Cisco Tetration™

Contents

Cisco Tetration overview

Q. What is the official name of this platform?

A. The official name is the Cisco Tetration Analytics™ platform. Other acceptable attributions are:

- Cisco Tetration
- 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 that can be 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 designed to address security and operational challenges for a multicloud data center. It uses machine-learning, behavior analysis, and algorithmic approaches to offer a holistic workload-protection strategy and network-performance insights. This approach allows customers to gain application insights, auto generate whitelist policy and enforce a consistent policy to enable zero-trust model. In addition, the platform also tracks process-behavior deviations, identify software vulnerabilities in a multicloud infrastructure allowing you to reduce attack surface and identify indicators of compromise much faster.

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

A. Applications are critical entities within the data center. One of the key challenges customers face is how to provide a secure infrastructure for applications without compromising agility. Even today, the majority of data centers are designed with traditional perimeter-only security, which is insufficient. A new approach is needed to address this challenge. Cisco Tetration addresses this challenge in a comprehensive way using a multidimensional workload-protection approach.

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 minimize lateral movement, reduce the attack surface, and more quickly identify Indicators Of Compromise (IOCs). The market for such solutions within the data center is greatly underserved. Although solutions are available that address some of these needs, 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 complete visibility into application components, communications, and dependencies to enable implementation of a zero-trust model in the data center
- Automatically generate whitelist policy based on application behavior. It also provides a mechanism for including any existing security policy based on business requirements
- Enforce this segmentation policy across a multicloud infrastructure consistently, to minimize lateral movement
- Identify software vulnerabilities and exposures to reduce attack surface
- Provide process behavior baselining and identify deviations for faster detection of any IOCs
- Gain pervasive visibility that provides network performance insights in real time across the data center infrastructure
- Retain data over the long term for historical analysis without loss of detail

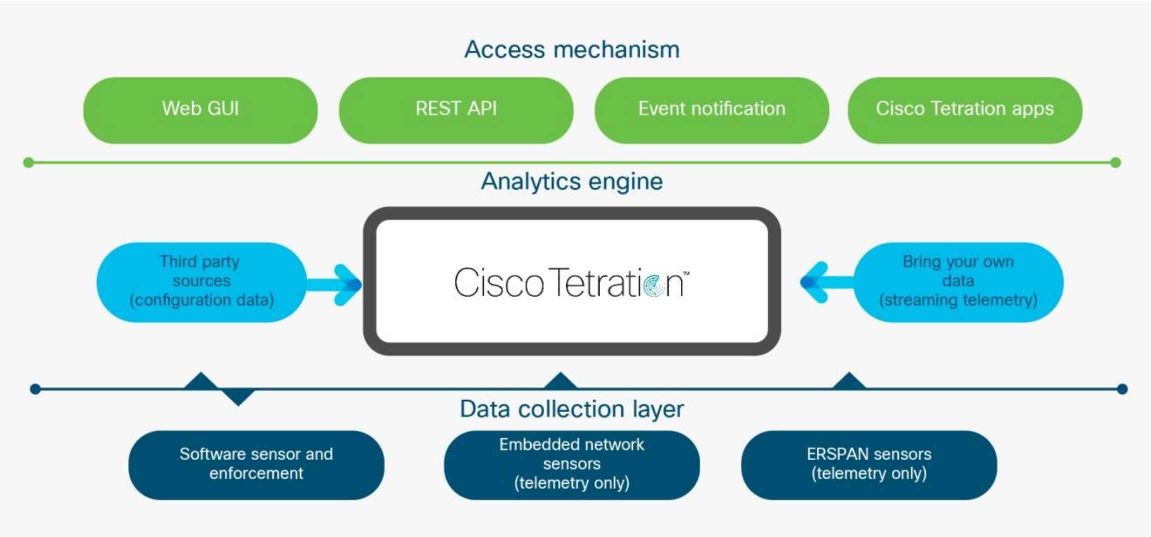
To achieve these capabilities, Cisco Tetration uses software sensors on servers (virtual machines or bare metal), hardware sensors (embedded in the switch's Application-Specific Integrated Circuit [ASIC]), and Encapsulated Remote Switched Port Analyzer (ERSPAN) sensors to collect telemetry data. Cisco 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


Access mechanism
Web GUI
REST API
Event notification
Cisco Tetration apps
Analytics engine
Third party sources (configuration data)
Cisco Tetration
Bring your own data (streaming telemetry)
Data collection layer
Software sensor and enforcement
Embedded network sensors (telemetry only)
ERSPAN sensors (telemetry only)

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, bare metal, or container host). 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, process data, and the software packages installed, and they also act as policy-enforcement points when enforcement is turned on.
- Hardware sensors are embedded into the switch 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, which 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. What are NetFLow sensors?

A. These out-of-band sensors are designed to generate Cisco Tetration telemetry data using NetFlow records. This NetFlow data is delivered to out-of-band virtual machines running these sensors. These sensors, which understand only NetFlow packets, strip the NetFlow header and generate Cisco Tetration telemetry data. This approach can be used in parts of the network in which software and hardware sensors or ERSPAN 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 a 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.
- **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.
- **Process behavior baseline and deviation:** Collect the complete process inventory along with the process hash information, baseline the behavior, and identify deviations.
- **Software inventory and vulnerability detection:** Identify all the software packages and versions installed on the servers. Using Common Vulnerabilities and Exposures (CVE) database, detect if there are any associated vulnerabilities or exposures.
- **Neighborhood graphs:** Search for a specific application workspace and see a two-hops view of its communication with other servers within the data center.
- **Forensic analysis:** Use long-term data retention, with full granularity, for forensic analysis. (This capability is now extended to VDI desktop virtual machines.)

