Cisco Tetration Platform

The Cisco Tetration™ platform addresses data center operational and security challenges by providing comprehensive workload-protection capability and unprecedented insights across a multicloud infrastructure.

Product overview

Applications are guiding the design of data center infrastructure. Today’s applications are dynamic, using virtualization, containerization, microservices, and workload mobility technologies, with communication patterns between application components constantly changing. Now, 76 percent of data center traffic is east-west, a fundamental change from traffic patterns in the past. This technological shift has contributed to an increased attack surface and free lateral movement within the data center infrastructure. This dynamic environment has created several challenges that organizations must address:

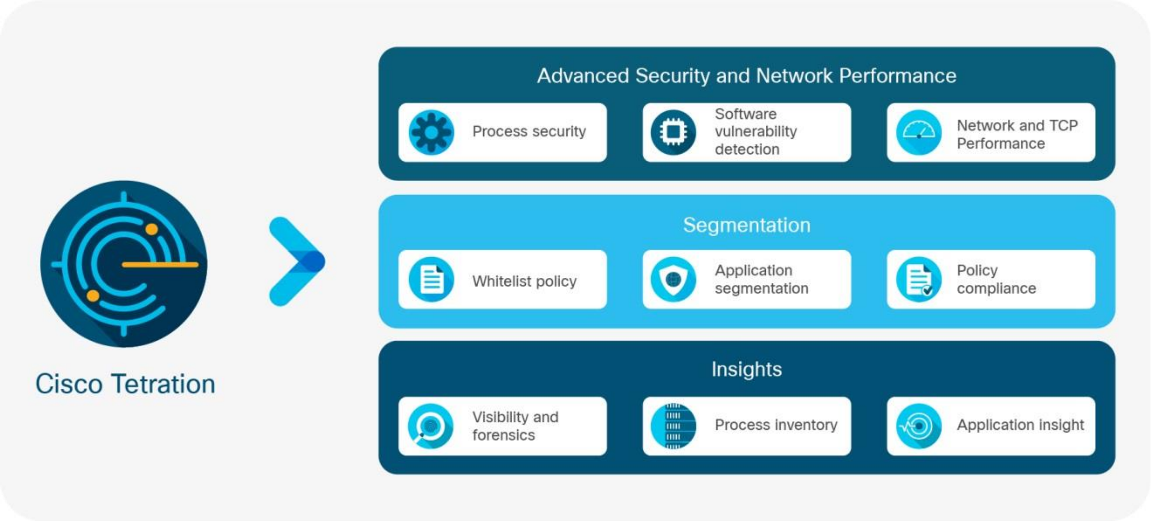
- Insufficiency of static perimeter-based security model in a data center to cope with current technology
- Lack of ability to auto generate whitelist policies for segmentation based on application behavior
- No consistent approach to implementing segmentation using whitelist across a multicloud infrastructure
- Lack of a comprehensive approach to reduce the attack surface, minimize lateral movement, and detect behavior deviations

Cisco Tetration™ platform is designed to fully address these challenges using comprehensive traffic telemetry data collected from both servers and Cisco Nexus® switches. The platform performs advanced analytics using an algorithmic approach and provides comprehensive workload protection for a multicloud data center. This algorithmic approach includes unsupervised machine-learning techniques and behavioral analysis. The platform provides a ready-to-use solution for:

- Complete visibility into application components, communications, and dependencies to enable implementation of a zero-trust model in the data center
- Automatic generation of a whitelist policy based on application behavior and including any existing security policy mandated by business requirements
- Consistent enforcement of this segmentation policy across a multicloud infrastructure to minimize lateral movement
- Identification of software vulnerabilities and exposures to reduce attack surface
- Process behavior baselining and identification of deviations for faster detection of any Indicators of Compromise (IOCs)

Figure 1 shows the supported use cases for the Cisco Tetration platform.

