IDC Analyze the Future

IDC Business Value Brief: Cisco Tetration Analytics

Cisco Datacenters Get Pervasive Visibility and Reduced Security Risk with 70% Less Time and Cost

Sponsored by: Cisco

Matthew Marden
June 2016

Overview

Cisco Systems, with over 70,000 employees and annual worldwide revenue of close to $50 billion, is a leading provider of networking solutions. In total, Cisco has almost 3,000 business applications at datacenters around the world that support its employees and customer-facing services. At this scale of operations, Cisco must constantly improve its ability to balance performance, agility, security, and cost.

Cisco IT has been engaged in a multiyear transformation to simplify:

- Migration of select applications to a private cloud
- Implementation of software-defined networking-(SDN)-based zero-trust operations
- Compliance with evolving security policies

In particular, security has been and remains a priority for Cisco, even as the explosion of east-west traffic in recent years has greatly expanded the attack surface. To bolster security, Cisco has wanted to implement "zero-trust operations" that include the use of whitelist policies. This operating model changes default communication permissions between applications from "permit any" to "permit none" unless explicitly otherwise allowed. This prevents attacks from propagating across applications, tenants, and data. Compliance can be validated quickly by comparing actual traffic flows with whitelist policies in place.

Cisco understands that successful private cloud migration, zero-trust operations, and compliance require visibility into the complex dependencies between application components, users, and databases. Understanding inherent dependencies for all of Cisco's thousands of distributed business applications would be prohibitively expensive if done manually. Further, Cisco would risk blocking application flows and carrying out ineffective migrations without full visibility.

Business Value Highlights

Organization: Cisco

Location: San Jose, California

Challenge: Improve compliance and create a zero-trust security environment by understanding all traffic flows with minimal effort while enabling migration of thousands of applications to SDN and cloud

Solution: Cisco Tetration Analytics

Expected benefits from the use of Cisco Tetration:

- Avoid 3,650 hours of IT staff time per 100 applications (70% less staff time) in dependency mapping and establishing zero-trust operations

Other projected benefits:

- IT staff time savings to:
  - Create natural groupings of internal users, partners, labs, databases, infrastructure, and so forth
  - Improve availability and performance of user applications
  - Identify infrastructure cost efficiencies
  - Validate compliance of existing application flows
  - Enable error-free application traffic analysis

June 2016, IDC #US41485516

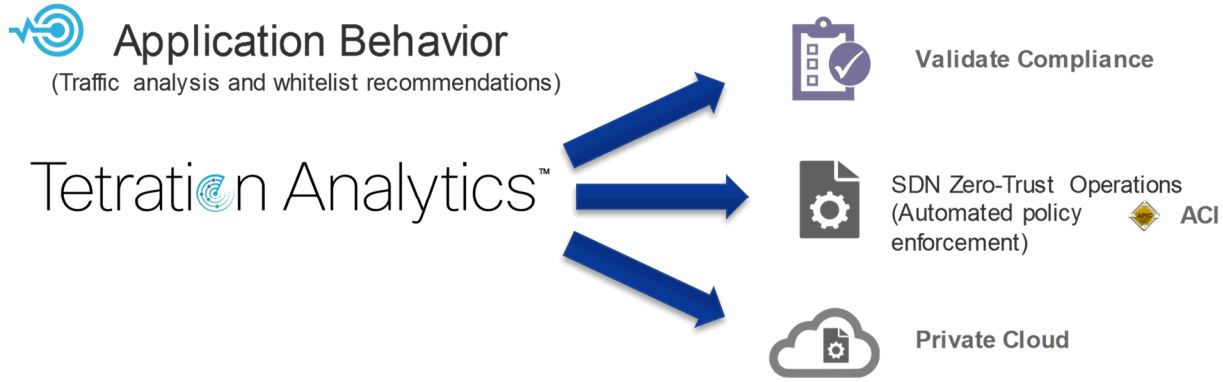
To address these challenges, Cisco is turning to Tetration Analytics (Cisco Tetration), its turnkey datacenter and networking analytics platform, to provide comprehensive, real-time insights that it needs to efficiently and accurately understand its application environment. On an ongoing basis, Tetration is providing a better, more complete understanding of application behavior, regardless of where Cisco is in the migration journey to SDN.

