How to Manage Risk at the Mobile Endpoint

govloop

Lookout®

Executive Summary

Where users go, threats will follow. So it comes as no surprise that the widespread use of mobile devices in the workplace, whether agency-issued or employee-owned, has caused a spike in mobile threats. It's a big spike, too. According to Lookout research, more than half of personal mobile devices were hit by phishing attacks in 2022. More than 30% of personal and enterprise users faced attacks in each quarter of that year.

The problem is, many agencies still rely on legacy mobile device management (MDM) and antivirus tools, leaving mobile users vulnerable to gaps in application, device and network protections. So the increase in attacks caught those agencies off guard.

That's why all government agencies now face mandates to secure their devices via a comprehensive mobile endpoint protection and response (EDR) program.

To help with EDR implementation, GovLoop partnered with data protection and cloud security provider Lookout for this playbook, which:

- ► Describes the challenges all agencies face
- ► Details the five essential areas of mobile security
- ► Offers examples of how EDR works
- ► Explores the importance of threat intelligence

Need to Know

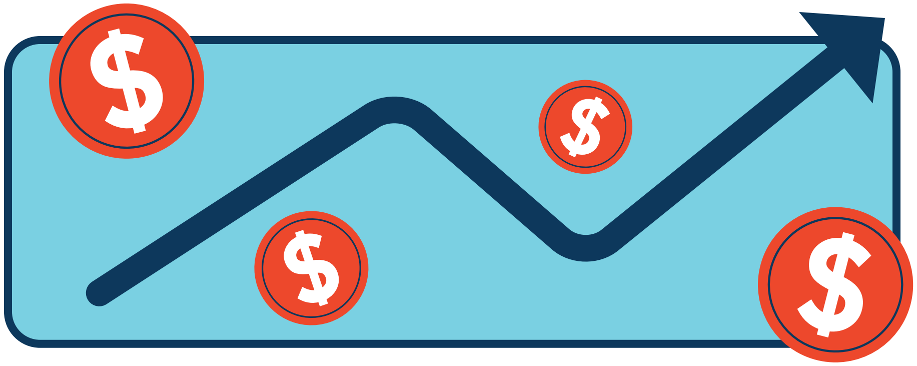
Protect People, Devices and Privacy

In May 2021, the White House **Executive Order** on cybersecurity ordered civilian agencies to implement **endpoint protection and response** programs and **emphasized the need** for "special consideration for mobile devices ... due to their technological evolution and ubiquitous use."

The mandate from that order is clear: Government agencies must improve mobile device security to protect their constituents' privacy.

And that's not the only way the federal government is addressing the issue. The American Data Privacy and Protection Act (ADPPA), which would be the first national data privacy law, has been **reintroduced in Congress**. The bipartisan, bicameral bill was approved by the Committee on Energy and Commerce in July 2022 by a 53-2 vote, but never got to the floor of the House or Senate.

State governments are also at work. **New privacy laws** focused on the use of personal information collected by businesses and other organizations are set to take effect this year in California, Colorado, Connecticut, Virginia and Utah.



Beware of Rising Cyber Insurance Costs

As attacks have surged, organizations have turned to cyber insurance to offset financial risks.

By 2022, 80% of state and local governments had purchased coverage against ransomware attacks, according to Sophos' **State of Ransomware in State and Local Governments 2022** report.

Between the spike in demand and the costs of payouts to attack victims, the price of that insurance has, predictably, jumped. According to **Fitch Ratings, the increase for standalone coverage was up**:

- 91% in 2021
- 62% in 2022

While the price of premiums has settled somewhat, getting cyber insurance at all can be difficult for organizations that don't have effective security controls in place. Among those state and local governments, 96% say they upgraded their cyber defenses to lower the costs of premiums and secure coverage.

Cost isn't the only issue. Some insurance is simply no longer available. For instance, in March 2023, Lloyd's of London **stopped coverage** in its policies for nation-state cyberattacks, due to their potential severity.

8 Gaps in Mobile Device Management

MDM isn’t perfect. Here’s where it can fall short compared with a more advanced EDR approach.

1 **No phishing protection:** MDM doesn’t protect against malicious URLs from email, SMS texts, browsers and social media apps and websites that don’t encrypt login credentials or leak data.

2 **No app protection:** MDM doesn’t defend against malicious apps, such as surveillanceware, adware and riskware that can gain unauthorized remote access and steal or leak information. Nor does it offset the risk posed by non-malicious apps with inherent vulnerabilities or risky behaviors.

