

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.

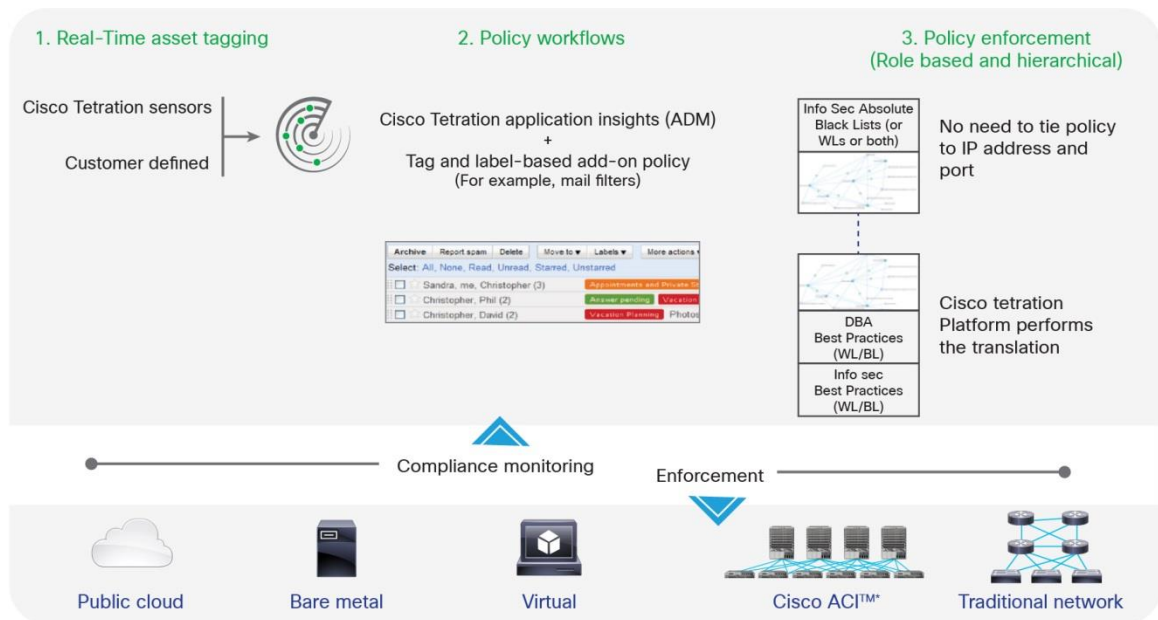
Product overview

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.

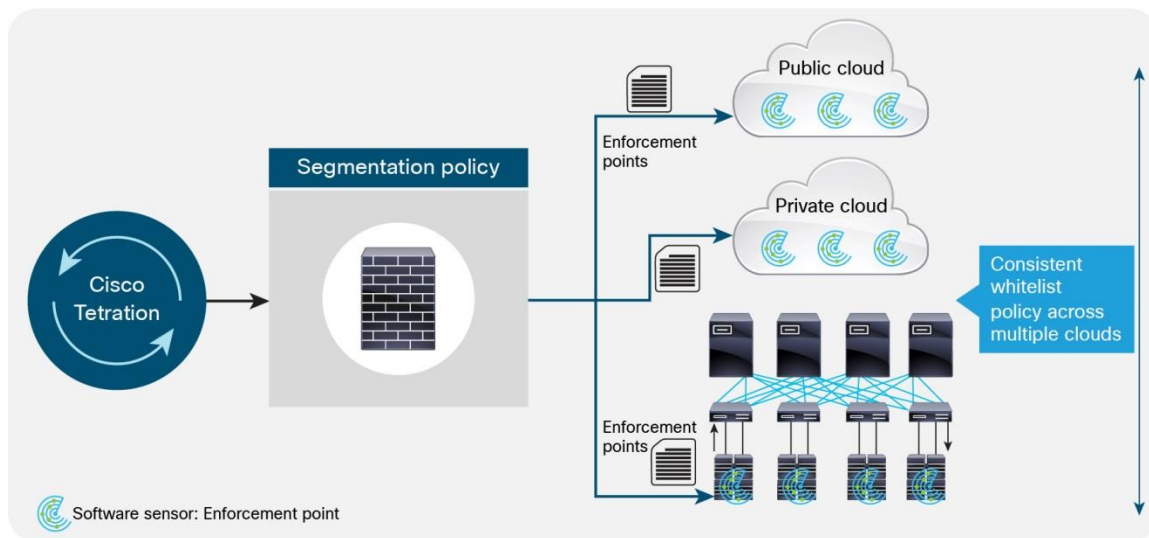
A workspace is a collection of topology views, asset inventories, and policies that is saved as a snapshot and supports version control. Version control enables rollback to restore the workspace to a previously validated snapshot. Multiple workspaces can be owned by a single tenant and can be included 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	<p>Plug zero-day vulnerabilities.</p> <p>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.</p>
Distributed deployment architecture	<p>Deploy a scalable deployment architecture for heterogeneous workloads distributed across a hybrid data center.</p> <p>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.</p>
Real-time asset tagging	<p>Eliminate time-consuming manual creation of lists of resources to segment applications. Define application segmentation default and absolute policies using the asset tags.</p> <p>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.</p>
VMware vCenter and Amazon Web Services (AWS) integration	<p>Automate the import of virtual machine attributes and public cloud tags using vCenter and AWS integration. These tags can be used to define application segmentation policy.</p> <p>Importing the virtual machine attributes and AWS tags allows data center administrators to extend the same constructs for to create segmentation policies. As new virtual machines are added with the same tags and attributes, those virtual machines inherit the same policy.</p>
Application workspaces	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Visualize the application topology • Visualize the policy map • Back-test the policy against historic data stored on the cluster appliance

