Cisco Tetration Platform

Behavior-based application insight and zero-trust policy

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 gaps in enforcement infrastructure. Network and security operations teams are having difficulty implementing effective segmentation for today's dynamic applications. To address this challenge effectively, network and security operations teams need better insight into applications, and they need to automate the required whitelist policy generation and enforcement.

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. In addition, the platform is designed to normalize and automate policy enforcement within the application workload itself, track policy compliance deviations, and keep the application segmentation policy up-to-date as the application behavior changes. With this approach, the Cisco Tetration platform provides consistent application segmentation across virtualized and bare-metal workloads running in public and private clouds and on-premises data centers.

Benefits

- Use behavior-based application insight to automate whitelist policy.
- Use application segmentation to enable efficient and secure zero-trust deployment.
- Provide consistent policy enforcement across on-premises data centers and private and public clouds.
- Identify application behavior changes and policy compliance deviations in near-real time.
- Support comprehensive telemetry processing in a heterogeneous environment to provide actionable insights in minutes.
- Enable long-term data retention for deep forensics, analysis, and troubleshooting.

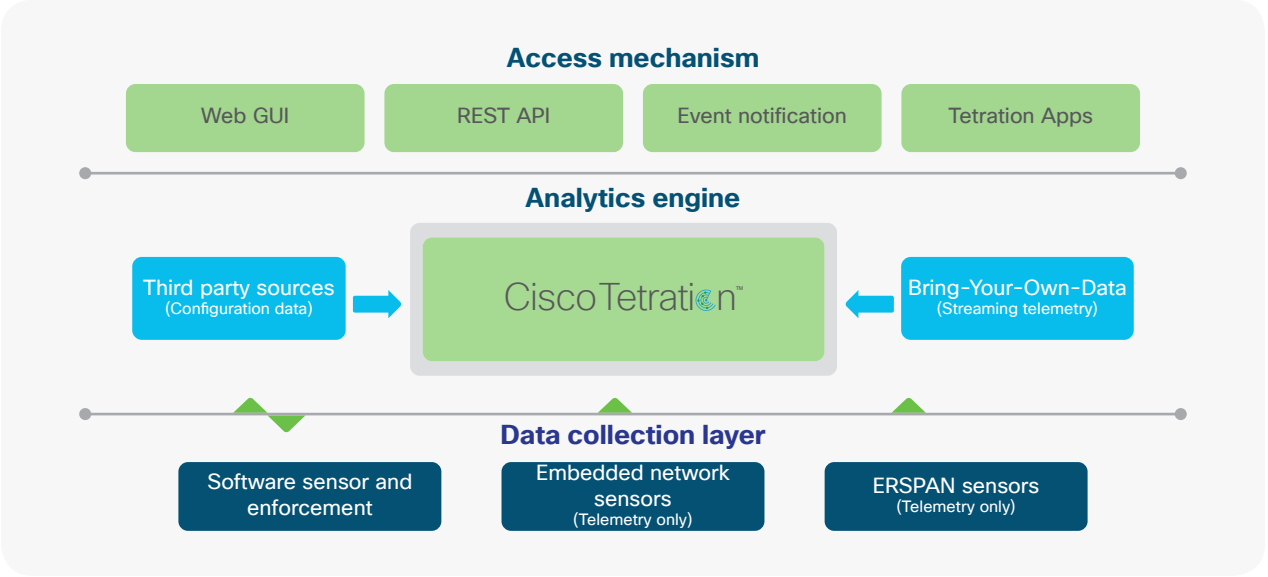
“Cisco’s Tetration Analytics Platform has provided us unprecedented visibility into our network and applications and is enabling us to migrate from a legacy blacklist policy model to a significantly more secure whitelist policy model driven by ACI.”

– 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 1.2 million telemetry events per second). This 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. In addition, streaming telemetry from other sources can also be ingested into the platform and accessed using Cisco Tetration applications.

Figure 1. Cisco Tetration platform architecture



“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 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 policy recommendations:** By using advanced algorithms, the platform generates a granular segmentation policy for each application. 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.
- **Policy impact analysis:** 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.
- **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.
- **Server process inventory:** Extending the server behavior-analysis capabilities beyond network constructs, the platform provides the capability to inventory the server processes, process hash information, and other process-related information. Using this, you can find out servers that executed a certain process or with a specific binary process hash.
- **Neighborhood graphs:** Users can quickly identify two-hop server neighbors for a selected server and see the communication details and traffic pattern. The graphs also provide accurate information about the server hops between two servers. In addition, you can generate preconfigured and custom alerts.

“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

- **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) virtual 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. Its machine-learning capabilities drastically reduce the amount of human input required to understand communication patterns. The policy enforcement model enables secure zero-trust operation for applications using application segmentation. Its self-monitoring and self-diagnostics capabilities eliminate the need for big data expertise to operate the cluster.

For more information

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

C45-737257-04 01/18