3 **Poor privacy protection:** Many MDM tools allow employers to monitor all device activity, with no privacy settings to protect users.

4 **Poor protection against network attacks:** MDM is insufficient against threats that exploit weaknesses in how websites or apps establish TLS/SSL connections over Wi-Fi, cellular and other networks.

5 **No threat notification:** MDM can’t detect mobile security events.

6 **Can’t detect root/jailbreaks in real time:** Operating system (OS) exploits, which are particularly effective in the gap between patches and upgrades, can be used to elevate permissions. Side-loaded apps can also introduce threats. MDM is not sufficient protection against them.

7 **Insufficient adaptive access:** MDM provides some protection when high-risk mobile devices –– which may contain viruses, malware and vulnerabilities –– attempt to access corporate devices. But it needs help to enact policies to prevent authentication.

8 **No threat remediation:** MDM can wipe devices but does not provide threat detection or self-remediation.

Know the Numbers

More than 50% of personal devices were hit by phishing attacks in 2022.

Source: Lookout Global State of Mobile Phishing

More than 30% of personal and enterprise users were attacked per quarter in 2022.

Source: Lookout Global State of Mobile Phishing

A 625% increase in voice phishing (vishing), SMS phishing (smishing) and QR code phishing (quishing) took place in the second quarter of 2022.

Source: KnowBe4

Nearly $4 million is the estimated cost of a successful mobile phishing attack on an organization of 5,000 employees, based on the Factor Analysis of Information Risk (FAIR) model.

Source: Lookout Global State of Mobile Phishing

Top 6 Mobile Phishing Targets in 2022

1. Insurance (34.5%)
2. Banking (34.1%)
3. Legal (31.7%)
4. Health care (31.2%)
5. Financial services (30.3%)
6. Government (27.9%)

Source:
Lookout Global State of Mobile Phishing

The Playbook: 5 Essential Areas of Mobile Security

The vast majority of all cyberattacks — 91% — start with phishing, and as seen in the data points above, threat actors are increasingly aiming those attacks at mobile devices.

"It's the easiest way in," said Joe Wall, Vice President of Risk Partners for Lookout. "And it's the easiest way in because typically there's no protection on that device, and there's no visibility from an organizational standpoint."

To counter the threat, public sector agencies must address five key areas of mobile device security.

1

Mobile EDR

You can't secure smartphones and other handhelds the same way you secure desktops, laptops or servers. Mobile devices overlap employees' personal and professional lives. And they're, well, mobile. They connect via cellular service, Wi-Fi and Bluetooth. Workers use them for everything from SMS messaging and social media to scanning QR codes. That's why, unlike typical scams, **87% of mobile phishing attacks** occur via something other than email.

So it stands to reason that securing mobile devices doesn't fall within traditional network security processes — or the MDM programs agencies use. In particular, MDM lacks visibility into zero-day threats or other attacks happening on a device and doesn't provide the ability to respond while attacks are underway.

"MDM is great for managing devices," Wall said. "It's nonexistent for protecting a device."

The cloud-native solution is mobile EDR, which extends to mobile devices the traditional EDR that protects laptops, desktops and servers.

Mobile EDR delivers visibility into personal and agency-owned devices connecting to the network and real-time telemetry on the full range of mobile threats. Whether they're running iOS, Android or ChromeOS, it mitigates the risks of compromise while protecting user privacy.

2

Mobile Endpoint Protection

Most agencies have visibility into desktop and laptop apps, but they can be blind to how mobile devices are handling data.

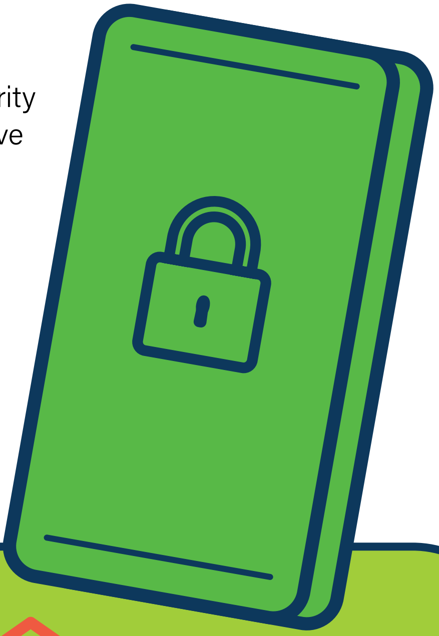
Think of each mobile device as a remote office, often connecting via public networks and packed with personal and agency information attackers can exploit to gain access to the network.

Endpoint protections must secure the device, its software and its access to the network, and protect the agency and user all while integrating with the agency's zero-trust architecture and complying with privacy regulations.

Moving toward **zero trust** is essential. It's part of the federal mandates for improving cybersecurity, which state and local governments follow. Zero trust recognizes that the cloud, edge computing and the Internet of Things have extended agency networks far beyond traditional network perimeters. It focuses on continual authentication and authorization of every user, device and service accessing a network.

In addition to enhancing data protection and ensuring secure access to public and private clouds, zero trust also greatly simplifies security for BYOD devices. It's part of a comprehensive mobile endpoint protection solution that:

- Manages risks and identify threats in real time
- Provides insights into app permissions and data access controls
- Ensures a device's multifactor authentication (MFA) isn't compromised



3

Mobile Risk and Compliance

To ensure effective risk management and compliance with government mandates, a mobile EDR strategy must not only secure mobile devices but also integrate with an agency's overall security architecture.

Just remember: Mobile EDR should complement MDM programs, not replace them. As Wall puts it, EDR needs to address app and device threats, authentication and other factors while MDM handles basic management functions, such as wiping a device that is lost or stolen.

Integration enables organizations to aggregate threat intelligence and optimize risk management. For example, a mobile security platform integrated with security information and event management (SIEM) systems, with MDM or unified endpoint management (UEM), effectively manages laptops and desktops as well as mobile devices.

A mobile EDR solution also can help agencies comply with critical security and privacy requirements, such as those from the **National Institute of Standards and Technology** and the **Office of Management and Budget**, and seamlessly enforce single requirements, such as the federal ban on TikTok.

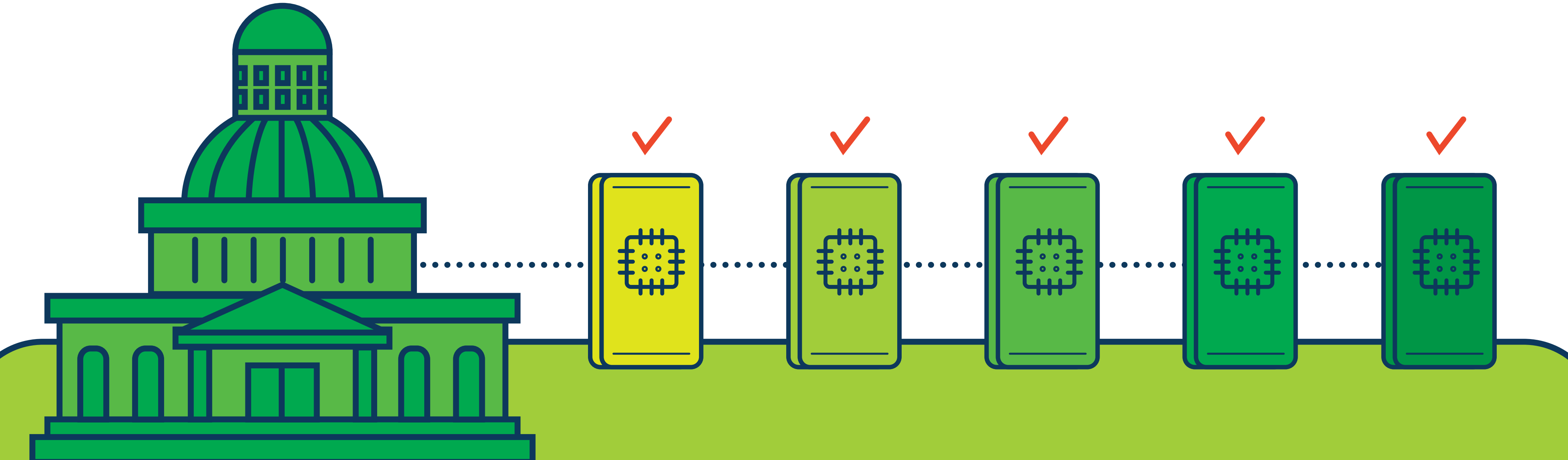
4

Mobile Vulnerability and Patch Management

Desktops and servers are managed devices connected to office networks. They give IT teams a common image to patch. The prime target: an unpatched server.

Delivering upgrades and security patches to mobile devices is more complicated. MDM can ensure a minimum version of an OS is running on a device. But it can't provide complete coverage for software running on unmanaged personal smartphones and tablets that are connecting via Wi-Fi and cellular networks. That requires comprehensive, scalable endpoint security that gives teams consolidated control over devices.

"You need to have one pane of glass, and one view of your devices," Wall said. "You need that not only from a vulnerability standpoint, but also knowing what OS each device is on and whether they need to update or apply patches."



5

Phishing and Content Protection

Phishing is a component of more than 90% of cyberattacks. Phishing sites are constantly changing, with more than 1.5 million sites created each month. Some operate for only a few hours before being dismantled. Anti-phishing solutions that operate from a list of known phishing domains and websites aren't sufficient to address the threats.

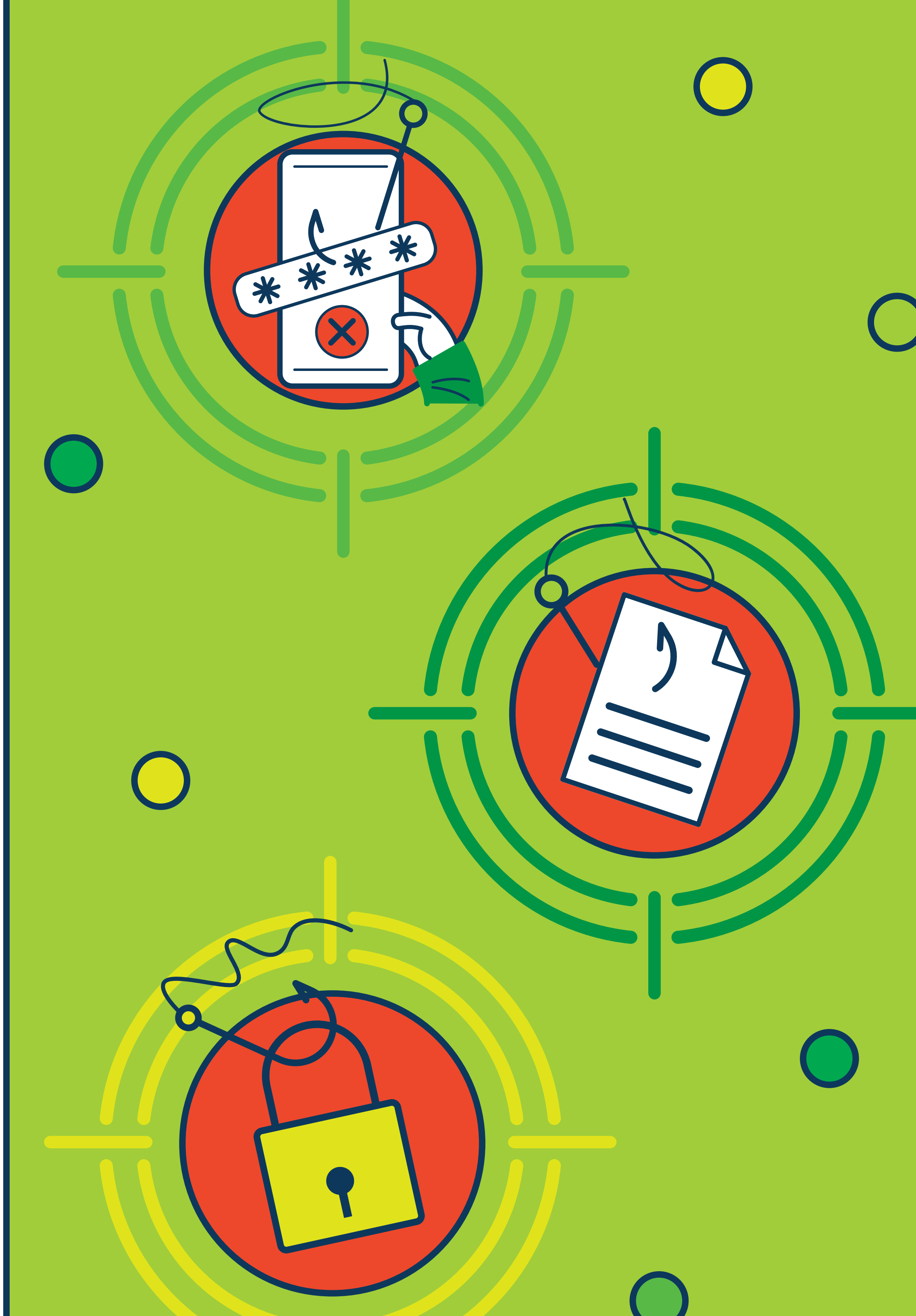
"This is a landscape that's growing very, very quickly," Wall said.