Feature	Description
	<ul style="list-style-type: none"> • 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 <p>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.</p>
One-click policy enforcement on heterogeneous workloads across a hybrid data center	<p>Enforce the security framework using application segmentation and reduce the surface vulnerable to attack.</p> <p>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.</p>
User-defined analytics, reports, alerts, and dashboards using custom applications	<p>Use industry-standard notebook applications to create custom live content.</p> <p>Use custom applications to:</p> <ul style="list-style-type: none"> • 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	<p>Monitor policy compliance on a minute-by-minute basis and generate alerts for policy noncompliance.</p> <ul style="list-style-type: none"> • 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

Cisco Tetration platform software is licensed based on the number of workloads (virtual machines and bare-metal servers) on which the platform performs analytics. Telemetry data can be collected using software sensors, hardware sensors, or ERSPAN sensors, or any combination thereof. Two licenses are offered:

- **Base license:** This license provides the comprehensive telemetry data collection, application insight, forensics, policy recommendation, and policy simulation functions
- **Add-on license for policy enforcement and application segmentation:** The policy enforcement capability is licensed separately from the base functions. Customers must purchase the policy enforcement license if they want to use the platform's automated enforcement capability

If a customer has multiple Cisco Tetration clusters, software licenses can also 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 (SEULA; see https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/cisco-tetration.pdf) terms.

Deployment models and scale

The Cisco Tetration platform provides an appliance-like experience. It offers flexible deployment options based on the data center size and whether the deployment is based on physical hardware or in a public cloud. Three deployment options currently are available.

Cisco Tetration (large form factor) platform option

This deployment option consists of 36 servers and 3 Cisco Nexus® 9300 platform switches. It is suitable for data centers hosting more than 5,000 servers (virtual machine or bare metal). Table 2 shows the verified and supported scale, and Table 3 shows the power and the cooling requirements for this deployment option.

Table 2. Cisco Tetration Analytics large-form-factor scale

Platform characteristic	Specification
Number of concurrent servers (virtual machine or bare metal) from which telemetry data can be analyzed	Up to 25,000
Number of flow events that can be processed per second	2 million per second