Figure 1. Cisco Tetration use cases

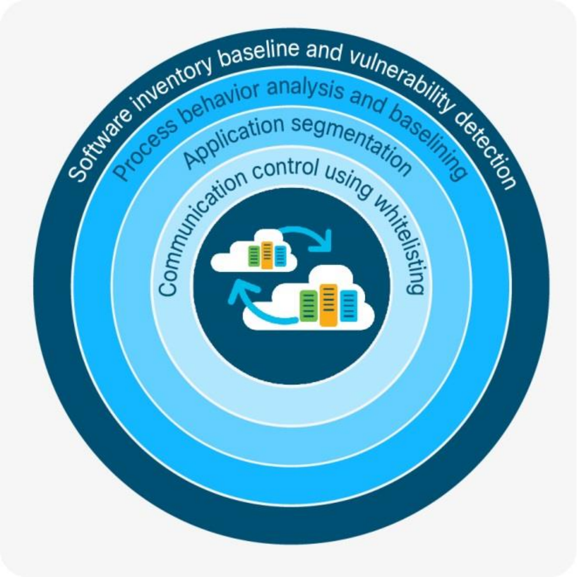


Data center use cases

Cisco Tetration platform features and functions support critical data center security and operations use cases:

- **Workload protection:** The Cisco Tetration platform enables holistic workload protection for multicloud data centers by using:
  - Whitelist-based segmentation, which allows for implementation of a zero-trust model
  - Behavior baselining, analysis, and identification of deviations for processes
  - Detection of common vulnerabilities and exposures associated with the software packages installed on the servers
  - The ability to act proactively, such as quarantining servers when vulnerabilities are detected and blocking communication when policy violations are detected

Figure 2. Multidimensional workload protection approach using Cisco Tetration


Software inventory baseline and vulnerability detection
Process behavior analysis and baselining
Application segmentation
Communication control using whitelisting

By using this multidimensional workload protection approach (Figure 2), Cisco Tetration significantly reduces the attack surface, minimizes lateral movement in case of security incidents, and quickly identifies anomalous behaviors within the data center.

To learn more about workload protection, refer to the Cisco Tetration Platform for Workload Protection data sheet https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-740328.html or the Cisco Tetration Application Segmentation data sheet https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-738476.html.

- **Network Insights.** Robust data-plane telemetry information from servers as well as network, in conjunction with machine learning, allows the Cisco Tetration platform to provide better network and flow performance insights to the operations team. Using this capability, users can:
    - View TCP performance details, such as application response times, network roundtrip times, window size reduction, and handshake latency
    - Display a hop-by-hop view of each flow across the data center fabric, along with burst information, congestion, and packet-drop indicators
    - Identify whether a bottleneck is caused by an application or the network

All this information is available in time-series views, providing the capability to display historical information and compare details over time.

To learn more about network insights use cases, refer to the Cisco Tetration Network Insights data sheet.

Features and benefits

Table 1 lists the main features and benefits of the Cisco Tetration platform.

