Agencies Optimistic about Security Response, but Lack Crucial Visibility

After a trying year that tested the public and private sector's agility and security capabilities, government agencies remain focused on accelerated IT modernization, and strengthening cyber defenses to protect an increasingly digital government infrastructure.

The Office of Management and Budget (OMB) and General Services Administration (GSA) just loosened the reins on payback requirements for the $1B Technology Modernization Fund (TMF), and asked agencies to submit projects that fall into one of four categories: modernizing "high priority" systems; cybersecurity; public facing digital systems; and cross-government services and infrastructure. From a policy perspective, the emphasis is clear.

New research, however, suggests agency leaders do not have the visibility into assets or nefarious activity they need to protect modern, increasingly cloud-based operations.

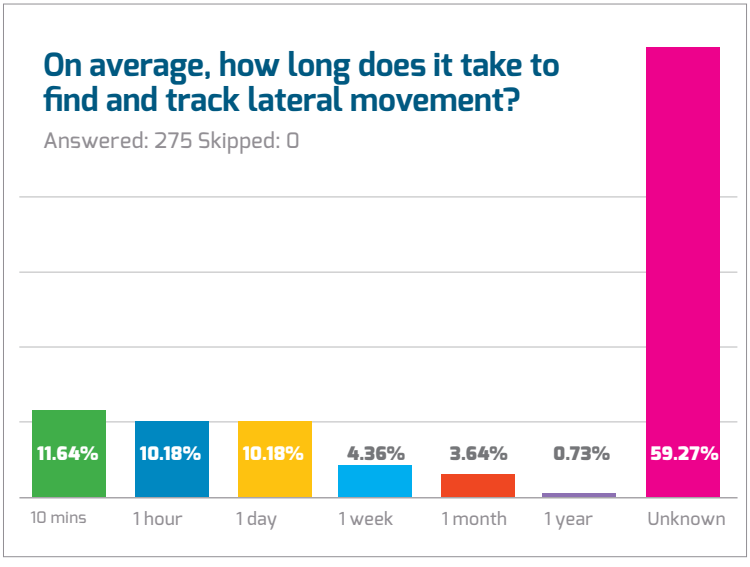
The SolarWinds breach made the importance of finding and tracking lateral movement quickly, painfully obvious. Ten percent of Federal IT and Operations leaders say this takes more than an hour, and 15 percent, more than one day.

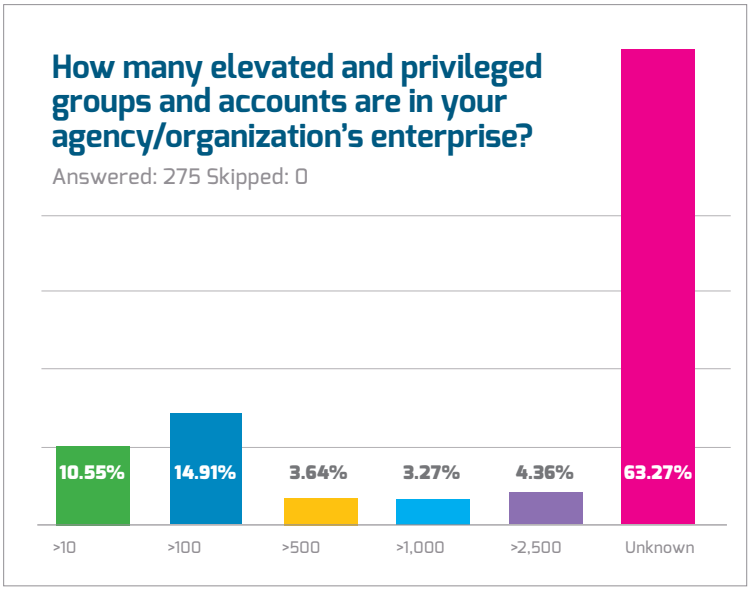
Compounding the problem, agencies take too long to quarantine threats. Forty-two percent of IT security leaders say it takes longer than an hour to quarantine suspicious assets. Thirty-four percent say it takes longer than a day.

Agencies Don't Know What They Don't Know

A deeper dive into the survey's findings reveals a larger number of respondents that simply don't know how long it takes to quarantine suspicious assets (nearly 36 percent), discover and track lateral movement (close to 34 percent) or even how long it takes to identify compromised assets after a zero-day incident (30 percent).

That startling lack of visibility leads Matt Marsden, AVP of Technical Account Management at Tanium, to believe, "Federal IT and security leaders have a false sense of security. It takes too long to discover threats and much too long to quarantine threats. As a community, we focus on the mechanics of response. The more important question is how long did it take to identify a potentially





compromised asset or discover an intrusion in the first place?"

"It's no secret that increasingly hybrid environments – legacy systems, multi-cloud, BYOD due to telework – have complicated cyber efforts," says Marsden. "And, I'd argue that one of our biggest challenges is throwing good money after bad, i.e. the sunk cost fallacy. An agency invests in a tool that should lead to an outcome. When they do not get the promised outcome, they add a few more features, and a bit more cost. It's the age-old problem of bolting on new features that don't do what modern enterprises require.

The new Cybersecurity Executive Order, the just-released TMF guidelines, all point to an understanding we can't secure government with incremental cyber product updates."

These new opportunities come at a time when decisionmakers say they face an increasingly complex threat from nation-state actors – again underscored by events like the SolarWinds attack, where Russian hackers trawled government systems for sensitive information.

And, as we are all well aware, agencies face continued heighted risk due to the number of endpoint devices outside of the enterprise perimeter. Thirty percent admit their attack surfaces have expanded, and just over half say they are managing as many as five cloud providers.

Traditionally, agencies would lock down rights and privileges on the endpoint, creating a strong account and execution privilege posture.

The research shows that agencies have invested in cloud-based security tools including endpoint detection and response (EDR), endpoint protection platforms (EPPs) and cloud access security broker (CASB) solutions - 54.9 percent use up to five of those tools. But, IT teams are not tooled appropriately to provide secure connectivity or remote management and visibility of their users. The risks will continue to increase exponentially unless we focus on the foundation of security and IT hygiene.

"They're facing these new problems that they hadn't faced before because when you're dealing with a majority remote workforce. You can't use a lot of your tools anymore," said Marsden. "So they have to do a lot of retooling and feel much more vulnerable because endpoints are more exposed than they were in the past."

The numbers also hint at the kind of tool sprawl that can complicate IT and security strategy – 22.9 percent of respondents use more than 20 cloud-based security tools, while 11 percent use between 15-20. Marsden believes the reported number of tools is low, explaining that organizations across the board often find themselves managing as many as 100 tools. "That's unsustainable," he said, because agencies "can't staff that effectively." Instead, he said, "what they wind up with is a bunch of tools that they install and forget."

There are no easy answers as assets expand and more functions move to the cloud. But, increasing visibility into assets and activity across systems is critical to identifying and responding to potential problems before they escalate and impact Federal missions.

"You've got to have awareness, that is as close to the same speed as whatever it is that you're trying to defend against," said Marsden. "And you have to have that awareness across your entire estate of devices."