

Cisco Tetration Platform

Contents

Cisco Tetration overview	3
Architecture and use cases	4
Product details	7
Deployment options, licensing, and pricing.....	9
Support for Cisco ACI and other software-defined networking solutions.....	10
Ecosystem.....	10
Solution deployment and services.....	11
Channels.....	13

Cisco Tetration overview

Q. What is the official name of this platform?

A. The official name is the Cisco Tetration™. Other trademarked attributions are:

- Cisco Tetration Analytics™
- Cisco Tetration™ OS
- Tetration Analytics™

Q. Why is this platform called “tetration”?

A. “Tetration” is a mathematical term used to indicate very large numbers. It represents the fourth order of [iterated exponentiation](#). The engineering team used this term to indicate the huge volume of data being processed to provide meaningful results and to suggest massive scaling.

Q. How can customers find out more?

A. Go to <https://www.cisco.com/go/tetration>.

Q. Briefly, what is the Cisco Tetration platform?

A. Cisco Tetration is an analytics platform that uses machine-learning, behavior analysis, and algorithmic approaches to address key operational and security use cases within the data center. This approach allows customers to gain application insights, generate whitelist policy, and enforce a consistent policy for effective application segmentation in a diverse infrastructure. Cisco Tetration uses a number of modern big data technologies such as Apache Spark, Hadoop (Hadoop Distributed File System [HDFS]), Druid, and Kafka as core foundation components.

Q. From the customers’ point of view, why would they need the Cisco Tetration platform?

A. Applications are critical entities that customers are struggling to secure within the data center. Customers need a whitelist-based zero-trust model to provide better security for applications. Cisco Tetration, using rich telemetry and algorithmic approaches, provides a deep understanding of application dependencies and granular segmentation policies, and it enforces these policies consistently across a diverse environment. This approach addresses critical operational and security use cases within the data center.

Both Cisco® and third-party installed-base customers can gain immediate benefits in the time needed to complete these tasks. What previously took months or was simply impossible to do now takes weeks or less and is possible.

Q. Why do data centers need the Cisco Tetration Analytics platform?

A. Enterprise data centers are getting bigger and much more complex, with hundreds or thousands of interdependent applications. Cisco has been seeing rapidly increasing complexity in data centers due to increases in east-west traffic, application onboarding, virtualization, containerization, security threats, and cloud migrations.

Organizations have an imminent need within the data center to understand application behavior and dependencies, as well as to enforce secure and consistent whitelist policy. The market for such solutions is highly underserved. Solutions are available that address some of these needs, but they do not provide a comprehensive approach to meet these requirements at scale. Cisco Tetration, using big data technologies, is a single platform that provides a ready-to-use solution to address all these requirements at data center scale.

Q. Can you explain Cisco Tetration capabilities in simple terms?

A. The Cisco Tetration Analytics platform offers a ready-to-use solution that enables network administrators, security operations, and application owners to:

- Gain visibility into application components, communications, and dependencies to enable implementation of a zero-trust model in the network
- Perform real-time asset tagging, allowing administrators to associate specific characteristics with traffic telemetry data and workloads
- Automatically generate whitelist policy based on application behavior; it also provides a mechanism for including any existing security policy based on business requirements
- Enforce consistent policy across heterogeneous infrastructure and apply application segmentation
- Enhance the server protection within the data center by providing process inventory, process binary hash details, and the capability to search based on this information across the data center

