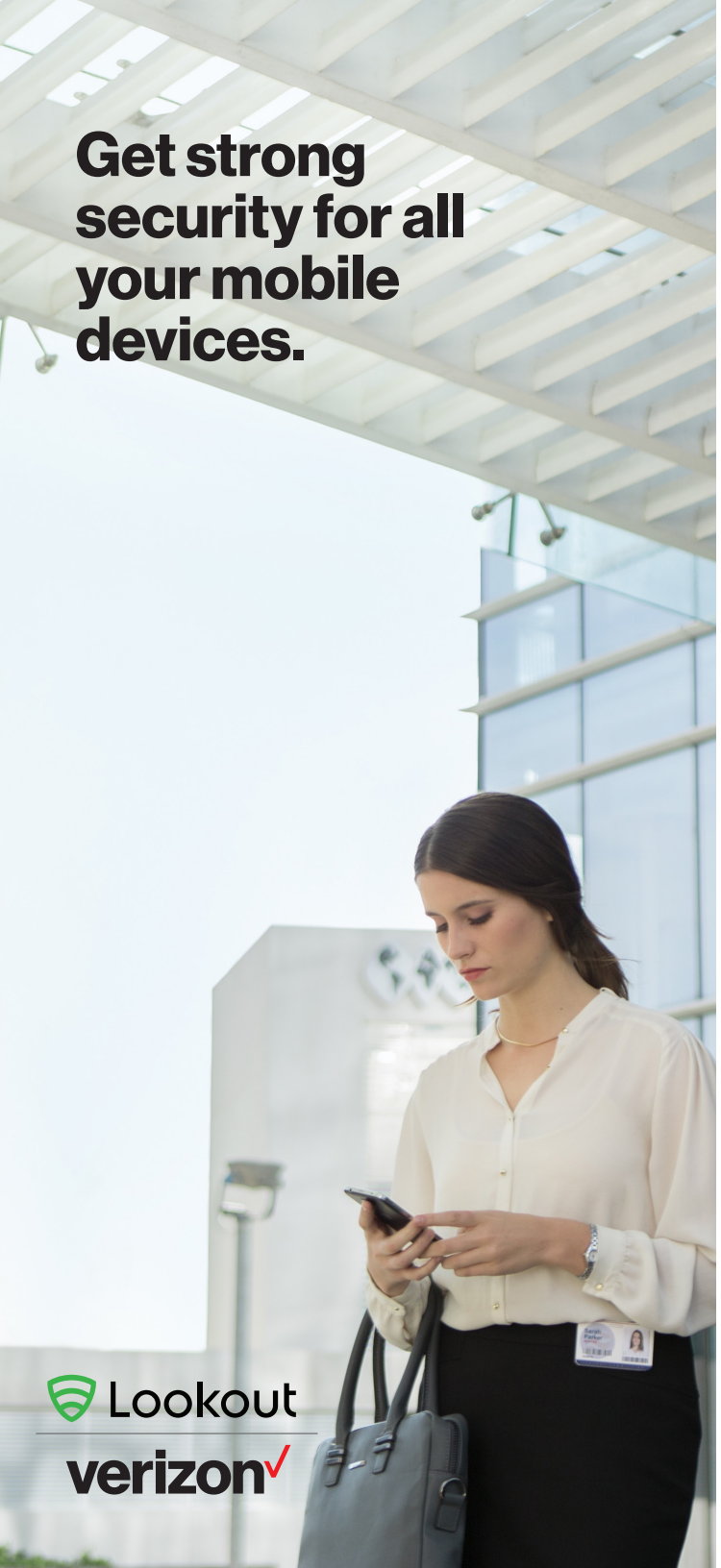


Get strong security for all your mobile devices.

Lookout

verizon

Mobile devices are often the tool of choice for employees to do their jobs, whether it's sending information to a client or customer, sharing documents with a team member or connecting to a conference call. The challenge, however, is that these mobile devices now offer would-be hackers a tempting target. Historically, organizations focused on protecting networks and PCs from cyber attacks and malware. In an increasingly mobile world, they need a better way to secure mobile devices too. Lookout Mobile Endpoint Security delivers advanced security and protection that helps organizations fight data compromise via their mobile devices. Lookout uses policy-based security measures to help protect your organization from a broad spectrum of risk across apps, devices, the network, and web and content.

The mobile risk matrix

Lookout Mobile Endpoint Security, with service on the Verizon 4G LTE network, provides advanced security that lets you extend policies to the mobile devices your company owns. Lookout uses security intelligence from its global network of 100 million devices and a massive data set of 40 million mobile apps to deliver advanced mobile security. Its cloud-first, device-assisted approach to security helps limit the impact on both device performance and the user experience.

The solution also includes the Lookout console, which provides administrators with visibility and control to help protect against mobile risks, and to safeguard your organization's data. Whenever a suspected threat is detected, Lookout will alert the user with instructions on how to address the threat. Lookout also sends a notification email to the administrator with details about the threat. Most issues, however, can be resolved by the end users themselves, which reduces the need for administration time.

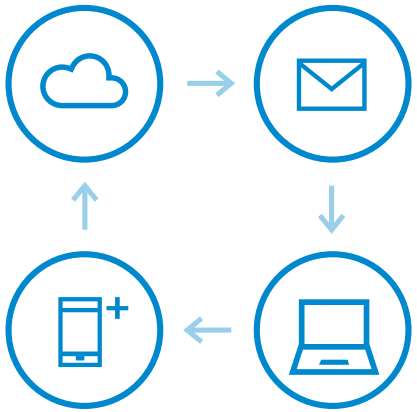
The console also lets administrators create and apply security policies and controls for all the devices in your organization. It provides an at-a-glance view of each device's level of access, and as your security protocols change, you can update policies quickly and easily.

Vectors →

Components of risk	Apps	Device	Network	Web and content
Threats	• Spyware and surveillanceware • Trojans • Other malicious apps	• Privilege escalation • Remote jailbreak/ root	• Man-in-the-middle • Fake cell towers • Root certificate authority (CA) installation	• Phishing • Drive-by-download • Malicious websites and files
Software vulnerabilities	• Out-of-date apps • Vulnerable software development kits (SDKs) • Poor coding practices	• Out-of-date operating system (OS) • Dead-end hardware • Vulnerable pre-installed apps	• Network hardware vulnerabilities • Protocol stack vulnerabilities	• Malformed content that triggers OS or app vulnerabilities
Behavior and configurations	• Apps that leak data • Apps that breach company security policy • Apps that breach regulatory compliance	• User initiated jailbreak/root • No PIN code/ password • USB debugging	• Proxies, virtual private networks (VPNs), root CAs • Auto-joining unencrypted networks	• Opening attachments and visiting links to potentially unsafe content

How it works

The Lookout app communicates with Lookout Security Cloud and compares data with network of 100+ million devices.



Lookout Security Cloud notifies administrator with an email including details when a noncompliant device is detected.

The Lookout app is installed on mobile devices for 24/7 detection.

The risk can be remediated quickly through the administrator's mobile device management platform.

- Install the Lookout app on all your employees' mobile devices for 24/7 threat detection. The app is easily deployed via your company's mobile device management platform or via email.
- Once installed, the app connects to the Lookout Security Cloud, which helps protect you based on security intelligence from a global network of 100 million devices and a massive data set of 40 million mobile apps.

If any risks are detected, Lookout alerts the end user and sends a notification email to your IT administrator with device and threat details.

- If any risks are detected, Lookout alerts the end user and sends a notification email to your IT administrator with device and threat details.
- End users can counteract the threat on their device. In addition, the administrator can also remediate possible threats using your organization's mobile device management (MDM) platform.

