Governments Are Concerned About TikTok.

They Need to Think Bigger

The Federal government and numerous states have banned employees from using TikTok on government-owned devices over concerns that user data could be accessed by foreign governments. In a recent interview with MeriTalk, Kristina Balaam, senior security intelligence engineer, and Frank Johnson, vice president of U.S. Federal at endpoint-to-cloud data security provider Lookout, discussed the Federal ban, how IT teams can identify risky apps, and why governments should be concerned about more than TikTok.

MeriTalk: The Federal ban on use of TikTok on government devices became law in December, as we know, and in late February, OMB memo M-23-13 provided guidance to agencies on how to remove TikTok from agency devices. They had up until March 29 to get this done. How big was this job, and was that enough time?

Balaam: If agencies had mobile device management (MDM), removing the TikTok app itself from agency devices by the deadline would be a relatively smooth process. But if agencies were relying on a manual process and had a large number of employees or devices, it seems like a pretty monumental task.

In any event, an MDM is just as its name implies. It manages the devices, but a more comprehensive approach is required to actively detect threats and diagnose vulnerabilities on mobile devices. Monitoring of application network activity for things like suspicious apps, adversary in the middle attacks, and data exfiltration come to mind.

Johnson: I agree. If agencies did not have a centrally managed MDM, they had to procure one and stand it up; there's no way that can be done in 30 days.

After 90 days, the ban applies to all new contracts – I interpret that as all prime contractors and their subcontractors. It's possible to see guidance in the future across the 16 regulated industry sectors that are designated as critical infrastructure by the Cybersecurity and Infrastructure Security Agency. This is just the start of efforts to make it harder for nation-state enemies to get access to our app data.

I must note, though, that far too many people are interpreting M-23-13 as "all I need to do is get TikTok off the phone." But TikTok is just the tip of the iceberg. Millions of connected devices, databases, and apps are sending mountains of data from West to East every day. All of that risk needs to be visually detected and controlled.

MeriTalk: Let's take a step back and talk about the concern that the TikTok app raises. The apps we use collect all sorts of data, much of which is used to improve the user experience. What is different about TikTok?

Balaam: The big difference is that TikTok is owned by a parent company, ByteDance, which is based in China. Chinese law allows for many exceptions to data privacy protections if the Chinese government decides it wants to access data that's being collected by private companies. That has led to a lot of concern about how TikTok data is being collected and used. TikTok collects personal information that could be used to build profiles with things like user interests, sexual orientation, and relationship status. Those profiles could be used in influence campaigns designed to push certain types of content – content that could influence political leanings and elections, for example. That capability, combined with the staggering popularity of TikTok – 150 million users over age 18 in the United States alone – concerns policymakers.

Johnson: Some people will say, "Well, other social media apps do just the same thing that TikTok does." There is one huge difference. Those other social media platforms are U.S.-based companies, with data stored in the United States, accessed by U.S. citizens. TikTok is not.

MeriTalk: What do you make of ByteDance's congressional testimony that TikTok's data on U.S. users is stored on American soil, by an American company, and overseen by American personnel?

Johnson: It's not good enough. This is about access and control. Databases can be accessed from anywhere. There is no way they can prove that no one who is a Chinese national or works for the Chinese government has access to that data.

MeriTalk: Big picture, what's the potential universe of risky apps?

Balaam: It's big. For example, more than 9 million apps identified in the Lookout data corpus communicate with IPs, domains, or servers in China.

Even within official app stores, some apps are requesting way more permissions than should be granted. Many free apps have extensive advertising software development kits (SDKs) that collect information about user interactions with the app or with the device, and that data helps build a profile on the kinds of advertising that might be relevant to that user. Many popular SDKs are coming out of China. We need to be concerned about where that data is going, how it's being used, and who might have access to it.

Johnson: It's not just apps. It's millions of connected devices, infrastructures, databases, access control, and cloud, too. The good news is that we're highly aware now. It's about time.

MeriTalk: Thinking about apps specifically, how should agency IT teams go about identifying them?

Balaam: We know that apps from legitimate stores, like Google Play and the Apple Store, go through a stringent vetting process. Usually, unnecessary permissions are flagged, and the developers have to explain why they've asked for them.

But – especially in the case of Android devices – users can sideload apps. That means installing an app that isn't from an official app store. These unofficial apps are one of the biggest things that IT teams need to identify, because typically those apps aren't vetted as extensively. A lot of the threats that our threat intel team sees, especially from nation-state actors, come from third-party sources.

