Lookout

TOP TAKEAWAYS

3 Key Considerations

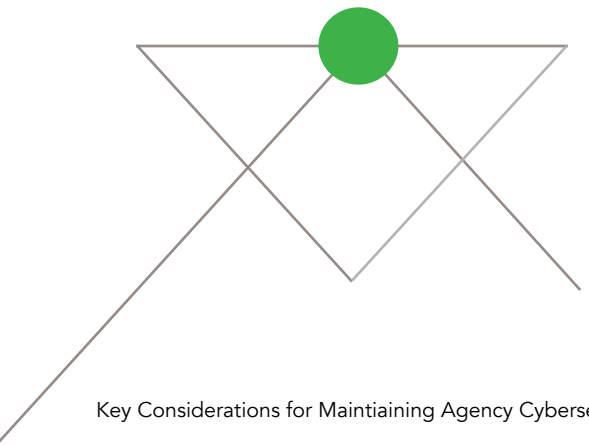
for Maintaining Agency Cybersecurity in the BYOD Era

Overview

More than ever, the lines between work lives and home lives have blurred. As the COVID-19 pandemic moved workers out of the office and into the wild west of telework, homes transitioned to workplaces, kitchens turned into offices, and personal devices and networks turned into professional ones. Lately, however, as we look out to a post-pandemic world, many in government are beginning to speculate that this shift to remote work may be more than temporary.

"The initial uptick of telework and the experiences has found that many organizations are just as productive as they were while they were in the office — and some more so," said Michael T. Geraghty, chief information security officer for the State of New Jersey during **a recent webcast from Lookout** and Government Executive that looked to security and mobility within the broader telework schema.

As agencies begin to contemplate the possibility of a more permanent telework culture and continue to mature remote work tools and technologies, however, the main question becomes: How can government successfully secure remote employees for the long-term?



> Now that it appears this is going to go on for a lot longer than anticipated, agencies are realizing it's time to figure out how to secure all of this new infrastructure, which exists inside and outside of our perimeter and outside of our traditional boundaries."
>
> Tim LeMaster | *Director of Systems Engineering,* Lookout

1. Security looks different in the BYOD era

With the shift to telework, malicious actors are seizing opportunities to attack a new plethora of vulnerable endpoints arising as staff connect to less secure home networks. Moreover, when the pandemic hit in March and agencies begin to transition to remote work as quickly as possible many in the public sector have turned to bring-your-own-device policies in order to keep employees online.

"Prior to lockdown, most mobile devices were government issued. Now, that has changed and many in government are launching significant BYOD programs," said Tim LeMaster, Lookout's director of Systems Engineering during a separate interview, pointing to the DOD, which has **expanded its telework policy in recent months** to include BYOD, **among capabilities**.

In the absence of secure networks and agency-mandated security controls, these personal devices may be less-protected, creating new threat vectors for government organizations.

"Personal devices have introduced some new risks," explained LeMaster during the webcast. "If it's someone's personal device, they may have applications on there that, if it were an organizationally owned device, they may not load. There's some of those apps we've seen in our work with firms, at Lookout, that we use and enjoy recreationally with no malicious intent, but they collect a lot of data from the device, from the users, and share that with other services, like for advertising purposes."

In addition to data mining, phishing threats are also on the rise as malicious actors look to take advantage of the new threat vectors mobile platforms produce, said LeMaster. Workers are using their smartphones more often to read professional emails, giving them less information on a single screen about who the sender might be or where the URL might lead. Moreover, they can no longer turn to a coworker to ask if an email or link seems suspicious. To top it off, malicious actors are getting more creative, LeMaster said, and phishing attacks are now coming into devices via SMS messages, social media and more — mediums where many employees let their guard down.

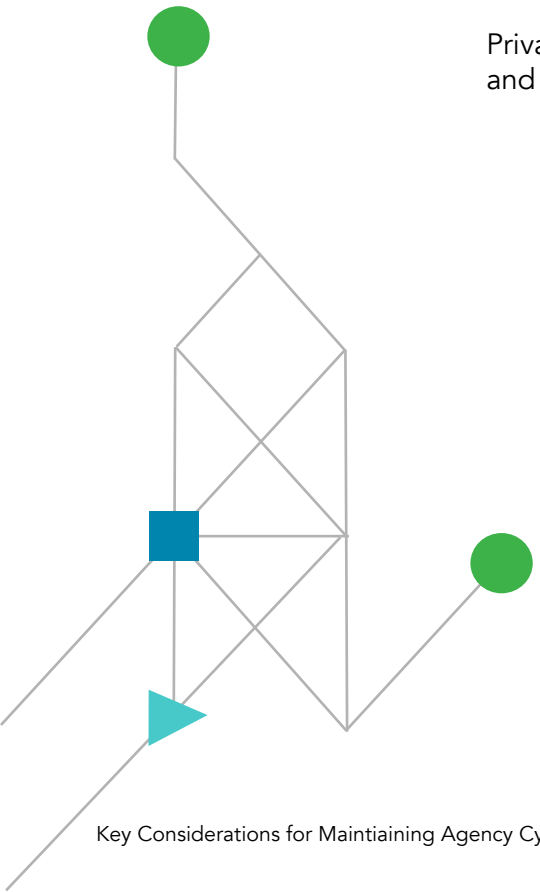
More than ever, it's important for agencies to have strategies and technologies that protect endpoints.

