-create inventory filters that will match a specific set of workloads and use these filters within the policy constructs. Any workload that meets the inventory filter criteria will inherit the same policy. This capability enables data center administrators to quickly develop consistent policies for their applications.
VMware vCenter, AWS security tags and Kubernetes integration	**Automate the import of virtual machine attributes, container attributes and public cloud tags using vCenter and AWS integration. These tags can be used to define application segmentation policy.** Importing the virtual machine attributes, container attributes and AWS tags allows data center administrators to extend the same constructs to create segmentation policies. As new virtual machines or containers are added with the same tags and attributes, those virtual machines inherit the same policy.

Feature	Description
Application workspaces	**Socialize and collaborate on policy definition and validation across organizational boundaries. Define, discover, visualize, and validate the data center security policy framework through multifaceted click-through views of topology, policy, and resources. Use built-in workflows to collaboratively define a policy set for policy enforcement across microsegments.** Follow the built-in workflow to define the policy set for enforcement, or use the workflow as a starter template and edit it to customize it. Refine the workflow further by using Application Dependency Mapping (ADM) and flow search tools to: ● Visualize the application topology ● Visualize the policy map ● Back-test the policy against historic data stored on the cluster appliance ● Troubleshoot policy by clicking through deep dives into the flow data ● Find the detail you need within the entire flow ● Query billions of historical records using schema-based or metadata-tag-based queries and receive a response in less than a second ● Use the collaborative features of the workflow to build consensus across the organization using Role- Based Access Control (RBAC) and workspaces. Then save the policy as a template with version control
One-click policy enforcement on heterogeneous workloads across a hybrid data center	**Enforce the security framework using application segmentation and reduce the surface vulnerable to attack.** Enforce policies with a single click. Use the mechanism in Linux and Microsoft Windows environments to enforce security policy. The Cisco Tetration platform normalizes the policy. The final policy set inherits the priorities set by RBAC-authorized users across the workspaces owned by a single tenant.
Software vulnerability detection	**Extend the policy enforcement capabilities to quarantine or control server communication based on software vulnerabilities and exposures.** Quickly identify if any of the package versions have known vulnerabilities or exposures, along with the severity. Get an accurate inventory all the servers that have the vulnerable package. Then tie this information to a policy that designates a specific action, such as quarantining a specific server.
User-defined analytics, reports, alerts, and dashboards using custom applications	**Use industry-standard notebook applications to create custom live content.** Use custom applications to: ● Create live reports, which can use local data together with external Internet-based context information ● Create custom alerts and avoid alert fatigue ● Build dashboards with graphics using open-source libraries
Policy compliance and notifications	**Monitor policy compliance on a minute-by-minute basis and generate alerts for policy noncompliance.** ● Generate policy-related alerts through the Kafka messaging interface ● These alerts can be monitored in the user interface. In addition, they can be consumed by other northbound systems such as the Security Incident and Event Management system (SIEM)

Licensing

The Cisco Tetration platform software is licensed based on the workload equivalence number (virtual machines and bare-metal servers). For complete cloud workload protection features, two licenses are required:

- **Tetration Detect (Base license):** This license is mandatory and provides the comprehensive telemetry data collection, visualization, application insight, policy recommendation, and policy simulation functions.
- **Tetration Protect (Policy enforcement):** The license provides the policy enforcement capability to protect the workloads using segmentation and beyond. The policy enforcement license must be purchased to use the platform's automated enforcement capability.

For organizations with multiple Cisco Tetration clusters, software licenses can be pooled across those clusters.

Licensing terms

In addition to being subject to the Cisco End User License Agreement (EULA; see https://www.cisco.com/go/eula), Cisco Tetration software is subject to Cisco Supplemental End User License Agreement terms (SEULA; see https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/cisco-tetration.pdf).

Deployment models and scale

Information regarding the deployment options and supported scale can be found in the platform datasheet - https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html?cachemode=refresh.

Supported operating systems

Tables 2 and 3 provide software sensors and compatibility information for the visibility and policy enforcement capabilities.

