NETWORK INSTRUMENTS

Eighth Annual State of the Network Global Study

EXECUTIVE SUMMARY

Network data is valuable and it is under attack. Large-scale security breaches are becoming almost commonplace, and network teams are increasingly accountable.

The 2015 State of the Network Study recently uncovered how IT resources are shifting in the battle to protect the integrity of network data. One such change is the way in which security teams turn to network teams for assistance in many aspects of security, from flagging anomalies, to leading investigations, and taking preventative measures.

In fact, out of the 322 respondents, nearly a quarter spent 10-20 hours per week working exclusively on security issues. These duties are in addition to managing network upgrades (in the past year migrations to 40 and 100 Gb have doubled), SDN, cloud, and big data initiatives.

KEY TECHNOLOGY STATISTICS

EMERGING TECHNOLOGIES

- Deployment rates for 40 Gb, 100 Gb, and SDN have doubled since last year; technologies will be mainstream by 2016

SECURITY

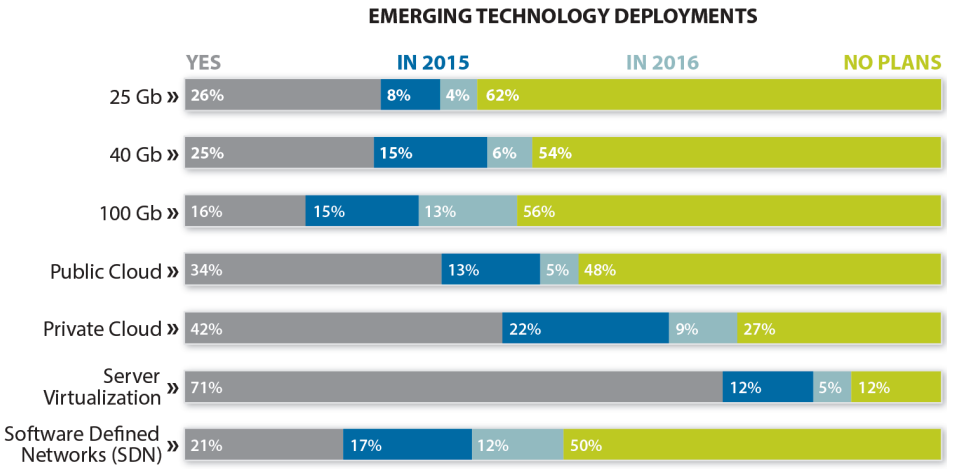
- 85 percent of network teams are involved with security investigations; nearly a quarter of network operations teams spend 10-20 hours per week on security issues
- Network teams are engaged in multiple facets of security from implementing preventative measures (65 percent) to investigating attacks (58 percent) and validating security tool configurations (50 percent)
- Half indicated correlating security issues with network performance to be their top challenge; 44 percent cited the inability to replay anomalous security issues

APPLICATION AND NETWORK PERFORMANCE MONITORING

- By 2016 more than half of respondents expect their organization's bandwidth consumption to surge by more than 50 percent
- 75 percent cited isolating issues to the network, system or application as their top application troubleshooting challenge; the biggest challenge by far for the past eight years

EMERGING TECHNOLOGIES

Unlike the adoption of emerging technologies covered by past studies which had been gradual, the year-over-year implementation rates for 40 Gb, 100 Gb, and SDN nearly doubled since last year. This growth rate is projected to continue over the next two years as these technologies approach mainstream adoption of nearly 50 percent.



RAPID ADOPTION OF NEW TECHNOLOGY

The rapid adoption is likely being driven by a combination of factors including the need to support:

- Increased flexibility and scalability in virtualized datacenter environments
- Growing use of bandwidth-intense, real-time applications

HANDLING NETWORK SECURITY

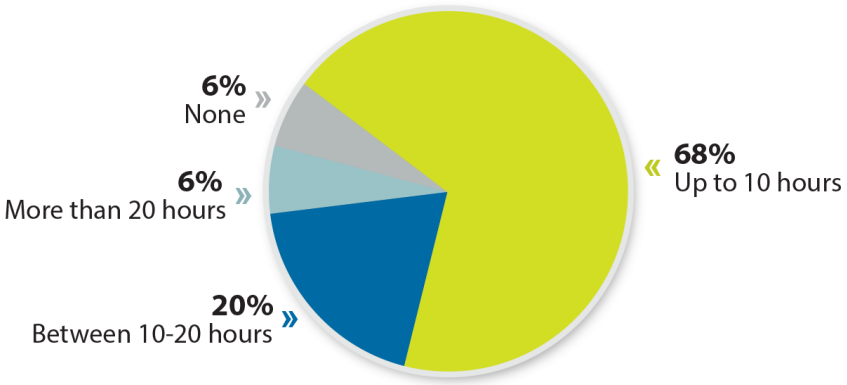
According to the Ponemon Institute, 43 percent of companies were victims of attacks in 2014. Given the regular media coverage of high-profile breaches, it is not surprising that security teams seek additional resources to augment defenses and investigate attacks.

The study found that 85 percent of respondents indicated that their organization's network team was involved in handling security.

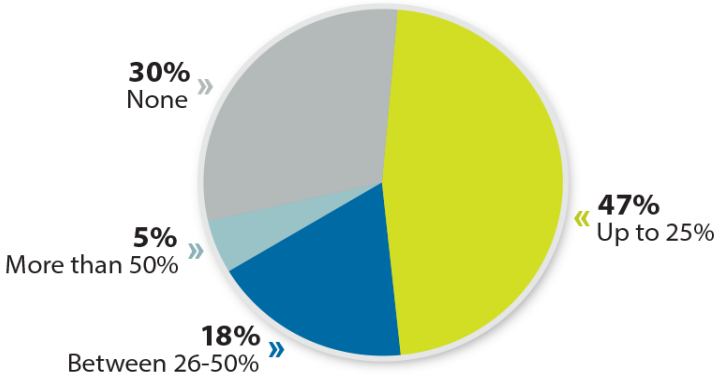
Not only have network teams spent considerable time managing security issues but the amount of time has also increased over the past year:

- One in four spends more than 10 hours per week on security
- Almost 70 percent indicated time spent on security has increased; one-quarter said time spent increased by more than 25 percent

TIME SPENT ON SECURITY



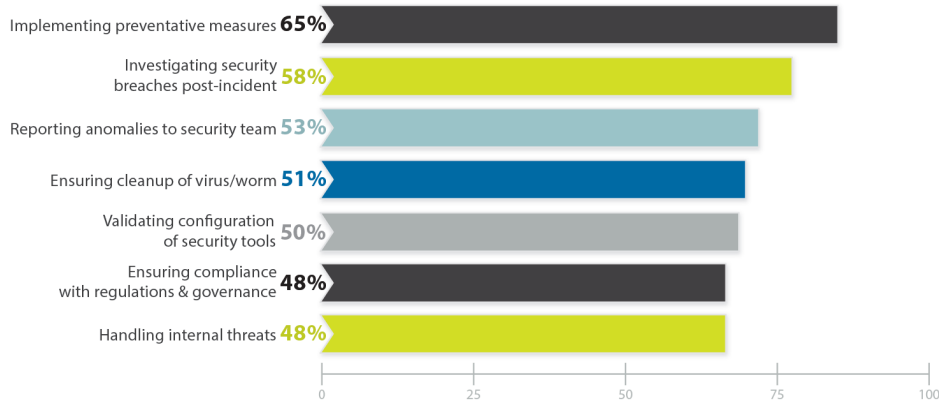
HAS THIS TIME INCREASED OVER THE PAST 12 MONTHS?



NETWORK TEAMS TO THE RESCUE

With the increased profile and budgets for security, many network engineers are pulled into investigations and new IT projects to reevaluate security strategies and spending.

NETWORK TEAM ROLES IN SECURITY



From the number of responses above 50 percent, the majority of respondents are involved with many security-related tasks. Additionally, the top two roles for respondents – implementing preventative measures (65 percent) and investigating security breaches (58 percent) – mean network teams are working closely with security teams on handling threats both proactively and after-the-fact.

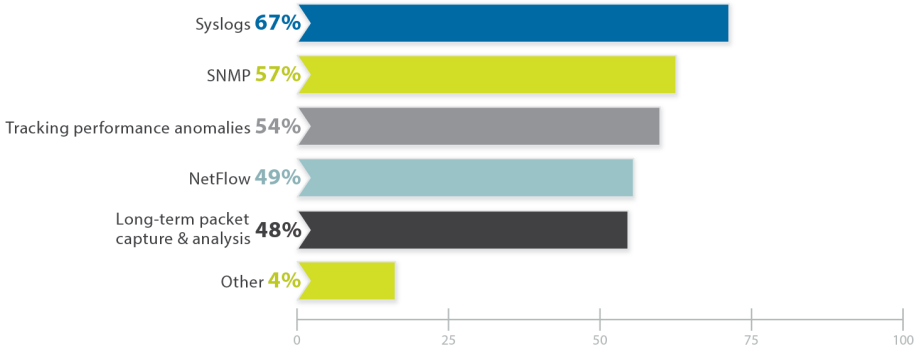
KEY INSIGHT

Network teams are called upon to help with many facets of network security because:

- The network team has visibility into all the traffic, understands what's normal behavior, and can make quick policy changes like blocking specific IP addresses
- Both teams often look at the same anomaly to determine if it's a security or network issue

Syslogs were cited by over two-thirds of respondents as the primary method for detecting security issues, followed by SNMP (57 percent) and performance anomalies (54 percent).

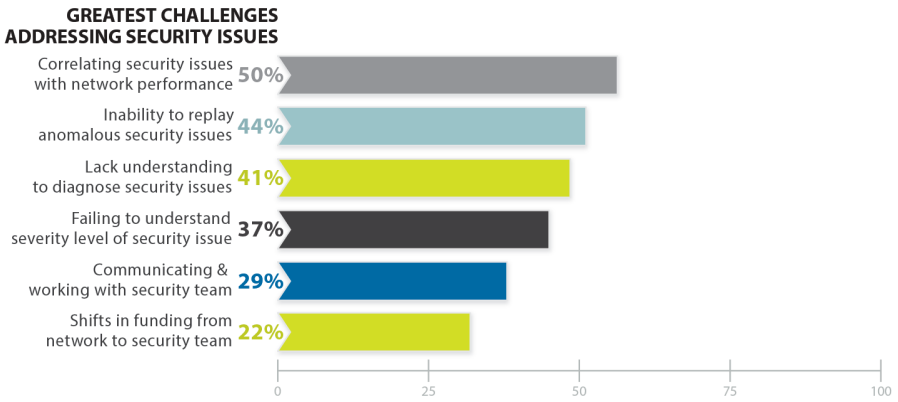
METHODS FOR IDENTIFYING SECURITY ISSUES



TOOLS TO ADDRESS THE CHALLENGE

Security appliances frequently use syslogs such as firewall logs. However, the study also indicated a high reliance on SNMP, possibly for its use in penetration testing to identify SNMP vulnerabilities and to leverage related exploits. Additionally, SNMP can be used to alert engineers to anomalous device and utilization behaviors as well as to identify rogue devices.

Half of respondents indicated the greatest security challenge was an inability to correlate security and network performance. This was followed closely by an inability to replay anomalous security issues (44 percent).



THE PACKET CAPTURE SOLUTION

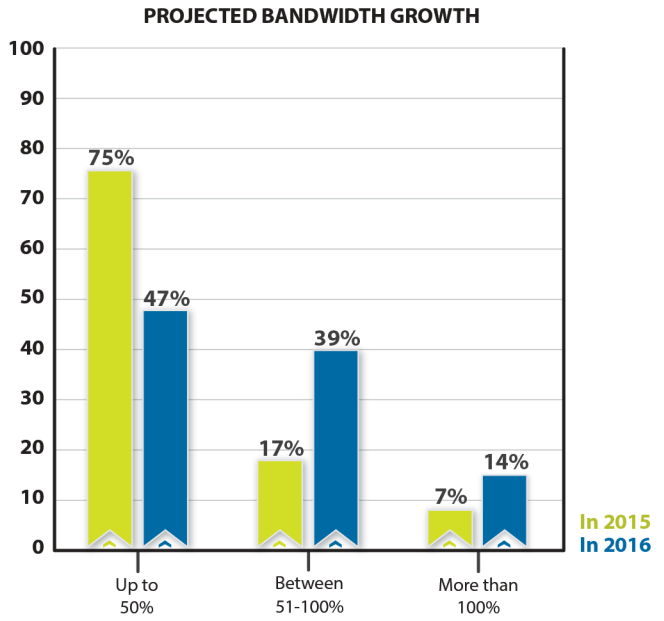
Both of these challenges point to the inability of the network team to gain context to quickly and properly diagnose security issues. The first is the inability of the performance management solutions to integrate with security tools.

The second points to long-term packet capture being an under-utilized resource in security investigations. Replaying the events would provide greater context for investigations.

APPLICATION AND NETWORK PERFORMANCE MONITORING

The State of the Network Study for the past eight years has consistently focused on two of the primary challenges for network teams: anticipating bandwidth demand and ensuring successful application delivery.

Projected bandwidth growth is a clear factor driving the rollout of larger network pipes. The most significant takeaway from the above chart is that over half of engineers expect bandwidth demand for their organizations to grow by more than 51 percent in 2016. This number also represents an expected surge in bandwidth growth compared to last year, when only 37 percent expected bandwidth demand for their organization to grow by more than 51 percent in the second year.

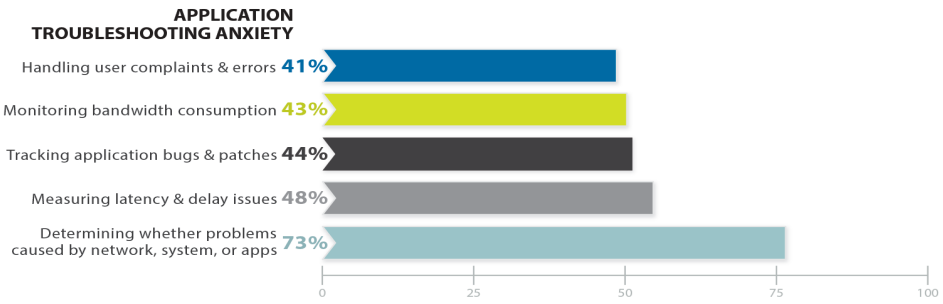


APPLICATION OVERLOAD

There is a perfect storm that's driving this unabated growth of bandwidth demand:

- Users with multiple devices to access network resources and larger files
- Real-time unified communications applications require significant pipes
- Unified computing, private cloud, and virtualization initiatives

For every year of the State of the Network, the top application troubleshooting challenge has been isolating the problem to the network, system, or application. Compared to last year, the challenge remains consistent. Noteworthy is an increase in the number of respondents having difficulties measuring latency and delay this year (48 percent) compared to last year (31 percent).



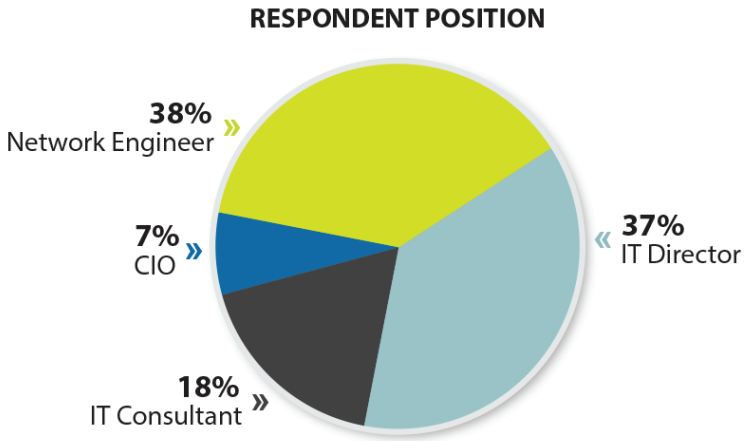
ENSURING VISIBILITY

As more applications are virtualized and migrated to the cloud, this introduces new visibility challenges and sources that can impact performance and delay. These challenges are expected to remain constant into the future as both engineers and tools adapt to provide greater support for these new environments.

RESEARCH AND METHODOLOGY

Study questions were designed based upon interviews with network professionals and 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 population 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.



For more information about the study's methodology or the results, contact Stephen Brown at sbrown@networkinstruments.com.

NETWORK INSTRUMENTS®
JDSU Performance Management

SOTN-150320-V17