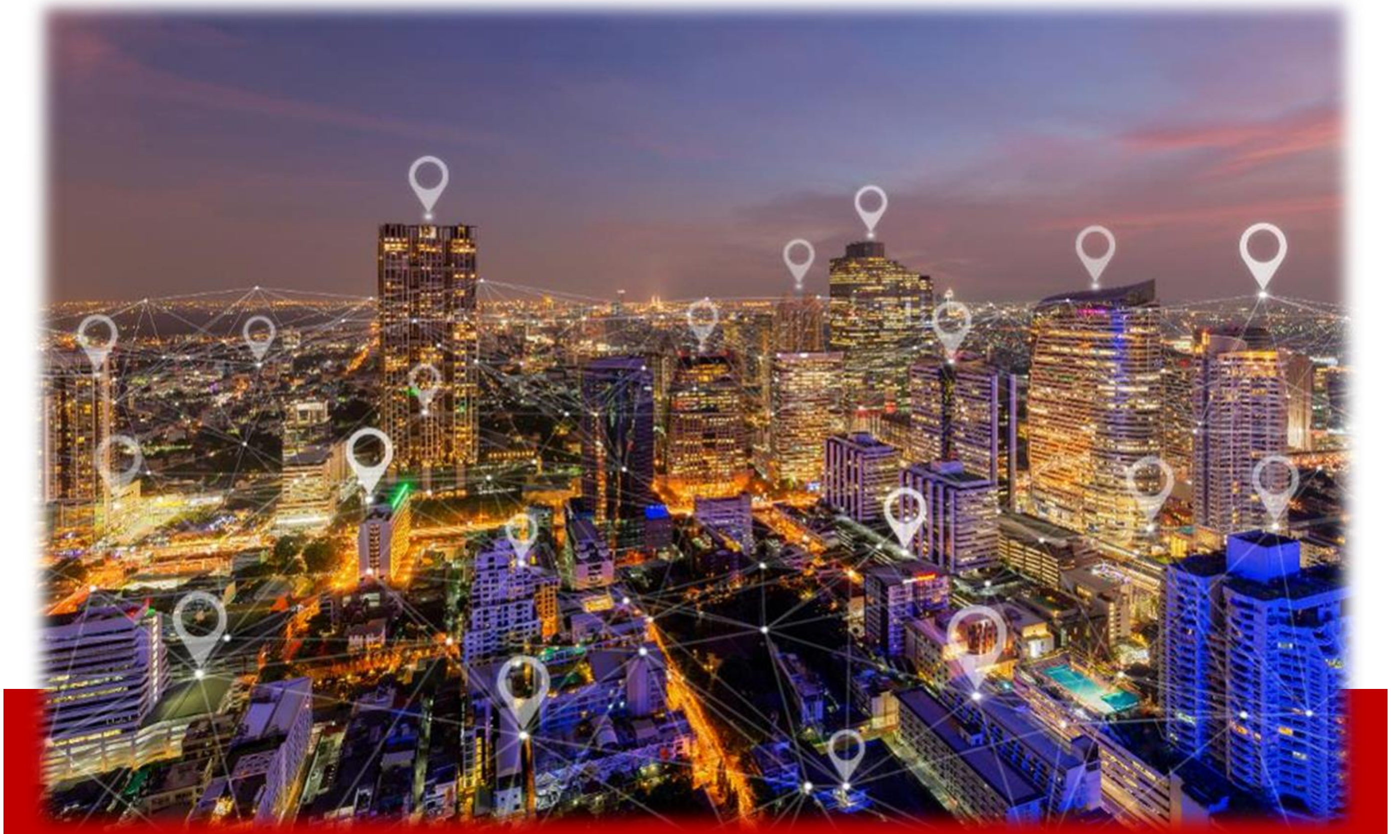

New Expectations for the Network Perimeter

Patchwork network of legacy solutions won't keep bad actors out

By Barrett Lyon, Co-founder and CEO, Netography

U.S. government agencies are placing increased importance on cross-network visibility for cloud and on-prem environments and, with that, the significance of having shared visibility and traffic analysis across networks for real-time detection and remediation is moving to the forefront.

Help or hindrance?

No one can accuse the government of rushing into anything, and security is no exception. In recent years, however, there has been a noticeable acceleration of security initiatives as the import of a robust cyber defense plays out on a global stage. Dating back to the establishment of the American Technology Council in 2017 to the creation the following year of the Cybersecurity and Infrastructure Security Agency (CISA), government entities have been moving at relative warp speed (note, I said relative) to safeguard those assets that are deemed essential by the Federal government.

Over the course of this journey, the one thing that has become apparent is that a patchwork network of legacy solutions isn't up to the task of keeping the bad actors out. What passed for high tech 15 years ago is now acting as a hindrance rather than a help. Reliance on legacy systems comes with a list of disadvantages as long as your arm – everything from unpatched vulnerabilities and point products no longer suited to today's environment to cost inefficiencies and a lack of personnel trained to use the products. These impediments translate into security vulnerabilities that turn government agencies into sitting ducks from a cybersecurity standpoint. Moreover, legacy solutions are incapable of protecting dynamically and are limited in the kinds of attacks they can detect and stop.

Unfortunately, the government has lagged behind in adopting new and innovative technologies due, in part, to a lengthy approval process before a vendor can be sanctioned to work with the Federal government. Luckily, that's starting to change. The Department of Defense (DoD) has come to recognize the importance of utilizing pioneering technologies from private-sector companies, as have various branches of the military. To that end, a grant program through AFWERX and the Small Business Innovation Research has been developed to foster innovation and speed the vetting process, in effect giving grant recipients the green light to partner with entities from within the DoD.

Novel times, novel measures

Today's novel Work from Home (WFH) situation calls for novel security solutions. Thanks to a massive exodus of workers from the walls of their office buildings to the walls of their homes, the network perimeter has all but vanished. Remote workers, the use of unsanctioned equipment (that's also likely to be running an outdated security solution, assuming it has one at all), data scattered across different locations, and a variety of cloud services mean but one thing: Shared, cross-network visibility is a must.

Lacking shared visibility and traffic analysis across your network means you are foregoing the chance for real-time detection and remediation. And while some cloud solutions may bill themselves as offering "real-time" analytics, if you want to detect and remediate as events happen rather than hours or days, out-of-the box solutions aren't going to cut it.

Like enterprises, government entities need real-time protection against millions of network-based threats across their entire infrastructure, whether it's on-premises, in the cloud, or a hybrid environment. Today's WFH challenges mean an unprecedented number of end-users in remote locations. This makes it even more critical that network systems utilizing Virtual Private Networks (VPNs) — which by all accounts come with their own set of security issues — are monitored for any anomalies or known threats that might be present on the network as a result of using the VPN.

To be truly effective, a system needs to offer network and security teams shared visibility into their security posture at any — and every — point in time. As government agencies begin to take advantage of enterprise solutions, they need to ensure that they aren't simply patching a one legacy solution with yet another only to cause more problems down the road. Solutions should break down the silos rather than establish new ones.

Because of the highly sensitive nature of government data, it's especially important that a security solution also offers high-performance processing power. This allows complex algorithms to run in real-time, and means automatic remediation translates into a significant reduction in mean-time-to-repair. Another feature to look for is single-pane view of traffic flow, whereby agencies get full network visibility of cloud and on-premises devices with minimal effort.

There are new expectations for the network perimeter. Isn’t it time your network security solution provides them?

About the Author

Barrett Lyon is the co-founder and CEO of Netography, whose Security Platform provides cross-network visibility, encompassing cloud and on-premises environments. His experience and successes have led to collaboration with Tier 1 and Tier 2 carriers, as well as national security agencies in North America and Europe to mitigate and track hundreds of DDoS attacks. He holds multiple technology patents and is a pivotal subject in the best-selling cybersecurity book, Fatal System Error. Barrett can be reached online at @BarrettLyon and at our company website https://netography.com/.