Cisco Tetration Platform

The Cisco Tetration Analytics™ addresses data center operational and security challenges by providing comprehensive workload-protection capability and unprecedented insights across a multi-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 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

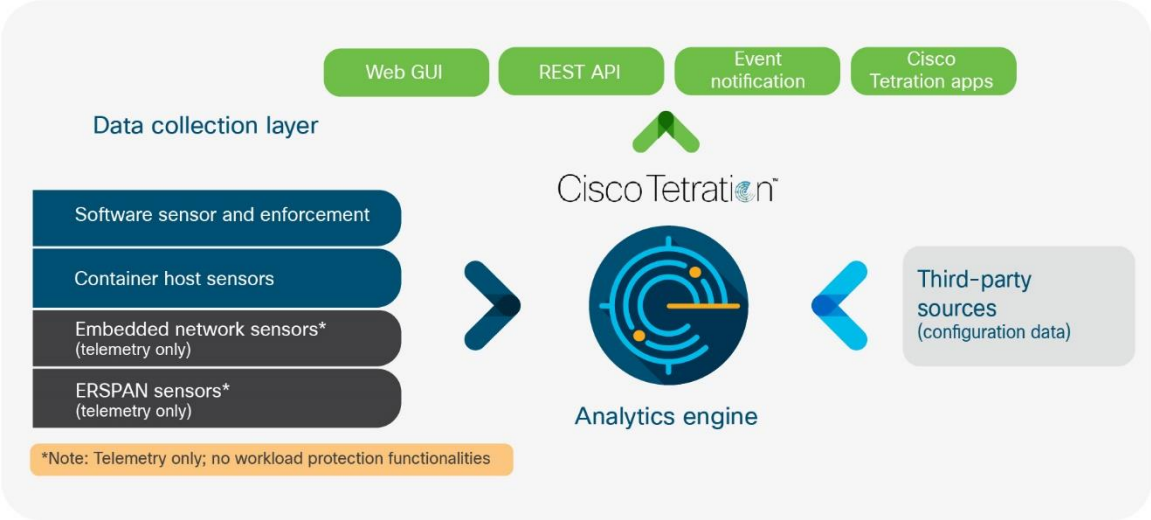
The Tetration platform is designed to fully address these challenges using comprehensive traffic telemetry data collected from both servers and Cisco Nexus® switches. The platform performs advanced analytics using an algorithmic approach and provides comprehensive workload protection for a multicloud 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)

To enable all these functions, comprehensive Tetration telemetry data is collected using custom-developed sensors: 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 Tetration platform.

Figure 1. Cisco Tetration platform architecture



The 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. Three 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. It provides the most comprehensive telemetry data. These software sensors can collect telemetry data and also act as enforcement points. Software sensors collect following information:
    - **Flow information:** Details about flow endpoints, protocols, and ports; when the flow started; how long the flow was active; etc.
    - **Interpacket variation:** Any interpacket variations seen within the flow. Examples include variations in the packet's Time To Live (TTL), IP/TCP flags, and payload length
    - **Process details:** Processes executed on the server, including information about process parameters, start and stop time, process binary hash, etc.
    - **Software packages:** Inventory of all the software packages installed on the server along with the version and distributor information
  - **Hardware sensors:** These sensors are embedded in Cisco Nexus 93180YC-EX, 93108TC-EX, 93180YC-FX, and 93108TC-FX switches. Switch has the capability to collect information from at line-rate across all ports without any impact to CPU. Even the telemetry export happens from the switch Application-Specific Integrated Circuit (ASIC) itself
  - **ERSPAN sensors:** ERSPAN sensors collect flow information and interpacket variations only. These sensors can be used in specific portions of the network where using hardware and software sensors is not feasible. Software sensors are still assumed be the predominant means of collecting telemetry data, with hardware sensors and ERSPAN used to fill the gaps

- **Analytics layer:** Data from the sensors is sent to the Tetration platform, which is the brain that performs all the analyses. This multinode 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)
  - Autogenerated whitelist policy for application segmentation
  - Policy impact analysis to test a policy before enforcing it in the network
  - Automated policy enforcement for segmentation for multicloud environments
  - Monitoring to track policy compliance deviations and update policy in near-real time
  - Baselining the processes running on each server and identifying behavior deviations
  - Discovering all the software packages installed on the server and identifying any vulnerabilities and exposures
  - Pervasive visibility in real time across the data center infrastructure that provides network performance insights
  - Long-term data retention for historical analysis without loss of detail
- **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 Analytics 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 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 notifications northbound systems can subscribe to for 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

Features and benefits

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

Table 1. Cisco Tetration Analytics 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
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
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
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
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

Data center use cases

Cisco Tetration platform features and functions support critical data center security and operations use cases, which are summarized in Table 2.

Table 2. Cisco Tetration Platform 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 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 near-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 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.
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.
Process- behavior baselining and deviation	Cisco Tetration collects and baselines the process details running on each of the servers. This information includes process ID, process parameters, user associated with it, process start time, and process hash (signature) information. You can search for servers running specific process or process hash information and see a tree-view snapshot of all the processes running on a server. Cisco Tetration platform has algorithms available to track behavior pattern changes and find similarities to malware behavior patterns. One example would be to detect a privilege escalation followed by a shell code execution. Tetration raises security events for such behavior deviations. Security operations teams can customize those events, their severity, and associated actions by using simple-to-define rules. Using this information, security operations can quickly identify indicators of compromise and take remediation steps to minimize the impact.

