The Keys to a Secure Hybrid Workplace

MARKET TRENDS REPORT

govloop

paloalto NETWORKS

Executive Summary

The post-pandemic workplace won't be anything like what government agencies have been used to. It won't be bound to agency offices and in-house data centers, obviously, as most agencies had started digital transitions to one degree or another before COVID-19 hit. But it won't be like the past year and a half, either, with so many employees working from home via whatever collaboration tools agencies could put in play quickly.

The hybrid environment most agencies will return to will be a different breed, requiring agencies to support employees working from anywhere and collaborating in hybrid groups involving the office, the home and any number of locations on the road. In June, the White House announced that the federal government would continue to offer flexible, hybrid working conditions post-pandemic. Many state and local government agencies will likely follow suit.

There are advantages to hybrid workplaces, ranging from lower office-space overhead to the ability to recruit and retain talented workers no matter where they live. But there also are challenges. Agencies need to provide a seamless, consistent experience for employees, no matter where they are, or where the people they are collaborating with are located. And, critically, agencies need to secure access, communications and transactions across the board in a hybrid environment. Implementing a zero-trust architecture for identity and access management in the cloud is likely an essential step.

To learn more about managing and securing the hybrid workplace, GovLoop partnered with enterprise cybersecurity provider Palo Alto Networks. In this report, we'll discuss the post-pandemic challenges agencies face, how they can manage and secure a hybrid environment, and the importance of zero trust.

"We want to create a more efficient, competitive, and flexible federal workforce. I want to make sure that cybersecurity and IT improvements are at the fore-front of future telework conversations."

—Sen. James Langford, R-Okla.

(from hearing: Senate Hearing on Pandemic and Federal Teleworking | C-SPAN.org)

By The Numbers

An employer-employee disconnect?

A recent survey found that...

55%

of workers prefer working from home at least three days a week....

...But:

68%

of employers want their employees in the office at least three days a week...

...And finally:

21%

of execs said they prefer working in the office 5 days a week; 18% want 4 days.

Employers said they were concerned that a company culture wouldn't survive a purely remote work environment.

From the U.S. Office of Personnel Management's Federal Employee Viewpoint Survey 2020:

59%

of federal government employees worked from home every day at the height of the pandemic.

3%

of federal government employees worked from home every day before the pandemic.

86%

of feds said their unit had met the needs of their customers during COVID-19, down from 94% pre-COVID.

48%

of federal employees said their work demands were greatly or somewhat increased during the pandemic.

The Pandemic Effect

17%

of U.S workers teleworked 5 days or more a week before COVID-19.

44%

telework 5 days or more per week during the pandemic.

Embracing the New Work Model

Challenge: Security, Consistency Create Hybrid Headaches

The first challenge an agency might face is whether to abandon some of its old practices and fully commit to operating a hybrid environment. It's a decision with an organization-wide impact and should come from the top.

"It's really going to be a policy question," said Elton Fontaine, Director of Systems Engineering for Palo Alto. "If you're going to embrace hybrid work, you need to now view it as a permanent, and not just a temporary, solution."

Once that decision is made, agencies will add an IT strategy, which will have to address other challenges. That includes:

The employee experience. "The biggest challenge in a hybrid workforce is you have to deliver a consistent employee experience," Fontaine said. Application performance, for instance, should feel the same whether employees are in the office, at home or connecting from a coffee shop. And they should feel the same whether the applications are hosted in an on-prem datacenter, a public cloud, or in an application repository. Consistency is essential to enabling collaboration regardless of employee location.

Security. Likewise, security has to be a consistent—and seamless—experience. If security steps are slowing down work, Fontaine, noted, even employees who aren't tech-savvy suddenly become adept at disabling a virtual private network connection or skirting security procedures. An agency needs to ensure a consistent approach no matter where the user is located or where the applications and data are hosted, rather than shifting policies for different scenarios. "If you get to the point where you're trying to make differentiated policies depending on these various locations, you're already losing the battle," Fontaine said.

The talent gap. A hybrid work environment will depend heavily on integrating cloud and on-premises operations. Most agencies lack the in-house expertise to cover every aspect, nor do they have the automated tools that can take some of the burden away from IT staff.

Solution: A Foundation of Zero Trust

Agencies looking to effectively manage a hybrid work environment should consider making several key elements part of their policies.

Consistent Security through Zero Trust. In a hybrid environment, a consistent experience depends on consistent security. A zero trust model, which recognizes that trust is a vulnerability and focuses on authenticating users and devices continually, can provide consistent application of security controls regardless of a user's location—and do it without hurting the user experience. Zero trust not only increases security substantially, but it increases productivity as well. Its features include:

- A zero trust architecture
- Next generation firewalls
- Identity and device management
- Enhanced security

Many agencies already have identity management programs in place and have often talked about moving toward zero trust. They may already have many of the tools they need in place, and just need some guidance to get there. "I think people are not as far away as they think," Fontaine said.

Automate. Managing a hybrid workforce across an environment that involves multiple clouds and on-premises data centers will rely heavily on automation tools. Integrating an automated solution can make zero trust as dynamic as the enterprise, while handling tasks that could be too big for IT staffs to handle on their own. It's also critical to managing the expanding use of the Internet of Things. "You're offloading the administrative burden, and you're making it tenable to sustain an agency-wide security strategy," Fontaine said.