Specifically, Tetration is helping Cisco IT achieve (see Figure 1):

- Deep and near-real-time visibility into its application environment
- Staff efficiencies and cost-effective migrations to SDN zero-trust operations and private cloud
- Substantially better compliance by monitoring policies and data flows between customer-facing, production, lab, and partner systems

FIGURE 1

Using Cisco Tetration to Understand Application Behavior to Establish Zero-Trust Security Environments



Source: IDC and Cisco, 2016

Cisco's IT administrative teams are seeing tangible results in validating compliance, grouping applications logically, profiling existing policies, and improving application availability and performance, all with an investment of minimal staff time compared with relying on more manual processes.

In earlier phases, Cisco IT addressed these goals for some applications by using Cisco Application Centric Infrastructure (Cisco ACI), a leading SDN solution. However, it quickly discovered the limitations of manual application profiling, which was needed for its massive application base.

Most importantly, Tetration is enabling Cisco to migrate more applications to ACI and its SDN solution by mapping application interdependencies in far less time and with much higher accuracy and confidence. As a result, Cisco can migrate more applications and reduce its security exposure without needing to

invest a prohibitive amount of staff time. Once applications have been successfully migrated, the dynamic policy enforcement umbrella of Cisco ACI extends compliance across its datacenters, even as application and tenant policies are modified.

Based on interviews with several Cisco IT managers and a review of documents pertaining to the use of Tetration, IDC has projected the time savings that Cisco can expect to achieve in characterizing applications to prepare them for migration to ACI and application of whitelist security models. Cisco expects that it will need 70% less staff time to carry out application traffic analyses and establish zero-trust operational environments by using Tetration and ACI (reducing the staff time needed per 100 applications from 5,200 IT staff hours to 1,550 IT staff hours). As a result, IDC projects that Cisco will realize staff time savings of 3,650 hours for every 100 applications it migrates to its SDN zero-trust security environment, in addition to ongoing efficiencies that have not been quantified for this study (see Figure 2).

Cisco expects that it will need 70% less staff time to carry out application traffic analyses and establish zero-trust operational environments by using Tetration and SDN.

FIGURE 2

Cisco IT Datacenter Operations: Manual Approach Versus Automation with Cisco Tetration and Cisco ACI

(1) Understanding Application Behavior
(Traffic analysis and whitelist security recommendations)

	Manual Approach	Cisco Tetration Analytics
Staff hours (per 100 apps)	4,000	1,250
FTE costs ($100/hour)	$400,000	$125,000

(2) Establishing Zero-Trust Operations
(And automated policy enforcement)

	Manual Approach	SDN e.g., Cisco ACI
Staff hours (per 100 apps)	1,200	300
FTE costs ($100/hour)	$120,000	$30,000

Overall Impact of Cisco Tetration
(Total of efficiencies from 1 and 2)

70% less staff time =

	Manual Approach	Automation with Cisco	Cisco Tetration Benefit
Staff hours (per 100 apps)	5,200	1,550	3,650
FTE costs ($100/hour)	$520,000	$155,000	$365,000