Table 1. Cisco Tetration platform primary features and benefits

Feature	Benefit
Software sensors	● Capture all activity on a server, including east-west traffic, eliminating blind spots ● Designed to operate within administrator-defined computing SLAs (the default is within 3% of CPU utilization) ● Reside outside the data path and do not affect application performance ● Supports bare metal servers, virtual machines and containers
ERSPAN sensors	● Collect rich telemetry data from portions of the network in which software and hardware sensors are not present ● Collect data from multiple vantage points for better correlation and analysis
NetFlow sensors	● Collect summarized flow telemetry data from portions of the network in which software and hardware sensors are not present, collects telemetry in NetFlow format ● Collect data from multiple vantage points for better correlation and analysis
Hardware sensors	● Line-rate telemetry required for Tetration within the switch's Application-Specific Integrated Circuit (ASIC), eliminating any impact to the switch CPU ● Telemetry that enables Cisco Tetration to provide rich network performance insights
Anyconnect NVM proxy sensor	● Collect telemetry from Anyconnect NVM agent running on end point devices such as laptops, desktops, smart phones, etc., ● This provides information around user, device name, FQDN, processes running on the device as well as what URL or application was accessed. ● Correlate the user data with the user group within an organization ● Define specific policies for segmentation using user and user group information, that can be enforced on the workloads
Comprehensive telemetry information	● Comprehensive telemetry data enables application behavior–based analytics and monitoring of behavior deviations ● Information is independent of whether the payload is encrypted or unencrypted ● Collection of process details and software package information allow detection of behavior deviations and vulnerabilities
Real-time asset tagging	● Associates business context with the telemetry data in the form of tags ● Provides the flexibility to search for inventory and traffic and even define policies based on this metadata ● Administrators can tie business policy to application segmentation policy ● The northbound REST API is used to keep this information up to date
VMware vCenter and Amazon Web Services (AWS) resource tags	● Integrate with VMware vCenter to consume virtual machine attributes in the form of tags in an on-premises data center ● Integrate with AWS to map AWS resource tags in the Tetration platform ● Define policies or search inventory and traffic based on these well-known attributes
Sensor Network Address Translation (NAT) and Port Address Translation (PAT) support	● Sensors can be deployed in environments in which NAT or PAT is applied between servers and the Tetration platform ● NAT and PAT are suitable for deployments with multiple domains with overlapping IP addresses
Near-real-time flow visibility	● Search tens of billions of flows and get actionable insight in less than a second ● Perform faster troubleshooting and anomaly detection for more effective data center operations ● Effectively identify application behavior deviation and better manage network policy compliance
Support for data center scalability	● Collect telemetry data from every packet in the data center without any sampling ● The platform can process millions of unique flows per second ● Long-term data retention supports forensics and analysis operations
Ease of deployment and use	● The platform functions as an appliance with ready-to-use support for critical operation use cases ● Unsupervised machine learning reduces the need for human interaction
Platform security	● User access is controlled through Role-Based Access Control (RBAC) for both the GUI and REST API ● Communication between different platform components is completely secured using a built-in firewall

Feature	Benefit
Platform self-monitoring	● Self-monitoring eliminates the need for extensive in-house big data expertise to operate this platform ● Monitoring extends all the way to the sensors to facilitate easier operations ● Use an option to enable the Cisco® Smart Call Home function to report known error states
Microsoft Active Directory integration	● User authentication and authorization is performed through the external Active Directory ● This integration eliminates the need to maintain user login credentials locally on the Tetration platform
Multitenancy support	● The multitenant-capable GUI and back end enables the platform to be shared across multiple groups and organizations ● RBAC controls are implemented to partition and present only authorized data
Open interface	● Use the open REST API for northbound system integration ● Use the notification mechanism to more easily monitor compliance-based events and detect anomalies ● Developers can access the data lake and write their own applications using Python or Scala

Cisco Tetration applications

The Cisco Tetration platform provides access to the data lake in the cluster through Tetration applications. Using these applications, developers, programmers, and data scientists can access the information in the data lake and write their own applications using Python, Scala, or Spark SQL. These applications can run as microservices on the platform itself and can be triggered to run using various mechanisms:

- An application can run as a one-time job.
- Applications can be scheduled to run periodically (hourly, daily, weekly, etc.).
- Applications can be triggered based on data dependencies.

Developers can also bring data from other data sources using JSON-based streaming telemetry data and compare this data with the flow information in the data lake. If required, applications can trigger external notifications through the Kafka message bus or display the processed data in the Cisco Tetration web UI dashboard. Streaming telemetry data can be brought in simultaneously from up to 10 different data sources.

Table 2 summarizes the specifications for Cisco Tetration applications.

