Cisco Tetration Platform for Workload Protection
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product overview</td>
<td>3</td>
</tr>
<tr>
<td>Features and benefits</td>
<td>5</td>
</tr>
<tr>
<td>Key capabilities for Cisco tetration cloud workload protection functionality</td>
<td>6</td>
</tr>
<tr>
<td>Deployment options and scale</td>
<td>9</td>
</tr>
<tr>
<td>Licensing</td>
<td>9</td>
</tr>
<tr>
<td>Supported operating systems</td>
<td>10</td>
</tr>
<tr>
<td>Ordering information</td>
<td>10</td>
</tr>
<tr>
<td>Put Cisco expertise to work to accelerate adoption</td>
<td>10</td>
</tr>
<tr>
<td>Cisco Capital</td>
<td>10</td>
</tr>
<tr>
<td>For more information</td>
<td>11</td>
</tr>
</tbody>
</table>
The Cisco Tetration™ platform offers effective workload protection for multicloud data centers by containing the lateral movement, proactively identifying workload behavior anomalies, and reducing the attack surface.

Product overview

Today’s data centers consist of a multicloud infrastructure that use bare-metal, virtualized, and container-based workloads. As everything revolves around software, applications running on these infrastructures are the crown jewels, they are dynamic—they are constantly evolving. One of the key challenges that you face is how to provide a secure infrastructure for applications without compromising agility. Even today, the majority of datacenters are designed with traditional perimeter-only security, which is insufficient. A new approach is needed to address this challenge.

The Cisco Tetration platform is designed to address this challenge in a comprehensive and scalable way. Tetration enables a holistic workload protection for multicloud data centers by using:

- Whitelist-based microsegmentation, which allows implementation of a zero-trust model
- Workload behavior baselining and proactive identification of anomalies
- Detection of common vulnerabilities and exposures associated with the software packages installed on the servers
- Act proactively by quarantining server(s) when vulnerabilities are detected and blocking communication when policy violations are detected
- Understand the datacenter security posture and where to focus in order to improve the overall datacenter security

Figure 1.
Multidimensional workload protection approach using cisco tetration

By using this multidimensional workload protection approach (Figure-1), Cisco Tetration significantly reduces the attack surface, minimizes lateral movement in case of security incidents, and more quickly identifies Indicators Of Compromise (IOCs).
The Cisco Tetration platform makes it possible to implement such security approach seamlessly by collecting rich telemetry from servers, applying machine learning and other algorithmic approaches, and automating the application policy lifecycle.

- **Software sensors:** These lightweight sensors run as user processes and can be installed on servers running Linux or Microsoft Windows operating systems. These servers can be virtualized or bare-metal or container-based and run in on-premises data centers or on any public cloud. The CPU overhead for these sensors by default is capped at 3 percent, and is self-monitoring to guarantee the Service-Level Agreement (SLA). These software sensors can collect telemetry data and also act as enforcement points for segmentation. They collect the following telemetry data:
  - **Flow information:** Contains details about flow endpoints, protocols, and ports, when the flow started, how long the flow was active, etc.
  - **Interpacket variation:** Captures any interpacket variations seen within the flow, including variations in the packet’s Time To Live (TTL), IP/TCP flags, and payload length
  - **Process details:** Captures processes executed on the server, including information about process parameters, start and stop time, process binary hash, etc.
  - **Software packages:** Creates an inventory of all the software packages installed on the server along with the version and distributor information

- **Analytics:** Cisco Tetration is a big-data platform designed to support modern data center scale requirements. Tetration processes the information from the sensors, providing a ready-to-use solution including:
  - Accurate insight into application-component communications based on observed behavior
  - Automated and consistent whitelist policy recommendations for applications
  - Flexibility to extend policy definition using workload context and other attributes such as users, user groups, location, etc.,
  - One-click policy enforcement to enable consistent application segmentation
  - Monitoring to track policy compliance deviations and update policy in near-real time
  - Baselining of the processes running on each server, its communication behavior and identifying deviations
  - Discovery of all the software packages installed on the server and identification of any vulnerabilities and exposures
  - In-depth forensics using powerful search filters, visual queries, customer events, and more

- **Access:** In addition to having a robust web-based user interface, Cisco Tetration provides system-generated, northbound event notification and the flexibility to define events with right severity. These capabilities enable you to carry out security operations efficiently and proactively.
Features and benefits

Table 1 lays out the key features of the Cisco Tetration workload protection features and their benefits.

