Cisco Tetration Platform

Holistic workload protection for a multicloud datacenter

Applications are guiding 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 minimize lateral movement. Network and security operations teams are having difficulty implementing a secure infrastructure. This challenge is exacerbated even more when it is a multi-cloud datacenter. To address this challenge effectively, network and security operations teams need better insight into applications and a holistic workload protection strategy.

The Cisco Tetration platform (Figure 1) addresses these requirements using unsupervised machine learning, behavior analysis, and algorithmic approaches. It provides a ready-to-use solution to accurately identify applications running in the data center and their dependencies and the underlying policies between different application tiers. The platform is also designed to implement a zero-trust model using whitelist policy and segmentation, monitor the behavior of the processes running on the servers, and identify software-related vulnerabilities and exposures. With this approach, the Cisco Tetration platform provides a multidimensional security approach across virtualized and bare-metal workloads running in a multicloud environment.

Benefits

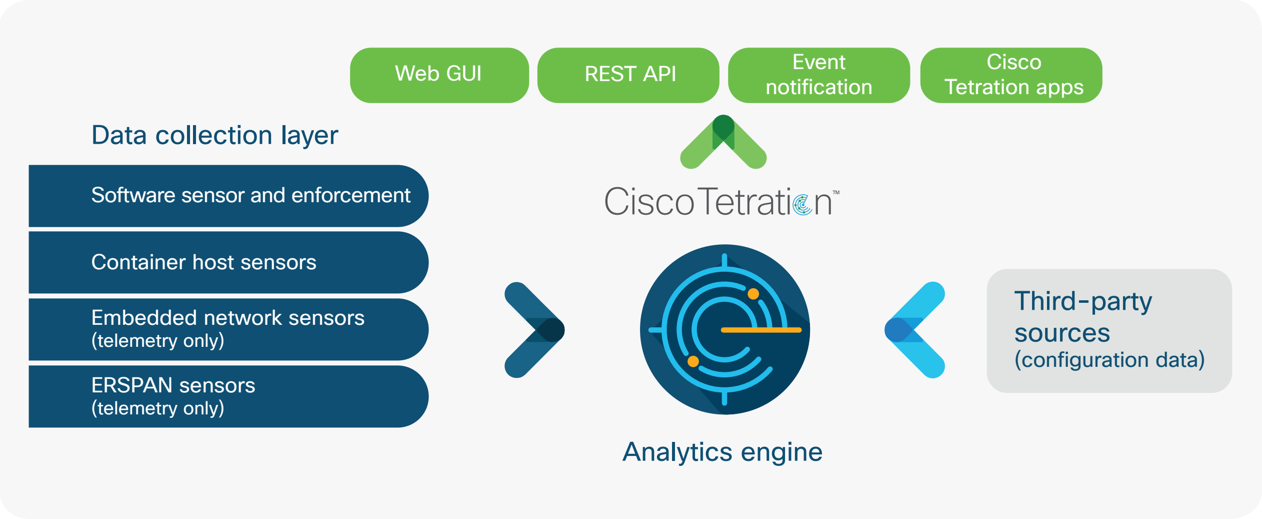
- Uses behavior-based application insight to automate whitelist policy.
- Minimizes lateral movement using application segmentation to enable a secure zero-trust model.
- Identifies anomalies faster by using process-behavior deviations.
- Reduces the attack surface within the data center by quickly identifying common vulnerabilities and exposures.
- Collects comprehensive telemetry from a heterogeneous environment to provide actionable insights in minutes.
- Enables long-term data retention for deep forensics, analysis, and troubleshooting.

> **“Cisco’s Tetration Analytics has provided us unprecedented visibility into our network and applications and is enabling us to migrate from a legacy blacklist policy model to a significantly more secure whitelist policy model driven by ACI.”**
>
> **– Healthcare customer**

By using software sensors, hardware sensors, and Encapsulated Remote Switched Port Analyzer (ERSPAN) sensors across the data center infrastructure, the platform can support both existing (brownfield) and new (greenfield) deployments. Software sensors also act as enforcement points for application segmentation.

The Cisco Tetration platform is powered by big-data technologies to support data center scale. It can process comprehensive telemetry information received from sensors in near-real time (up to 2 million telemetry events per second). The platform can enforce consistent policy across thousands of applications running on tens of thousands of servers. It is also designed for long-term data retention, and it can search tens of billions of telemetry records from its data lake and return actionable insights in less than a second.