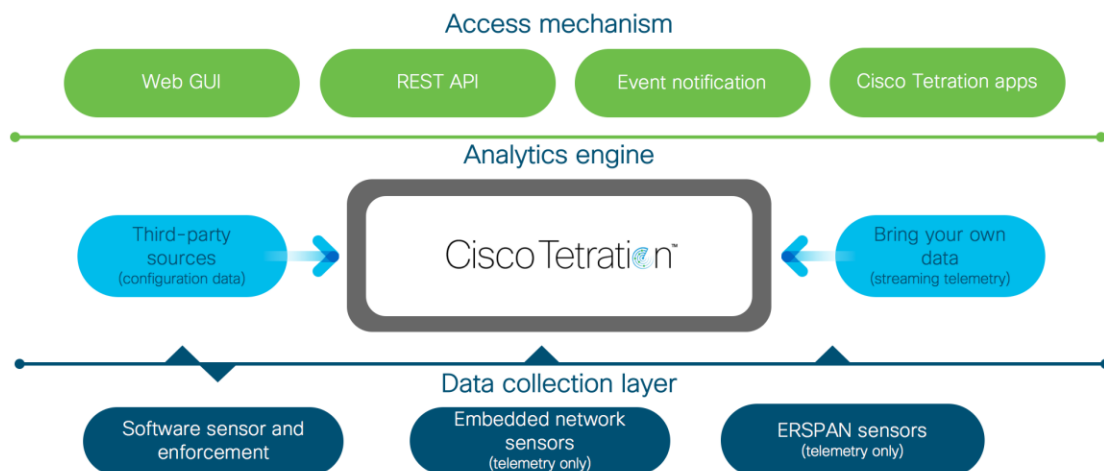
To achieve these capabilities, Cisco Tetration uses software sensors on servers (virtual machines or bare metal), hardware sensors (embedded in the switch ASIC), and Encapsulated Remote Switched Port Analyzer (ERSPAN) sensors to collect telemetry data. Cisco Tetration then uses modern technologies such as unsupervised machine learning, behavior analysis, etc. to support the functions. Overall, the Cisco Tetration Analytics application segmentation approach reduces the attack surface within the data center and increases the efficiency of data center operations.

Architecture and use cases

Q. What is the software architecture for the Cisco Tetration Analytics platform?

A. Figure 1 shows the architecture.

Figure 1. Cisco Tetration architecture



Q. What is the difference between a software sensor and a hardware sensor?

A. Software sensors and hardware sensor differ as follows:

- Software sensors are installed on the servers (virtual machine or bare metal). There are two types of software sensors: full-visibility and limited-visibility sensors. Full-visibility software sensors are available for major distributions of Linux, Microsoft Windows servers, and Microsoft desktops (Virtual Desktop Infrastructure [VDI] use case only) environments. These sensors collect telemetry data from every packet and every flow and also act as policy enforcement points. Limited-visibility software sensors provide only the conversation view required for application insights and policy generation on certain older operating systems.
- Hardware sensors are embedded into the switch Application-Specific Integrated Circuit (ASIC) itself. They collect flow data within the switch ASIC from all the ports.

Both types of sensors communicate the flow information to the Cisco Tetration Analytics platform in real time.

Q. What are ERSPAN sensors?

A. 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 out-of-band virtual machines running these sensors. These sensors understand only ERSPAN packets, strip the ERSPAN header, and generate Cisco Tetration telemetry data. This approach can be used in parts of the network in which software and hardware sensors are not feasible.

Q. How do users access information from the Cisco Tetration Analytics platform?

A. Cisco Tetration enables consumption of the information through an easy-to-navigate and scalable web GUI and through Representational State Transfer (REST) APIs. In addition, it provides 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 run on the platform, using the powerful computing resources available.

Q. Is this approach big data and analytics?

A. Yes, it is big data analytics. Without using big data analytics, the speed and scale required to support data center operations could not be achieved. We use these advanced technologies to address the use cases out of the box, thereby eliminating any need for advanced analytics capabilities to operationalize the platform. Big data focuses on the technology. We focus on the use case.

Q. What use cases are supported by the Cisco Tetration Analytics platform?

A. The platform supports the following use cases:

- Application behavior insight: Identify application components and their in-depth dependencies.
- Automated whitelist policy generation: Generate consistent whitelist policy based on application dependencies.
- Policy simulation and impact analysis: Simulate and perform impact analysis of a proposed whitelist policy.
- Automated policy enforcement: Enable effective application segmentation using consistent policy enforcement in a heterogeneous environment.
- Policy compliance: Detect policy deviation in minutes and help ensure application policy compliance
- Neighborhood graphs: Search for a specific application workspace and see a two-hops view of its communication with other servers within the data center.

-
- Process inventory: Collect the complete process inventory along with the process hash information for the application servers and enable searching based on the process name or hash in inventory.
 - Forensic analysis: Use long-term data retention, with full granularity, for forensic analysis. Now this capability is extended to VDI desktop virtual machines as well.