Table 2. Cisco Tetration applications specifications

Tetration applications data points	Specification
Maximum number of concurrent user applications that can be run on the platform	14
Maximum number of applications that can be submitted	100
Data limit for uploading external data to be used in an application	5 terabytes (TB) shared across all applications
Container specification for each application (upper limit)	3-core virtual CPU (vCPU) Approximately 6 GB of RAM
Python version	Release 3.0
Scala version	Release 2.11.0
Spark SQL	Release 1.6.2 (not fully ANSI compliant)

Software licensing

Cisco Tetration platform software is licensed based on the number of workload equivalents depending on the sensor type being used. Telemetry data can be collected using software sensors, hardware sensors or ERSPAN sensors, or in any combination. Workload is defined as a virtual machine, bare-metal server or container host. There are two types of licenses for on-premises solutions using appliance hardware or virtual form factor:

- **Tetration Detect (base license):** This license provides the comprehensive telemetry data collection, application insight, forensics, network performance, policy recommendation, and policy simulation functions.
- **Add-on Tetration Protect (policy enforcement):** 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.
- **Tetration Endpoint visibility license:** This license provides the comprehensive telemetry data collection from AnyConnect client installed in the end points (laptops, desktops, smart phones, etc.,) using NVM module. This provides insights into user, device, group, process ID, process hierarchy, OS as well as domain name accessed from the endpoint. This information is very powerful to give end to end view into users accessing applications. Customers must purchase the endpoint visibility license if they want to use the platform's capability to collect, analyze and provide visibility into end point device activities. This license can be independent of the Protect & Detect licenses. No additional agent installation is required. This does not include any other licenses required to enable AnyConnect NVM (those licenses are to be purchased separately).

If a customer has multiple Cisco Tetration clusters, software licenses can be pooled across those clusters.

Licenses for Cisco Tetration SaaS (software-as-a-service) offering:

- **Tetration Workload Protection license:** This license combines Tetration Detect as well as Tetration Protect features under one single SaaS license for customers. SaaS licensing is based on the number of workloads on which software sensors are installed. SaaS requires customers to deploy software sensors on bare metal, virtual machines, and container hosts.
- **Tetration Endpoint visibility license:** This license provides the comprehensive telemetry data collection from AnyConnect client installed in the end points (laptops, desktops, smart phones, etc.,) using NVM module. This provides insights into user, device, group, process ID, process hierarchy, OS as well as URL accessed from the endpoint. This information is very powerful to give end to end view into users accessing applications. Customers must purchase the endpoint visibility license if they want to use the platform's capability to collect, analyze and provide visibility into end point device activities. This license can be independent of the Protect & Detect licenses. No additional agent installation is required. This does not include any other licenses required to enable AnyConnect NVM (those licenses are to be purchased separately).

If a customer has Cisco Tetration SaaS licenses, they cannot be ported over to an on-premises license option.

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 the terms of the Cisco Supplemental End User License Agreement (SEULA; see https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/cisco-tetration.pdf).

Deployment models and scale

The Cisco Tetration platform provides an appliance-like experience. It provides flexible deployment options based on the data center size and whether the organization wants a deployment based on physical hardware or 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 servers. It is suitable for data centers hosting more than 5000 servers (virtual machine or bare metal).

Table 3 shows the verified and supported scale. Table 4 shows the power and the cooling requirements for the Cisco Tetration platform.

Table 3. Cisco Tetration standard platform scale

Platform characteristics	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	Up to 2 million per second
Number of hardware sensor enabled Cisco Nexus 9000 Series Switches	Up to 100

Table 4. Power and cooling specifications for large form factor

Platform requirements	Specification
Peak power for Cisco Tetration - 39-Rack-Unit [39RU] single-rack option*	22.5 kW
Maximum cooling requirements for Cisco Tetration - 39RU single-rack option*	50,000 BTUs per hour
Total weight for Cisco Tetration - 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 - 39RU dual-rack option	11.25 kW per rack (22.5 kW total)
Maximum cooling requirement for Cisco Tetration - 39RU dual-rack option	25,000 Btus per hour per rack
Total weight for Cisco Tetration - 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)

*For single-rack configuration, 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 small form factor deployment option consists of 6 servers and 2 Cisco Nexus 9300 platform switches. It is suitable for data centers that have fewer than 5000 servers (virtual machine or bare metal).