2. User-friendly mobile security can spur productivity

As agency IT teams look to adopt tools that protect public sector employees, networks and data from mobile threats, however, it's important to consider productivity and ease-of-use. Will a slew of disruptive and difficult-to-use security tools hobble workers? Will staff feel comfortable downloading an unknown tool their personal device? Either of these issues could inspire staff to find ways around the tools, creating shadow IT and a introducing a litany of unsecured devices to a network. The solution: equip employees with trusted, non-disruptive and easy-to-use applications.

"You want to make sure the user doesn't even know it's there," said LeMaster. "They just know they're protected unless a compromise is detected on the device, and then it gives the user everything they need to know to take immediate action."

Privacy is another major concern for any employee connecting their personal device with professional tools and networks.



> It's important to adopt trusted solutions that can not only ensure privacy is intact, but also help ensure the agency is enforcing necessary user privacy — checking to see if data is being harvested off of the device,"
>
> Tim LeMaster | *Director of Systems Engineering,* Lookout

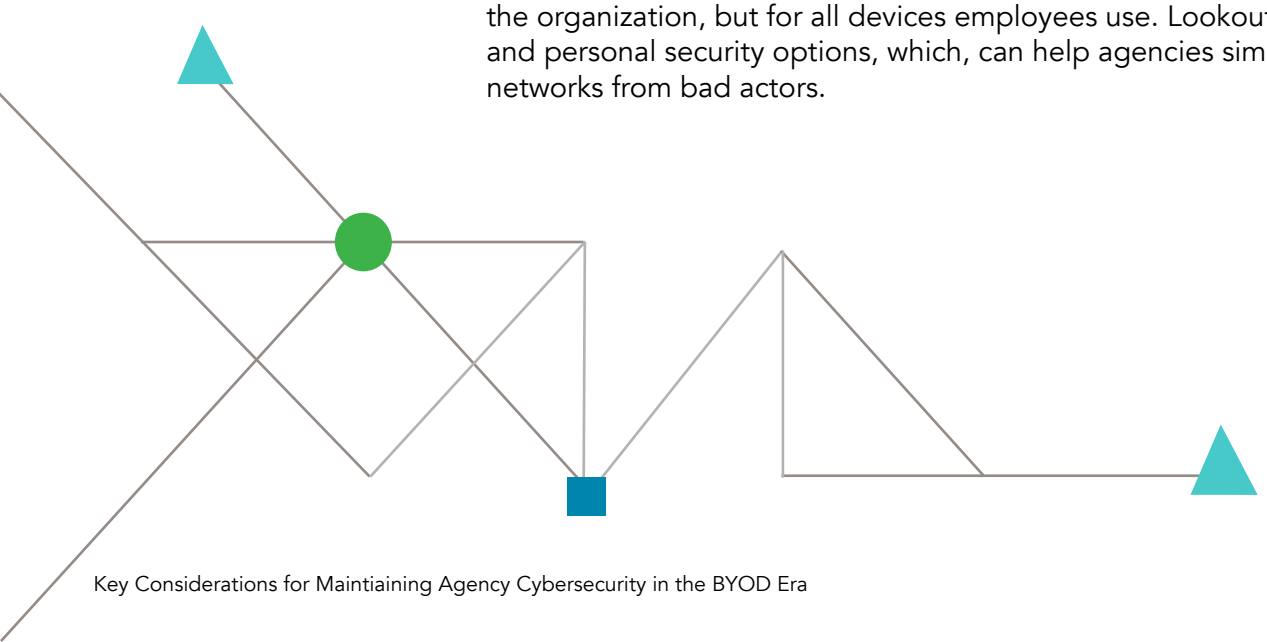
3. Agencies need the right tools to protect mobile endpoints

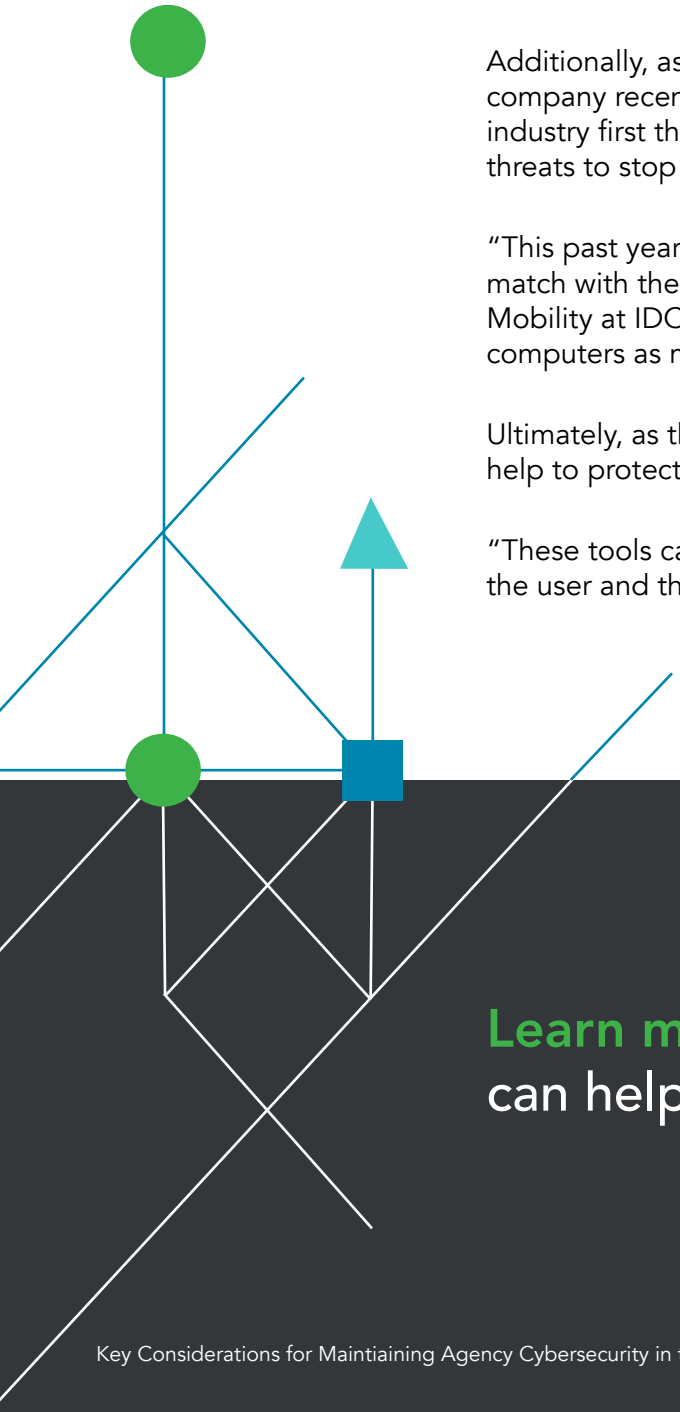
Ultimately, as personal devices and networks enter the picture alongside government-distributed ones — all of which live outside typical in-house security perimeters — it's become increasingly important for agencies to work with industry to implement controls that can keep government and constituent data safe on any device. Lookout has worked to create a suite of solutions that both agency security teams and users can trust. Not to mention that the tools that make up the **Lookout Security Platform** are specifically built to ensure they don't impede user productivity.

Lookout's **Modern Endpoint Protection** solution, for example, helps to monitor possible security threats for remote users, conducting near real-time analytics on a device and working in tandem with a mobile device management system to spot, alert and take action against suspicious behavior.

"If an employee downloads an application, Lookout Modern Endpoint Protection analyzes the application, determines if there is some risky behavior taking place with the app — like sending data to a suspicious foreign country — and the MDM can then take action, potentially blacklisting the app or turning off the users access to government networks until they take necessary action," explains LeMaster.

Moreover, with BYOD policies on the rise, agencies need to consider these solutions not just for devices issued by the organization, but for all devices employees use. Lookout's mobile security solution offers both enterprise-wide and personal security options, which, can help agencies simplify their security portfolios as they seek to protect networks from bad actors.





Additionally, as cyberattacks become more sophisticated, security tools must keep pace. In response to this, the company recently launched a comprehensive mobile **endpoint detection and response** (EDR) solution — an industry first that aims to arm organizations with the tools and info they need to conduct their own research and hunt threats to stop data breaches.

"This past year, we have seen organizations of all sizes and industries struggle to ensure their security protocols match with the unique needs of their remote workforce," said Phil Hochmuth, program vice president of Enterprise Mobility at IDC in a **press release**. "It is no longer sufficient to only have activity monitoring for desktop and laptop computers as mobile devices have become a primary tool employees use to stay productive away from the office."

Ultimately, as the workplace evolves, security must evolve alongside it. By adopting right security tools, agencies can help to protect endpoints and mitigate cyberattacks, even as they become more sophisticated.

"These tools can actually help improve privacy for users on their personal device while enhancing security for both the user and the agency without sacrificing the user experience," said LeMaster. "It's a win-win."

Learn more about how the Lookout Security Platform can help to keep your agency secure.