Press Contact
Sonus PR
for Viavi Solutions, Inc.
pr@viavisolutions.com

Press Release | 4/10/2017

Nearly 90 Percent of Enterprise Network Teams Spend Time Troubleshooting Security Issues; 80 Percent Report More Time Spent on Security vs. Last Year

Tenth Annual "State of the Network" Global Survey from Viavi Reveals Network and Security Trends from over 1,000 Network Professionals

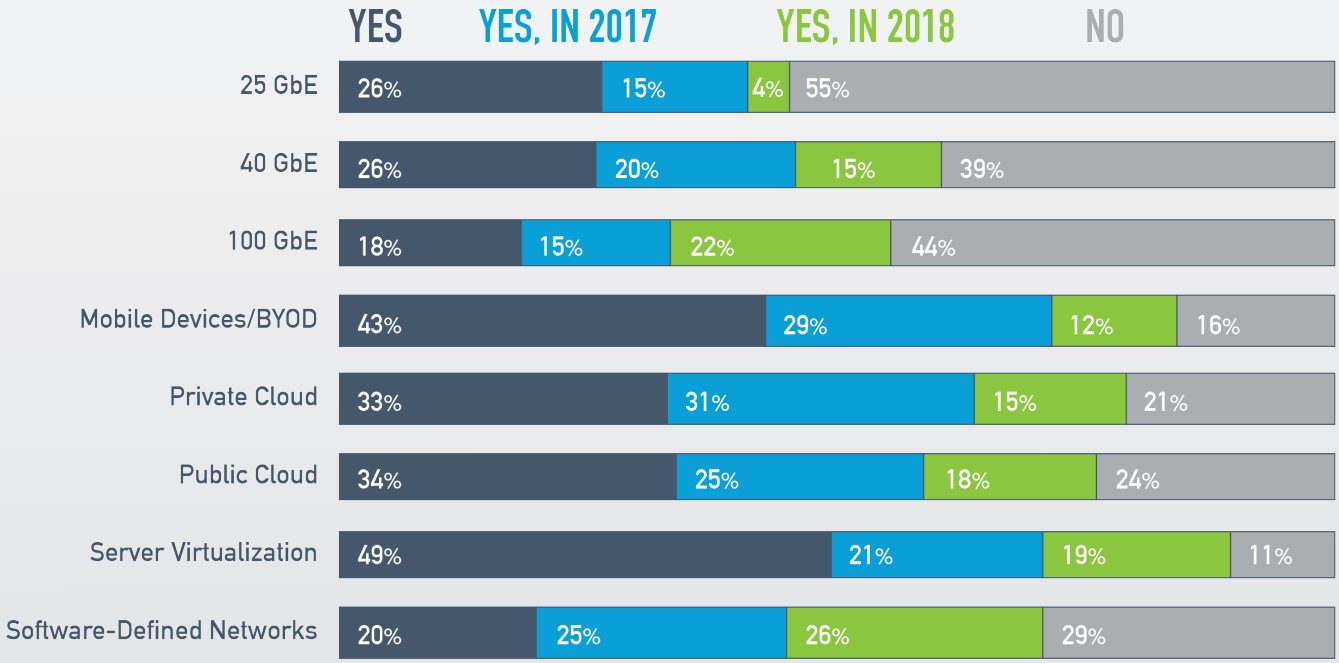
Milpitas, Calif., April 10, 2017 – Viavi Solutions (NASDAQ: VIAV) released the results of its tenth annual State of the Network global study today. This year's study focused on security threats, perhaps explaining why it garnered the highest response rate in the survey's history. Respondents included 1,035 CIOs, IT directors, and network engineers around the world. The study is now available for download.

"As our State of the Network study shows, enterprise network teams are expending more time and resources than ever before to battle security threats. Not only are they faced with a growing number of attacks, but hackers are becoming increasingly sophisticated in their methods and malware," said Douglas Roberts, Vice President and General Manager, Enterprise & Cloud Business Unit, Viavi Solutions. "Dealing with these types of advanced, persistent security threats requires planning, resourcefulness and greater visibility throughout the network to ensure that threat intelligence information is always at hand."