This is how they do it: The user gets a message saying, "Install this version of WhatsApp that's more secure," or they're directed to a third-party app store that is littered with malware. A policy that enforces a ban on sideloading is important. IT teams can take it a step further and limit the apps installed on a device to those that are necessary for work, and they can restrict the sources of those apps to long-time developers with good reputations and no ties to countries with questionable data privacy laws.

MeriTalk: Hybrid work comes with the use of non-government networks and devices. How can agency IT teams prevent the use of risky apps on personal devices and outside the traditional office?

Johnson: This is a huge area of vulnerability and a tough issue for any IT department, public or private, and for users. People want to have access to critical data, apps, and infrastructures so that they can work wherever they want or need to be. One solution is to provide everybody with a government-supplied phone enabled with security protections and controls. There is a huge cost associated with that, and it forces everyone to carry two phones.

Another solution is bring your own device (BYOD), where an organization loads its mobile endpoint security onto the employee's personal device and can isolate that device from the network if nefarious activity is observed. Traditional MDMs only give the organization a basic level of policy-based controls.

MeriTalk: What do agency IT teams need to really see the apps employees are using and determine whether those apps are okay or not okay?

Balaam: They need MDM to restrict certain apps on government-owned devices or on devices that are part of a BYOD program. They need a mobile endpoint detection and response (EDR) product to provide insight into apps on the device that are flagged as either suspicious or malicious. Mobile EDR comes with mobile threat defense capabilities, so you know whether the device has been jailbroken or rooted, meaning that an app can circumvent security policies. You can see whether a certain advertising SDK is being used and whether an app might have a vulnerability or is out of date.

You can also implement policies that dictate how the mobile devices that are accessing corporate or government networks and data are able to interact with potentially risky apps and servers in a country with less stringent or non-existent data privacy laws. For example, you can write a policy that says,

“Prevent any traffic leaving the mobile device from reaching servers with a top-level domain of .cn,” which is a Chinese-owned web domain. Or you can say, “Restrict this traffic from reaching this particular IP address if it’s associated with the older versions of TikTok.”

Johnson: The growing remote workforce is creating a surging need for complete visibility into the entire landscape of mobile threats. The combination of MDM and mobile EDR is vitally important. Lookout is the only U.S.-based, pure play mobile defense company built by U.S. citizens, managed by U.S. citizens, deployed by U.S. citizens, and accessed by U.S. citizens. No one else checks all those boxes.

MeriTalk: How does Lookout help government agencies remove or otherwise block risky apps from both government or devices and personal places?

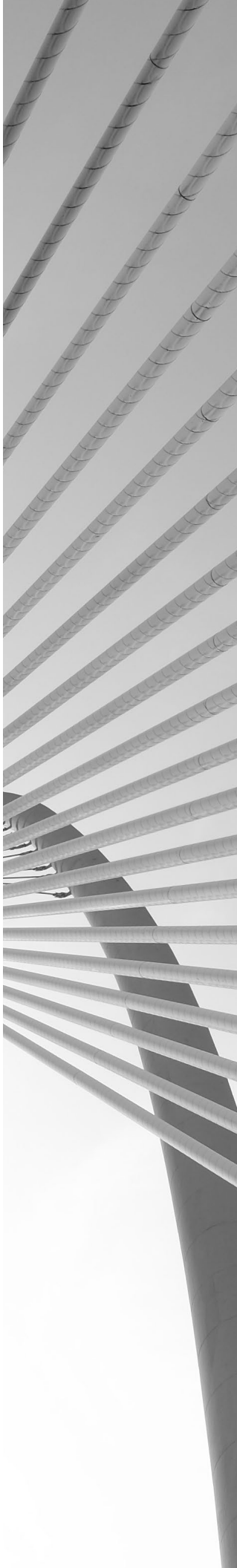
Balaam: Lookout enables agencies not only to restrict certain apps on mobile devices, but also to detect threats on mobile devices and defend them. Our safeguards alert users when their devices have shifted into a less secure state, and we take measures to ensure that the data is safe.

