When the National Association of State Chief Information Officers issued its annual list of top priorities heading into 2020, there was little surprise that cybersecurity ranked at the top of the list for the seventh year in a row; or that cloud services continued to rank in the top three. What did catch the attention of NASCIO officials was the appearance for the first time of “innovation and transformation through technology.”

Few CIOs, of course, could have anticipated the coming pandemic, as well as the need to fast-track all three of those priorities as the pandemic’s impact unfolded.

Although state and local governments were aided in part by their investments in cloud platforms and tools to support digital services, no one could have foreseen the massive relocation of employees outside the controlled IT environments of government offices. That exodus triggered a herculean push by agency IT departments and their vendors to expand state and local networks.

“I have spoken with many state CIOs who have seen their networks go from a few thousand nodes to 100,000-plus in a matter of weeks,” says Matthew Schneider, vice president for state, local and education markets at Palo Alto Networks.

However, as daily workloads shifted suddenly — from office cubicles and controlled enterprise IT environments to home offices and the cloud — it revealed something else: The reality that security demands have flipped inside out.

“Digital business and edge computing have ‘inverted’ access requirements with more users, devices, applications, services and data located outside of an enterprise than inside,” say Gartner analysts Neil MacDonald, Lawrence Orans and Joe Skorupa in their report, “The Future of Network Security is in the Cloud,” released last year.

As the bulk of work continues to flow outside the traditional protective barriers maintained by many agencies, it’s increasingly clear that investing in legacy security controls and point solutions is a road to diminishing returns.

The challenge now is not only how to secure data flowing across external networks and helping remote workers to work more securely. It’s also finding smarter security solutions at a time when states and localities are facing enormous budget pressures; demand for digital services remains on overdrive; and ransomware hackers have shifted their break-in strategies from government offices to employees’ home networks.

SECURING REMOTE WORKERS EVERYWHERE

The evolving reality of today’s distributed workforce — and the rush to scale services into the cloud — has created a new set of dynamics for state and local governments that require a new, more holistic and agile approach to security.

“We’ve recognized a couple of things,” Schneider says. “It’s not just about connectivity. It’s about secure access to all of your applications and all of your tools. We’re allowing critical resources to go home with our users. So we’re changing the way we think,” he says.

“We’re also recognizing that the disparity of tools that we built in place to protect the enterprise are not fitting into the scale of the digital transformation. I can’t lift and shift the
technology that’s built on IP addresses to a technology like containers, because these applications that don’t rely on IP addresses; they rely on understanding the workload all the way through … the user experience, with a consistent understanding of user visibility and context,” he explains.

That’s why technologies such “secure access service edge” or SASE solutions, like Palo Alto Networks’ Prisma Access, and other security-as-a-service capabilities are expected to increase dramatically. Gartner estimates that by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE solutions, compared to less than 1% at year-end 2018.

The need to empower workers anywhere and everywhere, meanwhile, are accelerating the adoption of cloud services, but also the need to put new security disciplines in place.

That’s borne out in a recent Palo Alto Networks and Accenture Security report, “The State of Cloud Native Security 2020.” It found that enterprises across five major industries now run 46% of their workloads in the cloud and expect that level to reach to 65% in the next 24 months. The findings, based on a survey of 3,000 IT professionals in the U.S., Germany, the United Kingdom, Australia and Singapore, also found:

- 94% of organizations now use more than one cloud platform and 6 in 10 use between two and five platforms.
- However, only 18% of enterprise organizations are considered highly prepared to keep their cloud estates secure, based on 19 measurements of preparedness.
- Among those highly-prepared organizations, half say they are reducing the number of security tools they use; and 51% agreed, using a single, end-to-end cloud security solution would improve their cloud security posture.

The study reinforces the conclusions of a broader 2019 Cloud Security Report produced by Cybersecurity Insiders, a community of 400,000 IT security professionals, which found that security teams must address the shortcomings of legacy security tools to protect their evolving IT environments.

**RE-ENVISIONING THE ENTERPRISE PERIMETER**

Enterprise firewalls have evolved and will continue to play an important role in this inverted security world. Expanded demands from users have pushed the domains of network security to adopt true conformance to SASE models, ensuring secure access to external applications and destinations. This consolidation of numerous capabilities into a single platform enables automated detection and response, aided by embedded machine learning to scale in accordance with threat levels.