Table 5 shows the verified and supported scale. Table 6 shows the power and cooling requirements for the Cisco Tetration-M SFF platform.

Table 5. Cisco Tetration-M platform scale

Platform characteristics	Specification
Number of concurrent servers (virtual machine or bare metal) from which telemetry data can be analyzed	Up to 5000
Number of flow events that can be processed per second	Up to 500,000 per second
Number of hardware sensor enabled Cisco Nexus 9000 Series Switches	Up to 100

Table 6. 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 Virtual option

With the Cisco Tetration Virtual (Tetration-V), you can deploy the Cisco Tetration platform in on-premises using hardware of your choice. The customer is responsible for purchasing the required hardware based on the specifications to run the Tetration software. This option is suitable for data centers that host fewer than 1000 workloads (virtual machine or bare metal). These workloads can be in on-premises or any public cloud.

Note: This consumption option does not currently support ingesting telemetry from hardware. It also does not support User Apps on the platform.

Table 7 shows the platform scale for Cisco Tetration-V.

Table 7. Platform scale for Cisco Tetration-V

Platform characteristic	Specification
Number of concurrent workloads (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	Up to 70,000 per second

Software Pre-requisites for Deploying Tetration-V

- VMware cluster running VMware vSphere 6.5
- Ability to access the VMware vSphere Flash Player GUI
- Cisco Tetration Analytics Software Only Orchestrator Appliance .ova file
- Cisco Tetration Analytics Mother RPM, Tetration Adhoc RPM, and rpminstall RPM

Table 8 shows the hardware system requirements for the virtual appliance option.

Table 8. Hardware instance requirements for the Cisco Tetration-V ESXi

Platform characteristic	Specification	Additional details
Number of CPU cores	128	Assumption is these will be cores, not hyperthreads
RAM	2 TB	6 virtual machines need 128 GB of RAM, which means the ESXi hosts needs 256 GB to start these virtual machines
Storage	18.1 TB	Storage should be high speed, such as SSD arrays or vSAN; expectation is initially 5000 IOPS
Network	10 Gbps	10 G network connectivity between the virtual machines
Number of virtual machines	55	

Note: Total includes some headroom for burst and upgrades; support requires these resources to be available. This consumption option does not currently support ingesting telemetry from hardware sensors.

Cisco Tetration SaaS option

With the Cisco Tetration SaaS option, customers can consume workload protection functionality without deploying the platform on premises. With this option, Cisco Tetration software runs in the cloud, managed and operated by Cisco. The customer is responsible for purchasing the required software subscription licenses and deploying software sensors on workloads.

This deployment option Is well suited for SaaS-only or SaaS-first customers, as it offers scale flexibility: You can start small and grow as your demand grows.

Note: This consumption option does not currently support ingesting telemetry from hardware sensors. It also does not support User Apps on the platform.

Platform support and compatibility

Tables 9–12 provide software and hardware support and compatibility information for the Cisco Tetration platform.

Table 9. 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, 7.4, 7.5 • CentOS Release 5.0 and later • CentOS Release 6.0 and later • CentOS Release 7.1, 7.2, 7.3, 7.4, 7.5 • Oracle Linux Release 6.0 and later • Oracle Linux Release 7.1, 7.2, 7.3, 7.4, 7.5 • SUSE Linux Release 11.2, 11.3, 11.4 • SUSE Linux Release 12.0, 12.1, 12.2, 12.3 • Ubuntu Release 12.04, 14.04, 14.10, 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

