Cisco Tetration Platform

The Cisco Tetration™ platform addresses important data center operational and security challenges by providing behavior-based application insight, automating whitelist policy generation, and enabling zero-trust security using application segmentation.

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 gaps in policy enforcement. This dynamic environment has created several challenges that organizations must address:

- A static security model implemented at the perimeter of the network is no longer sufficient.
- Organizations need to gain pervasive visibility into application communication and dependencies and generate a whitelist policy for segmentation.
- Organizations need to implement a consistent zero-trust model for applications in a heterogeneous environment, while being flexible enough to keep that policy up-to-date.

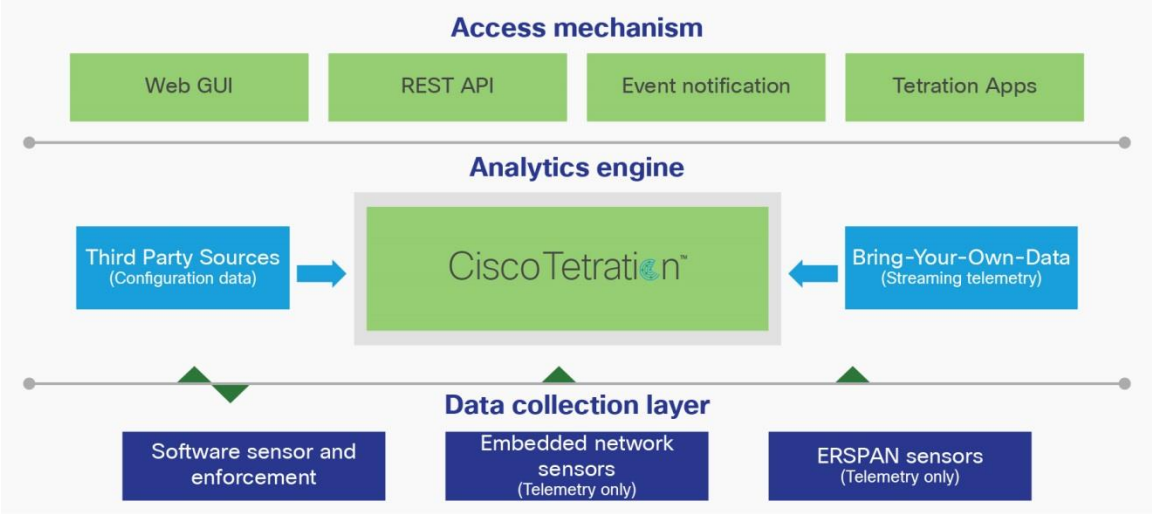
The Cisco Tetration™ platform is designed to address these challenges comprehensively using comprehensive traffic telemetry data collected from both servers and Cisco Nexus® switches. The platform performs advanced analytics using an algorithmic approach and enforces a consistent whitelist policy for applications. This algorithmic approach includes unsupervised machine-learning techniques and behavioral analysis. The platform provides a ready-to-use solution.

- It provides complete visibility into application components, communications, and dependencies to enable implementation of a zero-trust model in the data center.
- It performs real-time asset tagging, allowing administrators to associate business constructs with traffic telemetry data and workloads.
- It automatically generates segmentation policy based on application behavior. It also provides a mechanism for including any existing security policy based on business requirements.
- Organizations can enforce this segmentation policy across heterogeneous infrastructure consistently to implement application segmentation.

To enable all these functions, comprehensive Cisco Tetration telemetry data is collected using custom-developed sensors. Types of sensors used are: software sensors, hardware sensors, and Encapsulated Remote Switched Port Analyzer (ERSPAN) sensors. With these different types of sensors, the solution can support both existing (brownfield) and new (greenfield) data centers and any public cloud infrastructure.

Figure 1 shows the high-level architecture of the Cisco Tetration platform.

Figure 1. Cisco Tetration platform architecture



The Cisco Tetration platform has four main functional layers:

- **Data collection layer:** This layer consists primarily of sensor functions. Sensors are the eyes and ears of the Cisco Tetration Analytics™ platform. Two types of sensors are used:
  - **Software sensors:** These lightweight sensors run as user processes and can be installed on any server (virtualized or bare metal) running in on-premises data centers or on any public cloud. These software sensors can collect telemetry data and also act as enforcement points.
  - **Hardware sensors:** These sensors are embedded in Cisco Nexus 93180YC-EX, 93108TC-EX, 93180YC-FX, and 93108TC-FX Switches.
  - **ERSPAN sensors:** These out-of-band sensors are designed to generate Cisco Tetration telemetry data using copies of the network packets. These copied packets are delivered to these sensors using ERSPAN.

  Sensors are designed to monitor every packet and every flow. They do not collect any information from payloads, and no sampling is performed.

- **Analytics layer:** Data from the sensors is sent to the Cisco Tetration platform, which is the brain that performs all the analyses. This multi-node big data platform processes the information from the sensors and uses unsupervised and guided machine learning, behavior analysis, and intelligent algorithms to provide a ready-to-use solution for the following use cases:
  - Accurate insight into application component communications based on observed behavior
  - Automated grouping of similar endpoints (for example, web server clusters and database clusters)
  - Consistent whitelist policy recommendations for applications and monitoring for compliance deviations in minutes
  - Policy impact analysis to test a policy before enforcing it in the network
  - Automated policy enforcement that enables consistent application segmentation
  - Monitoring to track policy compliance deviations and update policy in near-real time

    - Pervasive visibility in real time across data center infrastructure
    - Long-term data retention for historical analysis without loss of detail
    - In-depth forensics using powerful search filters and visual queries
- **Enforcement layer:** Full-visibility software sensors act as the enforcement point for the segmentation policy generated by the platform, helping enable application segmentation. Using the software sensor and operating system capabilities, the Cisco Tetration platform provides stateful and consistent enforcement across public, private, and on-premises deployments. This layer also helps ensure that policy moves along with the workload, even when an application component is migrated from a bare-metal server to a virtualized environment. In addition, the enforcement layer helps ensure scalability, with consistent policy implemented for thousands of applications spanning tens of thousands of workloads.
- **Access layer:** The Cisco Tetration platform enables consumption of this data through an easy-to-navigate and scalable web GUI and through Representational State Transfer (REST) APIs. In addition, it provides Apache Kafka–based push notification to which northbound systems can subscribe to receive notifications about policy compliance deviations, flow anomalies, etc. Advanced users have access to the Hadoop data lake and can write custom applications using programming languages such as Python and Scala that are run on the platform using the powerful computing resources available.
- **Other data sources:** In addition to the sensors, additional configuration information is collected from third-party sources, such as load balancers, Domain Name System (DNS) server records, and the IP address management database. This configuration data is used to augment the information provided by the analytics platform. This platform also supports the use of streaming telemetry data collected from other sources for analytics and correlation.

Software, hardware, and ERSPAN sensors

The software sensors and the hardware sensors collect three types of telemetry information:

- **Flow information:** This information contains details about flow endpoints, protocols, and ports; when the flow started; how long the flow was active; etc.
- **Inter-packet variation:** This information captures any inter-packet variations seen within the flow. Examples include variations in the packet's Time To Live (TTL), IP/TCP flags, and payload length.
- **Context details:** Context information is derived outside the packet header. In the case of a software sensor, this information includes details about the process, including which process generated the flow, the process ID, and the user associated with the process.

ERSPAN sensors collect flow information and inter-packet variations only. ERSPAN sensors can be used in specific portions of the network in which the use of hardware and software sensors is not feasible. Software sensors are still assumed be the predominant means of collecting telemetry data, with ERSPAN used to fill the gaps.