Q. What new use cases are available in the new Cisco Tetration Analytics platform software release?

A. The following new use cases are supported:

- Real-time asset tagging: The Cisco Tetration Analytics platform allows administrators to identify assets based on business functions. These assets are tagged based on the criteria and the annotations provided by administrators either through the GUI or the northbound API. Each asset can have multiple tags (up to 64 tags) that can add organizational and operational semantics to the identity of the asset. The Cisco Tetration platform can automatically query virtual machine attributes from VMware vCenter and Amazon Web Services (AWS), and it can keep this information up-to-date with periodic synchronization. Now these servers can be referred to by these tags, and complex queries can be constructed with these tags as references. This capability allows the platform to respond easily to queries that do not assume IT-level expertise, thereby increasing the appeal of the Cisco Tetration platform to stakeholders such as business analysts and data scientists in addition to IT administrators.
- Automated policy enforcement: Full-visibility software sensors also act as the enforcement points for the detailed application policy generated by the platform, enabling application segmentation. Using this approach, the Cisco Tetration Analytics platform provides consistent enforcement across public, private, and on-premises deployments. This capability 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. This approach helps ensure scalability, with consistent policy implemented for thousands of applications spanning tens of thousands of workloads.
- Server process and process 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.
- 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.

Product details

- Q.** How does the Cisco Tetration platform work with existing data center infrastructure?
- A.** Customers with existing data center infrastructure, which can be Cisco or third party, can deploy the Cisco Tetration platform. Deployment is achieved by installing software sensors on virtual machines or bare-metal servers. These sensors, installed on the servers themselves, collect the required telemetry data for the analytics platform and can also act as enforcement points for the segmentation policy. Another option is to use ERSPAN sensors to generate the telemetry data based on the copied traffic.
- Q.** The Cisco Tetration platform uses a whitelist security model. What is the difference between a blacklist model and a whitelist model?
- A.** The blacklist and whitelist models differ as follows:
- Blacklist: I know you're a bad person by your name. You can't come in. Anyone I don't know can come in by default. This has been the traditional security model for many years.
 - Whitelist: Nobody can come in unless I know their name and trust them.
- Q.** Why is a whitelist model better?
- A.** The whitelist model provides more front-end protection (don't wait for malware to be identified first, then list the name, and then avoid it). A zero-trust model requires a whitelist policy.
- Q.** Where is the segmentation policy enforced?
- A.** Policy is enforced using the operating system capabilities of the workload. Full-visibility software sensors orchestrate the policy using IP sets in Linux-based servers and advanced firewall functions in Microsoft Windows servers.
- Q.** Is the policy information updated as the application behavior changes?
- A.** Using the rich telemetry data, Cisco Tetration continuously monitors for policy compliance and deviation. For example, if additional instances of a specific application component are added, Cisco Tetration will enforce the same policy automatically on those instances. Also, if the workload moves, policy moves with it, and no additional action is required from administrators.
- Q.** Can the Cisco Tetration Analytics platform send notification when policy deviations are identified?
- A.** Yes. Cisco Tetration Analytics supports northbound notification through the Kafka message bus. Any northbound system can subscribe to those notifications and take additional actions. For example, a Security Incident Event Management (SIEM) system could subscribe to those events and open tickets automatically.
- Q.** What is the impact of enabling telemetry capture on the server and switch CPU?
- A.** Software sensors are built in with self-monitoring capabilities and offer a Service-Level Agreement (SLA) that the sensor by default will consume no more than 3 percent of a single-core CPU. This threshold is configurable and can be reduced or increased. If the CPU utilization by the sensor exceeds this threshold, the Cisco Tetration platform will automatically throttle data collection and log the number of packets it has missed until the CPU utilization for the sensor returns within the SLA threshold.

For hardware sensors, all operations are performed in the switch ASIC without any impact on the CPU. The flow cache table that holds Cisco Tetration Analytics telemetry data is exported every 100 milliseconds (ms) by default directly from the ASIC.

