Press Contact
Steve Brown
JDSU
952.358.3820
Steve.Brown@jdsu.com

Press Release | 3/30/2015

Eighth Annual "State of the Network" Global Study from JDSU's Network Instruments Finds 85 Percent of Enterprise Network Teams Now Involved in Security Investigations

Deployment Rates for High-Performance Network Visibility and Software Defined Solutions Expected to Double in Two Years

Milpitas, Calif., March 30, 2015 – Network Instruments, a JDSU Performance Management Solution (NASDAQ: JDSU), released the results of its eighth annual State of the Network global study today. Based on insight gathered from 322 network engineers, IT directors and CIOs around the world, 85 percent of enterprise network teams are involved with security investigations, indicating a major shift in the role of those teams within enterprises.

Large-scale and high-profile security breaches have become more common as company data establishes itself as a valuable commodity on the black market. As such, enterprises are now dedicating more IT resources than ever before to protect data integrity. The Network Instruments study illustrates how growing security threats are affecting internal resources, identifies underutilized resources that could help improve security, and highlights emerging challenges that could rival security for IT's attention.

As threats continue to escalate, one quarter of network operations professionals now spend more than 10 hours per week on security issues and are becoming increasingly accountable for securing data. This reflects an average uptick of 25 percent since 2013. Additionally, network teams' security activities are diversifying. Teams are increasingly implementing preventative measures (65 percent), investigating attacks (58 percent) and validating security tool configurations (50 percent). When dealing with threats, half of respondents indicated that correlating security issues with network performance is their top challenge.

"Security is becoming so much more than just a tech issue. Regular media coverage of high-profile attacks and the growing number of malware threats that can plague enterprises – and their business – has thrust network teams capable of dealing with them into the spotlight. Network engineers are being pulled into every aspect of security, from flagging anomalies to leading investigations and

implementing preventative measures," said Brad Reinboldt, senior product manager for Network Instruments. "Staying on top of emerging threats requires these teams to leverage the tools they already have in innovative ways, such as applying deep packet inspection and analysis from performance monitoring solutions for advanced security forensics."

The full results of the survey, available for download, also show that emerging network technologies have gained greater adoption over the past year. Highlights include:

Highlights include:

- **40, 100 Gigabit Ethernet and SDN approaching mainstream:** Year-over-year implementation rates for 40 Gb, 100 Gb and SDN in the enterprise have nearly doubled, according to the companies surveyed. This growth rate is projected to continue over the next two years as these technologies approach more than 50 percent adoption. Conversely, survey respondents were less interested in 25 Gb technology, with over 62 percent indicating no plans to invest in equipment using the newer Ethernet specification.

- **Enterprise Unified Communications remains strong but lacks performance-visibility features:** The survey shows that Voice-over-IP, videoconferencing and instant messaging technologies, which enable deeper collaboration and rich multimedia experiences, continue making strides in the enterprise, with over 50 percent penetration. Additionally, as more applications are virtualized and migrated to the cloud, this introduces new visibility challenges and sources that can impact performance and delay. To that end, respondents noted a lack of visibility into the end-user experience as a chief challenge. Without visibility into what is causing issues, tech teams can't ensure uptime and return-on-investment.

- **Bandwidth use expected to grow 51 percent by 2016:** Projected bandwidth growth is a clear factor driving the rollout of larger network pipes. This year's study found the majority of network teams are predicting a much larger surge in bandwidth growth than last year, when bandwidth was only expected to grow by 37 percent. Key drivers for future bandwidth growth are being fueled by multiple devices accessing network resources and larger and more complex data such as 4K video. Real-time unified communications applications are also expected to put more strain on networks, while unified computing, private cloud and virtualization initiatives have the potential to create application overload on the backend.

Key takeaways: what can network teams do?

- Enterprises need to be on constant alert and agile in aligning IT teams and resources to handle evolving threats. To be more effective in taking on additional security responsibilities, network teams should be trained to think like a hacker and recognize increasingly complex and nefarious network threats.
- They also need to incorporate performance monitoring and packet analysis tools already used by network teams for security anomaly detection, breach investigations, and assisting with remediation.
- Security threats aren't the only thing dictating the need for advanced network visibility tools that can correlate network performance with security and application usage. High-bandwidth activities including 4K video, private clouds and unified communications are gaining traction in the enterprise as well.

State of the Network Global Study Methodology

Network Instruments has conducted its State of the Network global study for eight consecutive years, drawing insight about network trends and painting a picture of what challenges IT teams face. Questions were designed based on interviews with network professionals as well as IT analysts. Results were compiled from the insights of 322 respondents, including network engineers, IT directors, and CIOs from around the world. In addition to geographic diversity, the study's sample was evenly distributed among networks and business verticals of different sizes. Responses were collected from December 16, 2014 to December 27, 2014 via online surveys.