Lookout Mobile Endpoint Security

Protect the devices that go everywhere you go

Don’t overlook the devices your employees use the most

Traditional cybersecurity strategies have long been focused on protecting your fixed endpoints such as servers, laptops and desktops from cyberthreats. However, your security requirements have grown organically over time.

The problem is security on mobile devices is often overlooked, creating a gap in your security architecture. While mobile operating systems are considered to be more resilient, cyberattackers increasingly target them because mobile devices are at the intersection of our personal and professional life. These devices have a treasure trove of data and attackers use them as the initial intrusion into your organization.

As you evaluate mobile security solutions to add to your architecture, you face a familiar challenge of choosing between a comprehensive platform or best of breed solution. Because the growth in mobile devices has paralleled that of the cloud, an endpoint-to-cloud security solution will remove friction, increase usability and convenience, enable user freedom, and reduce operations cost when compared to a collection of standalone solutions.

Benefits

- Cloud-delivered mobile security
- Protects iOS, Android, and Chrome OS devices
- Endpoint detection and response built by threat researchers
- Lightweight app optimized for processor performance and battery life
- Secures company-owned and employee-owned devices
- Align with compliance requirements while preserving user privacy
- Frictionless deployment on all employee devices
- Scales to mobile fleets of hundreds ofthousands of endpoints

Today more than half of the devices employees use to access your organization’s data run iOS, Android, and Chrome OS.

Mobile has opened new opportunities for cybercriminals

Securing mobile devices is completely different from securing desktops and laptops. Consequently, there are new security requirements introduced by your mobile fleet that you need to address.

Mobile risks need modern endpoint protection

While mobile operating systems are more resilient, cyberattackers increasingly target them because they are at the intersection of our personal and professional lives. iOS, Android, and Chrome OS devices have a treasure trove of data and attackers are targeting them as the initial intrusion point into your business.

A common attack vector uses mobile malware which may include spyware, banking trojans, and rootkits. Malware can be delivered through any of the cellular, Wi-Fi and Bluetooth connections of mobile devices. Once the malware is executed, it undermines the overall safety of the mobile device.

Modern endpoint protection must detect threats in apps, the device, and network connections. It must protect the user, the device and the company while respecting privacy. It must work equally well for employee-owned and company-owned devices.

> "Mobile security has evolved from a tool for highly regulated industries and government agencies to an essential security solution for all organizations,"
>
> - **Phil Hochmuth**, Program Vice President, Enterprise Mobility at IDC.

Don't let mobile phishing be the attacker's entry point

Using traditional anti-phishing approaches on mobile devices quickly becomes a privacy issue because they inspect message content to block attacks. All mobile devices, even if company issued, are considered to be a personal device. And only inspecting email content would miss the other methods used for sending a phishing link to a mobile user.

Most anti-phishing solutions rely on a list of nefarious domains and web addresses. However, over 1.5 million mobile phishing sites are created every month. And most phishing sites are built and dismantled in a matter of hours or days. Solely relying on reputation-based methods to detect a mobile phishing attack is insufficient.

> 1 in 5 enterprise users are phished on mobile quarterly and 87% of mobile phishing attacks occur outside of email.

You need to know the right app and OS versions to patch successfully

Traditional vulnerability and patch management focused on servers, rather than endpoints. This was because desktops and laptops have been managed, used a common image and were regularly patched. Therefore, the primary vulnerability risk had been the unpatched server.

Today, it is only possible to ensure mobile devices run a minimum version of the operating system with mobile device management (MDM). But as employees increasingly use unmanaged personal smartphones and tablets for work, MDM cannot provide complete coverage. Traditional vulnerability management cannot fill this gap since it relies on devices attaching to the office network rather than home Wi-Fi or cellular networks.

> There were more than
> **260 vulnerabilities**
> disclosed for iOS devices in 2023

Mobile needs to be included in your Zero Trust Network Architecture

The freedom that phones and tablets has given us comes with risks. Each of us now represent a remote office network that needs to be secure. As we continue to work outside the reach of legacy perimeter security, there's no guarantee of who or what device you can trust.

Your mobile users are not using VPNs to connect to your organization's data in the cloud. They need access from wherever they are and you need to ensure they don't put your sensitive data at risk. Only low-risk devices should be permitted to access your organization's resources. Once access is granted, continuous assessment of risk enables you to dynamically modify access to protect your data.

"Ecrime threat actors remained the primary threat to most **mobile users** in 2023 and will likely continue as such in 2024."

Source: CrowdStrike Global Threat Report 2024

Prevent breaches with tools to detect and respond to incidents

While many organizations have comprehensive activity monitoring for servers, desktop and laptop computers, what they lack is the same telemetry for iOS, Android, and Chrome OS devices. As employees have increased their use of mobile devices for work, attacks on these devices have increased.

To be effective at stopping data breaches, security teams need the same comprehensive data for mobile devices that they have for servers, desktops and laptops. Because mobile operating systems never permitted kernel access and required apps to operate in isolation, it had been incorrectly assumed that collecting comprehensive telemetry was impossible.

