Time to Reevaluate Security Practices

State and local government leaders pushed themselves to the limit to keep government operations afloat in the initial phase of the pandemic. ***Sumit Sehgal****, Chief Technology Strategist, U.S., for McAfee shares insights to help organizations prepare for the future.*

Organizations moved quickly to adapt to the pandemic, adopting cloud-based technology and new approaches. Now what?

After pivoting quickly to keep government functioning, agencies are reevaluating. They recognize the way they typically provide citizen services may be too expensive to run full native cloud and that cloud-enabled doesn't always equal lower costs. Labor is another consideration. Running a cloud-based Microsoft Azure instance for your data center is different than running a hardware-based instance. Staff might not even know what that looks like from a security operations perspective. At the macro level, the challenge isn't so much the technology or moving stuff to the cloud. It's looking at long-term costs, labor and expertise to determine whether the organization can afford to keep everything it has done in recent months running the way it is.

What threats and vulnerabilities currently dominate the state and local government landscape?

The threat issues with security hygiene and complex, aging IT infrastructures are largely the same as pre-pandemic, but the attack vectors have changed. Instead of attacks against the infrastructure, we see an increase in very sophisticated email and voice phishing scams that are designed to harvest information. On the vulnerability side, organizations have moved complex IT infrastructure to the cloud without accounting very well for security. We're seeing a shift from traditional operating system and application vulnerabilities to cloud-related vulnerabilities. That's everything from identity to the way cloud applications are run to how access and attribution of data security occurs as it travels through that whole continuum.

How has the surge in remote work impacted cloud security?

It has forced people to look at security from the lens of cloud application security, data integration and interoperability. Besides confidentiality, they're investigating how they can frame their security architecture so that it's cloud native to begin with and applies things like identity management, privilege management and user behavior monitoring to the cloud world. The rapid shift to third-party security providers and cloud providers has caused some growing pains in terms of how people remotely access their applications, VPN or cloud. In some cases, applications that were running in the cloud don't work at scale from a security perspective. So, organizations must change their approach to protect citizen information.

How can organizations make the most of tools and approaches such as zero-trust architecture, adaptive security and user behavior analytics?

The bottom line is that even the best tool or approach will not fix a bad process. All the zero-trust technology in the world won't work if your identity and asset management processes give the system bad data. To fully utilize these approaches, agencies must look honestly at their processes and what they're doing regarding hygiene, security practices and things like that. Organizations also need to determine what they want from these tools, whether the tools align with their best practices and overall security approach, and how these tools impact the way they perform existing processes.

How can state and local governments simplify regulatory compliance and governance related to data privacy?

I see the potential for security and privacy practitioners to come together to create a standardized language that bridges security and privacy — similar to MS-ISAC, the Multi-State Information Sharing and Analysis Center, where everybody uses the same language when a security incident occurs. Ideally, security and privacy teams would watch for — and notify their counterparts of — unusual behavior or incidents that may impact the other's domain. We need something like this because cloud applications and the future we're headed into don't provide the same visibility.

What strategies can organizations employ to move forward with modernization while addressing the urgencies of the pandemic?

Standards-based approaches such as the NIST Cybersecurity Framework or the MITRE ATT&CK framework can help on both the security side and the application architecture side. Multiple agencies can create a structure that lets them design services and other things in the same manner. When done appropriately, that eases the burden of customization and enables organizations to scale or improve functionality and the user experience for things like security and analytics applications, as well as infrastructure management.