Source: IDC and Cisco, 2016

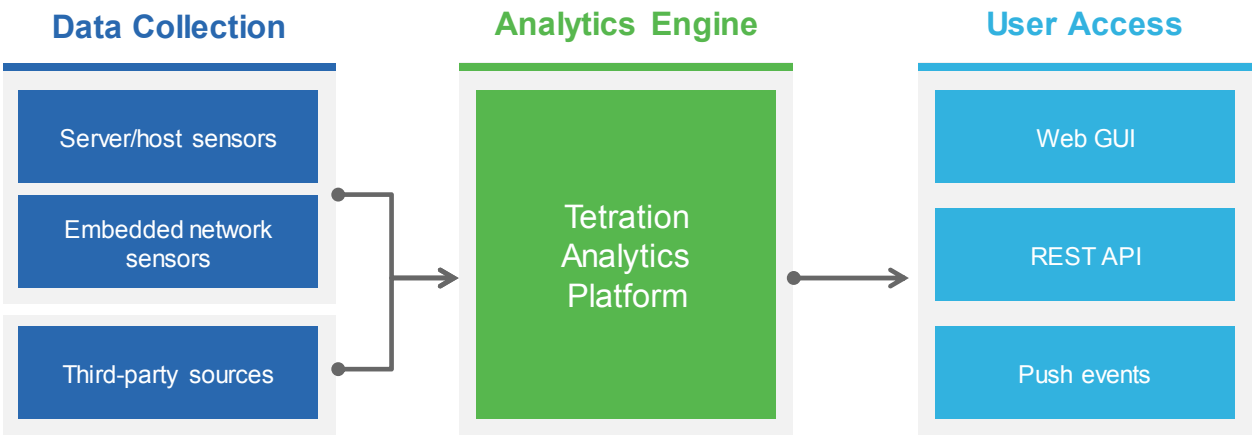
Overview of Cisco Tetration

Tetration Analytics is Cisco's turnkey datacenter and networking analytics solution designed to address the operational problems and security challenges organizations face as a result of insufficient visibility into their datacenter environments. Growth of application bases and shifting communication patterns between applications make it challenging for organizations to cost or time effectively collect telemetry, analyze data in real time, or address system complexity.

Cisco Tetration leverages Big Data technologies (Hadoop, Spark, Druid, and Kafka) with use case-specific algorithms built on this foundation. It uses software sensors that are installed on servers (virtual servers or bare metal) and hardware sensors that are embedded in Cisco switches (Cisco Nexus 92160CY-X and Cisco Nexus 93180CY-EX switch ASIC). Tetration is designed to provide an analytics platform capable of processing up to millions of flows per second and the capacity to retain billions of flow records without aggregation without requiring in-house data scientist or Big Data expertise (see Figure 3).

FIGURE 3

Overview of Cisco Tetration Analytics



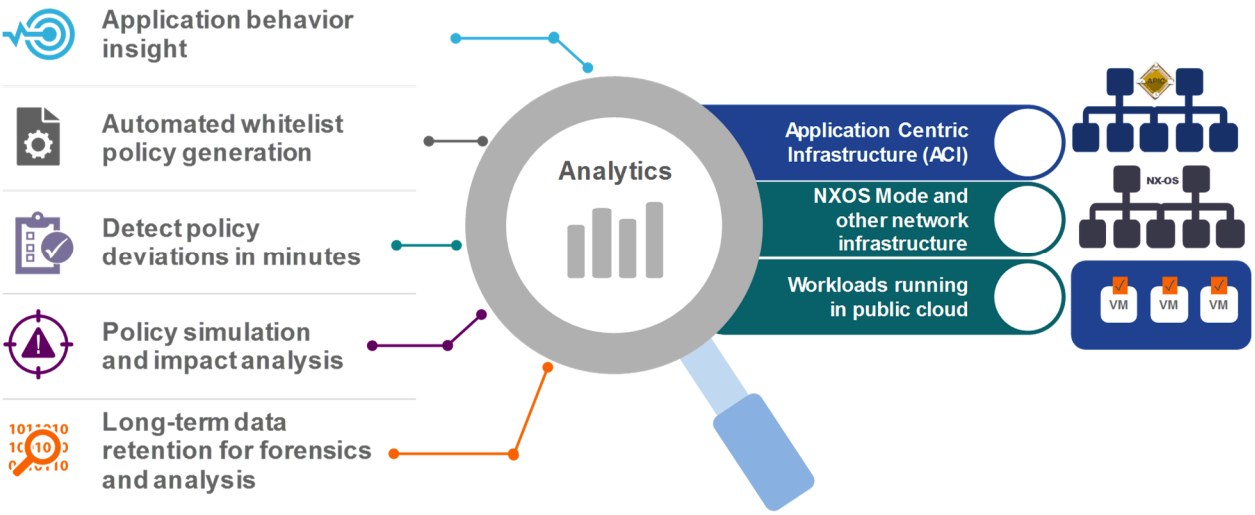
Source: IDC and Cisco, 2016

Cisco believes that Tetration has numerous potential use cases (see Figure 4), including:

