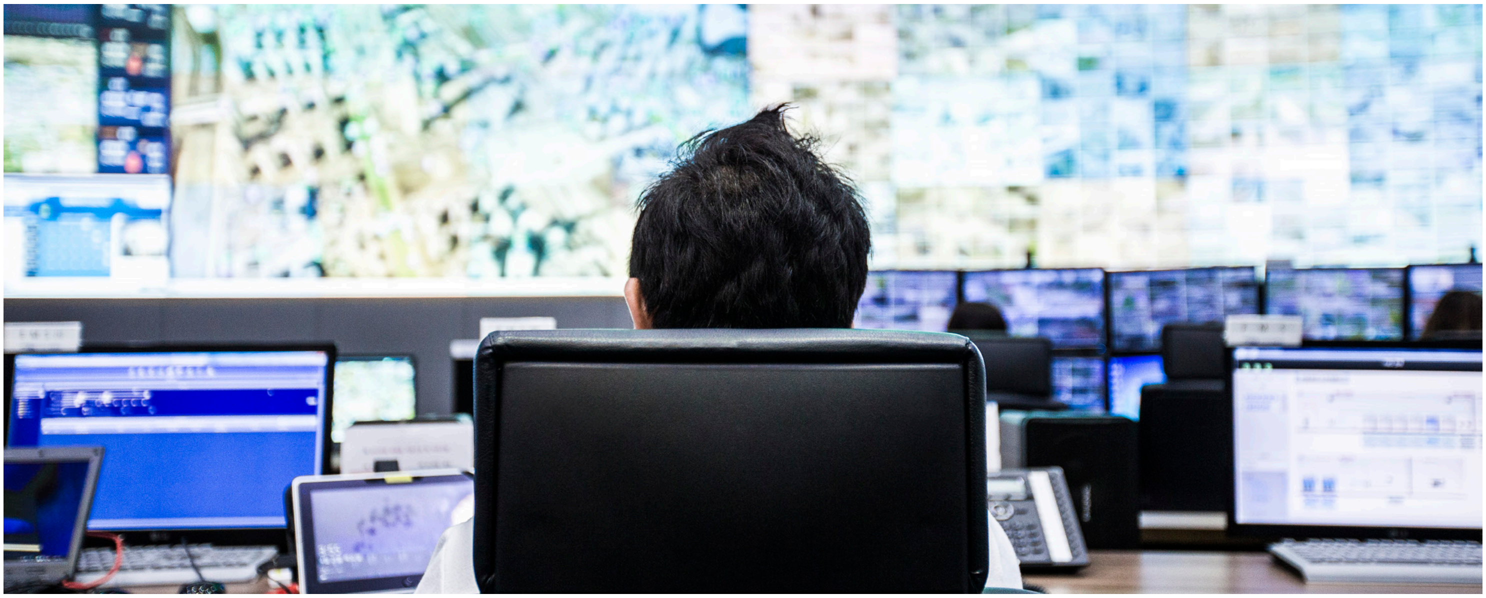
Unleashing IT NEXT-GENERATION DATA CENTER EDITION | VOLUME 5, ISSUE 4

Full visibility: All infrastructure, all applications, all data

Cisco and Intel® partnering in innovation



In mapping and recording a distributed IT environment, Cisco Tetration Analytics™ provides visibility and telemetry data across every application and infrastructure component.

“You can’t manage what you can’t see,” says Zeus Kerravala, founder and principal analyst at ZK Research. “You can’t secure it either.”

With three-quarters of application performance problems being identified by end users and not technology specialists[1], it’s safe to assume most IT teams have blind spots. And who can blame them? Modern enterprises rely on hundreds, if not thousands, of applications, which are increasingly distributed across multiple environments:

- Physical machines
- Virtual infrastructure
- Private clouds
- Public clouds

“Traditional monitoring solutions were built for monolithic, static applications, not distributed apps that are continually evolving,” says Yogesh Kaushik, senior director of product management for Cisco Tetration Analytics™. “If you can’t see where your apps are and what they are touching, how can you secure them? How can you patch everything?”

