A GOVERNMENT TECHNOLOGY Q&A

government technology

Securing the Distributed Workforce: The State of North Carolina

In this Government Technology Q&A, **Maria Thompson**, chief risk officer for the North Carolina Department of Information Technology, shares insights on how the state and other jurisdictions are securing their distributed workforce as they move into the future.

When the pandemic hit and North Carolina employees moved to remote work, what new cybersecurity concerns did you face? Having remote workers was not new to us. It was the number of additional endpoints connecting to our network that was a concern. Our first thought was, how do we gain visibility into all these remote endpoints and ensure they are protected and compliant? We also had to ensure our infrastructure could support incident response for all these remote devices.

What's driving the shift in focus to endpoint security? Locating and managing endpoints has long been a challenge. Modern solutions such as Tanium's can now help us get that level of visibility and control. They're critical because the boundaries and endpoints are now in workers' homes or in a café somewhere. Defense-in-depth is still important, but we need more emphasis on the endpoints because that's where the attacks are coming in.

How do you engage remote workers in threat reduction? When you can get up, go to the kitchen and grab a cup of coffee, it's easy to become complacent and forget about cyber hygiene. It's very important to keep security top of employees' minds. I'm using this opportunity to deploy tools that give us visibility and compliance at these endpoints, with the hope that as we move forward, workers will be more comfortable with these tools and we will be in even better shape than before.

Would you elaborate on what it means to have a security platform? A security platform is a way to tightly weave together our disparate security products into a holistic solution that supports end users from the minute they log on to the network until they go to bed at night. It is a program of solutions or processes to create the most secure end-user environment possible and quickly provide incident response when something anomalous happens with an end-user's device.

How does the security platform tie into the operations team's monitoring for anomalous behavior? One positive outcome of the pandemic is the operations team and security team are working more closely together. Without the operations folks, there's no way for the security team to do everything that it needs to do to secure the endpoints and end users. There's an understanding that we need to be part of operations' incident response process if they see something anomalous. In addition, even though a tool may have been purchased primarily for an operational need, it has security features that can enrich the data our SOC receives and thereby provide an even more granular level of control and visibility into what is happening.

Given that remote work will continue, how is your approach to overall security architecture changing? I think we'll see more frequent and more targeted attacks against end users in this remote environment. We need to establish a solid footprint into those endpoints, with solutions that enable network segmentation and granular, least-privilege access control so users can only access the resources they need to do their jobs. We also need threat monitoring and forensic capabilities on a user's endpoint, as well as threat hunting capabilities so we can assess our environment when we receive threat intelligence reports and respond proactively.

How can smaller organizations with limited funds protect their endpoints? Start by building relationships with neighboring organizations and partners. Learn from them. View your state as a resource to tap into rather than as a competitor. Look for opportunities to consolidate infrastructure and share the load. If you're not a member of the Multi-State Information Sharing and Analysis Center (MS-ISAC), become one. They offer a lot of free services that may not be in your toolkit. Finally, turn to private sector partners for best practices and to help you figure out the right solution for your organization.