Table 1. Key Features and Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| Zero-trust model using microsegmentation                                | ● Secure hybrid multicloud workloads and contain lateral movement using microsegmentation.  
● The Cisco Tetration platform allows only the required traffic between application components and users, blocking everything else. This approach prevents a persistent threat from entering or searching for additional vulnerabilities. |
| Application-first security                                              | ● Application workload protection using behavior- and attribute-driven policy for microsegmentation.  
● 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. |
| Automated whitelist policy generation                                   | ● Autogenerate 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 VMware vCenter, Kubernetes, OpenShift, Infoblox, DNS servers, 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.  
● Identify process behavior deviations based MITRE techniques and tactics as well as custom forensic rules  
● 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                                              | ● Use temporal analysis to baseline communication behavior between workloads and determine communication behavior anomalies.  
● Generate alerts for such communication anomalies are detected to enable proactive security operations. |
### Feature Benefit

| User-defined analytics, reports, alerts, and dashboards using custom applications | • Use industry-standard notebook applications to create customized live content.  
• Create live reports that can tie local data together with external, Internet-based context information.  
• Create customized alerts and avoid alert fatigue.  
• Build dashboards with graphics using open-source libraries. |
| --- | --- |
| Policy compliance and notifications | • Monitor policy compliance on a minute-by-minute basis and generate alerts for policy noncompliance.  
• Generate policy-related alerts through the Kafka messaging interface.  
• Monitor alerts through the user interface. Provide access for consumption by other northbound systems, such as Security Incident and Event Management (SIEM). |

### Key capabilities for Cisco tetratement cloud workload protection functionality

**Automated whitelist policy recommendation**

Using the Cisco Tetratement platform, you can automatically generate highly specific whitelist policies based on the application-communication behavior and dependency (Figure 2). Tetratement also provides the flexibility to include other predefined policies from higher level entities such as security operations. You can specify policy using abstract information including tags and annotations. For example, a security policy might specify that production servers cannot talk to nonproduction servers. With the latest release of Tetratement software, you can also use users, user groups information within the policy to restrict application access. Using this approach, Cisco Tetratement provides an infrastructure-agnostic whitelist that can be consumed through the northbound interface and enforced across different environments.

![Figure 2. Automated whitelist policy recommendation based on application behavior](image)

**Scalable policy enforcement to enable microsegmentation**

Cisco Tetratement microsegmentation allows network administrators to implement a secure, zero-trust model using an autogenerated application-whitelist policy. It normalizes this policy based on the priority and hierarchy before enforcing it. When policy enforcement is enabled for an application, software sensors carry it out using native operating system capabilities such as ipsets and iptables, in the case of Linux servers, and the Windows advanced firewall, in the case of Microsoft Windows servers. This approach delivers a stateful and consistent segmentation across multicloud data centers at scale (Figure 3). It also allows you to minimize lateral movement in case of security incidents.

In addition, in a virtualized environment, this mechanism helps ensure that segmentation policy moves with the workload, allowing increased application mobility without no need for an infrastructure-specific segmentation policy. As application dependencies and communication patterns evolve, Tetratement helps ensure that the policy is updated automatically.
Workload behavior baseline and anomaly detection

Cisco Tetration collects and baselines the process details running on each of the servers, including process ID, process parameters, the associated user, process start time, and process hash (signature) information. It provides a tree view snapshot of all the processes running on a server (Figure 4). Users can search for servers running specific processes or for process hash information. Cisco Tetration also has algorithms available based on MITRE techniques and tactics to track behavior pattern changes and match those to malware behavior patterns. Cisco Tetration raises security events for such behavior deviations. Security operations teams can customize those events, their severity, and associated actions using simple-to-define rules. In this way, security operations can quickly identify indicators of compromise and take remediation steps to minimize the impact.

Figure 4.
Process behavior baseline tree view
Software vulnerability detection

The Cisco Tetration platform discovers the installed software packages, package version, patch level, etc. The platform includes 19 years’ worth of Common Vulnerability and Exposures (CVE) database. Using this information, Tetration checks whether any of the software packages have known information-security vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database. When such a vulnerability is detected, complete details—including the severity and impact score—are included (Figure 5), and all the servers with the same version of the package installed for patching and planning purposes can quickly be identified. 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 identified vulnerabilities, including high-impact threats such as Specter and Meltdown.

Data exfiltration signals

The Cisco Tetration platform baselines the communication behavior between the workloads in the datacenter and between any external client to the server. It uses temporal analysis to capture the seasonality of the communication behavior. Cisco Tetration platform then looks for deviation in this behavior beyond set thresholds. When such deviations occur, it correlates with other security events associated with the workloads to determine if the pattern is similar to an event like data exfiltration. Alerts are generated for such events that can be integrated with SIEM system.
Composite security dashboard

It is highly critical for security operations team to understand the security posture of the datacenter and what elements of security aspects are contributing to the current posture. Cisco Tetration security dashboard is designed to provide a composite security score based on number of different aspects.

- Vulnerabilities associated with the software packages
- Process hash consistency and process behavior
- Segmentation policy compliance
- Data leak signals

It also provides the score breakdown for each of these elements to understand where to focus in order to improve the security posture.

![Security dashboard with composite security score](image)

Figure 7. Security dashboard with composite security score

Deployment options and scale


Licensing

Licensing terms

Tetration SaaS deployment:

SaaS subscription is governed by Tetration SaaS Offer Description (https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_tetration_saas_offer_description.pdf) and the Cisco Universal Cloud Agreement located at https://www.cisco.com/go/uca (or similar terms existing between you and Cisco) (the “Agreement”), and any software that you install is licensed under the Cisco End User License Agreement located at https://www.cisco.com/go/eula (the “EULA”).

On-premises deployment models:

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

Supported operating systems


Ordering information


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.
For more information