-
- Q.** What OS versions do the software sensors support?
- A.** Please see the Cisco Tetration Analytics data sheet for the full list of supported operating systems for both telemetry and enforcement:
<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html?cachemode=refresh>.
- Q.** What Cisco Nexus[®] switch models support Cisco Tetration Analytics telemetry?
- A.** The following Cisco Nexus switches have built-in capability in the ASIC to collect packet telemetry data and export it to the Cisco Tetration platform:
- Cisco Nexus 93180YC-EX
 - Cisco Nexus 93108TC-EX
 - Cisco Nexus 93180YC-FX
 - Cisco Nexus 93108YC-FX
- A.** Please see the Cisco Tetration data sheet for information about the required software versions for Cisco NX-OS Software and Cisco Application Centric Infrastructure (Cisco ACI[™]) deployments:
<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html?cachemode=refresh>.
- Q.** How much network traffic does Cisco Tetration telemetry generate?
- A.** Cisco Tetration Analytics collects only metadata, not the packet itself; therefore, the bandwidth requirement is very low. Typical sensor overhead is less than 2 percent of the actual aggregate traffic being monitored. For example, for Cisco IT, a single cluster is monitoring approximately 100 Gbps of traffic, but the sensor traffic overhead is less than 2 Gbps.
- Q.** What are Cisco Tetration applications?
- A.** The Cisco Tetration platform provides access to the data lake in the cluster. Using Cisco Tetration applications, developers, programmers, and data scientists can access the information in the data lake and write their own applications using Python or Scala. 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 and compare it with the flow information from the data lake. If required, these applications can also trigger external notifications through the Kafka message bus.
- Q.** Is security a part of this product?
- A.** Yes. With automated enforcement of the policy, Cisco Tetration Analytics offers security with effective application segmentation. This segmentation approach is confined to the applications within the data center infrastructure. The current release focuses on enabling customers to move their applications to a secure, zero-trust model. This is the foundational piece for security. Cisco Tetration Analytics currently does not support threat intelligence and threat protection functions.

Q. Is this an “open” platform?

A. Cisco Tetration Analytics is very open.

- All policies can be exposed on the Cisco Tetration Analytics platform (JSON, XML, or YAML).
- REST APIs allow customers to query information through northbound systems.
- Kafka provides a streaming interface to publish information to multiple consumers. This “push interface” enables the northbound system to subscribe to notifications.
- Through Cisco Tetration Analytics applications, developers can gain access to the data lake, write their applications using custom logic, and if needed, publish events northbound.

Deployment options, licensing, and pricing

Q. What are the deployment options for the Cisco Tetration Analytics platform?

A. The Cisco Tetration Analytics platform is an on-premises solution. It is designed to provide an appliance-like experience with hardware and software. Three deployment options are available:

- Cisco Tetration Analytics platform (large form factor with 39 rack units [39RU]): This deployment option consists of 36 servers and 3 Cisco Nexus 9300 platform servers. It is suitable for data centers hosting more than 5000 servers (virtual machine or bare metal). The large form factor can collect and analyze telemetry data from up to 25,000 servers (virtual machines and bare metal).
- Cisco Tetration-M (small form factor): This deployment option consists of 6 servers and 2 Cisco Nexus 9300 platform switches. It is suitable for data centers having less than 5000 servers (virtual machine or bare metal).
- Cisco Tetration Cloud (AWS public cloud): With this deployment option, the Cisco Tetration Analytics software can run in an AWS instance. The AWS instance for the Cisco Tetration Analytics platform is owned by the customer. This option is suitable for data centers hosting less than 1000 servers (virtual machine or bare metal).

Q. What are the components of Cisco Tetration Analytics pricing?

A. Cisco Tetration Analytics pricing consists of two components:

- Hardware component: This component is either the Cisco Tetration platform or Cisco Tetration-M hardware price, if the customer will be running Cisco Tetration Analytics within the customer’s own data center. This component is not required if the customer is planning to run Cisco Tetration Analytics in the AWS cloud.
- Software license: This component is the software subscription license for the analytics software. It is based on the number of workloads (virtual machines or bare-metal servers) from which the telemetry data is collected and analyzed. The customer can choose a 1-, 3-, or 5-year term with annual billing or a prepay option.

Q. What are the software subscription license components?

A. Cisco Tetration software is licensed based on the number of workloads (virtual machines or bare-metal servers) from which the platform performs the analytics. Telemetry data can be collected from software sensors, hardware sensors, or both. Cisco Tetration Analytics offers two licenses:

- The base license provides the fundamental features: collection of rich telemetry data, application insight, deep forensics, and policy recommendations.
- An add-on license provides policy enforcement and application segmentation capabilities. Enforcement licenses are required only for the number of software agents that will also act as enforcement points.

-
- Q.** Who are the target customers, users, and buyers?
- A.** Cisco Tetration is targeted at administrators, security operations, and line-of-business managers in midsize and large data centers. Segmentation is a high priority for many applications and security operation teams, and effective segmentation and consistent enforcement of policy on the premises and in public and private clouds are essential.
- Q.** Are there competitors?
- A.** There are number of smaller players that cover silo use cases using different approaches, but all lack scale, correlation capabilities, flexibility, consistent enforcement, and long-term retention capacity.