Customer benefits

Adding Lookout to your enterprise helps you:

Protect sensitive enterprise data. Get visibility and control to help protect your enterprise from mobile threats across the app, device, network, and web and content levels.

Reduce risk. Set custom policies that help fight against threats and data leakage, which strengthens your ability to maintain compliance.

Drive digital transformation. Securely unlock your enterprise's digital transformation and mobile productivity across personal and corporate-owned devices—without compromising employee privacy or user experience.

Low total cost of ownership. Limit your help-desk tickets with a solution that easily integrates with your existing MDM solution.

Respects data privacy. Collect only the data necessary to deliver protection against the spectrum of mobile risk, with robust privacy controls that limit the data collected and displayed to administrators.

Easy ordering. Make ordering and billing easy using the Verizon Wireless Business Solution Store.

Lookout + MDM: Securely enable mobility for your organization.

Combined with an MDM solution, cloud-based Lookout Mobile Endpoint Security provides you with a more comprehensive way to defend your enterprise data.

MDM

- Device management and data wipe
- Separation of personal and enterprise data
- Access to enterprise applications
- Authentication and single sign-on
- Mobile access to content

Lookout Mobile Endpoint Security

- Protection against app-based risks
- Detection of network-based risks
- Detection of device-based risks
- Custom remediation policy across threat types
- Easy to deploy and maintain with your MDM solution

Lookout can also integrate with your organization's MDM solution, including MobileIron® and Maas360.

Combined with an MDM solution, cloud-based Lookout Mobile Endpoint Security provides you with a more comprehensive way to defend your enterprise data.

Example use cases

Protecting employee devices

Challenge

A hypothetical biotech company developing a process that turns organic waste found in landfills into high-grade biofuels might want to patent the process and related products to protect its ideas and drive long-term profitability. Whether its employees work from laboratories, manufacturing facilities or the field, they stay connected using their mobile devices. As part of the typical work activity in this scenario, it's likely that employees will use those mobile devices to share sensitive information with other team members when needed. But what happens to that valuable, yet sensitive information, as well as the company's long-term profitability, if some of those employees' smartphones get hacked? To keep that from ever happening, the company needs a way to protect its devices and information without getting in the way of collaboration and efficiency.

Solution

By choosing Lookout Mobile Endpoint Security and connectivity on the Verizon Wireless 4G LTE network, the company can extend needed security to employee- and company-owned devices with a quick installation and easy setup.

Results

Once installed, Lookout can help the company detect mobile threats in near real time and monitor apps that access sensitive materials. The service operates in the background without slowing down device performance or affecting the user experience. Plus, it allows the company to better protect its intellectual property and the potential awarding of any pending patents.

Securing risky networks

Challenge

Law firms need to make sure that sensitive client and case information stays protected. But with today's highly mobile attorneys, keeping this information secure becomes extremely difficult. For example, whether during domestic or international travel, it wouldn't be uncommon for an attorney to use a connection in an internet café to access and download work files to a tablet. But in such situations, the attorney has no way of knowing if the café's network security has been compromised, leaving that sensitive information vulnerable to theft by hackers.

Solution

By using Lookout for end-to-end mobile security, law firms can help keep sensitive information safe if their attorneys happen to connect their tablets or other smart mobile devices to compromised networks. For example, Lookout can detect "man-in-the-middle" attacks almost immediately. If this happens, it can alert the firm's security administrator and the attorney with directions on how to deal with the situation, including instructing the attorney to immediately log off the compromised network and delete it from the list of available networks.

Results

With security alerts and next-step information from Lookout, a law firm's attorneys can find safe networks to use. This helps law firms protect sensitive documents against theft and prevent security breaches that can have a negative impact on the firm and its clients.

Learn more:

To find out more about how Lookout can help improve your mobile security and keep sensitive information protected, contact your Verizon Wireless business specialist or visit **enterprise.verizon.com/contact-us**.