Table 3. Power and cooling specifications for Cisco Tetration platform

Platform requirements	Specification
Peak power for Cisco Tetration Analytics (39-Rack-Unit [39RU] single-rack option) [*]	22.5 kW
Maximum cooling requirements for Cisco Tetration Analytics (39RU single-rack option)	50,000 BTUs per hour
Total weight for Cisco Tetration Analytics (39RU single-rack option)	1800 lb (800 kg)
Power Distribution Unit (PDU) and power supply (39RU single-rack option)	4 x 3-phase PDUs (current and voltage ratings vary by geography)
Peak power for Cisco Tetration Analytics (39RU dual-rack option)	11.25 kW per rack (22.5 kW total)
Maximum cooling requirement for Cisco Tetration Analytics (39RU dual-rack option)	25,000 BTUs per hour per rack
Total weight for Cisco Tetration Analytics (39RU dual-rack option)	900 lb per rack (400 kg per rack)
PDU and power supply (39RU dual-rack option)	4 x single-phase PDUs per rack (current and voltage ratings vary by geography)

^{*} Because of weight requirements, 8 of the 36 servers will ship separately and will need to be racked and cabled onsite.

Cisco Tetration-M (small form factor) option

The Cisco Tetration-M deployment option consists of 6 servers and 2 Cisco Nexus 9300 platform switches. It is suitable for data centers with fewer than 5,000 servers (virtual machine or bare metal). Table 4 shows the verified and supported scale, and Table 5 shows the power and cooling requirements for the Cisco Tetration-M option.

Table 4. Cisco Tetration-M scale

Platform characteristic	Specification
Number of concurrent servers (virtual machine or bare metal) from which telemetry data can be analyzed	Up to 5,000
Number of flow events that can be processed per second	500,000 per second

Table 5. Power and cooling specifications for Cisco Tetration-M

Platform requirements	Specification
Peak power for Cisco Tetration-M (8RU)	5.5 kW
Maximum cooling requirement for Cisco Tetration-M (8RU)	13,500 BTUs per hour

Cisco Tetration Cloud (Amazon Web Services public cloud) option

With the Cisco Tetration Cloud Amazon Web Services (AWS) public cloud deployment option, the Cisco Tetration software can run in an AWS instance. The AWS instance for the Cisco Tetration platform is owned by the customer. This option is suitable for data centers hosting fewer than 1000 servers (virtual machine or bare metal). If software sensors are deployed on workloads running in a private cloud or on the premises, then AWS Direct Connect is required to connect to the Cisco Tetration Cloud. Table 6 shows the AWS instance type, Amazon Elastic Block Storage (EBS), and Amazon Elastic IP address (EIP) requirements to run Cisco Tetration Cloud in AWS. Table 7 shows the platform scale.

Table 6. AWS instance requirements for Cisco Tetration Cloud

AWS instance type	Specification
t2.medium	6 instances
m4.large	15 instances
m4.2xlarge	2 instances
m4.xlarge	3 instances
r4.large	13 instances
r4.2xlarge	23 instances
r4.xlarge	4 instances
m4.4xlarge	8 instances
Amazon EBS: General-purpose solid-state disk (SSD; gp2)	65 Terabytes (TB)
Amazon EIP	50 addresses

Table 7. Platform scale for Cisco Tetration Cloud

Platform characteristic	Specification
Number of concurrent servers (virtual machine or bare metal) from which telemetry data can be analyzed	Up to 1000
Number of flow events that can be processed per second	200,000 per second

Supported operating systems

Table 8 shows the operating systems supported for automated policy enforcement.

Table 8. Operating systems supported for policy enforcement

Server mode	Operating system	Distribution and release
Virtual machines and bare-metal servers	Linux (64-bit)	<ul style="list-style-type: none"> Red Hat Enterprise Linux Release 6.0 and later Red Hat Enterprise Linux Release 7.1, 7.2, and 7.3 CentOS Release 6.0 and later CentOS Release 7.1, 7.2, and 7.3 Oracle Linux Release 6.0 and later Oracle Linux Release 7.1, 7.2, and 7.3 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
	Microsoft Windows Server	<ul style="list-style-type: none"> 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

Tables 9, 10, and 11 provide hardware and software bundle part numbers for the Cisco Tetration Analytics LFF and Cisco Tetration-M SFF options.

