Infrastructure automation requires data visibility

How Cisco IT is streamlining its transition to a software-defined, zero-trust application environment.

IT departments are under intense pressure. Thrust to the frontlines of business productivity and differentiation, they are being asked to do more, to be more. Without spending more.

Many are looking to take advantage of software-defined architecture—and the centralized control and automation it delivers—to simplify and speed up their IT operations. But it requires a fundamentally different approach and a willingness to change.

"The old way of managing each piece of hardware is no longer sustainable," says Carol Goh, senior director of global infrastructure services for Cisco IT. "Everyone needs to have a software mindset."

With more than 2000 business applications dispersed among data centers around the world, Cisco IT has adopted this mindset. It is in the process of transitioning its entire IT environment to a software-defined, zero-trust, private cloud model. All of its applications will soon be managed and secured with Cisco® Application Centric Infrastructure (Cisco ACI™), the industry's leading software-defined networking (SDN) solution.

"ACI gives us simplicity and protection via automation," says Goh. "We can orchestrate everything through policies and endpoint groups instead of managing each piece of hardware and software individually. And its zero-trust, whitelist policy model gives us much better security and compliance."

MAPPING APPLICATION DEPENDENCIES

Before applications can be moved to a software-defined architecture, their connections and dependencies must be understood. Cisco IT was using a combination of tools to identify and analyze these connections, but the historical snapshots the tools provided were problematic.

"We were essentially mapping application dependencies and endpoint groups manually," Goh explains. "It was taking too much time, and we were working with outdated information because our application and network layers are constantly changing."

Cisco IT needed a more comprehensive and current view of its application environment, so it turned to Cisco Tetration Analytics™. Providing complete visibility of everything in a data

center—every packet, every flow, every speed—Tetration simplifies operational reliability, zero-trust operations, and application migrations to SDN solutions and the cloud.

"Tetration allows us to see all of our data and traffic flows in real time," says Goh. "That type of visibility makes it much easier to map application dependencies, build out contracts and endpoint groups, and establish whitelist policies. Post-migration, it will dramatically improve systems administration, monitoring, and troubleshooting."

MASSIVE TIME AND COST SAVINGS

The combination of Tetration and ACI has been a game changer for Cisco IT. According to an IDC Business Value Brief[1], Cisco IT expects to avoid 3650 hours of IT staff time per 100 applications—a 70 percent reduction—when performing traffic analyses and establishing zero-trust operational environments.

Deploying a full application environment, which used to take eight weeks, now takes eight minutes. Compute and storage density has been improved by 300 percent. Cisco IT has saved roughly $20 million in staff time and capital cost avoidance.

"Most importantly, Tetration is enabling Cisco to migrate more applications to ACI by mapping application interdependencies in far less time and with much higher accuracy and confidence," the IDC report states. "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 data centers, even as application and tenant policies are modified."

"Tetration has streamlined our transition to a software-defined, zero-trust architecture," says Goh. "We are now managing, securing, and monitoring more than 10,000 hosts and 200 business-critical applications across three clusters."

WATCH THE VIDEO

To learn more about Cisco IT's digital transformation and use of Tetration Analytics, watch this short video.

1 *IDC Business Value Brief: Cisco Tetration Analytics: Cisco Datacenters Get Pervasive Visibility and Reduced Security Risk with 70 percent Less Time and Cost,* sponsored by Cisco, June 2016.

Cisco Tetration Analytics now provides policy enforcement

Cisco Tetration Analytics™—which gathers telemetry data from software and hardware sensors to provide complete, real-time visibility across everything in a data center—just got better.

A new software release enables automated policy enforcement, regardless of where an application resides: virtual, bare metal, or physical servers, in private or public clouds, across any vendor's infrastructure. This new enforcement model binds policies to workload characteristics and behaviors while ensuring the policy stays intact even as the workload moves.

"We've taken the discovery, visibility, and analysis capabilities of Tetration and used them to automate the enforcement of security policies," says Adam Ozkan, senior product marketing manager at Cisco. "It's the industry's first engine that can apply security policies consistently and holistically across every application in a distributed IT environment."

In addition to the original, large scale platform, Cisco now offers two new deployment models for Tetration. A smaller scale platform (Tetration-M) and cloud-based appliance (Tetration Cloud) are both suitable for deployments up to 1,000 workloads. Regardless of the deployment model, Tetration can monitor workloads in private as well as public clouds.

"Enterprises worldwide are adopting multi-cloud strategies to realize their objectives for digital transformation, but these present ongoing challenges related to visibility and security," said Brad Casemore, research director at IDC. "Cisco Tetration Analytics addresses these challenges through pervasive visibility and application segmentation, which is designed to bolster security policy enforcement across hybrid application environments."

GET THE ANALYST REPORT

To learn more about the time savings and security improvements Cisco Tetration Analytics can deliver, download the IDC Business Value Brief.