Support for Cisco ACI and other software-defined networking solutions

- Q.** Does the Cisco Tetration platform work with the Cisco ACI platform?
- A.** Yes. The use of software sensors in brownfield (existing) and hardware sensors in next-generation Cisco Nexus 9000 Series leaf switches (Cisco Nexus 93180YC-EX, 93180TC-EX, 93180YC-FX, and 93108TC-FX) enables the use of Cisco Tetration Analytics in Cisco ACI environments. Whitelist policy recommendations from the analytics platform can be translated into Endpoint Groups (EPGs) and contracts for the Cisco ACI fabric. Because Cisco Tetration generates fine-grained policy, some aggregation and processing is required before the policies are enforced in Cisco ACI.
- Q.** Does the Cisco Tetration platform work with other software-defined networking solutions?
- A.** Cisco Tetration is designed to work with any Software-Define Networking (SDN) or programmable infrastructure. For example, whitelist policy recommendations use a generic JSON, XML or YAML format that can be enforced in any SDN-based network. These can be implemented using any automation infrastructure such as Ansible playbook, access lists on switches, traditional firewall rules, and host and virtual firewall rules.

Ecosystem

- Q.** How does the announcement of intent to acquire AppDynamics affect the Cisco Tetration Analytics platform?
- A.** Cisco Tetration and AppDynamics complement each other. AppDynamics focuses on Application Performance Management (APM). AppDynamics uses instruments within the application (Java, .Net, C#, etc.) and monitoring of individual application transactions and associated performance metrics. Cisco Tetration collects rich network telemetry data from servers and switches and generates application insights based on the communication behavior, enabling customers to implement effective application segmentation.
- Q.** Will there be any integration between AppDynamics and the Cisco Tetration platform?
- A.** We view these technologies as complementary, and both can provide full visibility across the network and application stack. Plans for integration and use cases that add value for customers are being discussed.
- Q.** What is the value of an ecosystem?
- A.** The Cisco Tetration Analytics platform provides actionable data center visibility to a wide range of operations and applications. Ecosystem partners can consume the policy recommendations from the platform and implement coarse-grained enforcement within the data center network or at the data center perimeter. They can also query the flow information from the Cisco Tetration Analytics platform through the REST API and implement their own logic. In addition, technology ecosystem partners can write applications on Cisco Tetration Analytics and make the applications available to customers.

- Q.** What companies are part of the Cisco Tetration ecosystem?
- A.** Cisco Tetration has a broad set of ecosystem partners. These partners are classified into the following categories based on use cases:

- Insight exchanges: ServiceNow, Splunk, IBM Qradar, ExtraHop, Infoblox, and Corvil
- Security orchestration: Tufin and AlgoSec
- Service assurance: Vnomic, Turbonomic, and Veeam
- Layer 4 through 7 services: Citrix, F5, and AVI Networks

Full details about the ecosystem partner integrations can be found in our solution overview documents:

<https://www.cisco.com/c/en/us/products/data-center-analytics/tetration-analytics/solution-overview-listing.html>.

- Q.** Was any partner involved in product development?
- A.** No. Cisco Tetration Analytics was almost entirely internally developed. Cisco has been seeing rapidly increasing complexity in customer data centers due to increases in east-west traffic, application onboarding, virtualization, containerization, security threats, and cloud migrations. Cisco understood that customers needed much better visibility into the behavior of distributed applications. The best way to achieve this was to monitor all the traffic with deep telemetry and real-time analytics.

