Cisco Tetration Analytics Opens the Door to Real-Time, Secure Application Segmentation With Automated Policy

Introduction

IT organizations are often under siege by a mix of elevated expectations for application delivery and a rising tide of security threats, not to mention the need to show ongoing improvements in operational efficiencies. Given this triple threat, this impact brief will examine the real and compelling promise of Cisco Tetration Analytics in both product and industry context.

Event

On February 1, 2017, Cisco announced significant advances in its Tetration Analytics, which was first introduced in Q2 2016. These advances include superior capabilities for optimizing and enforcing security, compliance, and other policies associated with both DevOps and application performance; more granular options for mapping application/infrastructure interdependencies to associated attributes and values; and new deployment options that make Tetration Analytics more accessible to mid-tier and smaller enterprises.

Cisco Tetration Analytics is designed for real-time visibility and control of applications running on public and private cloud, as well as legacy infrastructure environments, with support for migrations to software-defined networks (SDNs). It captures packet and flow data, as well as other data associated with workload, application, system, and broader infrastructure performance and availability. It employs machine learning to more proactively alert to issues and enforce policies. In doing so, it addresses a number of key stakeholder groups: security operations, network operations, and IT operations and lines of business, including development teams.

In its own words, Cisco delivers the Tetration platform as a "one-touch appliance: the servers and switches are prewired and the software is pre-installed." The new deployment options for Tetration include on-premises choices for mid-tier and large enterprises, as well as a new public cloud option, the Tetration Analytics Virtual Appliance deployed in Amazon Web Services (AWS). Both low-end on-premises and cloud-based offerings are designed for environments with fewer than 1,000 workloads. The Cisco Tetration Analytics Large Form Factor scales up to 10,000 workloads.

Market Context

Recent EMA research highlights how critical security issues are for advanced analytics targeting performance and change management.[1] This survey targeted operations, development, ITSM, and executive teams (only 6% of respondents were security professionals). The results were striking:

- When respondents were asked about managing application and service performance, the number one criterion for triage was *isolating security-related issues*, ahead of *isolating whether the problem is in the application, network, server, or database*.

Recent EMA research highlights how critical security issues are for advanced analytics targeting performance and change management.

[1] EMA, "Advanced IT Analytics: A Look at Real-World Adoptions in the Real World," April 2016.

- When respondents were asked about both performance and change management data source priorities, *Security Information and Event Management (SIEM)* came out on top, ahead of even transaction data and business process impacts.
- When addressing the value of advanced IT analytics (AIA) solutions in supporting the move to cloud, security ranked in three of the top four categories: *improved network security, compliance,* and *integrated security and performance.*

Also relevant to Cisco Tetration Analytics' design is the compelling use of insights into application-to-application and application-to-infrastructure interdependencies. Ninety-six percent (96%) of the AIA research respondents indicated a strong need for insights into application interdependencies in some form for managing performance and change. The top three were:

- Infrastructure-to-infrastructure
- Application-to-infrastructure
- Application-to-application (application ecosystem)

Cisco Tetration Analytics: A Closer Look

Cisco Tetration Analytics is designed to support a mix of infrastructure requirements including public cloud, legacy infrastructure, virtualized infrastructure, Cisco's own Application Centric Infrastructure, and bare metal. Its **software agents** capture interdependencies and enforce policies, and reside on systems carrying application components or workloads. These include support for Linux VM, Windows Server VM, bare metal support, and a universal agent for other systems environments. Its **embedded network agents** reside on either on-premises or cloud-based network switches, Nexus 9200-X and Nexus 9300-EX. The network agents can capture and model application/infrastructure changes but do not in themselves enforce policies. However, unlike the software agents, they can:

- Detect collisions between workloads
- Detect buffer issues
- Detect microbursts
- Help support service providers that don't own the actual workloads and so can't deploy software agents

Cisco Tetration Analytics also integrates via a REST API with third-party sources, such as load balancers, IP address management capabilities, DNS data, and CMDB- or CMS-related dependency insights.

Informed by these data sets, Tetration's forensics search engine can search across billions of flows in less than a second and can leverage advanced **machine-learning heuristics**. Cisco Tetration Analytics also leverages an **Apache Kafka** message broker to support more fluid versatility in support of different users, use cases, policies, and scheduling, among other requirements.

One of the outstanding features of the enhanced solution is its ability to **dynamically apply policies** based on unique insights into application and infrastructure interdependencies and behaviors in context with a myriad of associated attributes—in what Cisco calls "application segmentation." This capability unifies action with awareness in support of performance, DevOps, security, compliance, and change management requirements. The enforcement model binds policies to workload characteristics and other behaviors. And most critically, Tetration platform policies can trigger automatic actions or invoke approval and review.

Moreover, these policies can be informed by a new capability that Cisco calls "**tagging.**" Each entity (asset or CI) can have up to 32 tags. For instance, a given database could be denied Internet access. Or production workloads could be prohibited from communication with non-production workloads. Such policies can be created based on role in either a hierarchic or non-hierarchic manner. So that, for instance, a given developer could have access to a certain range of polices for a certain range of application/infrastructure entities, but he or she would be subject to other binding policies from a security manager or business-related policies informed from more senior management.

EMA Perspective

Cisco Tetration Analytics represents a bold move into the application and service delivery arena—a direction that was dramatically underscored with the announcement of Cisco's intention to acquire APM vendor AppDynamics, a vendor with leading-edge and largely complementary capabilities in terms of transaction-aware application performance and top-down application-to-infrastructure mapping.

According to the vendor, so far Cisco Tetration Analytics has received strong positive uptake in large enterprise environments, chiefly in industry verticals where security and compliance are paramount, such as healthcare, financial services, and large government or public sector organizations. Tetration's striking support for integrated security and risk minimization, its granular capabilities for policy creation and automated action, and its scalability across a wide range of infrastructure environments all bode well for its growth in the industry far beyond Cisco's traditional install base. This was underscored with the introduction of a cloud-based option for IT environments without core investments in Cisco hardware. EMA looks forward to watching Tetration's continued advances in terms of functionality, increasing breadth in deployment options, and broader industry adoption—all of which collectively suggest a bold new set of opportunities for Cisco.

Tetration's striking support for integrated security and risk minimization, its granular capabilities for policy creation and automated action, and its scalability across a wide range of infrastructure environments all bode well for its growth in the industry far beyond Cisco's traditional install base.