Server mode	Operating system	Distribution and release
Container host	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 10. 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 and later ● Red Hat Enterprise Linux Release 7.1, 7.2, 7.3, 7.4, 7.5 ● CentOS Release 6.0 and later ● CentOS Release 7.1, 7.2, 7.3, 7.4, 7.5 ● Oracle Linux Release 6.0 and later ● Oracle Linux Release 7.1, 7.2, 7.3, 7.4, 7.5 ● Ubuntu 14.04, 14.10, 16.04 ● SUSE Linux Release 11.2, 11.3, 11.4 ● SUSE Linux Release 12.0, 12.1, 12.2, 12.3
	Microsoft Windows Server (server core and full desktop)	● 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, Foundation, and Essentials ● Microsoft Windows Server 2012 R2 Standard, Datacenter, Foundation, and Essentials ● Microsoft Windows Server 2016 Standard, Essentials, and Datacenter Editions
Container host	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 11. Supported operating systems for universal software sensors

Server mode	Operating system	Distribution and release
Virtual machines and bare-metal servers	Linux	● Red Hat Enterprise Linux Release 4.0 (32-bit and 64-bit) ● CentOS Release 4.0 (32-bit and 64-bit) ● Red Hat Enterprise Linux Release 5.0 (32-bit) ● CentOS Release 5.0 (32-bit)
	AIX	● AIX Release 5.3, 6.1, 7.1, 7.2
	Solaris	● Solaris 11.0 (64-bit) on x86 architecture
	Microsoft Windows Server	● Microsoft Windows Server (32-bit and 64-bit)

Table 12. Supported hardware sensors

Product line	Platform	Minimum Software release
Cisco Nexus 9300 platform switches (Cisco NX-OS Software mode)*	Cisco Nexus 93180YC-EX, 93108TC-EX, and 93180LC-EX	Cisco NX-OS Release 9.2.1 and later
	Cisco Nexus 93180YC-FX, 93108TC-FX, and 9348GC-FXP	Cisco NX-OS Release 9.2.1 and later
	Cisco Nexus 9336C-FX2 and 93240YC-FX2	Cisco NX-OS Release 9.2.1 and later
Cisco Nexus 9300 platform switches (Cisco Application Centric Infrastructure [Cisco ACI™] mode)*	Cisco Nexus 93180YC-EX, 93108TC-EX, and 93180LC-EX	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 93180YC-FX, 93108TC-FX	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 9348GC-FXP	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 9336C-FX2	Cisco ACI Release 3.2(1m) and later
	Cisco Nexus 9500 series switches with N9K-X9736C-FX line cards	Cisco ACI Release 3.1(1i) and later

*Hardware sensors require an additional telemetry license on the switch. Refer to the appropriate switch data sheet for the telemetry license part number.

Ordering information

Table 13 provides hardware and software bundle part numbers for the Cisco Tetration LFF option.

Table 13. Hardware and subscription software bundle for Cisco Tetration LFF option

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION		Cisco Tetration 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
	TA-CL-G1-39-K9	Cisco Tetration hardware platform with 36 servers and 3 switches that will support processing of Cisco Tetration telemetry data from up to 10,000 servers (virtual machine or bare metal)
	C1-TA-SW-K9	Bundle part number for the Cisco Tetration software subscription license; see Table 17 for details
	C1-TA-V-SW-K9	Bundle part number for the Cisco Tetration software subscription license; see Table 17 for details
	ASF-DCV1-TA-QS-M	AS-Fixed part number for Cisco Tetration implementation services

Table 14 provides hardware and software bundle part numbers for the Cisco Tetration-M (8RU) option.

Table 14. Hardware and subscription software bundle for Cisco Tetration-M SFF option

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION-M		Cisco Tetration 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
	TA-CL-G1-SFF8-K9	Cisco Tetration hardware platform with 6 servers and 2 switches, required for Cisco Tetration-M
	C1-TA-SW-K9	Bundle part number for the Cisco Tetration software subscription license, see Table 17 for details
	C1-TA-V-SW-K9	Bundle part number for the Cisco Tetration software subscription license; see Table 17 for details
	ASF-DCV1-TA-QS-M	AS-Fixed part number for Cisco Tetration implementation services

Table 15 provides the software bundle part number for the Cisco Tetration software subscription license.