Further, as the needs of enterprises change and expand from physical use-cases to virtual and cloud-based operations, a firewall function will follow — provisioned to how and where the user needs security. This is in line with what agencies need around advanced capabilities for their firewall solutions beyond traditional perimeters, according to a new report from Forrester, including:

- Support for delivering zero-trust capabilities to the edge, such as content inspection, instruction detection/prevention, malware detonation, secure web gateway and zero-trust network access, all consumed as a service.
- Fourth generation firewall capabilities, that can extend management into the cloud and manage native public cloud security objects, like AWS security groups, containers, and Azure and Alibaba firewall objects.
- Strong endpoint component integration, to direct remote traffic through to a vendor edge network for content inspection and secure remote access.

“If you look at how much of the industry has approached zero trust, it’s been primarily zero trust inside of my network,” says Schneider.

**Recommendations for building your enterprise security platform**

1. **Build a strategy** to secure all users, all data, and all apps versus siloed stacks.
2. **Look for flexibility** to deliver consistent security services, in line with your user and data, to eliminate complexity and bolt-on solutions.
3. **Ensure consistency** of support for all cloud applications and environments.
4. **Ensure continuous evolution** with optimization and automation.
5. **Ensure you’re gaining capabilities**, not complexity as you expand your portfolio of security.
Many of those solutions "are not recognizing that every boundary is another exposure that could degrade trust. When I access agency data from a device from home, I’m actually connecting into a cloud gateway that may connect to a cloud resource or my cloud infrastructure. Every one of those boundary points has to re-establish trust in that zero-trust environment."

That extended operating environment makes it essential to "have a control plane, across the enterprise, all the way out to that end user, and that end user’s device, and then the context of that trust, all the way through the workflow session," he says. It also demands an enterprise operating platform capable of delivering zero-trust security services regardless of where users are or where they must go to get their data.

**ADDING SECURITY AND VISIBILITY TO SD-WAN**

Schneider points to Palo Alto Networks’ most recent innovation — the industry’s first and only next-generation CloudGenix SD-WAN — as an example of the capabilities agencies should be evaluating. This type of solution utilizes machine learning and automation to simplify network operations, enable app-defined policies and deliver a secure, cloud-delivered branch.

With this offering, there is a seamless networking onramp to the Palo Alto Network’s Prisma Access zero-trust network access solution, which has proven particularly valuable in helping enterprises enable secure remote work connectivity for employees during the pandemic (and beyond).

Schneider credits Palo Alto Networks’ shift over the past several years to a cloud-based approach — and its strategy to integrate key technology acquisitions, not merely rename them — among the key reasons why the company was recognized by Forrester in August for "leading the pack" among 11 well-known enterprise firewall providers.

**SUPERIOR SECURITY THROUGH AN INTEGRATED APPROACH**

The important message for state and local government leaders, however, is the ability they now have available to them to move away from costly patchwork point solutions to an integrated platform that provides superior security, while actually lowering total operating costs, Schneider says.

"We know phishing attacks are up by well over 100% at state and local governments," he says by way of example. "I talk with clients that are spending 15 to 20 hours a week for an analyst to respond to these phishing attacks, looking to see, is there malware that I have to remove out of the network? We have effectively removed the human element from phishing and malware analysis."

Eliminating that work practically pays for the platform, he contends. Add to that savings that come through reducing duplicative tools and repetitive, mundane processing tasks and the savings start to add up quickly.

State and local customers, in many instances, have reduced the volume of random alerts typically by 50-fold using Palo Alto Network’s integrated platforms, according to Schneider. And they’ve been able to quadruple the speed of response, all at lower total operating costs.

In summary, enterprise security paradigms are turning inside out as state and local governments adapt to a new era of remote workers. As the workforce in growing numbers chooses to operate outside the traditional protective barriers maintained by many agencies, it’s increasingly clear that investing in legacy security controls and point solutions is a road to diminishing returns. The challenge now is not only how to secure data flowing across external networks and helping remote workers to work more securely. The answers presented here seem to be a promising option for forward-thinking organizations in search of the next wave of technology.

**Learn more** how Palo Alto Networks can help your agency secure its IT future. Get a customized security assessment giving you complete visibility and customized security intelligence.

*This report was produced by StateScoop and underwritten by Palo Alto Networks.*