Training and Collaboration. Learning and development programs will become more important in a hybrid work environment as an essential tool for supporting employees and their career trajectories. And collaboration involving multiple settings (home, office and hotel rooms) will be the lifeblood of an organization. Agencies need to have the policies and tools in place to support employees under any circumstances.

Best Practices in the Hybrid Work Environment

1

Embrace the Reality.

Telework and hybrid work environments are the present and the future of agency operations, so it's best to pursue it enthusiastically. Strong support for the new environment will increase productivity and efficiency, improve security and can help in recruiting and retaining talent.

2

Adopt Telework-Ready Technology.

Security can include tools such as Firewall as a Service (FWaaS), zero-trust network access, a cloud secure web gateway and other steps. While choosing the tools that best fit their specific environment, agencies should also be sure only approved conferencing and collaboration tools are being used. The NSA and CISA have published Best Practices for Telework that can offer a guide. Other best practices include integrating effective technologies such as:

- A Secure Access Service Edge (SASE) model for secure access
- An integrated SaaS solution
- Cloud-based identity management

3

Keep Communications Open.

With a hybrid workforce, a lot of the beneficial features of working in an office have to be moved online, including collaboration, training and mentoring employees to support their careers. Whether using Slack, Microsoft Teams or another communication channel, it's important to build those communities, enhancing the channels with personal pages or other features, so people can communicate not just about work but develop some of the old water cooler chats as well.

4

Let Employees Set Boundaries.

Another aspect of the human element is recognizing that telework should have its limits. A lot of people didn't take time off during the pandemic and have started showing the effects of burnout. Some employees may feel they need to respond immediately to any communication, which can cause stress. Likewise, having certain tools doesn't mean you have to use them all the time. Zoom fatigue, for example, is a real thing.

5

Measure Performance.

How agencies measure productivity may have to adjust when schedules are flexible and employees are in dispersed locations. It may be best to measure over a longer period of time, rather than according to a strict, short-window schedule. Adapting measures to the new reality not only gives agencies a more accurate view, but it shows trust in employees.

6

Monitor, Maintain, Refine.

In the dynamic cloud-based environment necessary to supporting a hybrid workforce, continuous monitoring is essential in detecting and deterring threats, recognizing threat trends and maintaining a strong security posture. It helps manage the identities with access to the network, right-sizing access permissions and eliminating abandoned accounts. Information gleaned from monitoring also can help agencies improve their operations.

Case Study: Zero Trust Proves its Mettle

A zero trust platform has a lot of benefits, but one of Palo Alto's government customers saw the value in an emphatic way in 2020, when news broke of the SolarWinds hack, which raised alarms throughout the government.

With its zero trust system implemented, Palo Alto's agency customer was able to leverage the visibility provided by Cortex Data Lake to spot the attack, and the platform's automated response deterred any incursions, successfully deterring the network.

Data Lake, which provides log management and network visibility, is part of Cortex, Palo Alto's artificial intelligence-based platform for continuous security operations that extend into the cloud, providing endpoint security.

In addition to controlling access, the solution offers other benefits, such as pervasive visibility into the environment via the solution's control points, and the ability to correlate data on anomalous behavior and automate the response. Automated detection and response, identity-based access control and deep network visibility greatly enhanced the agency's security posture.

That proved effective in a particularly dangerous, high-profile attack. The agency was one of the few potential targets that was truly protected against the attack right from the start.

HOW PALO ALTO NETWORKS HELPS

Palo Alto Networks offers a full range of next-generation enterprise security solutions, including the components necessary for zero trust, and has extensive experience working with major corporations and federal government customers.

The company provides identity management, zero trust protection, application identity, cloud access security broker (CASB) services, next-generation firewall services, web application firewall services and other elements of complete, cloud-based security. Its solutions include Prisma Access, which is supported by SASE and is the industry's only complete cloud-delivered security platform. Cortex automates security through platforms including Cortex XDR, XSOAR and Data Lake.

Palo Alto's network and cloud-native security solutions—which extend detection and response capabilities and automates security operations and attack surface management—can provide the consistent, comprehensive security that organizations need to support a large, cloud-based hybrid work environment. And as it does with other potential customers, Palo Alto offers agencies a zero trust assessment at no cost. Learn more: paloaltonetworks.com

Conclusion

The work environment for government agencies, as it is for almost everyone else, is changing for keeps. "COVID has permanently transformed the way that we work," Fontaine said. And the next model for the workplace will require next-generation tools.

The hybrid workplace presents agencies with a lot of challenges, but perhaps the most important is providing consistency—in the employee experience and in security, which is the key to making it all work seamlessly and effectively.

"In a hybrid work environment, this is where consistency is imperative," he said. "You can't effectively implement and sustain zero trust if you're trying to configure different policies across a myriad of tools." A comprehensive, highly automated approach that embraces the change and proactively supports—and secures—both the employees and the enterprise can help agencies flourish in the post-pandemic world.

paloalto® NETWORKS

ABOUT CLIENT

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

govloop

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop