The network must be the security device

By Paolo Campoli

28 Oct 2015

The true power of the computer comes from being connected, and with more devices connected, its power grows exponentially. We see this today with cloud computing and increasing with the Internet of Everything (IoE), creating unprecedented opportunities for service providers through the interconnection of people, processes, data, and things.

Paolo Campoli

Largely because of this exciting evolution, we are now facing a similar inflection point with respect to security. To capture opportunities made possible by ever-expanding connectivity, security must evolve in lock-step. In effect: "The network must become the security device" and likewise, the deployment of network services through virtualised technologies requires security considerations.

So how have we evolved our approach to security as defenders? The truth is, not nearly enough. Caught in a cycle of layering on the latest security tool, it isn't unusual to find organisations with 40 to 60+ different security solutions that don't - and can't - work together or interoperate. Attackers are taking advantage of gaps in visibility and protection that this complexity and fragmentation creates to penetrate the network. Environmentally aware, attackers navigate through the extended network, evading detection and moving laterally until reaching the target. Once they accomplish their mission they remove evidence but maintain a beachhead for future attacks.

To truly address today's dynamic threat landscape, evolving business models, and considerable complexity, security must be embedded into the heart of the intelligent network infrastructure and across the extended network - from the data center out to the mobile endpoint and even onto the factory floor.

When the network is the security device, our approach to security can be:

• Pervasive - to persist across all attack vectors
• Integrated - to share information and capabilities with a rich ecosystem of applications and services
• Continuous - to allow for ongoing protection across the full attack continuum - before, during, and after an attack
• Open - to integrate with third parties, including complementary security technologies and threat intelligence feeds

This requires that we build technologies into network infrastructure that increase visibility across all network activity, provide context based on local and global threat intelligence, and allow control using analysis and automation to dynamically protect against detected threats. We must design infrastructure that is open so that new capabilities and intelligence to address complex and evolving threats can be easily incorporated. And we must embed security without impeding business-critical resources and processes.

Modern infrastructure

Cisco's NFV (Network Functions Virtualisation) architecture has inbuilt security capabilities, which assist African Service Providers to transform their networks to prepare for the digitisation in the IoT/IoE era. SDN also enhances the benefits of data center virtualisation, increasing resource flexibility and utilisation and reduces infrastructure costs and overhead and enables network programmability and code development to bring applications and networks closer. The result is a modern infrastructure that can securely deliver new applications and services in minutes, rather than days or weeks required in the past delivering with a platform capable of handling the most demanding networking needs of today and tomorrow.

©scanrail via 123RF

Advancing security

These capabilities were recently demonstrated globally by Light Reading, an independent media organisation, who requested that EANTC (an internationally recognised test center) conduct a series of validation and verification exercises on a number of Cisco SDN (software-defined networking) and virtualisation platforms. Findings from the EANTC report, which were recently announced at the SDN World Congress, showed the reliability of Cisco's secure NFV architecture.

Cisco is sponsoring the SDN Theatre at AfricaCom 2015 because in Africa, we're already seeing strong demand for secure SDN from industries with complex networks that need to quickly process large amounts of data and this includes service providers in particular. As connectivity continues to expand, security must advance right along with it. By embedding security everywhere across the extended network, not only does security become more effective against advanced attacks, it also becomes a business enabler. Only then can businesses take full and secure advantage of opportunities presented by new digital business models and the IoE.

ABOUT THE AUTHOR

Paolo Campoli, head of Middle East and Africa Global SP Sales and SP CTO for the EMEA Sales Region at Cisco