"Executive Order 14028 (EO)...directs the Federal Government to adopt a robust Endpoint Detection and Response (EDR) solution...[for] workstations, mobile phones, servers"

Source: Office of the President OMB M-22-01

Gain better visibility into apps to reduce risk

Most organizations have visibility into how their desktop and laptop applications are handling data, but not for mobile devices. Because of how iOS, Android and Chrome OS run their apps, it is challenging to inspect them. Without such insight, your security team will have no idea how these apps are handling your data.

With managed devices, you have visibility and controls over which apps employees use through mobile device management (MDM) or mobile app management (MAM). But they don't provide you insight into real-time app permissions and data access controls. With personal unmanaged devices you will not even have the limited visibility you get from MDM and MAM.

Mobile security must integrate with your broader security architecture

Some organizations manage their employee's mobile devices with tools like MDM or unified endpoint management (UEM). They also leverage Security Information and Event Management (SIEM) to aggregate threat intelligence. Prebuilt integrations with MDM/UEM and SIEM will enable you to maximize the immediate value from a mobile security solution.

"The mobile security market is all about partnerships, integrations, and ecosystems, rather than best-of- breed threat prevention and remediation (although these core capabilities are certainly important). Look to vendors that have strong partnerships with key channels, such as mobile operators, as well as strong integrations with EMM/SIEM platforms"

- **Phil Hochmuth**, Program Vice President, Enterprise Mobility at IDC.

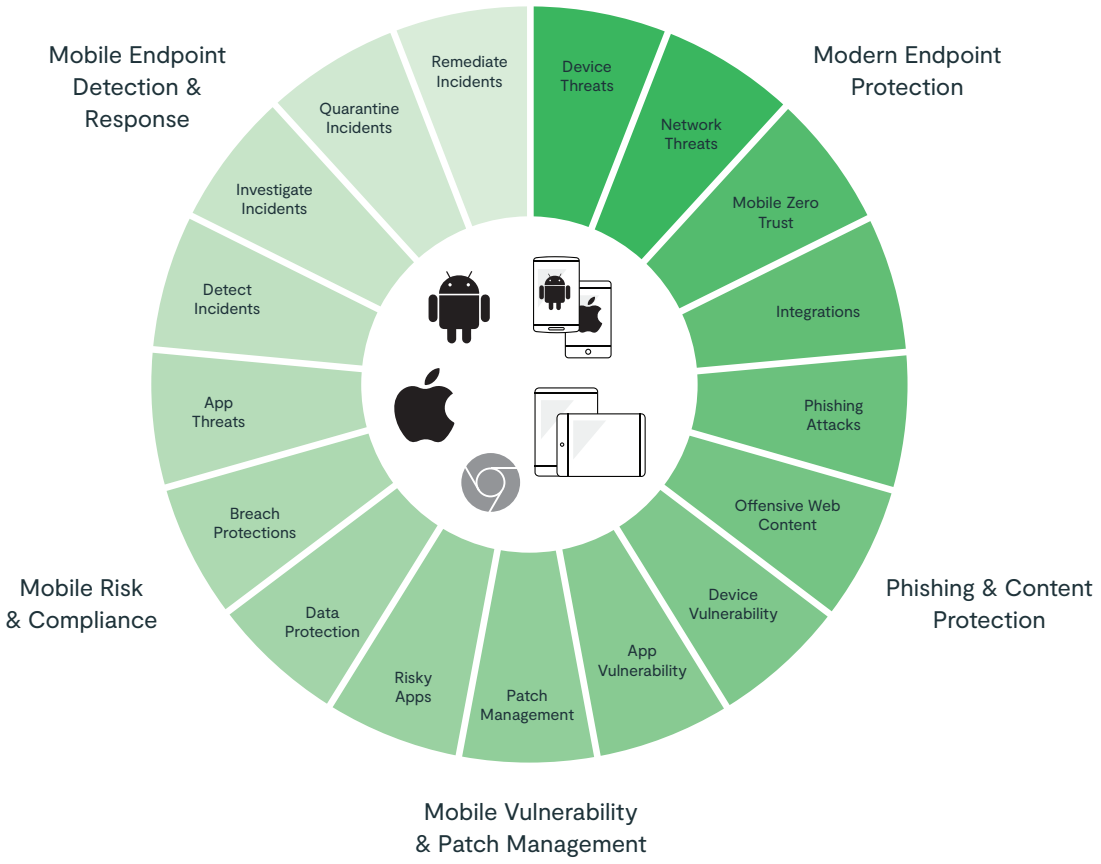
Endpoint security built for mobile from the ground up