- **Application behavior insights:** Capturing real-time traffic data between application components and behavioral analysis to find application groups, communication patterns, and service dependencies
- **Whitelist policy recommendations:** Providing whitelist policy recommendations for an application once application behavior has been understood
- **Policy simulation:** Simulating whitelist policy and testing it before moving it into production
- **Policy compliance:** Monitoring for deviations from policies once applied
- **Flow search and forensics:** Searching up to billions of flow records in near real time

FIGURE 4

Cisco Tetration Analytics Platform



Source: IDC and Cisco, 2016

Implementation of Cisco Tetration

Cisco's IT team has found it challenging to achieve full visibility into and understanding of complex dependencies between applications, hosts, and network infrastructure that change with regularity and identifying and taking into account changes made to underlying infrastructure that are not in line with security policies. As a result, even with strong security policies in place, as well as the use of a number of best-of-breed security solutions, gaps in security can arise that potentially leave it vulnerable to attacks.

In 2014, Cisco began deploying its Application Centric Infrastructure to support its move to a private cloud model of delivering business applications and services. It viewed this deployment as a component of making its datacenters into strategic assets rather than cost centers and to ensure that it has the operational flexibility and scalability to meet fluid IT and business challenges. As of May 2016, Cisco had migrated its most elastic and critical applications to its Cisco ACI environment.

The deployment of ACI along with the use of numerous security solutions from Cisco and other vendors enhanced Cisco's security position by providing greater visibility into its datacenter environment and providing efficiencies through policy-based security deployments. As a result, Cisco has enforced security more efficiently and effectively, thanks to automation, policy, and orchestration enabled by Cisco ACI. In particular, Cisco has substantially limited the security exposure of applications for which it could justify the staff time costs required to place within its whitelist security environment.

It is time consuming for any organization to profile application behavior and dependencies well enough to migrate applications. The challenges are the same whether migrating them to new datacenters, the public cloud, or the private cloud. As Cisco IT moved to its new private cloud, it too was faced with prohibitive staff time costs to carry out effective migration of applications. Consequently, Cisco sought an analytics-based solution that would enable it to migrate more applications to its Cisco ACI zero-trust security environment. Cisco began using Tetration in early 2016 and intends to leverage Tetration to migrate hundreds of applications to its ACI zero-trust security environment.

Benefits

IDC conducted several interviews with Cisco IT staff members and reviewed detailed analyses of the benefits that Cisco is achieving and expects to achieve with Tetration. On the basis of this information, as well as IDC's work in the datacenter and network security areas, IDC believes that the benefits detailed in the sections that follow are of the type, scope, and scale that an organization such as Cisco can reasonably expect to achieve with Tetration.

Cisco is leveraging efficiencies achieved with Tetration in mapping application interdependencies to migrate more applications to its SDN zero-trust environment. This will result in the application of whitelist security models to many more applications and harden its network security while reducing its attack surface. In addition, Tetration provides ongoing efficiencies by providing visibility into application interdependencies and flows — whether the applications are in ACI or not — which translates to better compliance, easier resolution of problems, higher availability, and ultimately improved performance of applications.

Addressing the Challenge of Migrating Applications to an SDN Zero-Trust Environment

IT security managers at Cisco explained that while they are confident in their existing datacenter and networking security ecosystem, they recognize that their inability to cost effectively move more applications to a whitelist security model leaves open potential vulnerability. In particular, they noted that the company faces the risk of security attacks and breaches such as spear phishing, which involves attackers sending emails to employees seeking access to certain databases. When an attack succeeds, the endpoint being used can become infected and the attacker can move on to other databases, hosts, and ports.