Companies use around 20 monitoring tools on average, he explains, which all provide a different and limited picture of what’s happening. If something goes wrong, it can take months to determine the source and scope of the problem.

“Many tools focus on each element individually, not how those elements are interacting with each other or how they relate to what the user is experiencing,” says Kerravala. “And many only show one slice of time or averages over time, so they miss a lot.”

VISIBILITY AND FORENSICS

What’s needed is a holistic mapping and analytics platform that provides visibility and telemetry data across every application and infrastructure component—all at once.

- Cisco Tetration Analytics with Intel® Xeon® Processors, is a new platform that provides unprecedented visibility and fine-grained forensics across everything in an IT environment, in real time.
- It creates a topology map that shows all applications, their connections, and their dependencies.

“Mapping is very important, more important than people realize,” Kerravala claims. “You need to see what is touching what, and the dependencies between applications and systems. Everyone has a story of turning a server or some other infrastructure off and having something else unexpectedly go down with it because they didn’t know the two were connected.”

One of the biggest security risks in modern IT environments is open connections between systems—many of which are unknown or forgotten. With Cisco Tetration Analytics, every connection is revealed. And all of the data flowing through those connections is recorded.

“[Cisco Tetration Analytics] captures every packet and every flow at every speed,” says Kaushik. “It’s like a DVR for your entire data center.”

- The platform provides unmatched forensic capabilities to better understand anomalies, performance dips, breaches, and other issues.
- IT specialists can easily see everything that happened before, during, and after the event.

“Investigations that used to take months can be done in minutes or hours,” Kaushik explains. “You can zoom in and see exactly what happened at any moment in time, in extremely granular detail. You can see what machine was compromised, what it talked to, and what those machines talked to. It’s like stepping into the scene of a crime as it happens instead of trying to piece it together with limited information after it has occurred.”

MACHINE LEARNING

With better visibility comes better security, anomaly detection, and forensics. But capturing every packet and flow at every speed creates its own challenges.

“Everyone loves data,” says Kerravala, “But big data requires big analytics. And that’s hard to do.”

For Cisco IT, which is already using the platform, this means processing and filtering millions of events every second—one billion packets every day. That’s why Cisco Tetration Analytics includes a robust machine learning and analytics engine that helps filter out the noise and draw attention to data worthy of investigation.

“Machines are good at processing data, and humans are good at making decisions,” says Kaushik. “Tetration processes huge volumes of data in real time and serves it up to humans in ways that make sense. Instead of searching for needles in a massive haystack, users get a focused and actionable decision tree.”

The resulting time savings are significant.

- According to an IDC Business Value Brief, Cisco IT expects to avoid 3650 hours of IT staff time per 100 applications in application dependency mapping and establishing zero-trust operations—a 70 percent reduction—by using the combination of Cisco Tetration Analytics platform and Cisco® Application Centric Infrastructure (Cisco ACI™).[2]

“Manual processes are too slow for an increasingly digital world, and companies need to rethink their entire IT strategy,” says Kerravala. “The siloed, bottom-up approach of systems management and security isn’t sustainable. You need full visibility of all elements, all applications, and all data—and you need automation and analytics to interpret and act on that data.”

With an application dependency map and DVR-like recording and playback, there’s never been a better way to manage and secure a distributed IT environment.

WATCH THE VIDEO

To see how Cisco Tetration captures every packet and every flow at line rate, watch the video at cisco.com/c/en/us/products/data-center-analytics/tetration-analytics/index.html.

[1] *Network Purchase Intention Study*, ZK Research, 2016

[2] *Cisco Tetration Analytics, Cisco Data Center Get Pervasive Visibility and Reduced Security Risk with 70 percent Less Time and Cost, Sponsored by Cisco*, IDC Business Value Brief, June 2016