Research Spotlight

Cloud Computing and Network Security Operations Transformation

Date: March 2016 **Author:** Jon Oltsik, Senior Principal Analyst

Research Overview

In early 2016, Tufin commissioned the Enterprise Strategy Group (ESG) to complete a research survey of 150 IT and cybersecurity professionals with knowledge of or responsibility for network security policies, processes, technologies, and operations at their organizations. Survey respondents were located in North America and came from enterprise organizations (i.e., those with over 1,000 employees). Respondents represented numerous industry and government segments with the largest participation coming from manufacturing (20%), the financial services industry (17%), retail/wholesale (15%), and business services (13%). Note that this project follows a similar research study that was completed in 2015.

Based upon the data collected for this research project, ESG concludes:

- Enterprise organizations are embracing cloud computing and software-defined networking (SDN) technologies, altering their network security operations.
- Network security operations continue to grow more difficult each year.
- Private/public cloud infrastructure presents numerous automation, monitoring, and security challenges.
- Network security operations automation is a critical success factor but enterprise organizations admit that there is a lot of work ahead in this area.
- While network security operations automation was considered critical or very important two years in row, enterprises haven't made much progress on this initiative yet.

Enterprise Organizations are Embracing Cloud Computing and SDN

The ESG research indicates rapid adoption of cloud and SDN technologies at enterprise organizations. For example:

- Sixty-nine percent of organizations employ a private cloud in IT production while another 15% are conducting a proof-of-concept project around private cloud infrastructure.

- Nearly half (49%) of enterprise organizations have implemented SDN and are committed to SDN as part of their long term strategy. Another 29% are committed to SDN and are currently engaged in a proof-of-concept project. Of those organizations using SDN, 51% are committed to more than one SDN technology.
- Sixty-five percent of enterprise organizations claim they are using IaaS and PaaS significantly, while another 26% use IaaS and PaaS to some extent but not significantly. Interestingly, 61% of organizations use more than one cloud service, aggravating network security operations challenges.
- Nearly one-third (31%) of organizations claim that supporting cloud computing initiatives is a primary driver for their network security operations strategy.

Cloud and SDN adoption represent a significant change to network security operations. Security personnel must learn new technologies, understand their security capabilities, monitor threats and vulnerabilities, and modify existing security policies and controls to accommodate a variety of virtual technologies. This can be a daunting set of tasks.

Network Security Operations Grow Increasingly Difficult

Aside from the transition to cloud computing and SDN, day-to-day network security operations grow more problematic. For example:

- Sixty-three percent of survey respondents claim that network security operations has become more difficult over the past 2 years.
- What's making network security operations more difficult? More than half (55%) of survey respondents who believe that network security operations have become more difficult over the past 2 years point to an increase in the number of devices on the network, 52% say that network security operations encompasses more types of networking and security technologies than it used to, 50% claim that they have more applications today than in the past, and 48% blame an increase in network traffic.
- A vast majority (76%) agree that implementing and/or modifying network security controls requires a lot of manual processes.

In aggregate, organizations are making massive changes to their IT infrastructure but continue to depend upon manual processes for network security operations. This mismatch overwhelms network and security operations teams and forces them into a constant game of catch up. Regrettably, they are falling farther and farther behind in many cases.

Cloud Computing and Network Security Operations Challenges

The ESG research clearly indicates that cloud computing is only exacerbating network security operations challenges:

- Sixty-nine percent of respondents agree that their organizations are still learning how to apply security policies to public/private cloud infrastructure. Additionally, 52% agree that the security team does not have the appropriate staff level to manage network security operations for cloud infrastructure while 49% claim that their organization does not have the right level of cloud computing skills to provide the right security controls and oversight for cloud computing security.
- When asked to identify cloud security policy enforcement challenges, 30% of respondents say that their organizations use several different public/private cloud offerings, making network security operations especially challenging; 23% claim that their traditional physical security controls don't align well with cloud computing; and 23% indicate that their network security operations tools weren't designed for cloud computing. This problem is certainly intensified because many organizations are using multiple SDN technologies and cloud services.

Enterprise organizations find themselves in a paradoxical situation. Many are rapidly embracing cloud computing for business enablement and IT agility but the ESG data clearly indicates that infosec teams aren't adequately prepared for the cloud onslaught. To catch up, enterprise organizations need to add headcount, provide cloud computing training to cybersecurity personnel, and adopt security processes and controls designed to accommodate cloud computing.

Network Security Operations Automation

Cloud computing is often supported with things like Agile software development and DevOps efforts to automate, orchestrate, and accelerate application development and deployment. With regard to network security operations automation, ESG research reveals:

- When asked how important it was for their organizations to automate their network security operations in the future, 31% said it was critical, while 58% claimed it is very important to do so.
- Why the emphasis on network security operations automation? Eighty-six percent of respondents believe that network security automation can help the security operations team do more with existing resources, 85% agree that network security automation can help them enforce a unified security policy baseline across physical and cloud environments, and 84% believe that automation can help them avoid human errors.
- When asked to compare an ideal model for network security operations automation with their organization's existing processes and controls, 61% of respondents said that their organization's existing network security operations processes, monitoring capabilities, and security controls weren't close to an ideal situation of comprehensive network security operations automation.

The good news is that security professionals know that network security operations automation is essential for supporting cloud security. Unfortunately, the bad news is that there is a lot of work ahead.

The Bigger Truth

Based upon the data collected for this project, ESG concludes that enterprise organizations may be at a crossroads with cloud computing. Business and IT leaders are moving ahead with cloud computing initiatives to achieve business benefits but CISOs and cybersecurity teams lack the right skills, processes, tools, and oversight to accommodate these changes. This will only increase IT risk.

What come be done to bridge this gap? ESG believes that CISOs must:

- Invest in cloud computing training for the IT and cybersecurity staff.
- Supplement existing security infrastructure with monitoring tools and security controls designed for cloud computing.
- Build central command-and-control capabilities for security monitoring and operations for all workloads regardless of whether they run on physical infrastructure, virtual infrastructure, or public/private cloud platforms.
- Invest in tools and processes for network security operations automation to align with Agile development and DevOps processes used for cloud computing.