STATE OF THE NETWORK

Press Contact
Sonus PR
for Viavi Solutions, Inc.
pr@viavisolutions.com

EMERGING TECHNOLOGY DEPLOYMENTS



Highlights of the 2017 study include:

- **Network team members' involvement in security:** Eighty-eight percent of respondents say they are involved in troubleshooting security-related issues. Of those, nearly 80 percent report an increase in the time they spend on such issues, with nearly three out of four spending up to 10 hours a week on them.

- **Evolution of security threats:** When asked how the nature of security threats has changed in the past year, IT teams have identified a rise in email and browser-based malware attacks (63 percent), and an increase in threat sophistication (52 percent). Nearly one in three also report a surge in distributed denial of service (DDos) attacks.

Press Contact
Sonus PR
for Viavi Solutions, Inc.
pr@viavisolutions.com

- **Key sources of security insight:** Syslogs were cited by nearly a third of respondents as the primary method for detecting security issues, followed by long-term packet capture and analysis (23 percent) and performance anomalies (15 percent).

- **Overall factors driving network team workload:** Bandwidth usage in enterprises continues to surge, with two out of three respondents expecting bandwidth demand to grow by up to 50 percent in 2017. This trend is in turn driving increased adoption of emerging technologies including software-defined networks (SDN), public and private clouds and 100 Gb. Network teams are managing these major initiatives while simultaneously confronting an aggressive rise in security issues.

"A combination of new technology adoption, accelerating traffic growth and mounting security risks has spawned unprecedented challenges throughout the enterprise market," commented Shamus McGillicuddy, Senior Analyst at Enterprise Management Associates. "The need to detect and deal with security threats is notably complicated by the diverse mix of today's enterprise traffic, which spans across virtual, public and hybrid cloud environments in addition to physical servers."

Key takeaways: what should IT service delivery teams do?

- Know your "normal" – Recognizing abnormal traffic is critical for pinpointing an ongoing attack or security issue. Start comparing network traffic and behavior over points in time, either manually with freeware analyzer Wireshark, or using automated benchmarking in commercial network performance monitoring and diagnostic (NPMD) tools.

- Speed discovery with traffic evidence – According to the recent Mandiant M-Trends report, the median number of days that attackers were present on a victim's network before being discovered is still 146 days; despite the use of IDS and other traditional security tools. Using packet capture with retrospective analysis, network teams can rewind to the time of the incident(s) and track exactly what the hackers accessed.

- Ensure long-term packet retention – For high-traffic enterprise, data center, or security forensics applications, a purpose-built appliance with its own analytics may be the next step. Depending on size and volume, there are appliances that can capture and store up to a petabyte of network traffic for later analysis, simplifying forensic investigation for faster remediation.

Press Contact
Sonus PR
for Viavi Solutions, Inc.
pr@viavisolutions.com

- Facilitate effective network and security team cooperation – Ensure successful collaboration between network and security teams on investigations with documented workflows and integration between security, network forensics, and performance management tools.

State of the Network Global Study Methodology

Viavi (and previously Network Instruments) has conducted its State of the Network global study for 10 consecutive years, drawing insight about network trends and painting a picture of the challenges faced by IT teams. Questions were designed based on interviews with network professionals as well as IT analysts. Results were compiled from the insights of 1,035 respondents—nearly 40 percent more than in the 2016 study—including network engineers, IT directors and CIOs from around the world.

About Viavi Solutions

Viavi (NASDAQ: VIAV) is a global provider of network test, monitoring and assurance solutions to communications service providers, enterprises and their ecosystems, supported by a worldwide channel community including Viavi Velocity Solution Partners. We deliver end-to-end visibility across physical, virtual and hybrid networks, enabling customers to optimize connectivity, quality of experience and profitability. Viavi is also a leader in high performance thin film optical coatings, providing light management solutions to anti-counterfeiting, consumer electronics, automotive, defense and instrumentation markets. Learn more about Viavi at www.viavisolutions.com. Follow us on Viavi Perspectives, LinkedIn, Twitter, YouTube and Facebook.