When an attack succeeds at gaining access to an endpoint, the potential scope of damage is related to the security architecture in place and the potential attack surface. Cisco's IT managers explained the importance of having a whitelist security model in place to reduce the potential impact of an attack: "*In a whitelist security environment, only necessary ports for that particular user are available through the device, which reduces the attack surface. In other words, an attacker is denied access to all hosts without explicit permission, as opposed to the presumption of access in a typical blacklist environment, where hosts have potential access to the full mesh of other hosts.*"

To improve its security posture by applying a whitelist security model — and also to capture other efficiencies and performance benefits of SDN — Cisco has migrated its most elastic and critical applications to its ACI environment. Once applications are within the ACI environment, ACI provides SDN-based zero-trust operations by recommending and applying a whitelist security model and enforcing cloud and application policies in the network fabric.

However, migrating any application to an SDN environment requires deep insight into application behavior and dependencies. Because most of Cisco's business applications reside in a distributed and complex environment, they have large numbers of inherent dependencies between internal users, partners, application components, and databases. This means that it takes substantial amounts of IT staff time to accurately and completely map each business application using manual processes. Even with this time investment, it is very challenging to obtain an accurate and complete view of application behavior through manual processes, which presents the risk of blocking important application flows and leads to failed migrations to its SDN environment. These factors prevented Cisco's IT team from taking on what an IT security manager termed the *gargantuan task* of migrating more applications to an SDN zero-trust environment.

Supporting Staff Efficiencies Through Improved Visibility into Application Environment

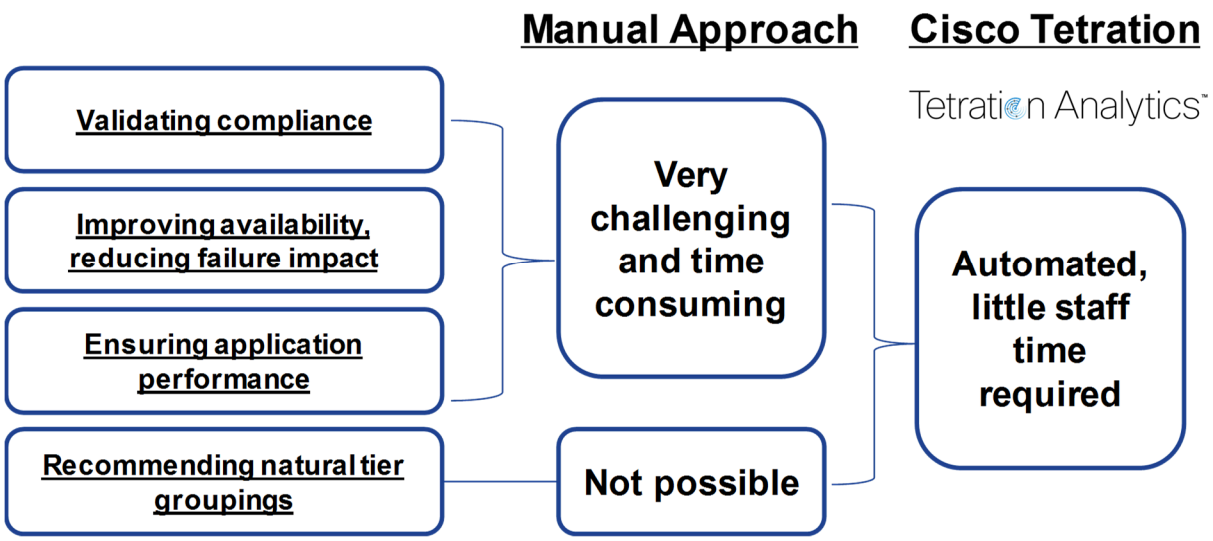
Cisco's IT team reports that Tetration not only supports its efforts to migrate more applications to its SDN zero-trust environment but also supports more efficient and robust management of its overall application environment. Of particular value is increased insight into application behavior and dependencies, which it realizes regardless of whether an application has already been migrated to its ACI whitelist environment. According to an IT security manager at Cisco, "*Even without creating a whitelist security model for an application, Tetration helps us validate and check compliance by giving us the visibility and oversight needed to remediate noncompliance connections, so it serves as a pseudo-enforcement mechanism*." The IT security manager noted that Tetration is especially beneficial for applications already in production: "*We get the biggest return on investment when Tetration is implemented around our production data servers – because that's where the gold is*."

