Cisco Tetration Platform
## Contents

- **Product Overview** .................................................. 3  
- **Data Center Use Cases** ........................................ 4  
- **Features and Benefits** .......................................... 5  
- **Cisco Tetration Applications** .................................. 6  
- **Software Licensing** ............................................... 7  
- **Licensing Terms** .................................................. 8  
- **Deployment Models and Scale** ................................. 8  
- **Platform Support and Compatibility** ......................... 11  
- **Ordering Information** ........................................... 13  
- **Put Cisco Expertise to Work to Accelerate Adoption** ...... 16  
- **Cisco Capital** ..................................................... 16  
- **Document History** .............................................. 17
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 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)
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.

# Features and Benefits

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| **Day-0 readiness** | ● Plug day-0 vulnerabilities.  
● Policy from the Cisco Tetration platform allows only the required traffic, blocking everything else. This approach prevents a persistent threat from entering or searching for additional vulnerabilities on day 0. |
| **Automated whitelist policy generation** | ● Auto-generate whitelist policy based on application dependency and behavior.  
● 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. |
| **Extend policy definitions 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, and other CMDB systems to 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 mechanism 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. |
| **Process inventory baselining** | ● 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 critical process-behavior deviations. |
| **Software vulnerability detection** | ● Get a baseline software inventory and the 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. |
| **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 Cisco Tetration platform.  
● Define policies or search inventory and traffic based on these well-known attributes. |
<p>| <strong>Software sensors</strong> | ● Capture all activity on a server, including east-west traffic, eliminating blind spots. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed to operate within administrator-defined computing SLAs (the default is within 3% of CPU utilization).</td>
<td>• Reside outside the data path and do not affect application performance. • Supports bare metal servers, virtual machines, and containers.</td>
</tr>
<tr>
<td>ERSPAN sensors</td>
<td>• 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.</td>
</tr>
<tr>
<td>Hardware sensors</td>
<td>• Line-rate telemetry required for Tetration within the switch’s Application-Specific Integrated Circuit (ASIC), eliminating any impact to the switch CPU.</td>
</tr>
<tr>
<td>AnyConnect® NVM proxy sensor</td>
<td>• Collect telemetry from AnyConnect NVM agent running on endpoint devices such as laptops, desktops, smartphones, etc. • This provides information around user, device name, FQDN, processes running on the device as well as what URL or application was accessed. • Correlate the user data with the user group within an organization. • Define specific policies for segmentation, using user and user group information, that can be enforced on the workloads.</td>
</tr>
<tr>
<td>Support for data center scalability</td>
<td>• 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.</td>
</tr>
<tr>
<td>Ease of deployment and use</td>
<td>• 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.</td>
</tr>
<tr>
<td>Platform self-monitoring</td>
<td>• 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.</td>
</tr>
<tr>
<td>Open interface</td>
<td>• 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.</td>
</tr>
</tbody>
</table>

### 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

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

Software Licensing

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

- **Tetration Detect (base license)**: This license provides the comprehensive telemetry data collection, application insight, forensics, policy recommendation, and policy simulation functions.

- **Add-on Tetration Protect (policy enforcement)**: The policy enforcement capability is licensed separately from the base functions. Customers must purchase the policy enforcement license if they want to use the platform's automated enforcement capability.

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

If a customer has multiple Cisco Tetration clusters, software licenses can be pooled across those clusters.
Licenses for Cisco Tetration SaaS (Software-as-a-Service) offering:

- **Tetration Workload Protection license:** This license combines Tetration Detect as well as Tetration Protect features under one single SaaS license for customers. SaaS licensing is based on the number of workloads on which software sensors are installed. SaaS requires customers to deploy software sensors on bare metal, virtual machines, and container hosts.

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

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

**Licensing Terms**

In addition to being subject to the Cisco® End User License Agreement (EULA; see [https://www.cisco.com/go/eula](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](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-M (small form factor) Option**

The Cisco Tetration-M small form factor deployment option consists of 6 servers and 2 Cisco Nexus 9300 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

<table>
<thead>
<tr>
<th>Platform characteristics</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of concurrent servers (virtual machine or bare metal) from which telemetry data can be analyzed</td>
<td>Up to 5000</td>
</tr>
</tbody>
</table>
### Platform characteristics

<table>
<thead>
<tr>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of flow events that can be processed per second</td>
</tr>
<tr>
<td>Number of hardware-sensor-enabled Cisco Nexus 9000 Series Switches</td>
</tr>
</tbody>
</table>

Table 4. Power and Cooling Specifications for Cisco Tetration-M

### Platform requirements

<table>
<thead>
<tr>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak power for Cisco Tetration-M (8RU)</td>
</tr>
<tr>
<td>Maximum cooling requirement for Cisco Tetration-M (8RU)</td>
</tr>
</tbody>
</table>

### Cisco Tetration (large form factor) Platform Option

This deployment option consists of 36 servers and 3 Cisco Nexus 9300 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.

