The Why, What, and How of Cisco Tetration

Why Cisco Tetration?

With the above trends as a backdrop, Cisco has seen specific changes within the multicloud data center.

- **Infrastructure is changing.** It is now common for an enterprise to have not only a data center or two (or more) but also many remote locations with server assets, as well as one or more cloud infrastructure partners. The “data center perimeter” today contains the data center, remote mini data centers, and cloud infrastructure partners.

- **Application development is changing.** Today’s applications are dynamic, using heterogeneous virtualization, containerization, micro-services, and workload mobility technologies, with communication patterns between application components constantly changing.

- **Traffic patterns are changing.** Now, 76 percent of data center traffic is east-west, a fundamental change from traffic patterns in the past. In addition, data center fabrics are being built at Nx100Gbps to support these traffic volumes.

- **These changes are opening up new attack vectors.** When an enterprise’s perimeter expands to encompass public cloud providers, the attack surface also changes. With more rapid application development occurring in more places, more often, there are more software vulnerabilities. As traffic shifted inside to east/west, where there is little to no segmentation, malicious code can now roam freely inside the “trusted intranet.”

Recent years have seen a relentless pace of change and digital acceleration across industry verticals. Some trends include:

- **Business trends:** High-performing application/infrastructure and security integrity are top of mind for CXOs due to their growing online presence.

- **People and process trends:** Teams are asked to work together efficiently to support and meet service levels for the business, giving rise to the terms “DevOps,” “DevSecOps,” and “NetDevOps.”

- **Technology trends:** As infrastructure and applications become increasingly critical to the business, new requirements for visibility, security, workload protection, and service operations in this complex (virtualized, multigigabit, containerized, multicloud, etc.) environment have emerged.
Because these trends and changes drive new initiatives and requirements for the multicloud data center, Cisco has created Cisco Tetration™ from the ground up expressly to meet these requirements. Cisco Tetration enables the business objectives of CXOs and executives, while enabling disparate teams to work together using a single platform as a pane of glass, and fulfills the day-to-day tasks of app developers, architects, SecOps, NetOps, and IT operations:

Figure 1. Cisco Tetration: features and benefits

Planning and design
- Planning and design for infrastructure and application migration, consolidation, or expansion
- Planning and design for disaster recovery and business continuity projects
- Hybrid-cloud cost analysis
- Performance and capacity management

Implementation
- Implementation of Software Defined Networking (SDN)
- Model and test policy before implementation – validate and simulate policy in real time or against historical data
- Zero-trust and application micro-segmentation deployment
- Implementation of consistent application security policy for cloud and infrastructure migration

Operations and optimization
- Pervasive visibility in the multi-cloud datacenter
- Asset and inventory discovery
- Reduced Mean Time To Resolution (MTTR)
- Policy compliance
- Security forensics

What is Cisco Tetration and Which specific use cases does it address?

Cisco Tetration is a turn-key solution that provides actionable insights to deliver business outcomes for application/infrastructure performance and security integrity in the modern heterogeneous, multicloud data center. The main use cases fall under three broad categories: Application Insight, Workload Protection, and Network Insight (as shown below).

Figure 2. Cisco Tetration main use cases
### Application insight

Application insight is a prerequisite to any successful data center consolidation, expansion, or migration. It is also a prerequisite to any SDN, application migration, or micro-segmentation initiative. Without understanding the dependencies of an application, these initiatives may be delayed or fail. Some of the functions included in this category are:

- Workload and application discovery in the multicloud data center
- Complete visibility of all communication in, out, and within the multicloud data center
- Automated mapping of all application dependencies (ADM) to enable implementation of a zero-trust model
- Automatic generation of a whitelist policy based on empirical analysis of every packet of every flow at multi-100Gbps speeds, including intent-based security policies mandated by business requirements
- Conversation analysis to show impact of traffic/load to prepare applications for cloud migration
- Hardening of application segmentation rules via simulation and what-if scenarios
- On-going application compliance and policy analysis for day-2 operations

### Workload protection

It is imperative the workloads be protected to provide a secure infrastructure for business-critical applications and data. Cisco Tetration enables holistic workload protection by securing communication between workloads as well as the workloads themselves. Some of the functions included in this category are:

- One-click deployment of whitelist policy for application micro-segmentation, protecting communication between workloads
- Process inventory and behavior baselining, analysis, and identification of deviations for the processes
- Full inventory of all software packages running on the workload, and the ability to detect common vulnerabilities and exposures associated with these packages by comparing against 19 years of CVE database
- Ability to detect anomalous behavior including side-channel attacks such as Spectre/Meltdown, privilege escalation, and shellcode attacks
- Actionable security insight, such as quarantining server(s) when vulnerabilities are detected, and blocking communication when policy violations are identified