A comprehensive mobile EDR platform can give agencies effective prevention, and real-time detection and response to this ever-evolving threat.

It's no longer enough to simply inspect email content for threats. That misses all the other ways cybercriminals send phishing links, including via SMS messages or QR codes. Traditional anti-phishing efforts also lead to privacy concerns, since mobile devices are considered personal regardless of who owns them.

To keep pace with that threat landscape, agencies need mobile security powered by artificial intelligence (AI). Such solutions scour the internet for threat intelligence on phishing, malware and ransomware, providing proactive protection against those threats.

"You take the largest datasets on mobile threats, apply AI and machine learning, and quickly identify patterns and malware as they start to happen," Wall said. "And then you quickly respond to that."



3 Use Cases for Mobile Endpoint Control

Given the ubiquity of mobile devices and the sheer effort threat actors put into compromising them, all agencies require a comprehensive, in-depth approach to protecting devices, apps and data. An integrated, cloud-native approach provides the needed comprehensive visibility and control without infringing on privacy. Here are three ways Lookout's solution helps agencies protect against obvious and hidden threats.

1. Blocking TikTok or Other Apps

Early in 2023, the federal government moved to **ban the popular video-sharing app TikTok** from government phones, over fears the company's Chinese owners would allow their government to spy on U.S. users or spread propaganda and misinformation. Other countries, including Canada and those in the European Union, have taken similar steps. India banned TikTok in 2020.

Lookout offers two straightforward approaches for U.S. agencies that need to enforce the ban.

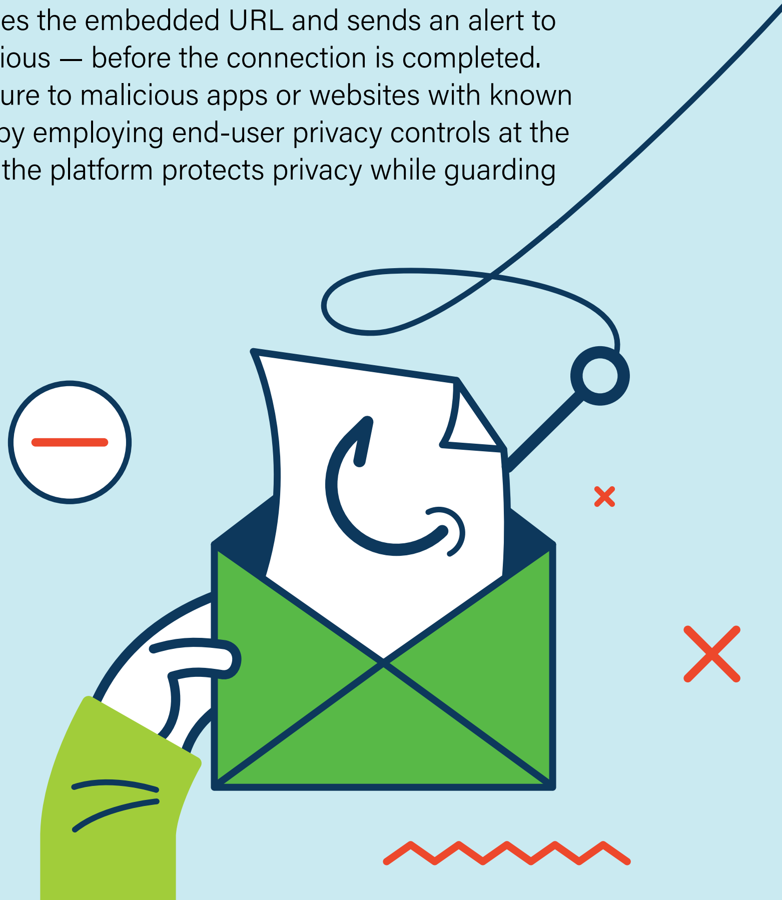
The first uses app identification and access control. Via Lookout Mobile Endpoint Security and an MDM solution, an administrator simply gets the application URL from the Apple Store or Google Play, and then adds the TikTok app to the deny list. If the app is detected on a device, the agency can flag it for non-compliance and block access to customer domains, single sign-on, enterprise apps and data. The user would have to remove TikTok to regain access to the organization's resources.

In the second approach, the admin blocks TikTok by identifying and denying the appropriate root domains. End users are notified, and access is denied.

2. Protecting Devices From Hidden Threats

Today, attackers can send phishing links via any iOS, Android or ChromeOS apps –– from email and social media to messaging, gaming and even a phone's camera. And they're growing more inventive, even hiding invisible malicious links inside QR codes.

As users click on links or scan codes, Lookout Phishing and Content Protection first verifies the embedded URL and sends an alert to the user if it is malicious — before the connection is completed. This prevents exposure to malicious apps or websites with known vulnerabilities. And by employing end-user privacy controls at the moment of contact, the platform protects privacy while guarding against the attack.



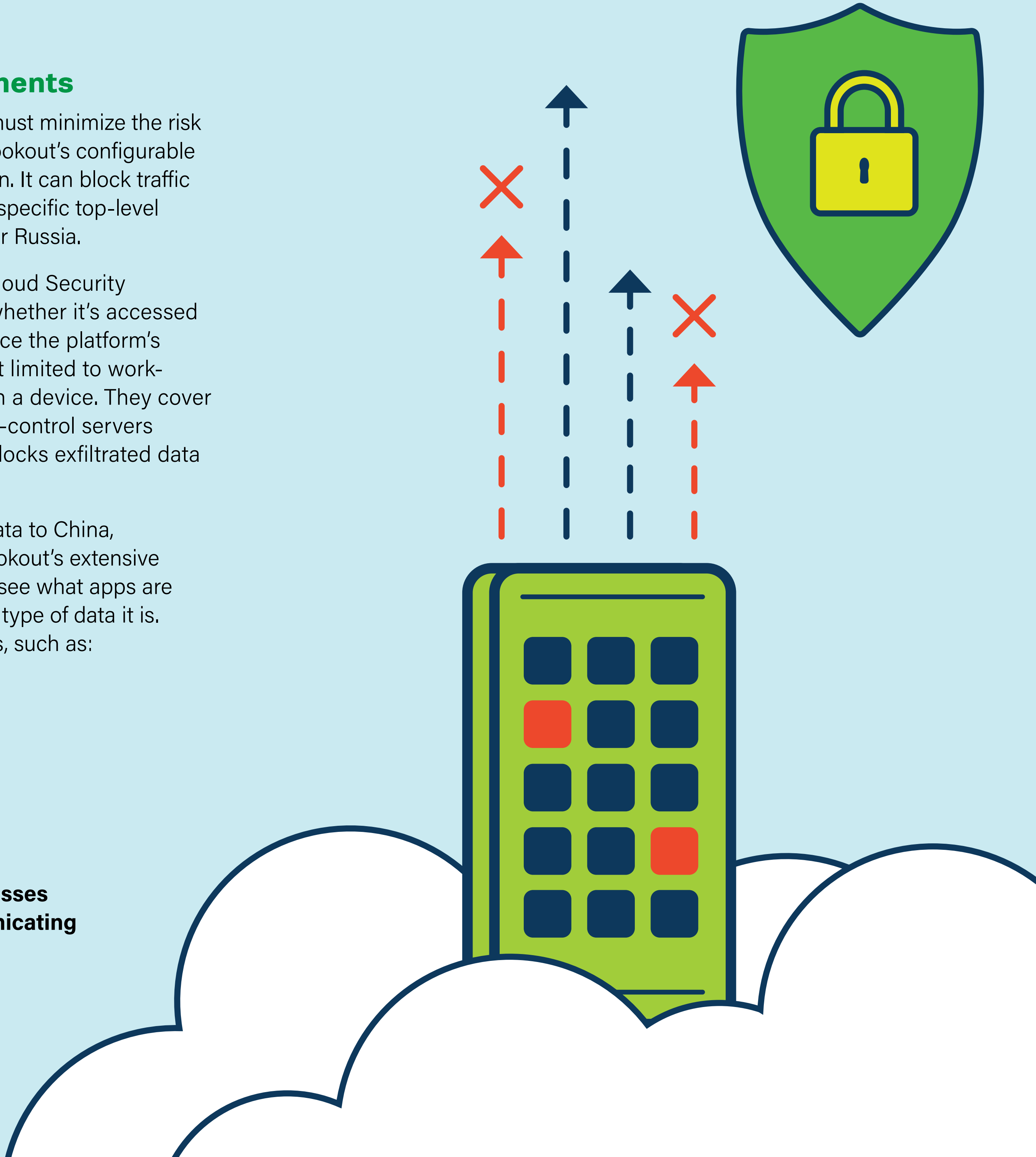
3. Blocking Adversarial Governments

In addition to targeting specific apps, agencies must minimize the risk of sharing data with adversaries. That's where Lookout's configurable Phishing and Content Protection engine comes in. It can block traffic with apps, domains and IP addresses, including specific top-level domains such as .cn for China, .ir for Iran or .ru for Russia.

For example, admins can rely on the Lookout Cloud Security Platform to block any domain that ends in .cn, whether it's accessed from a browser or from within a mobile app. Since the platform's policies are defined at the DNS level, they aren't limited to work-related apps or links, but extend to every app on a device. They cover API traffic or communications to command-and-control servers within that domain, so the platform effectively blocks exfiltrated data from being sent to an adversary.

With more than 9 million mobile apps sending data to China, monitoring traffic is a monumental challenge. Lookout's extensive repository of security telemetry makes it easy to see what apps are sending data to another country, as well as what type of data it is. Admins can analyze those apps for deep insights, such as:

- **The code libraries they use**
- **The data they can access**
- **The URLs, domains and IP addresses with which the apps are communicating**



Lookout®

Is Your Agency's Mobile Device Data at Risk?

The Lookout Mobile Risk Assessment helps government understand their risk based on mobile data access, existing controls such as EMM, and the resulting security gaps. Learn how to minimize risk to mission-critical data regardless of where it's stored or how it's being accessed.

Try our Free Mobile Risk Assessment

bit.ly/3CRZQ6H

Lookout Mobile Endpoint Security is FedRAMP and StateRAMP JAB P-ATO Authorized

AUTHORIZED & JAB StateRAMP

FedRAMP™

How Threat Intelligence Enables Real-Time Response

Until now, government agencies have tended to overlook the collection and analysis of threat data to protect against these mobile threats. That needs to change.

Think of it as untapped brain power.

"We're seeing a very evolving mobile threat landscape, which requires real-time analysis and proactive action before the attack occurs," said Wall. "We're seeing a steady increase of malware and malicious apps growing more sophisticated in how they target Android and iOS vulnerabilities to steal sensitive data and gain access to perform unauthorized functions at organizations."

> **"We're seeing a very evolving mobile threat landscape, which requires real-time analysis and proactive action before the attack occurs."**
>
> — Joe Wall, Lookout

Evolving to Meet the Threat

Threat intelligence collects, processes and analyzes vast amounts of data on attacks to determine motives, preferred targets and typical attacker behaviors.

For example, Lookout builds mobile threat datasets by:

- **Conducting continuous, automated threat hunting**
- **Combining the resulting data with incident reports from firms around the globe**
- **Applying steps such as mobile forensics to reveal how an attack got started**