Use case	Description
Software inventory and vulnerability detection	The Cisco Tetration platform baselines the installed software packages, package version, patch level, etc. The platform includes 19 years' worth of vulnerability and exposure information and is designed to receive constant updates as new ones are found. Using this, Tetration checks for any known information-security vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) system that the software packages have. When a vulnerability is detected, complete details—including the severity and the impact score–can be found. You can then quickly find all the servers with the same version of the package installed for patching and planning purposes. Security operations can predefine policies with specific actions, such as quarantining a host when servers have packages with certain vulnerabilities. This capability can be used to identify a broad set of vulnerabilities, including high impact threats such as Specter and Meltdown.
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.
Network performance monitoring	Robust data-plane telemetry information from software and hardware sensors 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 round-trip times, window size reduction, and handshake latency • Display a hop-by-hop view of each flow across the data center fabric along with 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.
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 Tetration platform provides access to the data lake in the cluster through Tetration applications. Using 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 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 3 summarizes the specifications for Tetration applications.

Table 3. 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

Tetration applications data points	Specification
Scala version	Release 2.11.0
Spark SQL	Release 1.6.2 (not fully ANSI compliant)

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:

- **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.

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 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 4000 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	Up to 2 million per second
Number of hardware sensor enabled Cisco Nexus 9000 Series Switches	Up to 100

Table 5. 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 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 4000 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 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 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 option

With the Cisco Tetration Cloud option, you can deploy the Cisco Tetration platform in the Amazon Web Services (AWS) or Microsoft Azure public cloud. With this deployment option, Cisco Tetration software can run in a public cloud instance. You are responsible for purchasing the required instances directly from the public cloud vendor to run the Tetration software. This option is suitable for data centers that host fewer than 1000 servers (virtual machine or bare metal) and have a significant AWS or Microsoft Azure presence.

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 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)	67 TB
Amazon EIP	50 addresses

Table 9 shows the instance types and elastic IP address requirements for running Cisco Tetration Cloud in Microsoft Azure.

Table 9. Microsoft Azure instance requirements for Cisco Tetration Cloud

Microsoft Azure instance type	Specification
Standard A8m v2	13 instances
Standard D14 v2	26 instances
Standard A4m v2	19 instances
Standard DS2 v2	19 instances
IP addresses	20 addresses
Managed premium disk	67 TB

Table 10 shows the platform scale for Cisco Tetration Cloud. The supported scale is the same for AWS and Microsoft Azure.

Table 10. 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	Up to 200,000 per second

Platform support and compatibility

Tables 11–14 provide software and hardware support and compatibility information for the Cisco Tetration platform.

Table 11. 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 • CentOS Release 5.0 and later • CentOS Release 6.0 and later

Server mode	Operating system	Distribution and release
		• CentOS Release 7.1, 7.2, 7.3, 7.4 • Oracle Linux Release 6.0 and later • Oracle Linux Release 7.1, 7.2, 7.3, 7.4 • SUSE Linux Release 11.2, 11.3, 11.4 • SUSE Linux Release 12.0, 12.1 • 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
VDI desktop virtual machines	Microsoft Windows Desktop (VDI use case only)	• Microsoft Windows 7 Desktop • Microsoft Windows 8 Desktop • Microsoft Windows 10 Desktop

Table 12. 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 • CentOS Release 6.0 and later • CentOS Release 7.1, 7.2, 7.3, 7.4 • Oracle Linux Release 6.0 and later • Oracle Linux Release 7.1, 7.2, 7.3, 7.4 • Ubuntu 14.04, 14.10, 16.04 • SUSE Linux Release 11.2, 11.3, 11.4 • SUSE Linux Release 12.0, 12.1
	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 13. 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 (64-bit)

Table 14. Supported hardware sensors

Product line	Platform	Minimum Software release
Cisco Nexus 9300 platform switches (Cisco NX-OS Software mode)*	Cisco Nexus 92160YC-X	Cisco NX-OS Release 7.0(3)I5(2) and later
	Cisco Nexus 93180YC-EX, 93108TC-EX, and 93180LC-EX	Cisco NX-OS Release 7.0(3)I5(2) and later
	Cisco Nexus 93180YC-FX, 93108TC-FX, and 9348GC-FXP	Cisco NX-OS Release 7.0(3)I7(2) 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 2.2(2e) and later
	Cisco Nexus 93180YC-FX, 93108TC-FX**	Cisco ACI Release 2.3(1f) and later
	Cisco Nexus 9348GC-FXP	Cisco ACI Release 3.0 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.

**To support the network performance monitoring feature using hardware sensors, Cisco ACI Release 3.1 is required.

Ordering information

Table 15 provides hardware and software bundle part numbers for the Cisco Tetration Analytics LFF option.

Table 15. 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 10,000 servers (virtual machine or bare metal)
	C1-TA-SW-K9	Bundle part number for the Cisco Tetration Analytics software subscription license; see Table 17 for details
	ASF-DCV1-TA-QS-M	AS-Fixed part number for Cisco Tetration Analytics implementation services

Table 16 provides hardware and software bundle part numbers for the Cisco Tetration-M (8RU) option.

Table 16. 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, see Table 17 for details
	ASF-DCV1-TA-QS-M	AS-Fixed part number for Cisco Tetration Analytics implementation services

Table 17 provides subscription software bundle part numbers used for the Cisco Tetration platform and Cisco Tetration-M options.

Table 17. 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 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

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

Tables 18 and 19 provide bundle part numbers for the Cisco Tetration Cloud option.

Table 18. 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 19. 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 to Cisco Tetration Cloud
	C1-TA-BASE100-K9	Cisco Tetration detect subscription software license in multiples of 100 workload equivalence. 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	Add-on Cisco Tetration protect subscription software license for policy enforcement in multiples of 100 workload equivalence. 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 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 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 C78-737256-10 03/18