"Even without creating a whitelist security model for an application, Tetration helps us validate and check compliance by giving us the visibility and oversight needed to remediate noncompliance connections."

According to Cisco, Tetration provides benefits by improving its ongoing understanding of application flows to detect potential threats; recommending natural tier groupings, which can mean more efficient problem resolution; allowing for easy checking of load balancers to improve availability; and isolating latency and bandwidth bottlenecks (going forward). IDC has not quantified these ongoing efficiencies attributable to Tetration, but Figure 5 provides a qualitative overview of its impact.

FIGURE 5

Efficiencies of Cisco Tetration



Source: IDC and Cisco, 2016

Supporting Efficient and Cost-Effective Application Migrations to an SDN Zero-Trust Environment

Meanwhile, Tetration is supporting efficient and cost-effective migration of more applications to a zero-trust environment. In particular, Cisco IT is benefiting from Tetration's ability to export a complete whitelist to any SDN solution with substantially less staff effort and ACI's commonality in importing the whitelist and then using it as is, which generates efficiencies in implementing whitelist recommendations.

According to Cisco's IT team, carrying out manual modeling of application behavior is not only time consuming but potentially ineffective. An IT security manager explained: "*Without Tetration, manual processes will miss flows, which means that migration of applications to SDN will fail.*" Further, when done manually, application traffic analysis requires substantial amounts of staff time to complete steps that include identifying hosts, updating network details, identifying network dependencies, setting security policies, and configuring devices. Only after completing these tasks can the application be migrated to an SDN environment, where a whitelist security model can be applied.

Because of the prohibitive amount of time required to carry out application traffic analysis manually and the probability of missing flows, Cisco has moved only some of its applications to its SDN zero-trust security environment. However, Tetration makes successful migration of more applications to an SDN zero-trust environment possible by significantly reducing the staff time requirements associated with those steps. As a result, Cisco anticipates extending its whitelist security model to more of its application base.

"Without Tetration, manual processes will miss flows, which means that migration of applications to SDN will fail."

According to Cisco, Tetration reduces the amount of IT staff time required to prepare an application for migration to an SDN zero-trust environment and then to implement whitelist security models by 70%. As a result, on a per 100 user basis, Cisco will need only 1,550 hours per 100 applications of staff time using Tetration compared with 5,200 hours per 100 applications using more manual processes based on efficiencies.