Table 15. Bundle for Cisco Tetration-V option (AWS, Azure, or ESXi)

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION-V		Cisco Tetration 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 software subscription license
	ASF-DCV1-TA-QS-M	Optional AS-Fixed part number for Cisco Tetration implementation services

Table 16 provides subscription software bundle part numbers used for the Cisco Tetration platform for on-premises appliances as well as virtual deployment models (including Azure, AWS, and ESXi)

Table 16. Subscription software license for Cisco Tetration LFF and Cisco Tetration-M SFF options

Bundle part number	Part numbers included in bundle	Description
C1-TA-SW-K9		Bundle part number for the Cisco Tetration software subscription license
	C1-TA-BASE-1K-K9	Cisco Tetration detect subscription software license in multiples of 1000 workload equivalence. 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	Add-on Cisco Tetration protect subscription software license for policy enforcement in multiples of 1000 workload equivalence. 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-ENDPT-K9	Cisco Tetration endpoint visibility software subscription license in multiples of 1 end points. Choose a quantity between 1000 and 999999. For example, a quantity of 5000 will provide license price for up to 5000 endpoint AnyConnect agents onto Tetration
C1-TA-V-SW-K9		Bundle part number for the Cisco Tetration software subscription license, applicable only to Cisco Tetration-V
	C1-TA-BASE100-K9	Cisco Tetration Detect subscription software license in multiples of 100 workload equivalence; choose a quantity from 1 to 10 (for example, a quantity of 5 will provide the license price for up to 500 software sensor instances)
	C1-TA-ENF100-K9	Add-on Cisco Tetration Protect subscription software license for policy enforcement in multiples of 100 workload equivalence; choose a quantity from 1 to 10 (for example, a quantity of 5 will provide the license price for up to 500 software sensor instances)

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

- 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.
- You can select the annual billing option or prepay for the entire term.
- You can add more software sensor instance licenses.
- This software subscription license can be used with both Cisco Tetration hardware clusters and the Cisco Tetration Virtual option.

Table 17 provides subscription software bundle part numbers used for the Cisco Tetration SaaS deployment option.

Table 17. Software bundle for Cisco Tetration SaaS option

Bundle part number	Part numbers included in bundle	Description
C1-TAAS-SW-K9		Cisco Tetration bundle part number that includes the software subscription license for SaaS option.
	C1-TAAS-WP-FND-K9	Bundle part number for the Cisco Tetration workload protection subscription license. You need minimum quantity of 100, with a 1 or 3 year term.
	C1-TAAS-ENDPT-K9	Cisco Tetration endpoint visibility software subscription license for endpoints. Choose a quantity between 1000 and 999999. For example, a quantity of 5000 will provide license price for up to 5000 endpoint AnyConnect agents onto Tetration

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.
- You can select the annual billing, a monthly or quarterly option, or prepay for the entire term.
- You can add more software sensor instance licenses.
- This software subscription license can be used only with a Cisco Tetration SaaS deployment.

Licensing terms

Your license for Cisco Tetration-V software does not include hardware or ESXi licenses required to run the software. You are responsible for acquiring the required hardware based on specifications and Vmware ESXi licenses. Cisco Tetration Virtual performance may vary, because of underlying hardware performance or configuration.

In addition to being subject to the Cisco EULA (see https://www.cisco.com/go/eula), your 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 adoption

Cisco provides professional and support services from Advisory, Implementation and Optimization to ongoing Solution Support, 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 provides hardware, software, and solution-level support.

We offer a selection of custom and fixed-price, fixed-scope services for Cisco Tetration that help you experience faster time to value, comprehensive adoption in your environment, optimized policies and application performance, and solution wide support.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information about the Cisco Tetration platform, please visit https://www.cisco.com/go/tetration 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 C78-737256-14 11/18