Table 9. Hardware and subscription software bundle for Cisco Tetration platform option

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION	TA-CL-G1-39-K9	Cisco Tetration Analytics bundle part number that includes the hardware, software subscription license, and Cisco Advanced Services–Fixed (AS-Fixed) service for deployment. AS-Fixed is included at no additional cost.
		Cisco Tetration Analytics hardware platform with 36 servers and 3 switches that will support processing of Cisco Tetration Analytics telemetry data from up to 25,000 servers (virtual machine or bare metal).
	C1-TA-SW-K9	Bundle part number for the Cisco Tetration Analytics software subscription license. See Table 11 for details.
	ASF-DCV1-TA-QS-M	AS-Fixed part number for Cisco Tetration Analytics implementation services.

Table 10. Hardware and subscription software bundle for Cisco Tetration-M option

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION-M	TA-CL-G1-SFF8-K9	Cisco Tetration Analytics bundle part number that includes the hardware, software subscription license, and Cisco Advanced Services–Fixed (AS-Fixed) service for deployment. AS-Fixed is included at no additional cost.
		Cisco Tetration Analytics hardware platform with 6 servers and 2 switches, required for Cisco Tetration-M.
	C1-TA-SW-K9	Bundle part number for the Cisco Tetration Analytics software subscription license.
	ASF-DCV1-TA-QS-M	AS-Fixed part number for Cisco Tetration Analytics implementation services.

Table 11. Subscription software license for Cisco Tetration and Cisco Tetration-M options

Bundle part number	Part numbers included in bundle	Description
C1-TA-SW-K9		Bundle part number for the Cisco Tetration Analytics software subscription license.
	C1-TA-BASE-1K-K9	Cisco Tetration Analytics subscription software license in multiples of 1000 servers (virtual machine or bare metal). Choose a quantity between 1 and 25. For example, a quantity of 5 will provide the license price for up to 5000 software sensor instances.
	C1-TA-ENF-1K-K9	Cisco Tetration Analytics subscription software policy enforcement add-on license in multiples of 1000 servers (virtual machine or bare metal). Choose a quantity between 1 and 25. For example, a quantity of 5 will provide the license price for up to 5000 software sensor instances.

Also note the following additional information about the software subscription license part number:

- You can select a 1-year, 3-year, or 5-year subscription term
- The subscription price includes software support
- The subscription tier is selected automatically based on the quantity entered
- Enforcement is an add-on license and cannot be ordered without the base software license
- The subscription is set up to renew automatically at the end of the period
- You can select the annual billing option or prepay for the entire term
- You can add more software sensor instance licenses

Licensing terms

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

Tables 12 and 13 provide software and hardware bundle part numbers for the Cisco Tetration Cloud option.

Table 12. Software bundle for Cisco Tetration Cloud option

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION-V		Cisco Tetration Analytics bundle part number that includes the software subscription license for the virtual form factor.
	C1-TA-V-SW-K9	Bundle part number for the Cisco Tetration Analytics software subscription license.
	ASF-DCV1-TA-QS-M	Optional AS-Fixed part number for Cisco Tetration Analytics implementation services.

Table 13. Subscription software license for Cisco Tetration Cloud option

Bundle part number	Part numbers included in bundle	Description
C1-TA-V-SW-K9		Bundle part number for the Cisco Tetration Analytics software subscription license, applicable only for Cisco Tetration Cloud.
		Cisco Tetration Analytics subscription software license in multiples of 100 servers (virtual machine or bare metal). Choose a quantity between 1 and 10. For example, a quantity of 5 will provide the license price for up to 500 software sensor instances.
	C1-TA-ENF100-K9	Cisco Tetration Analytics subscription software policy enforcement add-on license in multiples of 100 servers (virtual machine or bare metal). Choose a quantity between 1 and 10. For example, a quantity of 5 will provide the license price for up to 500 software sensor instances.

Licensing terms

Your license for Cisco Tetration Cloud software does not include the public cloud (for example, AWS) instances required to run the software. You are responsible for acquiring the required public cloud instances directly from your public cloud provider (for example, AWS). Not all public cloud environments are certified for use with Cisco Tetration Cloud. Please check the Cisco Tetration documentation for requirements for supported public cloud environments. Cisco Tetration Cloud performance may vary, because Cisco cannot guarantee public cloud (for example, AWS) service levels.

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

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>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)