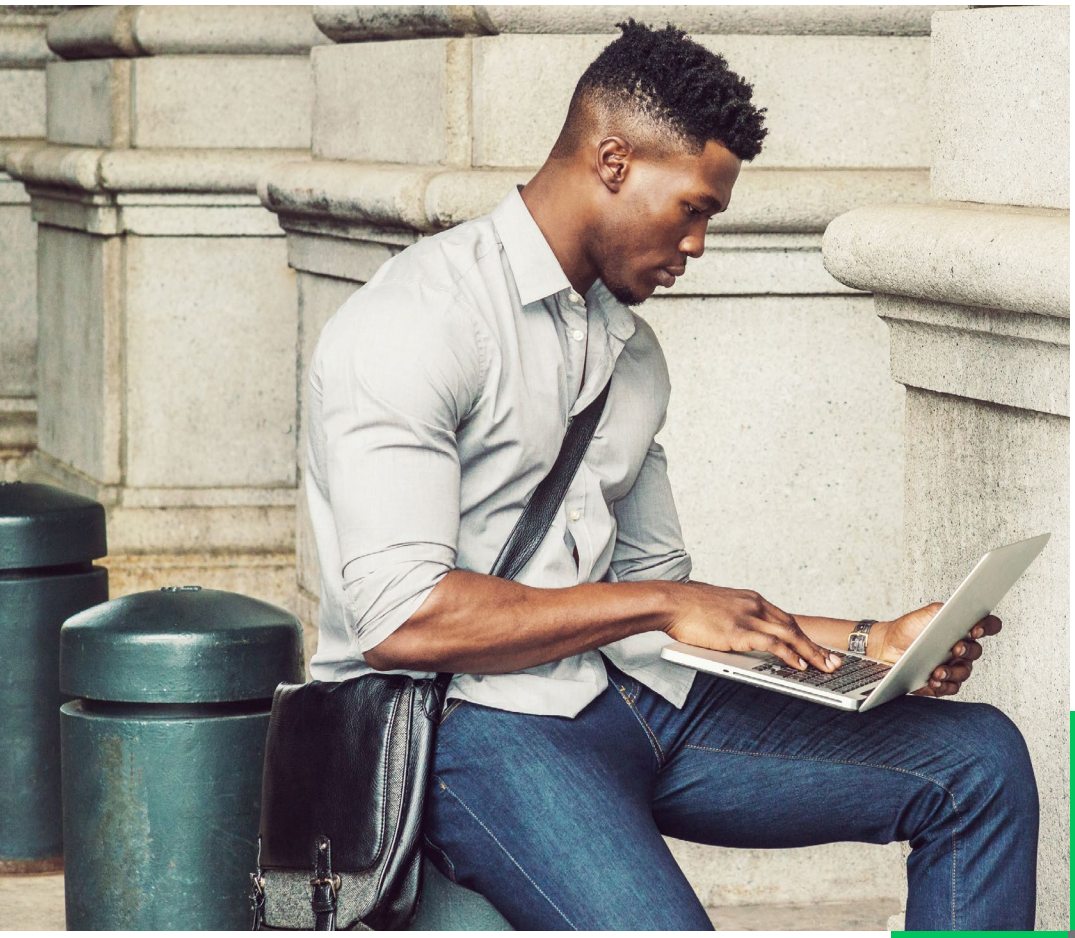
Lookout allows agencies to implement the policies we just talked about – to limit certain interactions with servers that are part of the .cn top-level domain, or with a particular IP address or domain name. Our product can be used on agency devices and on personal devices, as long as the individual installed Lookout on their personal phone and it is registered as part of the agency’s tenant.

MeriTalk: How does Lookout’s approach differ from other security providers?

Balaam: We have been in the mobile threat defense game a very long time. Our dataset is extensive, and so it provides a lot more visibility into mobile threats than other security providers. If you encounter an app or a malware family that has never been seen before, you rely on the platform provider’s ability to recognize vulnerabilities in your device, rather than its knowledge that a particular app is malicious. If you’re looking at a security provider that doesn’t have the same kind of data that we do, their visibility into the threats is a lot more limited, and their mobile threat defense platform might be a lot more limited as well.

Johnson: Here’s an example of what we can do. Our threat intel team, of which Kristina is a member –recently confirmed that Pinduoduo, a very popular Chinese ecommerce app, contained a zero-day exploit that allowed it to compromise Android devices. This app, distributed on third-party app stores, exploits vulnerabilities to gain privileged access on users’ operating systems and install apps, grant permissions without user interaction, remove apps from devices, make it impossible for users to remove certain apps, infect third-party apps present on the device with malicious code, and access and manipulate data that is private to third-party apps. While TikTok is in the news because of its popularity, Lookout threat intel found an app that can exploit American citizens through a zero-day attack today. This is a vivid example of why our governments and citizens should be concerned.





MeriTalk
Improving the Outcomes of Government IT

Learn more about how Lookout can help your agency protect data from adversarial nation states:

Schedule a demo | Contact Sales

Lookout