Figure 1. Cisco Tetration platform architecture


Web GUI
REST API
Event notification
Cisco Tetration apps
Data collection layer
Software sensor and enforcement
Container host sensors
Embedded network sensors (telemetry only)
ERSPAN sensors (telemetry only)
Cisco Tetration™
Third-party sources (configuration data)
Analytics engine

> **“We needed up to a month to map a complex application, and Cisco Tetration allows us to do this in days or less. This will help us complete a significant IT initiative with major cost implications in far less time.”**
>
> **– The Huntington National Bank**

Make informed security and operational decisions using behavior analysis

The Cisco Tetration platform provides a ready-to-use solution using unsupervised machine learning and a behavior-based algorithmic approach:

- **Application insight:** This platform is designed to provide insight into application dependencies and behavior baselining using machine-learning techniques. It can also automatically identify and group application-component clusters (for example, database clusters) using communication patterns and process information. Using this real-time telemetry data, it can automatically generate the whitelist policy required for application segmentation.
- **Application behavior-based whitelist policy:** By using advanced algorithms, the platform auto generates a granular whitelist policy for segmentation. It also provides the capability to merge the business policy requirements with the policy generated based on application insights. This normalization and hierarchical merging of policies helps ensure that administrators with reduced scope cannot override higher level business policy intentions. The platform supports a “try before you apply” mode to allow you to simulate the whitelist policies and analyze their impact before you apply the policies in production networks.
- **Automated policy enforcement:** The platform provides consistent policy enforcement through software sensors across public and private clouds and on-premises deployments. Because the policy is enforced on the workload itself, the platform supports both virtualized and bare-metal environments. This approach also helps ensure that policy moves along with the workload, even when an application component migrates from a bare-metal server to a virtualized environment.
- **Process-behavior deviation identification:** Behavior of the servers can be determined by baselining the processes that are running on the server and identifying the any deviations from those baselines. In Cisco Tetration, algorithms are available to match these deviations to malware execution patterns, thereby enabling faster detection of anomalies. These behavior pattern mapping includes high-impact threats such as Specter and Meltdown.
- **Detection of vulnerabilities associated with software packages:** Cisco Tetration platform also baselines the installed software packages, package version, patch level, etc. The platform includes 19 years’ worth of vulnerability and exposure information. Using this data, Tetration platform checks whether any of the software packages have known information-security vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database. When a vulnerability is detected, you can find complete details, including the severity and the

> “The big ROI for us of using Cisco Tetration is not having to do application mapping again; the dynamic mapping means that we don’t have to go through the exercise again for future initiatives.”
>
> – The Huntington National Bank

impact score, and locate all the servers that have the same version of the package installed. You can also predefine policies with specific actions, such as quarantining a host, when servers have packages with certain vulnerabilities.

- **Compliance and auditability:** The platform monitors application components for policy compliance. It can detect any compliance deviations in minutes using behavior-analysis techniques and trigger a notification. In addition, enforcement policies are updated automatically to accommodate certain application-behavior changes.
- **Network performance:** The platform extends machine-learning capabilities to provide some critical network-performance information that operations team didn’t have before. It offers a per-flow path view, TCP performance metrics, network data-plane performance metrics, and much more. All this information is available in a time-series view, allowing users to go back in time and search for the details.
- **Search engine for visibility, troubleshooting, and forensics across the data center:** The platform collects and stores comprehensive traffic flow data. In addition to visibility into your servers, you can now deploy software sensors on Virtual Desktop Infrastructure (VDI) machines for visibility into your VDI environments. You can then query this data for visibility and forensics purposes across the entire data center and use this data to troubleshoot network and application problems.

The Cisco Tetration platform is unlike any other in the industry. It is a ready-to-use platform with advanced management capabilities to enable quick deployment with few configuration requirements. Using machine-learning capabilities, the platform drastically reduces the amount of human input required to understand communication patterns. And with its holistic workload capabilities, the platform allows you to build a more secure infrastructure for applications and significantly reduces the risk of exposure.

For more information

For more information about the Cisco Tetration platform, please visit www.cisco.com/go/tetration.