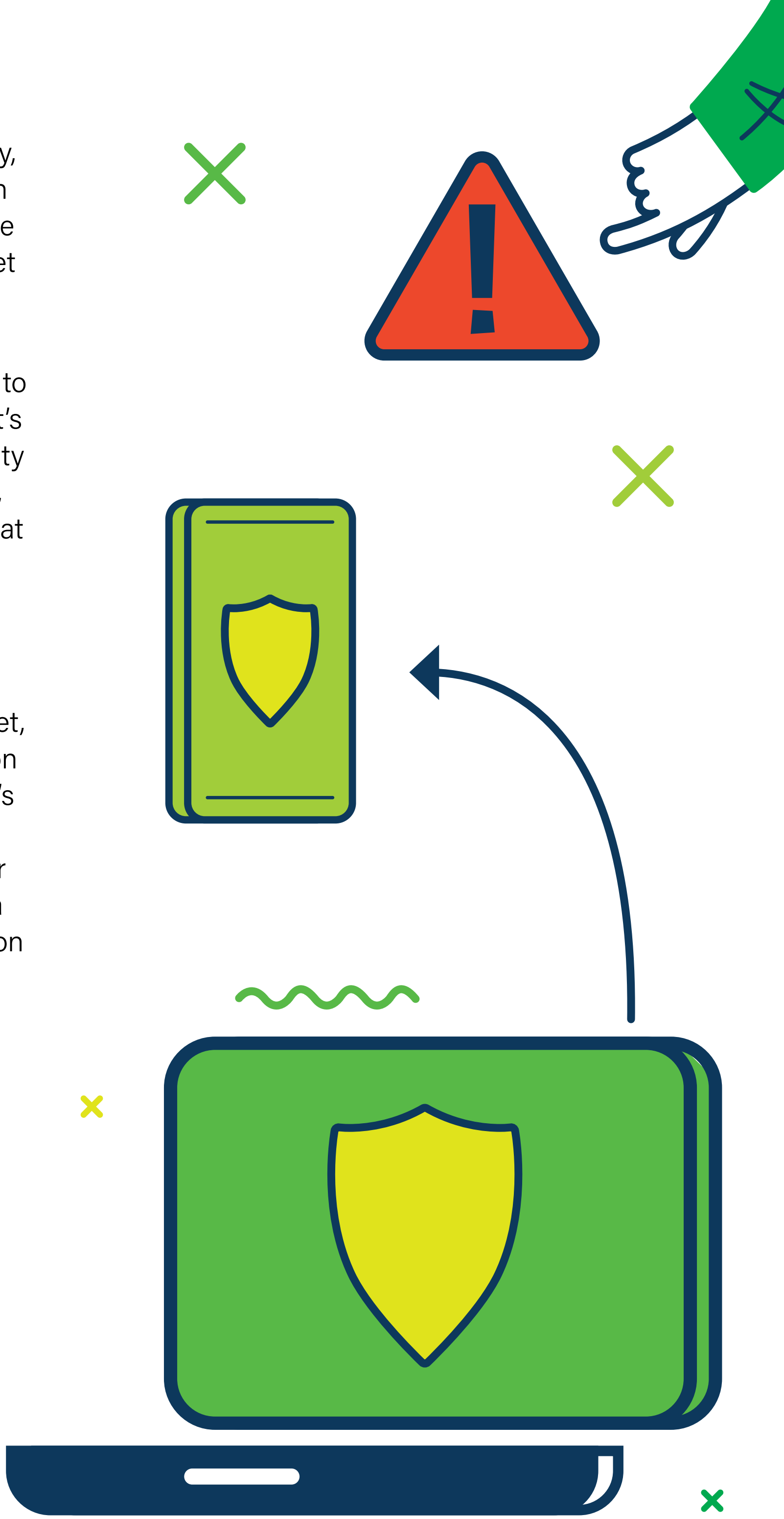
A mobile EDR platform bolstered by such intelligence has vital context and insights on the motives and techniques threat actors are using. This enables agencies to be proactive, so they can stop attacks in real time, before the attackers get through.

Artificial intelligence and machine learning (ML) also play critical roles in threat intelligence. Applying AI and ML to a large dataset can also help identify patterns in malware as they occur, enabling a quick response. "It really boils down to speed and delivering what's best for the customer, by utilizing AI and ML with the dataset," Wall said.

Delivering threat intelligence should be easy, and it is. Agency customers can receive it in a few ways, including via dashboards, where admins can view reports. Plus, users can get updates on their devices via a mobile app.

It's all about extending endpoint protection to every device on an agency's network. "That's No. 1: providing some protection and visibility to the mobile device," Wall said. "Otherwise, you're flying blind if you don't have any threat intelligence to back up what you're seeing happening at that mobile device."

Lookout has built the world's largest and most comprehensive mobile security dataset, which supports both its Mobile EDR solution and Threat Advisory Service. The company's cloud-native security solution can apply zero-trust practices to any agency device or app, regardless of location. Lookout offers a customized mobile risk assessment based on a **two-minute survey**.



Conclusion

Mobile devices, whether agency-issued or personally owned, are integral to public sector operations because they are inseparable from the employees using them. Threat actors have noticed, making mobile devices a prime target in their efforts to gain access to networks.

MDM is widely used for mobile management, but it doesn't protect devices. Agencies need a comprehensive strategy for mobile endpoint protection that complements MDM and integrates with their overall security strategies. A cloud-native mobile EDR solution can provide the visibility, control and threat intelligence tools required to enable real-time responses. It can help agencies protect devices, data and users' privacy, while maintaining full compliance with all government mandates.

Lookout®

Thank you to Lookout for their support of this valuable resource for public sector professionals.

govloop

About GovLoop

GovLoop's mission is 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 the public sector.

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

www.govloop.com | **@GovLoop**