### Network insight

Gaining pervasive visibility in the modern data center – which is agile, multigigabit, heterogeneous, and multicloud – is no easy task. Not only does Cisco Tetration offer pervasive visibility in this environment near real-time, it allows the operator to go back upwards of a year to “replay” the network insight “recording.” This level of deep and pervasive visibility enables planning and operations teams to make intelligent decisions about network changes and bandwidth upgrades. Some of the specific functions in this category include:

- Visibility of every packet of every flow at every speed, 24x7, in the multicloud data center (public or private) with bare-metal, container, and virtualized workloads
- Association of all network flows with system process and owner context
- Insight into the hop-by-hop path and performance statistics for an application all the way from the data center client to the initiating server process
- Ability to determine whether workload latencies are due to network and/or application constraints, hence reducing Mean Time To Resolution (MTTR)
- Ability to visualize neighborhood relationships
- Collection of performance metrics, including application latency, SRTT, TCP retransmissions, window sizes, and long TCP handshakes
- Ability to search on all historical flows contained in the platform, which may include up to a year or more of data
How is Cisco Tetration implemented?

Legacy approaches neither meet nor scale for the new requirements of the changing data center. Cisco Tetration represents a paradigm shift that leverages Artificial Intelligence (AI) and big data analytics to address the modern data center that has the following characteristics: (1) it is multicloud, where boundaries extend beyond on-premises data centers; (2) it has heterogeneous environments with a combination of bare-metal hosts, virtualized workloads, and containers; and (3) it is dynamic with changing traffic patterns at multi/100-Gigabit+ speeds and predominantly east-west traffic patterns. By leveraging algorithmic approaches, Cisco Tetration is able to automate the identification of application flows at 100+ Gigabit speeds, across private data center, cloud, and hybrid deployments at a level of detail that can enable the application dependency mapping, security enforcement, and added business value required by customers. Cisco Tetration high-level architecture is shown in the figure below:

![Cisco Tetration high-level architecture](https://blogs.cisco.com/datacenter/tetration-open-platform-enables-strong-partner-ecosystem-choice-and-flexibility-benefits-to-customers)

Figure 3. Cisco Tetration high-level architecture

There are three layers in the architecture:

**Input and telemetry:** Cisco Tetration collects telemetry and other context information from sensors and third-party sources. Sensors are deployed across heterogeneous environments, in public or private clouds, across virtual machines, to containers, and bare-metal servers. Sensor options include software sensors, hardware (Cisco Nexus® 9000 CloudScale series) sensors, container sensors, ERSPAN sensors, and Cisco IOS® NetFlow sensors. Further context may be obtained from load balancers, location information systems, IP Address Management (IPAM), the Configuration Management Database (CMDB), and Security Information and Event Management (SIEM) systems. With comprehensive telemetry across the heterogeneous infrastructure, Tetration gains true pervasive visibility in the complex environment.

**Big data analysis:** The telemetry of the communication flow and the system context from hundreds or thousands of agent sources are sent securely to the Tetration big data platform, which analyzes the data, using unsupervised machine learning and behavior analysis. The relationships among the workloads, and the state and health of the workloads and network, are derived. The algorithmic approach and artificial intelligence employed by Cisco Tetration results in the use cases of Application Insight, Workload Protection, and Network Insight described previously. The platform further preserves the data in a data lake, as well as in computed results and a time-series database. There are several delivery models for the platform, including on-premises appliance, virtual appliance, and Software-as-a-Service (SaaS).

---

Data access: Operators require access and the ability to manipulate their data. Cisco Tetration is an open platform that is accessible via GUI, REST API, and an event notification message bus. Operators may even leverage the compute and storage of the platform to write their own user apps in Python or Scala. Cisco Tetration is optimized to provide search query results of historical flow data in subsecond response times. The open APIs and event notification bus are leveraged by Tetration ecosystem partners for integration with SIEM, CMBD, and other tools.

Summary

In summary, Cisco Tetration is purpose-built to address industry trends impacting our customers’ businesses. The solution leverages streaming telemetry, behavior analysis, unsupervised machine learning and artificial intelligence, and big data analytics to deliver pervasive visibility, automated intent-based policy, workload protection, performance management, and much more. As a unified platform, Cisco Tetration allows various teams to work together efficiently across organizational silos and integrates with an ecosystem of partner solutions to increase value throughout the IT data center environment.