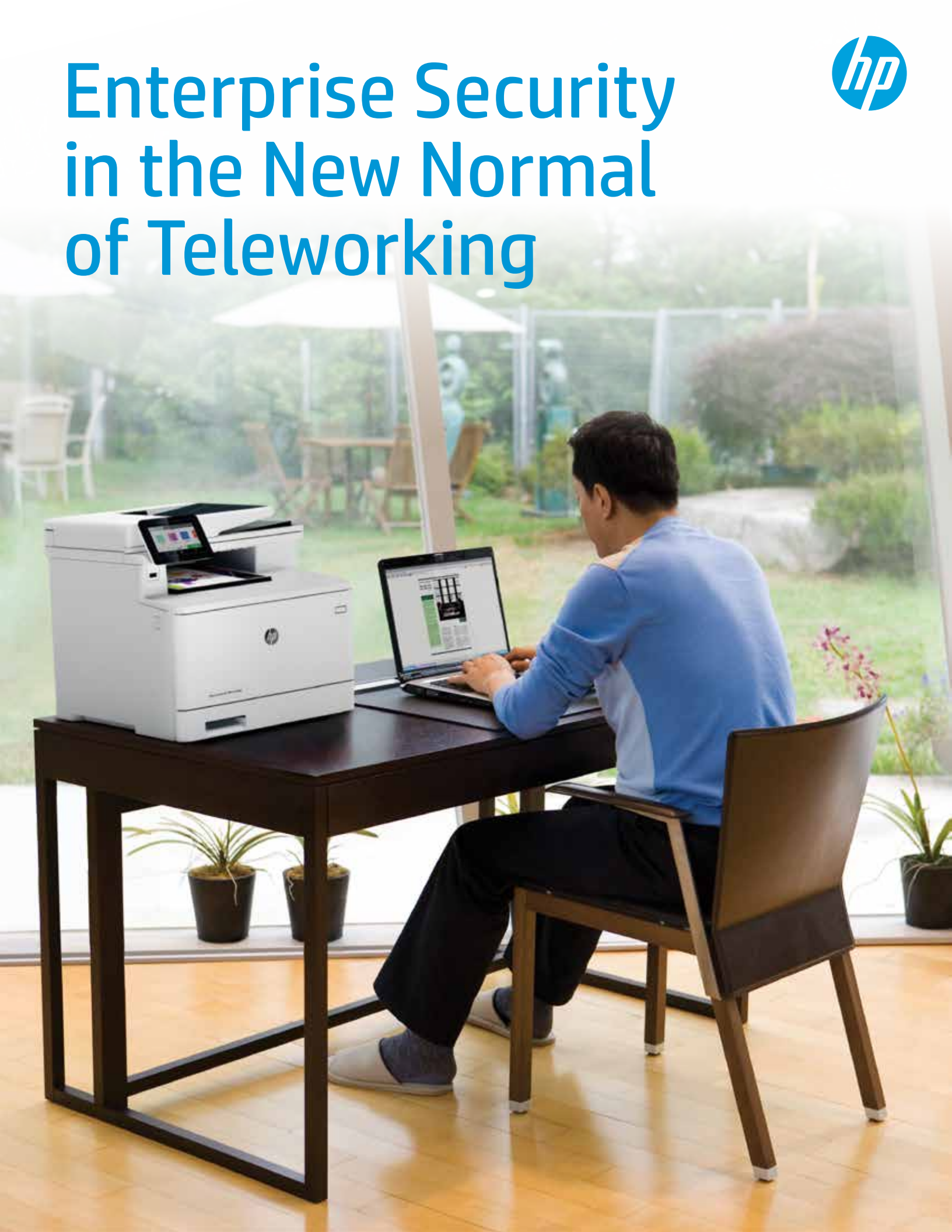
Enterprise Security in the New Normal of Teleworking



Until recently, remote teleworking has been the exception rather than the rule for workplaces across the country. As recently as a few years ago, 29 percent of employees could work from home,[1] with only 12 percent doing so at least one full day a month, according to the most recent government data.[2]

All that has changed. With millions of Americans now working from home, people across the country — including state and local government employees — have transformed their home into their new office. Employers, both private companies and public-sector agencies, have integrated remote work into their operations. Indeed, teleworking is set to become the new normal for months or even years to come. Many organizations are allowing employees to work from home for the rest of the year or permanently, if they choose.[3]

Just as private-sector companies are preparing their organizations for teleworking, state and local governments need to do the same. However, as the public sector transitions to this new way of working, security also needs to be top of mind.

The first phase of mass migration to telework was heavily focused on network connectivity, increased VPN support as well as new notebooks. The second phase will be marked with the enterprise requirements of extending enterprise security capabilities to these workers. Telework comes with increased security risks, including malware, ransomware, phishing attacks and more.

"All organizations are going to have to make this migration toward solving for cybersecurity around more than just a VPN or internet connection. They're going to have to realize that the new network edge is actually at the end user's device," says Sherbam Naum, senior vice president of corporate strategy and technology at HP.

With more devices connecting to their networks remotely, public-sector organizations must strengthen their security posture and look to modern security architectures founded on zero-trust and real-time visibility. To meet their security needs in this new era of teleworking, state and local governments should consider adopting hardware-based security, designed into the platform, that does not depend on detection to provide protection. By applying virtualization-based security, enterprises can defend their remote endpoints, even when not connected to their enterprise infrastructure. State and local governments can apply virtual container solutions, cloud-based security infrastructure, along with automated firmware intrusion detection and repair systems and built-in hardware security automatically. This paper discusses how this approach can help state and local governments bolster their enterprise security as they transition to the new normal of teleworking.

One study found

14% of American workers never changed their device passwords

21% of them have shared a work-related password electronically

Current Telework Security Challenges

Like many organizations, state and local governments face a variety of security challenges related to people, processes and technology.

State and local governments have traditionally taken a "big bang" approach to development that has left them with monolithic legacy systems, which have more security vulnerabilities than modern architectures designed to combat today's emerging security threats.

As more employees work from home, government agencies also contend with home wireless networks that likely aren't as secure as office networks. While network security is an issue, so are device security and employee behavior. Employees may be using personal devices, such as laptops and mobile phones, to remotely access systems and work-related information, especially if they don't have workplace-issued devices. They also might engage in behaviors that put the network at risk, such as downloading unauthorized applications, failing to regularly change their passwords, or even worse, sharing their passwords with others. One study found that 14 percent of American workers never changed their device passwords and 21 percent of them have shared a work-related password electronically.[4]

State and local governments also use third-party software-as-a-service applications (SaaS) that extend their technology capabilities, but these applications also increase their security risks and attack surface. The speed at which government agencies have had to transition to remote work also has left these entities with security risk opportunities that hackers are looking to exploit.

Teleworking provides a number of key advantages for the enterprise, yet it also makes remote workers prime targets for phishing scams, malware and ransomware attacks. As state and local governments transition to this new way of working, they must find an effective way to deal with increasingly sophisticated security threats. To accomplish this, they must reduce IT complexity, modernize their endpoint security strategy, and transform their enterprise security infrastructure to incorporate real-time threat intelligence and monitoring. Adopting a zero-trust, containment-based approach within a unified security platform can help state and local governments gain more visibility into their remote work environments and move from defense to offense when it comes to enterprise security.

Securing the Enterprise in the Era of Remote Work

An effective enterprise security solution is one that takes a holistic approach to security across software, hardware and firmware to secure devices and ensure data protection and privacy. Virtual containers are a key part of this holistic approach.

"With users no longer operating behind the enterprise or government infrastructure, everything is decentralized," Naum says. "State and local governments now have to ask what happens to a device when it's sitting in someone's home and what happens when the user is left to be the final cybersecurity decision-maker. When a user is outside the corporate firewall and enterprise security infrastructure, containment provides protection to isolate threats if, for example, a user opens an email with malware attached to it."

State and local governments should consider enterprise security solutions that include features and capabilities such as virtual containers, or micro-virtual machines (micro-VM), that provide hardware-enforced application isolation to strengthen endpoint security. Many existing solutions try to identify malware and use network connections to provide protection, but with virtual containers, suspicious websites can be opened in their own isolated environments and the malware is tricked into believing it has gained entry into government systems. Once the application containing the malware is closed, the malware is deleted with no impact to the enterprise.

An effective enterprise security solution is one that takes a holistic approach to security across software, hardware and firmware to secure devices and ensure data protection and privacy.

A containment-based approach can help government agencies enhance browser security — without the need for restrictive whitelisting — in the event employees visit untrusted sites. Virtual containers also provide protection for common files, so employees can safely view PDFs, images, video content, Microsoft Word, Excel and PowerPoint files without a disruption to their workflow and without government agencies compromising their own security.[5]

In the remote work era, state and local governments also will need hardware-based security. As work leaves the confines of the office, employees may work inside their homes or in public communal workspaces, like co-working environments, libraries or even coffee shops. Protecting the information on their devices from public viewing will be just as critical as isolating security threats. Protecting the enterprise from lateral movement from a compromised device into enterprise resources via the VPN connection is paramount.

Security Solutions at a Glance

- Look for enterprise security solutions with capabilities such as **virtual containers**, or micro-virtual machines (micro-VM), that provide hardware-enforced application isolation to strengthen endpoint security.
- **Hardware-based security** is just as important as software. Look for hardware capabilities such as an integrated privacy screen, which helps secure sensitive information.
- Ensure that your hardware technologies include **automated firmware** intrusion detection and repair capabilities, which can automatically respond and recover from an attack.

Government agencies should look for security providers that offer not just software, but also hardware-based capabilities like an integrated privacy screen that prevents users from having to implement additional tools to secure sensitive information, such as constituent data or personally identifiable information (PII). With just the click of a few keys on the computer, users should be able to quickly transition their PC to privacy mode. This protects against screen capture and gives employees more flexibility to do their work from anywhere, while also giving government agencies another method they can use to bolster device security.[6]

To secure their remote work IT infrastructures, government agencies should consider enterprise security solutions that include automated firmware intrusion detection and repair capabilities. With these capabilities, state and local governments can strengthen PC security by automating detection, prevention and recovery after a basic input/output system (BIOS) attack. Automatic intrusion detection and repair systems can automatically load only authentic firmware, constantly monitor firmware health and pinpoint anomalies that could indicate an attempted attack. These systems also have self-healing capabilities to automatically repair any BIOS or firmware corruption using isolated backups.[7] BIOS attacks are notoriously difficult to overcome. Recovery often involves a service event that includes a system board replacement. However, with automatic intrusion detection and repair systems, government agencies can avoid these events and potential disruptions that impact constituent services.

Conclusion

As state and local governments plan for re-opening offices with some employees still working from home, they must take a hybrid approach to strengthening enterprise security.

New telework security policies will be necessary, as will an enterprise-wide strategy to transition away from legacy systems to reduce IT complexity and security vulnerabilities. Government agencies also will need to do an inventory of their most critical business needs related to teleworking and align their technology investments with these needs.

"State and local governments need to identify the gaps in their cyber posture, and that starts with them looking at their business operations and identifying what they need to do to serve their constituents," Naum says. "We're already in a hybrid environment. The best thing for government agencies to do right now is identify what has changed. They need to define the necessary from the unnecessary to reduce complexity and attack surfaces. So they'll need to invest in supporting IT operations and security operations for this new hybrid model."

Hardware and firmware-based security solutions and a unified security platform that encompasses a container-based architecture can help government agencies make this transition, identify and isolate security threats and potentially prevent security incidents.

The future of work is here. With the help of these advanced technologies, state and local governments will be better equipped for this new reality and be better prepared to fully embrace the new normal of teleworking.

Endnotes:

1. https://www.brookings.edu/blog/up-front/2020/04/06/telecommuting-will-likely-continue-long-after-the-pandemic/
2. U.S. Bureau of Labor Statistics, American Time Use Survey. https://www.bls.gov/news.release/flex2.t01.htm
3. https://www.nytimes.com/2020/05/21/technology/facebook-remote-work-coronavirus.html
4. https://www.onelogin.com/press-center/press-releases/remote-work-security
5. http://h20195.www2.hp.com/v2/GetPDF.aspx/4aa7-2638enw.pdf
6. http://www1.hp.com/ctg/Manual/c05317278
7. http://h10032.www1.hp.com/ctg/Manual/c06216928

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com**.

For: hp

HP Inc. creates technology that makes life better for everyone, everywhere — every person, every organization, and every community around the globe.