### Cisco Tetration Platform Scale

<table>
<thead>
<tr>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of concurrent servers (virtual machine or bare metal) from which telemetry data can be analyzed</td>
</tr>
<tr>
<td>Number of flow events that can be processed per second</td>
</tr>
<tr>
<td>Number of hardware sensor enabled Cisco Nexus 9000 Series Switches</td>
</tr>
</tbody>
</table>

Table 5. Cisco Tetration Platform Scale

### Power and Cooling Specifications for Large Form Factor

<table>
<thead>
<tr>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak power for Cisco Tetration - 39-Rack-Unit [39RU] single-rack option</td>
</tr>
<tr>
<td>Maximum cooling requirements for Cisco Tetration - 39RU single-rack option</td>
</tr>
<tr>
<td>Total weight for Cisco Tetration - 39RU single-rack option</td>
</tr>
<tr>
<td>Power Distribution Unit (PDU) and power supply (39RU single-rack option)</td>
</tr>
<tr>
<td>Peak power for Cisco Tetration - 39RU dual-rack option</td>
</tr>
<tr>
<td>Maximum cooling requirement for Cisco Tetration - 39RU dual-rack option</td>
</tr>
<tr>
<td>Total weight for Cisco Tetration - 39RU dual-rack option</td>
</tr>
<tr>
<td>PDU and power supply - 39RU dual-rack option</td>
</tr>
</tbody>
</table>

Table 6. Power and Cooling Specifications for Large Form Factor
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>
<thead>
<tr>
<th>Platform characteristic</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of concurrent workloads (virtual machine or bare metal) from which telemetry data can be analyzed</td>
<td>Up to 1000</td>
</tr>
<tr>
<td>Number of flow events that can be processed per second</td>
<td>Up to 70,000 per second</td>
</tr>
</tbody>
</table>

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

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

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

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

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

**Platform Support and Compatibility**

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

**Table 9.** Supported Operating Systems for Full-Visibility Sensors

<table>
<thead>
<tr>
<th>Server mode</th>
<th>Operating system</th>
<th>Distribution and release</th>
</tr>
</thead>
</table>
Table 10. Supported Operating Systems for Enforcement

<table>
<thead>
<tr>
<th>Server mode</th>
<th>Operating system</th>
<th>Distribution and release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machines and bare-metal servers</td>
<td>Linux (64-bit)</td>
<td>● Red Hat Enterprise Linux Release 6.0 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Red Hat Enterprise Linux Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● CentOS Release 6.0 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● CentOS Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Oracle Linux Release 6.0 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Oracle Linux Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Oracle Linux Release 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 with Unbreakable Enterprise Kernel (UEK)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Ubuntu 14.04, 14.10, 16.04</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● SUSE Linux Release 11.2, 11.3, 11.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● SUSE Linux Release 12.0, 12.1, 12.2, 12.3</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server (server core and full desktop)</td>
<td>● Microsoft Windows Server 2008 R2 Standard, Datacenter, Enterprise, and Essentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Microsoft Windows Server 2012 Standard, Datacenter, Foundation, and Essentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Microsoft Windows Server 2012 R2 Standard, Datacenter, Foundation, and Essentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Microsoft Windows Server 2016 Standard, Essentials, and Datacenter Editions</td>
</tr>
<tr>
<td>Container host</td>
<td>Linux</td>
<td>● Red Hat Enterprise Linux release 7.1, 7.2, 7.3, 7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● CentOS release 7.1, 7.2, 7.3, 7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Ubuntu release 16.04</td>
</tr>
<tr>
<td>VDI desktop virtual machines (VDI use case only)</td>
<td>Microsoft Windows Desktop</td>
<td>● Microsoft Windows 7 Desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Microsoft Windows 8 Desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Microsoft Windows 10 Desktop</td>
</tr>
</tbody>
</table>

Table 11. Supported Operating Systems for Universal Software Sensors

<table>
<thead>
<tr>
<th>Server mode</th>
<th>Operating system</th>
<th>Distribution and release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machines and bare-metal servers</td>
<td>Linux</td>
<td>● Red Hat Enterprise Linux Release 4.0 (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● CentOS Release 4.0 (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Red Hat Enterprise Linux Release 5.0 (32-bit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● CentOS Release 5.0 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>AIX</td>
<td>● AIX Release 5.x and 6.x</td>
</tr>
<tr>
<td></td>
<td>Solaris</td>
<td>● Solaris 11.0 (64-bit) on x86 architecture</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server</td>
<td>● Microsoft Windows Server (32-bit and 64-bit)</td>
</tr>
</tbody>
</table>
Table 12. Supported Hardware Sensors (not supported on SaaS)

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

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

<table>
<thead>
<tr>
<th>Bundle part number</th>
<th>Part numbers included in bundle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1-TETRATION</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>TA-CL-39U-M5-K9</td>
<td>Tetration Gen2 39RU Cluster-supports up to 25K workloads</td>
<td></td>
</tr>
<tr>
<td>C1-TA-SW-K9</td>
<td>Bundle part number for the Cisco Tetration software subscription license; see Table 17 for details</td>
<td></td>
</tr>
<tr>
<td>C1-TA-V-SW-K9</td>
<td>Bundle part number for the Cisco Tetration software subscription license; see Table 17 for details</td>
<td></td>
</tr>
<tr>
<td>ASF-DCV1-TA-QS-M</td>
<td>AS-Fixed part number for Cisco Tetration implementation services</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Bundle part number</th>
<th>Part numbers included in bundle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1-TETRATION-M</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>TA-CL-8U-M5-K9</td>
<td>Tetration Analytics Gen2 8RU Cluster – up to 5K servers</td>
</tr>
<tr>
<td></td>
<td>C1-TA-SW-K9</td>
<td>Bundle part number for the Cisco Tetration software subscription license, see Table 17 for details</td>
</tr>
<tr>
<td></td>
<td>C1-TA-V-SW-K9</td>
<td>Bundle part number for the Cisco Tetration software subscription license; see Table 17 for details</td>
</tr>
<tr>
<td></td>
<td>ASF-DCV1-TA-QS-M</td>
<td>AS-Fixed part number for Cisco Tetration implementation services</td>
</tr>
</tbody>
</table>

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

### Table 15. Bundle for Cisco Tetration-V option (ESXi)

<table>
<thead>
<tr>
<th>Bundle part number</th>
<th>Part numbers included in bundle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1-TETRATION-V</td>
<td></td>
<td>Cisco Tetration bundle part number that includes the software subscription license for the virtual form factor</td>
</tr>
<tr>
<td></td>
<td>C1-TA-V-SW-K9</td>
<td>Bundle part number for the Cisco Tetration software subscription license</td>
</tr>
<tr>
<td></td>
<td>ASF-DCV1-TA-QS-M</td>
<td>Optional AS-Fixed part number for Cisco Tetration implementation services</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Bundle part number</th>
<th>Part numbers included in bundle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1-TA-SW-K9</td>
<td></td>
<td>Bundle part number for the Cisco Tetration software subscription license</td>
</tr>
<tr>
<td>C1-TA-BASE-1K-K9</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>C1-TA-ENF-1K-K9</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>C1-TA-ENDPT-K9</td>
<td></td>
<td>Cisco Tetration endpoint visibility software subscription license in multiples of 1 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</td>
</tr>
<tr>
<td>C1-TA-V-SW-K9</td>
<td></td>
<td>Bundle part number for the Cisco Tetration software subscription license, applicable only to Cisco Tetration-V</td>
</tr>
</tbody>
</table>
Bundle part number | Part numbers included in bundle | Description |
---|---|---|
C1-TA-BASE100-K9 | | Cisco Tetration Detect subscription software license in multiples of 100 workload equivalence; choose a quantity from 1 to 10 (for example, a quantity of 5 will provide the license price for up to 500 software sensor instances) |
C1-TA-ENF100-K9 | | Add-on Cisco Tetration Protect subscription software license for policy enforcement in multiples of 100 workload equivalence; choose a quantity from 1 to 10 (for example, a quantity of 5 will provide the license price for up to 500 software sensor instances) |

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

- You can select a 1-year, 3-year, or 5-year subscription term.
- The subscription price includes software support.
- The subscription tier is selected automatically based on the quantity entered.
- Enforcement is an add-on license and cannot be ordered without the base software license.
- You can select the annual billing option or prepay for the entire term.
- You can add more software sensor instance licenses.
- This software subscription license can be used with both Cisco Tetration hardware clusters and the Cisco Tetration Virtual option.

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

<table>
<thead>
<tr>
<th>Bundle part number</th>
<th>Part numbers included in bundle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1-TAAS-SW-K9</td>
<td></td>
<td>Cisco Tetration bundle part number that includes the software subscription license for SaaS option.</td>
</tr>
<tr>
<td>C1-TAAS-WP-FND-K9</td>
<td></td>
<td>Bundle part number for the Cisco Tetration workload protection subscription license. You need minimum quantity of 100, with a 1 or 3 year term.</td>
</tr>
<tr>
<td>C1-TAAS-ENDPT-K9</td>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>
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 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](https://www.cisco.com/go/tetration).

**For More Information**

For more information about the Cisco Tetration platform, please visit [https://www.cisco.com/go/tetration](https://www.cisco.com/go/tetration) or contact your local Cisco account representative.
### Document History

<table>
<thead>
<tr>
<th>New or revised topic</th>
<th>Described In</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated supported operating systems for visibility and enforcement, and licensing</td>
<td>Ordering information, licensing terms and supported operating systems</td>
<td>May, 13&lt;sup&gt;th&lt;/sup&gt; 2019</td>
</tr>
<tr>
<td>terms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updated product overview, key features and benefits and ordering information sections</td>
<td>Product overview, key features and benefits and ordering information</td>
<td>Jan, 30&lt;sup&gt;th&lt;/sup&gt; 2019</td>
</tr>
</tbody>
</table>