Table 2. Supported operating systems for full-visibility sensors

Server mode	Operating system	Distribution and release
Virtual machines and bare-metal servers	Linux	• Red Hat Enterprise Linux Release 5.0 and later • Red Hat Enterprise Linux Release 6.0 and later • Red Hat Enterprise Linux Release 7.1, 7.2, 7.3 and 7.4 • CentOS Release 5.0 and later • CentOS Release 6.0 and later • CentOS Release 7.1, 7.2, 7.3 and 7.4 • Oracle Linux Release 6.0 and later • Oracle Linux Release 7.1, 7.2, 7.3 and 7.4 • SUSE Linux Release 11.2, 11.3, and 11.4 • SUSE Linux Release 12.0, 12.1 and 12.2 • Ubuntu Release 12.04, 14.04, 14.10, and 16.04
	Microsoft Windows Server (server core and full desktop)	• Microsoft Windows Server 2008 Standard, Enterprise, Essentials, and Datacenter Editions • Microsoft Windows Server 2008 R2 Standard, Enterprise, Essentials, and Datacenter Editions • Microsoft Windows Server 2012 Standard, Foundation, Essentials, and Datacenter Editions • Microsoft Windows Server 2012 R2 Standard, Foundation, Essentials, and Datacenter Editions • Microsoft Windows Server 2016 Standard, Essentials, and Datacenter Editions
Container hosts	Linux	• Red Hat Enterprise Linux release 7.1, 7.2, 7.3, 7.4 • CentOS release 7.1, 7.2, 7.3, 7.4 • Ubuntu release 16.04
VDI desktop virtual machines	Microsoft Windows Desktop (VDI use case only)	• Microsoft Windows 7 Desktop • Microsoft Windows 8 Desktop • Microsoft Windows 10 Desktop

Table 3. Supported operating systems for enforcement

Server mode	Operating system	Distribution and release
Virtual machines and bare-metal servers	Linux (64-bit)	• Red Hat Enterprise Linux Release 6.0 to 6.9 • Red Hat Enterprise Linux Release 7.1, 7.2, 7.3 and 7.4 • CentOS Release 6.0 to 6.9 • CentOS Release 7.1, 7.2, 7.3 and 7.4 • Oracle Linux Release 6.0 to 6.9 • Oracle Linux Release 7.1, 7.2, 7.3 and 7.4 • Ubuntu 14.04, 14.10, and 16.04 • SUSE Linux Release 11.2, 11.3, and 11.4 • SUSE Linux Release 12.0, 12.1 and 12.2
Container hosts	Linux	• Red Hat Enterprise Linux release 7.1, 7.2, 7.3, 7.4 • CentOS release 7.1, 7.2, 7.3, 7.4 • Ubuntu release 16.04
	Microsoft Windows Server	• Microsoft Windows Server 2008 Standard, Datacenter, Enterprise, and Essentials • Microsoft Windows Server 2008 R2 Standard, Datacenter, Enterprise, and Essentials • Microsoft Windows Server 2012 Standard, Datacenter, Enterprise, and Essentials • Microsoft Windows Server 2012 R2 Datacenter, Enterprise, and Essentials • Microsoft Windows Server 2016 Standard, Datacenter, and Essentials

Ordering information

Information regarding the ordering options can be found in the platform datasheet - https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html?cachemode=refresh.

Put Cisco expertise to work to accelerate success

Cisco provides professional and support services to help organizations get the most value from the Cisco Tetration platform. Cisco® Services experts help integrate the platform into your production data center environment, define use cases relevant to your business objectives, tune machine learning, and validate policies and compliance to improve application and operation performance. Cisco Solution Support for Cisco Tetration Analytics provides hardware, software, and solution-level support.

One annual contract covers all support needs. With Cisco Tetration Analytics Services expertise, you experience faster time to value, comprehensive adoption in your environment, optimized policies and application performance, and solutionwide support.

Cisco Capital financing to help you achieve your objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce Capital Expenditures (CapEx), accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital financing is available in more than 100 countries. Learn more.

For more information

For more information about the Cisco Tetration platform, please visit https://www.cisco.com/c/en/us/products/data-center-analytics/tetration-analytics/index.html or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-738476-06 04/18