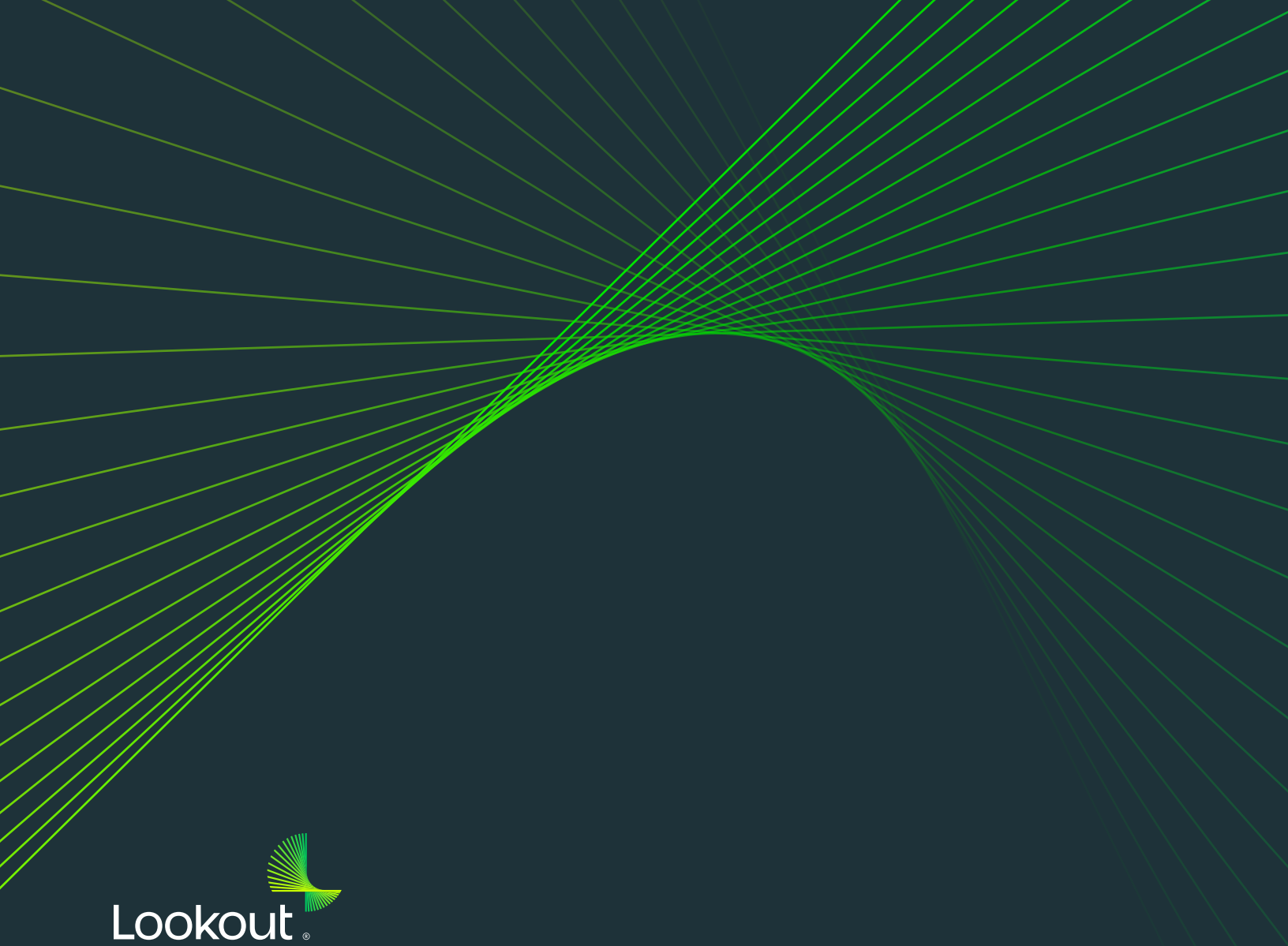
Lookout Mobile Endpoint Security (MES) is architected to address your ever-evolving mobile security requirements. Lookout MES is powered by the Lookout Security Graph and scales to hundreds of thousands of endpoints. Its cloud modules enable you to customize Mobile Endpoint Security to meet your needs.

Our Security Graph is powered by artificial intelligence to protect you from known and unknown threats. We have the largest mobile dataset from analyzing more than 215 million devices and more than 300 million apps. Our algorithms search the internet daily to find websites purpose-built for phishing and countless custom apps have been analyzed via our API.

Whether you download apps with new malware or are the target of the latest ransomware or phishing scam, you are protected without lifting a finger. When a threat or an attack occurs, we provide you with step-by-step instructions to investigate what is happening and how to fix it.

Lookout Mobile Endpoint Security





Lookout

About Lookout

Lookout, Inc. is the data-centric cloud security company that uses a defense in-depth strategy to address the different stages of a cybersecurity attack. Data is at the core of every organization, and our approach to cybersecurity is designed to protect that data in the modern threat landscape. With a focus on people and their behavior, the Lookout Cloud Security Platform ensures real-time threat visibility, and quickly halts breaches from initial phishing attempts to data extraction. To learn more, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and X.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo