We're here to help you enable work from anywhere.   View resources

Cisco Tetration Platform Data Sheet

Updated: March 10, 2020 · See Revisions

🔗 Share ▾   🈯 Translations   ⬇ Download   🖨 Print

The Cisco Tetration™ platform addresses data center security challenges by providing comprehensive workload-protection capability and unprecedented insights across a hybrid cloud 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 generate and manage 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

The Cisco Tetration platform is designed to fully address these challenges, using comprehensive traffic telemetry data collected from the workloads. 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 microsegmentation 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)

Data center use cases

The Cisco Tetration platform features and functions support critical data-center security 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
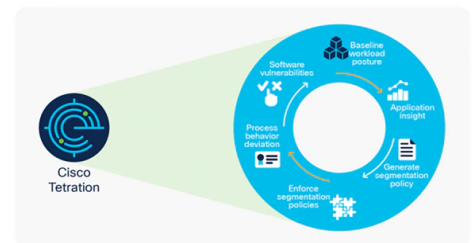

Figure 1.

Multidimensional workload protection approach using Cisco Tetration

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.

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
Zero-trust model using microsegmentation	- Secure hybrid multicloud workloads and contain lateral movement using microsegmentation. - Cisco Tetration platform allows only the required traffic between application components and users, blocking everything else. This approach prevents a persistent threat from entering or searching for additional vulnerabilities.
Application-first security	- Application workload protection using behavior and attribute-driven policy for microsegmentation. - Coordinate whitelist policy definitions and validations across organizational boundaries. Use built-in workflows to collaboratively define a policy set for policy enforcement across a multicloud environment. - Back-test the policy against historic data stored on the cluster appliance.
Automation of microsegmentation policies based on additional context	- Eliminate time-consuming manual creation of resource lists to segment applications. Define application segmentation default and absolute policies using asset tags. - Quickly develop consistent policies for applications using real-time asset tagging. - Associate rich business context with the servers. - Define policies based on users and user groups that need access. - Integrate with vCenter, Kubernetes, OpenShift, Infoblox, DNS servers, and other CMDB systems to automatically bring in the workload context.

automatically bring in the workload context.

One-click policy enforcement across a multicloud data center	• Enforce the security framework using application segmentation and reduce the surface vulnerable to attack. • Enforce policies with a single click. Use the mechanisms in Linux and Microsoft Windows environments to enforce security policy. • Normalize the policy for each server, eliminating the need for manual intervention to identify policy for each of the servers.
Identification of workload behavior deviations	• Get an accurate inventory of the processes running on each server. • Identify all servers currently executing or that have executed a process, including process hash. • Get a tree view of the process execution hierarchy for easier understanding. • Receive proactive notifications on process behavior anomalies.
Software vulnerability detection	• Get a baseline software inventory and version information installed on servers. • Quickly identify if any of the package versions have known vulnerabilities or exposures, along with the severity. • Get an accurate inventory of all the servers that have the vulnerable package. • Tie this information to a policy that designates a specific action, such as quarantining a specific server.
Data exfiltration signals	• Temporal communication behavior baselining between workloads to identify changes in those patterns. • Correlate with other activities within the workload to determine if it is an indicator of compromise. • Generate alerts for such events to enable proactive security operations.
Flexible telemetry collection options	**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 percent of CPU utilization). • Reside outside the data path and do not affect application performance. • Support bare-metal servers, virtual machines, and containers. **Other options:** • ERSPAN sensors. • Application Delivery Controllers (ADC) sensors - F5, Citrix NetScaler, and AVI. • NetFlow sensors.
Endpoint device and user context	• Either collect telemetry from Cisco AnyConnect ® Network Visibility Module (NVM) running on endpoint devices such as laptops, desktops, smart phones, etc., or collect endpoint device information from a Cisco Identity Services Engine (ISE) or VDI environment using Cisco Tetration software agents. • 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.
Support for data center scalability	• Collect telemetry data from tens of thousands of workloads across a multicloud data center. • Offer microsegmentation and workload protection capability across all workloads. • Flexible and scalable deployment options designed to support large and mega-large data centers.
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 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.
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 or above
Scala version	Release 2.11.0 or above
Spark SQL	Release 1.6.2 (not fully ANSI compliant) or above

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, ERSPAN sensors, NetFlow 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 workload protection license:** This license provides workload protection capabilities, including telemetry data collection, application insight, forensics, software vulnerability detections, policy recommendation, policy simulation, policy enforcement, and compliance tracking functions.
- **Tetration Endpoint license:** This license provides the comprehensive telemetry data collection from a Cisco AnyConnect client installed in the endpoints (laptops, desktops, smart phones, etc.), using an NVM module, VDI, or any endpoint device managed through Cisco ISE. This provides insights into user, device, group, process ID, process hierarchy, and OS as well as the domain names accessed from the endpoint. Customers must purchase the endpoint visibility license if they want to use the platform's capability to collect, analyze, and define policies and provide visibility into endpoint device activities. This license can be independent of the workload protection licenses. No additional agent installation is required. This does not include any other licenses required to enable AnyConnect NVM, VDI, or Cisco ISE (those licenses need to be purchased separately).

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

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

Licensing terms

Tetration SaaS deployment:

The SaaS subscription is governed by the Tetration SaaS Offer Description (https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_tetration_saas_offer_description.pdf) and the Cisco Universal Cloud Agreement, located at https://www.cisco.com/go/uca (or similar terms existing between you and Cisco) (the "Agreement"), and any software that you install is licensed under the Cisco End User License Agreement, located at https://www.cisco.com/go/eula (the "EULA").

On-premises deployment models:

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

Cisco Tetration offers both on-premises and Software-as-a-Service (SaaS) options allowing customers to choose the model that meets their business needs.

For on-premises deployments, they can choose a hardware-based appliance model (small or large form factors) depending on the number of workloads in the data center or a virtual appliance option that can run on their own hardware.

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, because it offers scale flexibility. You can start small and grow as your demand grows. Other benefits of the SaaS option include:

- Significant reduction in TCO (Total Cost of Ownership)
- Faster time to value

Note: This consumption option does not support ingesting telemetry from hardware sensors. It also does not support custom user applications on the platform.

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

Table 3.   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 4.   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
Rack specification	https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/r-series-racks/datasheet-c78-738217.html?cachemode=refresh

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 5000 servers (virtual machine or bare metal).

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

Table 5.   Cisco Tetration 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 6. 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)
Rack specification	https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/r-series-racks/datasheet-c78-738217.html?cachemode=refresh

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
- 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
Recommended number of ESXi hosts	4	Recommended to have atleast 4 ESXi hosts for redundancy purposes
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.

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	Linux	• Red Hat Enterprise Linux Release 5.7 and later

bare-metal servers		• Red Hat Enterprise Linux Release 6.0 and later • Red Hat Enterprise Linux Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 • CentOS Release 5.7 and later • CentOS Release 6.0 and later • CentOS Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 • Oracle Linux Release 6.0 and later • Oracle Linux Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 • Oracle Linux Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 with Unbreakable Enterprise Kernel (UEK) • SUSE Linux Release 11.2, 11.3, 11.4 • SUSE Linux Release 12.0, 12.1, 12.2, 12.3, 12.4 • Ubuntu Release 14.04, 16.04, 18.04 • IBM AIX versions 7.1 and 7.2
	Microsoft Windows Server (server core and full desktop)	• 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 • Microsoft Windows Server 2019 Standard, Essentials, and Datacenter Editions
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, 7.6, 7.7 • CentOS Release 6.0 and later • CentOS Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 • Oracle Linux Release 6.0 and later • Oracle Linux Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 • Oracle Linux Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 with Unbreakable Enterprise Kernel (UEK) • Ubuntu 14.04, 16.04, 18.04 • SUSE Linux Release 11.2, 11.3, 11.4 • SUSE Linux Release 12.0, 12.1, 12.2, 12.3, 12.4 • IBM AIX versions 7.1 and 7.2
	Microsoft Windows Server (server core and full desktop)	• 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 • Microsoft Windows Server 2019 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 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.x and 6.x
	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 (not supported on SaaS and Virtual appliance deployment)

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	Cisco Nexus 93180YC-EX, 93108TC-	Cisco ACI Release

Centric Infrastructure [Cisco ACI™] mode)*	EX, and 93180LC-EX	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 option.

Table 13. Hardware and subscription software bundle for Cisco Tetration 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-39U-M5-K9	Tetration Gen2 39RU Cluster-supports up to 25K workloads
	C1-TA-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-8U-M5-K9	Tetration Analytics Gen2 8RU Cluster – up to 5K servers
	C1-TA-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 (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-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 options.

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-CWP-K9	Cisco Tetration on-premises subscription license for workload protection. Minimum quantity is 100 and increments of 1 after that. This license combines previous base and enforcement capabilities. For example, a quantity of 500 will provide the license price for up to 500 workloads
	C1-TA-ENDPT-K9	Cisco Tetration endpoint visibility software subscription license is ordered in increments of 1 endpoint. Minimum quantity required is 1000. For example, a quantity of 1505 will provide license price for 1505 endpoints devices tracked through Cisco AnyConnect or Cisco ISE

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.
- 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 (Tetration-V) option.

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.

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.

Your license for Cisco Tetration Endpoint software does not include AnyConnect or AnyConnect NVM licenses. You are responsible for acquiring those licenses separately.

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 environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

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.

Document History

New or revised topic	Described In	Date
Updated product over, key features, and benefits and ordering information sections to include the updated content	Product overview, key features and benefits and ordering information	Jan, 30th 2019
Updated supported operating systems for visibility and enforcement, and licensing terms	Ordering information, licensing terms, and supported operating systems	May, 13th 2019
Updated the document to include new features, subscription PID updates, and supported operating systems	Features and benefits, ordering information, and supported operating systems	Jul 20th, 2019

Show more history >

Cisco Capital

Platform support and compa...

Ordering information

Put Cisco expertise to work ...

Our experts recommend

ServiceNow and Tetration Integration - Application Installation and
Configuration Guide

IDC Business Value Snapshot - Cisco Tetration

Cisco Tetration Analytics Internal FAQ

About Us

Customer stories

Investor relations

Social responsibility

Environmental sustainability

The Trust Center

Contact Us

Meet our partners

Find a reseller

Careers

We Are Cisco

Our People Deal

Partner with Cisco

Meraki

Webex

Webex Teams

Cisco Umbrella

Waiting for c.clicktale.net...

11:15:09 AM 4/30/2020

https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html