Solution deployment and services

- Q.** What type of skill set is required to deploy the Cisco Tetration Analytics platform?
- A.** The big data complexity is hidden from the users. The skill set needed to operate and use the platform is mainly the subject-matter expertise for the environment. No big data expertise is needed to deploy and operate Cisco Tetration. To accelerate adoption of this platform, it comes with Cisco Advanced Services at no additional cost during the initial launch period.
- Q.** What is delivered to the customer site?
- If the customer is deploying either a LFF or a Cisco Tetration-M (SFF) solution, it can be racked, stacked, and connected with base software loaded before it ships to the customer's facility. The customer has to answer a few questions about the environment and install the system software to complete the setup process.
 - Cisco Tetration Analytics is built on Cisco UCS® C-Series Rack Servers. It has three Cisco Nexus 9372 Switches to provide a full Clos network for the servers.
 - Cisco Tetration Analytics QuickStart Service is included with the Cisco Tetration Analytics product for the initial launch period. A Cisco Services expert will help each customer integrate Cisco Tetration Analytics in the data center, define the most relevant use cases, and transform data center operations to make them more efficient and secure. This strategy is in place to help ensure that customers get the most value from the solution and have a positive experience, as well as to support a smooth product ramp while the worldwide partner community develops practices to support Cisco Tetration Analytics.
 - Cisco Solution Support for Cisco Tetration Analytics provides centralized support for both Cisco and solution partner technologies. One service combines software, hardware, and solution-level support to streamline the support experience for complex issues in this multivendor solution.
 - The orchestration of product, services, solution partner ecosystem, and optional financing at launch underscores Cisco's intent to deliver solutions that fully address the customers' needs.

Q. If the Cisco Tetration Analytics platform is easy to install, why would Cisco provide quick-start service to customers?

A. The quick-start service provides the following benefits:

- With Cisco Tetration Analytics QuickStart Service, customers benefit from faster time to value, an improved IT user experience, and optimized policies and application performance for a more complete adoption. This service is especially important for larger, more complex deployments.
- For example, Cisco experts help tune machine learning to reduce noise and outliers, validate the policies that are most optimal for each customer's environment, and provide knowledge transfer to in-house staff to help them fully understand the capabilities of the platform.
- Providing advanced and solution support services in conjunction with the platform demonstrates Cisco's commitment to providing solutions that address customer needs and help ensure the best outcomes.

Q. What Cisco Services are available to support Cisco Tetration customers today?

A. The following Cisco Services are available:

- Cisco provides professional and solution support services for Cisco Tetration to help organizations get the most value from the solution. Additional Cisco Advanced Services offerings will be available in the second half of calendar year 2017.
- Cisco Tetration Analytics QuickStart Service is included with the Cisco Tetration platform for the initial launch period to help ensure that customers can successfully consume (adopt) the solution and get the most value from it. Key deliverables include an as-built document, an operations runbook summarizing policies and endpoints, and transfer of knowledge to in-house staff to help staff understand the capabilities of the platform.
- Cisco Tetration customers also receive solution-focused expertise with centralized issue management and resolution among Cisco and solution partner products through Cisco Solution Support. This global 24/7 support service resolves complex issues in multivendor environments on average 41 percent more quickly than product support alone. This capability makes Cisco Solution Support invaluable to customers who are investing in Cisco Tetration Analytics for its unique ability to deliver real-time visibility across the data center. Features and benefits include:
 - A primary point of accountability for resolving issues no matter where they reside, streamlining support from first call to resolution
 - A coordinated support framework with solution partner support teams, eliminating brokering support conversations
 - Solution-level expertise that results in faster time to resolution for complex issues
 - A single service for Cisco hardware, software, and solution-level support

Q. Does Cisco plan to offer additional services for customers who would like access to Cisco Tetration expertise beyond the initial deployment?

A. Yes. Customers can sign an additional service contract with Cisco Advanced Services to help with deployment and operations and continually optimize the data center applications environment and reduce security risks related to internal and external threats over the life of the subscription.

Cisco Services experts have deep experience and cross-technology expertise in data center operations, security, networking, and Hadoop (and collaborate with Cisco Tetration engineering teams).

Channels

- Q.** Who can sell the Cisco Tetration Analytics platform?
- A.** Any Cisco partner can sell Cisco Tetration Analytics. There is no specific Cisco Authorized Technology Partner (ATP) requirement.
- Q.** Can partners install the Cisco Tetration Analytics platform?
- A.** Right now, Cisco Tetration Analytics is bundled with the Cisco Advanced Services quick-start service to support integration and optimization of the solution in customer environments. Partners can expand on these basic services by getting educated about Cisco Tetration Analytics. After they are educated about Cisco Tetration Analytics deployment and operations, they will be authorized to perform the full installation.
- Q.** What skill sets should partners look for in installation engineers?
- A.** They should look for Linux administration, DevOps, and scripting knowledge, as well as familiarity with big data and analytics platforms.
- Q.** With what customers should partners position the Cisco Tetration Analytics platform?
- A.** Cisco Tetration provides value to a broad range of customers. The initial target industries are financial, healthcare, defense, intelligence, and other industries in which security and compliance are primary concerns.



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>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)