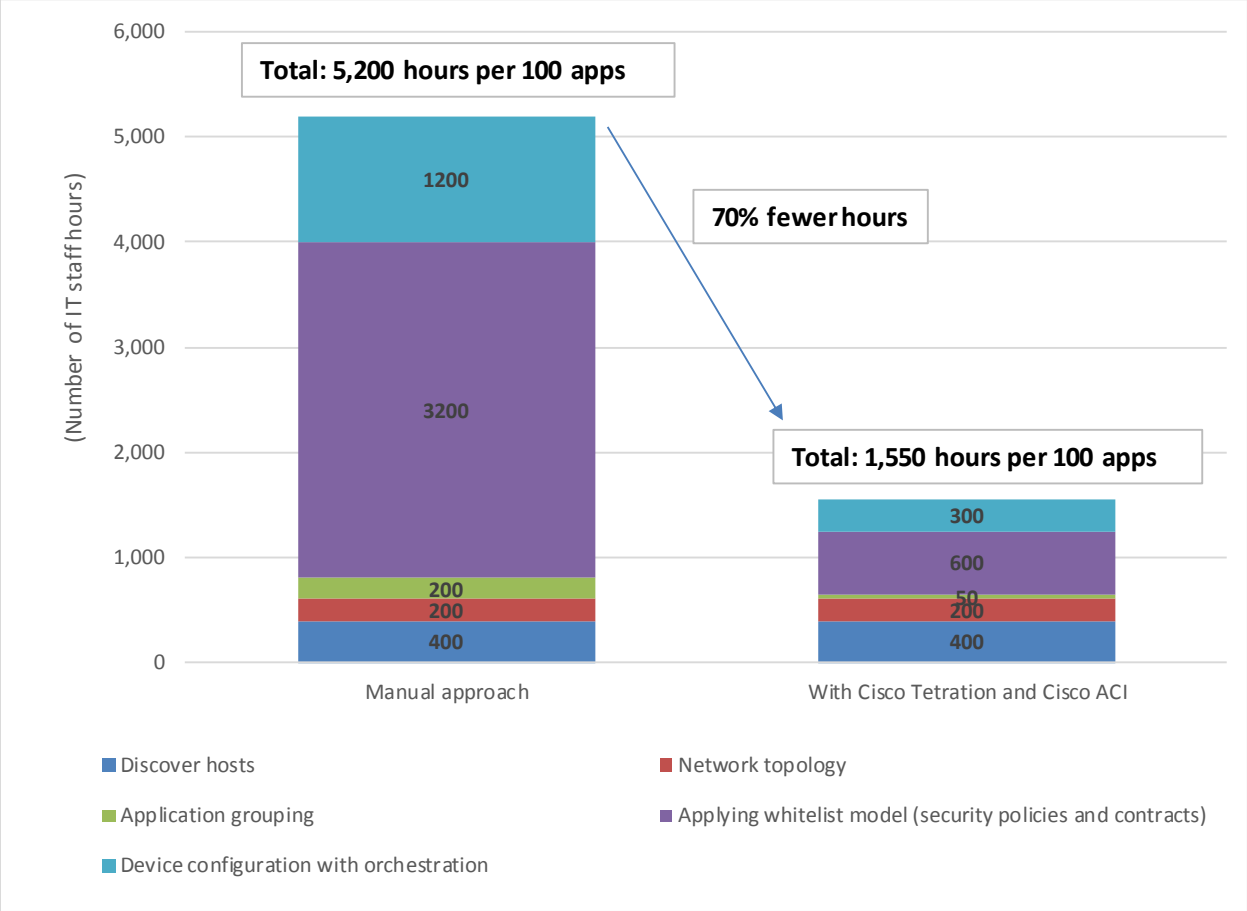
With Tetration, Cisco expects to reduce the staff time needed to carry out a traffic analysis by 69% compared with using manual processes. This means that Cisco's IT team will need to expend only 1,250 staff hours per 100 applications migrated to its SDN zero-trust environment compared with 4,000 hours per 100 applications using manual processes. In addition, based on early results of using Tetration Analytics and Cisco ACI together, Cisco IT is seeing a further 75% staff time efficiency in terms of implementing whitelist security models once applications are migrated, which means that 300 hours per 100 applications will suffice with Tetration compared with 1,200 hours. Specifically, Tetration and ACI support the following efficiencies:

- **Defining and creating security policies for whitelist security model:** With Tetration, Cisco's IT staff must spend far less time defining, creating, and validating packet flows before applying security policy. As a result, Cisco expects to save 2,600 hours of staff time per 100 applications (81% less staff time).
- **Application grouping:** Tetration automatically groups similar servers, which Cisco expects to result in 150 hours of staff time savings per 100 applications (75% less staff time) in determining dependencies.
- **Device configuration with orchestration:** ACI implements whitelist security models without needing change requests and approvals to be generated, which Cisco anticipates will avoid 900 hours of staff time per 100 applications (75% less staff time).

In total, these efficiencies with Tetration and ACI will enable Cisco to save 3,650 hours of staff time per 100 applications as it maps their dependencies to support migration to its SDN environment and then implements a whitelist security model. Assuming a $100 per hour fully loaded cost of IT staff time, this would represent a saving of $365,000 per 100 applications that Cisco migrates to ACI and applies whitelist security models (see Figure 6).

FIGURE 6

IT Staff Time Needed for Application Traffic Analysis and Whitelist Model Application: Cisco Tetration Versus Manual Approach, per 100 Applications



Source: IDC and Cisco, 2016

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2016 IDC. Reproduction without written permission is completely forbidden.