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

A. The following are the new use cases in addition to segmentation using whitelist policy, that enable Cisco Tetration to offer a multi-dimensional l workload protection:

- **Server process baseline and behavior deviation:** Cisco Tetration collects and baselines the process details running on each of the servers. This information includes process ID, process parameters, the 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 get 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, for example, 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 IOCs and take remediation steps to minimize the impact.
- **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 whether the software packages have known information-security vulnerabilities listed in the CVE database. When a vulnerability is detected, complete details—including the severity and 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 and exposures, including high impact threats such as Spectre and Meltdown.

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: no waiting for malware to be identified before you can 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; 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 and Event Management (SIEM) system could subscribe to those events and open tickets automatically.

Q. When a software vulnerability is found, can Cisco Tetration be used to take action?

A. Yes, administrators can define policies associated to a specific vulnerability or based on a vulnerability score. Tetration will automatically enforce the specified policy to all servers that meet the criteria.

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 sensor's CPU utilization returns to within the SLA threshold.

For hardware sensors, all operations are performed in the switch ASIC without any impact on the CPU. By default, the flow cache table that holds Cisco Tetration Analytics telemetry data is exported every 100 milliseconds 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
- Cisco Nexus 9500 series switches with N9K-X9736C-FX line cards

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. Cisco Tetration platform internally uses whitelisting, SELinux controls, certification-based authentication, and encryption to ensure that all communication to the cluster and within the cluster is secure.

Q. Is this an “open” platform?

A. Cisco Tetration 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 Virtual (Amazon Web Services [AWS], Microsoft Azure public cloud or Customer owned hardware running ESXi): With this deployment option, the Cisco Tetration software can run in an AWS, Azure public cloud or on-premises on customer owned hardware that meets the necessary requirements. The AWS or Azure instance for the Cisco Tetration platform is owned by the customer. This option is suitable for data centers hosting less than 1000 servers (virtual machine or bare metal).
- Cisco Tetration SaaS: Cisco Tetration software runs in the cloud and can be consumed by customers truly as a software service offering. Customer does not need to purchase, or maintain any hardware or Cisco with this offer. This deployment model scales to 10s of thousands of sensors.

Q. How will I connect to Tetration SaaS?

A. Tetration SaaS collects telemetry from software sensors from any data center environment (on-premises, private cloud, public cloud) over a encrypted port. No VPN is required or special FW rules necessary to send the telemetry to SaaS.

Q. What are the components of Cisco Tetration 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 its 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 workload equivalents (virtual machines, bare-metal servers, or container hosts) from which the telemetry data is collected, analyzed and policy enforced. The customer can choose a 1-, 3-, or 5-year term with annual billing or a prepayment option. Note: Software license for SaaS option is over 1- or 3-year term only.

Q. What are the software subscription license components?

A. Cisco Tetration software is licensed based on the number of workload equivalents (virtual machines, bare-metal servers, or container hosts) 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.

- SaaS license is a workload protection license. SaaS license includes both base as well as enforcement capabilities bundled into the same single SaaS license offer.

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-premises and in public and private clouds are essential.

Q. Who are the target market for Tetration SaaS?

A. Cisco Tetration SaaS is targeted for commercial, SMB, SaaS-first or SaaS-only customers. This consumption model has no CAPEX required, which significantly reduces the barrier to entry.

Q. Who are the target market for Tetration-V VMware ESXi?

A. Cisco Tetration-V VMware ESXi version is targeted for commercial, SMB or smaller deployments. This model completely decouples Tetration hardware from software. Customer can purchase their own hardware and provision Tetration software on it, via a single orchestrator. This model is ideal for smaller deployments, customer or partner Proof of Value (PoVs).

Q. Are there competitors?

A. A number of smaller players 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-Defined 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 policies 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. Is Cisco Tetration and AppDynamics complementary?

A. Yes. Cisco Tetration and AppDynamics complement each other. AppDynamics focuses on Application Performance Management (APM) and uses instruments within the application (Java, .Net, C#, etc.), 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 an effective holistic workload protection within the datacenter.

Q. Is there integration between AppDynamics and the Cisco Tetration platform?

A. We view these technologies as complementary; 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 Cisco Tetration (39-RU) or a Cisco Tetration-M (SFF) solution, it is 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 Unified Computing System™ (Cisco UCS®) C-Series Rack Servers. It has three Cisco Nexus 9372PX-E switches to provide a full Clos network for the servers.

- Cisco Tetration Analytics quick start 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 customer's needs.

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

A. With Cisco Tetration Analytics QuickStart Service, customers benefit from faster time to value, an improved IT user experience, and optimized policies and policy enforcement 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 Tetration includes solution support services to help organizations get the most value from the solution.
- Cisco Tetration Analytics quick start 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. Cisco Solution Support 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, 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. They also collaborate with Cisco Tetration engineering teams.

Channels

Q. Who can sell the Cisco Tetration Analytics platform?

A. Any Cisco partner can sell Cisco Tetration. 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 for the large or small form factor appliance based models. Partners can expand on these basic services by getting educated about Cisco Tetration Analytics. After becoming educated about Cisco Tetration Analytics deployment and operations, they will be authorized to perform the full installation.

Partners can offer implementation services as well as managed services for the Tetration-V (Virtual) as well as Tetration SaaS offers. Cisco Advance Services is not bundled as part of these offerings.

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.**

Printed in USA C67-737402-05 04/18