For the Cisco Tetration platform, you should use software sensors for to collect the greatest amount of information and achieve the greatest accuracy. Hardware sensors and ERSPAN sensors can be used to augment the data provided to the platform.

Additional characteristics of sensors

Full-visibility software sensors support a configurable CPU Service-Level Agreement (SLA). If the SLA value is set too low, or if the traffic volume on the server is too high, the platform will selectively miss an opportunity to inspect every packet to comply with the SLA. These missed opportunities are logged and displayed in the administration user interface, where optional adjustments to the SLA can be made.

Hardware sensors in the switch have a finite flow-record capacity, governed by trade-offs in scalability, metadata resolution, and cost. If the traffic volume is too high, or if large numbers of flows are short lived, the flow record capacity may limit the number of packets recorded in a given capture interval (between 100 milliseconds and 4 seconds). In this circumstance, filtering is available and recommended. Customers can specify high-priority applications and IP addresses for which the Cisco Tetration telemetry data needs to be collected.

Features and benefits

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

Table 1. Main features and benefits

Feature	Benefit
Software and hardware sensors	• A combination of hardware and software sensors captures all east-west traffic, eliminating blind spots. • Software sensors are designed to operate within administrator-defined computing SLAs (the default is within 3% of CPU utilization). • Both software and hardware sensors reside outside the data path and do not affect application performance. • Sensor traffic adds less than 1% of bandwidth overhead.
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 flow context information in addition to packet header data enables better insight.
Real-time asset tagging	• Associate business context with the telemetry data in the form of tags. • Tags provide 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 Cisco Tetration platform. • Define policies or search inventory and traffic based on these well-known attributes.
Limited-visibility software sensors	• Sensor coverage is extended to certain older operating systems. • Required connection information is tracked for Cisco Tetration application insight. • These sensors help create more specific and accurate policies for applications.
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.
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 Cisco Tetration platform. • NAT and PAT are suitable for deployments with multiple domains with overlapping IP addresses.
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.

Feature	Benefit
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.
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® Call Home function to report known error states.
Microsoft Active Directory integration	• User authentication is performed through the external Active Directory. • This integration eliminates the need to maintain user login credentials locally on the Cisco 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.

Data center use cases

Cisco Tetration platform features and functions support critical data center security and operations use cases. Table 2 summarizes the use cases.

Table 2. Supported use cases

Use case	Description
Application insight	You need to understand the application components and dependencies in the data center to successfully operate and implement application segmentation. This capability can also be used to migrate applications and to perform disaster-recovery planning. The Cisco Tetration platform uses real-time communication data between application components and machine-learning and behavior-analysis algorithms to identify application groups and their communications patterns and service dependencies. Application insight allows users and administrators to: • Group endpoint hosts and application clusters to create application views, augmented by attributes from VMware vCenter and AWS tags • Accurately understand the relationships between consumers and providers based on communication patterns • Understand the service dependencies for each component Organizations can also intelligently integrate information from third-party devices such as load balancers, the IP address management database, etc. to maintain an end-to-end view of application communication.
Automated whitelist policy recommendation	You need to be able to automatically generate a reliable whitelist policy and be able to update it in nearly real time as applications evolve. This capability enhances security, enabling consistent enforcement of the policy across different environments, including workloads running in the cloud, and enabling easier identification of anomalies. Using the Cisco Tetration platform, you can automatically generate highly specific whitelist policy based on the actual communication between endpoints. The platform also includes other predefined policies from higher-level entities such as security operations. You can specify policy by using network-level information as well as by using abstract information such as asset tags. For example, security policy might specify that production servers cannot talk to nonproduction servers. This policy can then be enforced using the Cisco Tetration policy enforcement capability (application segmentation). If you choose to enforce the policy using other technologies, the policy can be exported in programmatic formats JSON, XML, and YAML through the web-based GUI or REST API.
Application segmentation	Cisco Tetration application segmentation allows you to implement a secure zero-trust model using application whitelist policy. It then normalizes this policy based on the priority and hierarchy before enforcing it. When policy enforcement is enabled for an application, it is enforced through software sensors using native 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. This approach allows you to stateful and consistent segmentation across the heterogeneous infrastructure (on premises and in public and private clouds) at scale. In addition, in a virtualized environment, this mechanism helps ensure that segmentation policy moves with the workload, allowing you to increase application mobility without having to be concerned with infrastructure-specific segmentation policy. As application dependencies and communication patterns evolve, the platform helps ensure that policy is updated automatically.

Use case	Description
Policy impact analysis and compliance	Using the Cisco Tetration platform, you can simulate the whitelist policy and assess its impact before applying it in the production network. This impact analysis can be performed using historical data or real-time data without affecting the production traffic. This capability enables you to see how this whitelist policy would affect actual traffic flowing through the network. Also, you can immediately see which flows will be classified as compliant or noncompliant or dropped. After the policy is enforced, the platform monitors for continuous compliance. You can receive notification of any compliance deviation, thereby allowing you to proactively address any concern. If the deviation is legitimate, you can update the policy with a single click.
Server process and process hash inventory	Software sensors now extend the Cisco Tetration platform's capability to collect the complete process inventory along with the process hash information for the application servers. For each server, users can search based on the process details or the hash information. This feature extends the platform's capability to collect and baseline information beyond information about network traffic. Process hash information enables additional security capabilities as well.
Application neighborhood graphs	Using the neighborhood graphs function, users can search for a specific application server and see a two-hops view of its communication with other servers within the data center. Users can drill down to see traffic and communication patterns between one or more of these servers. Users also can query to see whether there is a communication path between two servers and the number of logical server hops between those two application servers. Preconfigured and user-defined alerts can be generated based on certain behavior changes.
Virtual Desktop Infrastructure (VDI) visualization	When VDI is used in the data center, the Cisco Tetration platform can provide visibility into the traffic and application workspaces being accessed by these VDI instances. This visibility is achieved by installing software sensors on the VDI virtual machines. This feature enables complete visibility into the communication occurring externally and within the data center for the VDI virtual machines.
Visualization and forensics	Cisco Tetration platform can be your search engine for all the flows in your data center. The search capability provided by the platform is uniquely powerful, allowing you to search tens of billions of flow records in less than a second. It allows complex filter expressions and visual-based search queries to find details that are critical to data center operations. This search capability allows you to find not only known issues, but also abnormal behaviors that may otherwise go unnoticed.

Cisco Tetration applications

The Cisco Tetration platform provides access to the data lake in the cluster through Cisco Tetration applications. Using Cisco Tetration 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 triggred 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 3 summarizes the specifications for Cisco Tetration applications.

Table 3. Cisco Tetration applications specifications

Cisco 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)

Licensing

Cisco Tetration Analytics 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 enforcment capability.

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

Licensing terms

In addition to being subject to the Cisco End User License Agreement (EULA; see https://www.cisco.com/go/eula), Cisco Tetration software is subject to Cisco Supplemental End User License Agreement (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 Analytics 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 5,000 servers (virtual machine or bare metal).

Table 4 shows the verified and supported scale. Table 5 shows the power and the cooling requirements for the Cisco Tetration platform.

Table 4. Cisco Tetration Analytics 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	2 million per second

Table 5. Power and cooling specifications for large form factor

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

Platform requirements	Specification
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)

*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 5,000 servers (virtual machine or bare metal).

Table 6 shows the verified and supported scale. Table 7 shows the power and cooling requirements for the Cisco Tetration-M SFF platform.

Table 6. 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 5,000
Number of flow events that can be processed per second	500,000 per second

Table 7. 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 (AWS public cloud) option

With the Cisco Tetration Cloud AWS public cloud deployment option, the Cisco Tetration software can run in an AWS instance. You are responsible for purchasing the required AWS instances directly from AWS to run the Cisco Tetration software. This option is suitable for data centers that host 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 platform. Table 8 shows the AWS instance type, Amazon Elastic Block Storage (EBS), and Amazon Elastic IP (EIP) address requirements to run Cisco Tetration Cloud in AWS. Table 9 shows the platform scale.

Table 8. 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 TB
Amazon EIP	50 addresses

Table 9. 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

Platform support and compatibility

Tables 10, 11, 12, and 13 provide software and hardware support and compatibility information for the Cisco Tetration platform.

Table 10. 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, and 7.3 • CentOS Release 5.0 and later • 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 • SUSE Linux Release 11.2, 11.3, and 11.4 • SUSE Linux Release 12.0, 12.1 and 12.2 • Ubuntu Release 12.04, 14.04, 14.10, and 16.04
	Microsoft Windows Server (server core and full desktop)	• Microsoft Windows Server 2008 Standard, Enterprise, Essentials, and Datacenter Editions • Microsoft Windows Server 2008 R2 Standard, Enterprise, Essentials, and Datacenter Editions • Microsoft Windows Server 2012 Standard, Foundation, Essentials, and Datacenter Editions • Microsoft Windows Server 2012 R2 Standard, Foundation, Essentials, and Datacenter Editions • Microsoft Windows Server 2016 Standard, Essentials, and Datacenter Editions
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 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, 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

Server mode	Operating system	Distribution and release
	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 Datacenter, Foundation, and Essentials • Microsoft Windows Server 2016 Standard, Essentials, and Datacenter Editions

Table 12. 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, and 7.2
	Solaris	• Solaris 11.0 (64-bit) on x86 architecture
	Microsoft Windows Server	• Microsoft Windows Server (64-bit)

Table 13. Supported hardware sensors

Product line	Platform	Software release
Cisco Nexus 9300 platform switches (NX-OS mode)*	Cisco Nexus 92160YC-X	Cisco NX-OS Release 7.0(3)I5(2) and later
	Cisco Nexus 93180YC-EX and 93108TC-EX	Cisco NX-OS Release 7.0(3)I5(2) and later
	Cisco Nexus 93180YC-FX and 93108TC-FX	Cisco NX-OS Release 7.0(3)I7(2) and later
Cisco Nexus 9300 platform switches (ACI mode)*	Cisco Nexus 93180YC-EX and 93108TC-EX	Cisco Application Centric Infrastructure (Cisco ACI™) Release 2.2(2e) and later
	Cisco Nexus 93180YC-FX and 93108TC-FX	Cisco Application Centric Infrastructure (Cisco ACI™) Release 2.3(1f) and later

* Requires separate Cisco Nexus 9300 telemetry license

Ordering information

Table 14 provides hardware and software bundle part numbers for the Cisco Tetration Analytics LFF option.

Table 14. Hardware and subscription software bundle for Cisco Tetration Analytics LFF option

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION		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.
	TA-CL-G1-39-K9	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 16 for details.
	ASF-DCV1-TA-QS-M	AS-Fixed part number for Cisco Tetration Analytics implementation services.

Table 15 provides hardware and software bundle part numbers for the Cisco Tetration-M (8RU) SFF option.

Table 15. 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 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.
	TA-CL-G1-SFF8-K9	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 16 provides subscription software bundle part numbers used for the Cisco Tetration Analytics LFF and Cisco Tetration-M SFF options.

Table 16. Subscription software license for Cisco Tetration Analytics 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 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 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.
- 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 Cloud option.

Licensing terms

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

Tables 17 and 18 provides bundle part numbers for the Cisco Tetration Cloud option.

Table 17. 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 18. 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.
	C1-TA-BASE100-K9	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 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.

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.
- 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 only with a Cisco Tetration Cloud deployment.

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 the 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), your Cisco Tetration Analytics 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 your 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/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 C78-737256-08 10/17