Lookout®

Security that works everywhere you go

Empower your workers to safely stay productive

We're living in a new normal

Your workers now expect to be able to work from anywhere and on any device. This rapid digital transformation means that your organization's protective perimeters are no longer in play. To fully leverage the productive potential of a remote workforce, you need security solutions that enable, not hinder your workers to stay productive.

Security has changed

We're using our mobile devices more.
In order to stay productive while working from home, we're turning to our smartphones and tablets for convenience and flexibility.

We're taking more risks.
Because we're asked to jump through more security hoops when working outside the office, many are taking security shortcuts to stay productive.

The lines between home and work are blurring
While working remotely, we're often moving between personal and professional tasks throughout the day – often on the same device – which makes security more complex.

Cybercriminals are focused on your remote workers

With the world's workforces suddenly working remotely, opportunities have opened up for cybercriminals to launch attacks. Without the protection of your office perimeters, your employees are more vulnerable than ever to cyber threats.

Mobile phishing attacks are spiking.
Phishing is one of the most lucrative attack vectors for cybercriminals. That's why it's alarming to see a spike in enterprise mobile phishing encounter rates in the first months of 2020, when the permanent shift to remote work began.

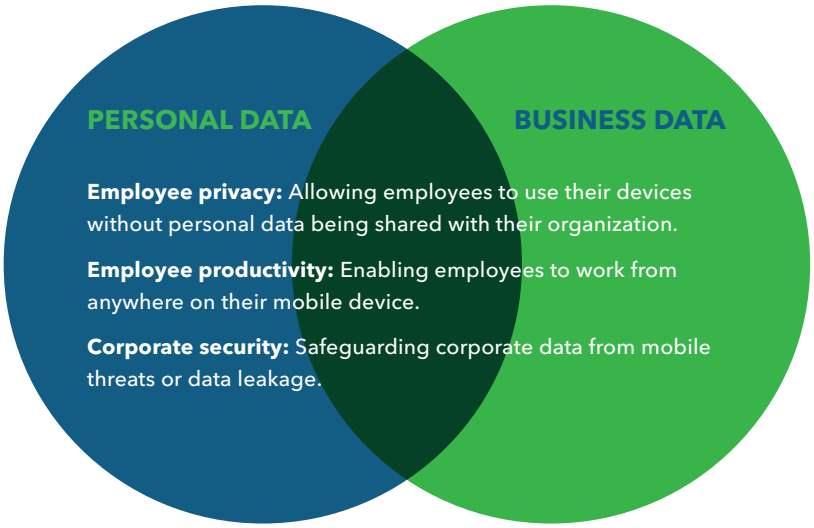
Productivity apps attract phishing attacks.
Some of the most common apps your employees use are cloud-powered productivity software. According to Lookout data, users are far more likely to be phished while using those apps.

Personal devices aren't always up-to-date.
Organizations are now letting employees use their personal devices to stay productive. Unfortunately, personal devices are far more likely to be out-of-date.

How to stay safe while working remotely

Establish a security baseline for mobile.
With workloads shifting to mobile devices, it's a good idea for companies to set a baseline of security expectations for devices that access corporate data. Here are some helpful questions to get started:

- Should personal devices be allowed to access company data?
- What operating systems are allowed access and what are the minimum OS versions required?
- What minimum security controls should be in place (e.g., passcode, encryption)?



Watch out for Shadow IT.
Often, with the best of intentions, employees use an unapproved app for work, which can put your organization's data at risk. Make sure only IT-approved apps are in use so you don't introduce unnecessary risks.

Deploy mobile security.
Even with the most robust training, employees will eventually make a mistake. Make sure you have a comprehensive solution that can secure your data even when your workers are outside your protective perimeter.

Let us secure your remote workforce today

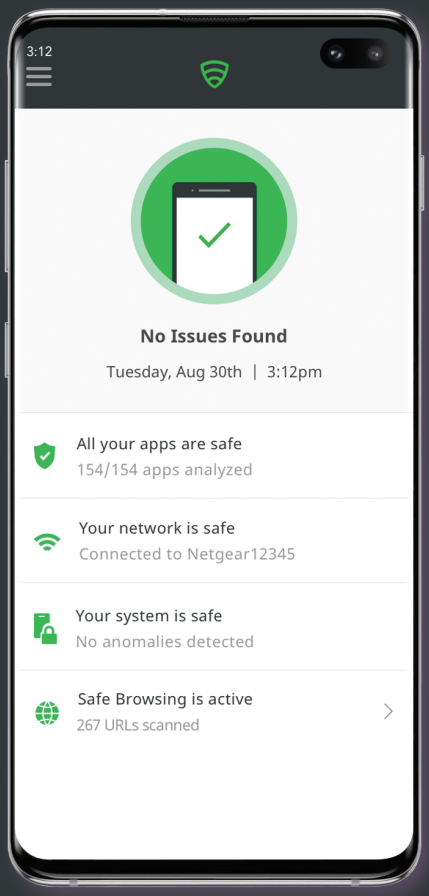
With your employees suddenly working remotely, security can feel like a daunting task. As everyone remains at home, workers will continue to use their smartphones and tablets to access sensitive data. Here at Lookout, we make it as simple as possible for you to move security to your mobile endpoints, regardless of whether your users are using a corporate or personal device.

Our platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect users from the full spectrum of mobile risks. This enables us to deliver modern endpoint security with the most comprehensive protection from device, network, app and phishing threats.

Here are some of our top security capabilities

- We stop mobile phishing threats regardless of the source.
- We protect against every type of mobile threats—app, device, network and phishing threats.
- We empower your employees to self-remediate mobile risks.
- We continuously monitor your device's health.
- We protect you without invading your privacy.

To learn more, visit **www.lookout.com** and follow Lookout on its blog, Facebook, LinkedIn, and Twitter.



About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, enterprises, government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

To learn more, visit www.lookout.com and follow Lookout on its blog, Facebook, LinkedIn, Twitter.

blog.lookout.com lookoutinc lookout lookout

Lookout®