Automation, Governance and Security in a Software-Defined World

For more than 15 years, virtualization platforms have revolutionized computing by completely decoupling processing power from hardware resources. This has led to cost savings, improved resource utilization, increased business agility and enabled cloud computing. The hypervisor has become the *de facto* standard for operational efficiency and agility in the modern data center.

Technological advancements and the adoption of virtualized servers and storage increased the need for network virtualization—and, in fact, this is already being consolidated in software-defined network (SDN) environments. Today, it is possible to reproduce the functions of switches, routers, firewalls and load balancers via software, in the same way the servers were virtualized.

As the challenge of the network infrastructure virtualization is being solved, software-defined data centers (SDDCs) are having a tremendous impact on IT and security operations in enterprises. The same operational efficiency of physical server virtualization is expected to be achieved on the network and with the same benefits: business agility, cost savings, configuration flexibility, automated provisioning and resource optimization capabilities.

This scenario has forced technical staff to transpose a barrier that has existed for years: full automation in network security operations. It is very clear that IT was at least 10 years ahead of security regarding process automation. This turnaround is more noticeable in the areas of governance through automatic means of assigning responsibilities to the correct stakeholders (IT or business) such as requests, approvals, risk analysis and risk acceptance.

Network security tools such as firewalls, access control systems and other security life-cycle-management tools must rely on third-party systems to have governance incorporated into the whole process. Often there is no real integration, just spreadsheets manually imported, undocumented scripts or email threads. This may not have such a big impact on physical data centers, with physical security appliances, but when everything, including security, is provisioned by software, governance must be built in on the security tools (or on the orchestration platforms).

Another big challenge is that transformations in the technological environment require changes in the vision of the managers and the operation teams, who must be much more familiar with the business processes supported by the underlying infrastructure. There are too many moving parts on the network and at the virtualized data center or SDDC, and they are becoming much more movable—network security teams simply cannot keep up with updating permissions. The IT and security market is clearly waiting for solutions that can abstract out the network infrastructure layer, representing it in terms of business services—in other words, creating an abstraction layer or giving

Julio Pontes, CISM, BS7799 LA, CCSK, CISSP
Is a professional with more than 20 years of experience in information security solutions design and implementation, managing and promoting information security practices in areas such as network infrastructure, security operations centers, public key infrastructure and information security governance.

context to the underlying network infrastructure. There is a pent-up demand for such solutions, and some vendors are already paying attention to that. The traditional network security management model is on the verge of exhaustion, and any network security operations team these days is familiar with one or more of the following:

- Even with new protection technologies, breaches still occur
- Poor automation of the network security infrastructure management
- Multiple solutions, multiple consoles, increased network complexity
- Increased integration needed between governance and network security automation
- Increased demand for agility caused by a software-defined world
- Network security's inability to keep pace with business

The definition of "governance" in academic books is sometimes very complex and is skipped by most technology professionals. One of the reasons for poor network security automation in the past was that its implementation did not consider governance accordingly. But, in fact, the fault could be the result of the days when procuring a server, a network appliance or installing software were the real bottlenecks.

Governance, put in simple terms, is the clear definition of the roles and responsibilities of the manager vs. the owner (whether of an organization, a process or business data) and, of course, the rules governing this relationship.

Automation and governance should walk together as twins. Once a process is automated, responsibilities and actions (rules) of each participant must be defined, recorded and tracked for continuous improvement. Put in this way, audit is only a consequence (or side effect) of this process. Therefore, professionals and the market, in general, can no longer prioritize the automated (software-defined) side of the coin and relegate governance to a secondary role.

The latest security incidents indicate that the root cause of many significant breaches is related to misconfiguration, which is a clear indication that in this software-defined world, automation and governance, at least in practice, are not running at the same pace.

Processes such as firewall rules revision, access credentials revision, network change impact analysis and security assessment of third-party connections are often performed manually or, even when automated, lack a seamless integration with governance processes—at least, in network security.

> "ENTERPRISES SHOULD LOOK FOR AUTOMATED GOVERNANCE SOLUTIONS CAPABLE OF INTEGRATING WITH AS MANY SECURITY SOLUTIONS AS POSSIBLE, GETTING RID OF MANUAL RECONCILIATION PROCESSES."

This may not appear relevant now, where part of the deployment and management of new business services and its underlying IT infrastructure is still manual. Until a few years ago, it was relatively easy to reconcile "out-of-band actions" (such as planning, risk assessments, approvals, documentation) running on different systems with the real actions taken at the entities where the policies are enforced (e.g., firewalls, routers and other security devices). But if the discussion about the importance of automation and governance walking together in software-defined environments is not brought to the forefront (maybe a new acronym is needed: governance defined by software [GDS]), all of the challenges the network security teams are facing right now may continue to grow on an exponential scale in an interconnected, software-defined and often application programming interface (API)-controlled environment. Enterprises should look for automated governance solutions capable of integrating with as many security solutions as possible, getting rid of manual reconciliation processes. This could be a challenge right now because the industry is somewhere in the middle of a transition from 100 percent physical to fully software-defined data centers, so whatever solution is chosen must support integration (preferably through API) with orchestration systems and physical and virtual security enforcement points.