

SAMSUNG

android

Mobile technology:
protecting your
growing business
from cybercrime

With remote working comes an increased threat of cyberattacks. To protect themselves, the UK's small and medium enterprises (SMEs) need to consider a 'zero-trust' strategy when it comes to their mobile technology.

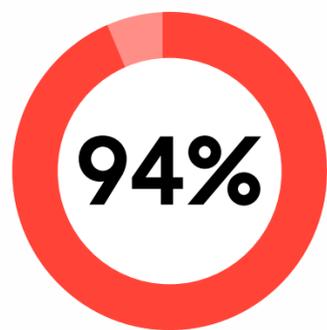
In March of 2021, Microsoft announced that several vulnerabilities in its Exchange Server allowed hackers to freely access email accounts, exfiltrate data, and install malware.

This sort of breach is called a 'zero-day' (or Oday) attack, a name that refers to the lack of lead-time to prepare for it (because, at the time of the breach, the vulnerabilities the hackers exploit are unknown to the attendant cybersecurity team).

According to reports, at least 7,000 businesses, of all kinds, were affected in the UK. But this Oday attack also had a global impact. Some larger businesses, such as the computer giant Acer, were hit especially hard; its data was held to ransom for \$50M (£38M).

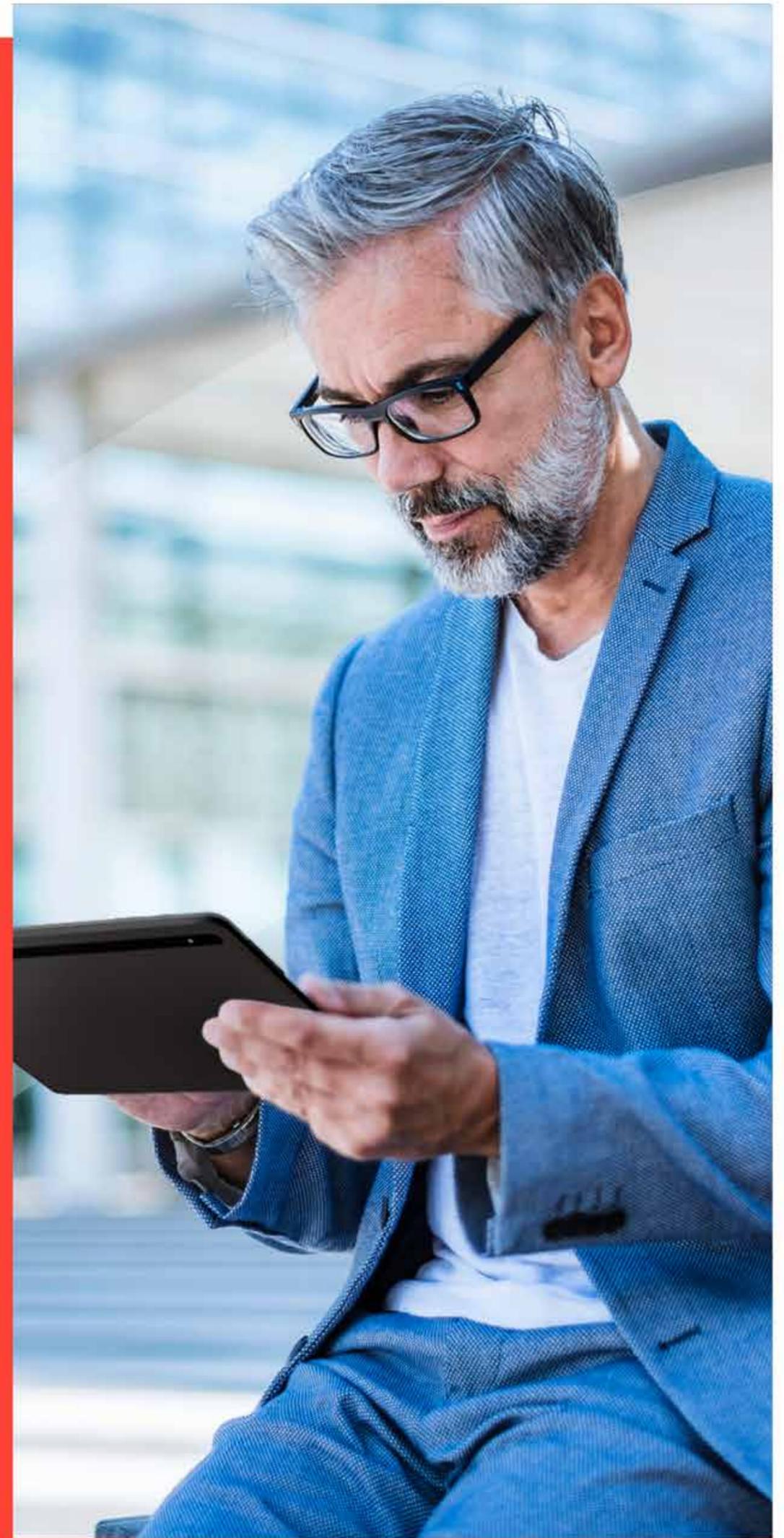
The takeaway here is that, cyber criminals have only become more prolific. Part of the reason for the growth of this threat is remote work. In the UK, vacancies that allowed for remote working tripled in 2020 and more than half of Londoners now work at home. For SMEs, that number is even higher.

For better or for worse, working remotely is here to stay. But its implementation was hasty and not without consequences.



of companies have experienced a security incident in the 12 months since April 2021.

More troubling still is that a small business in the UK is successfully hacked every 19 seconds.



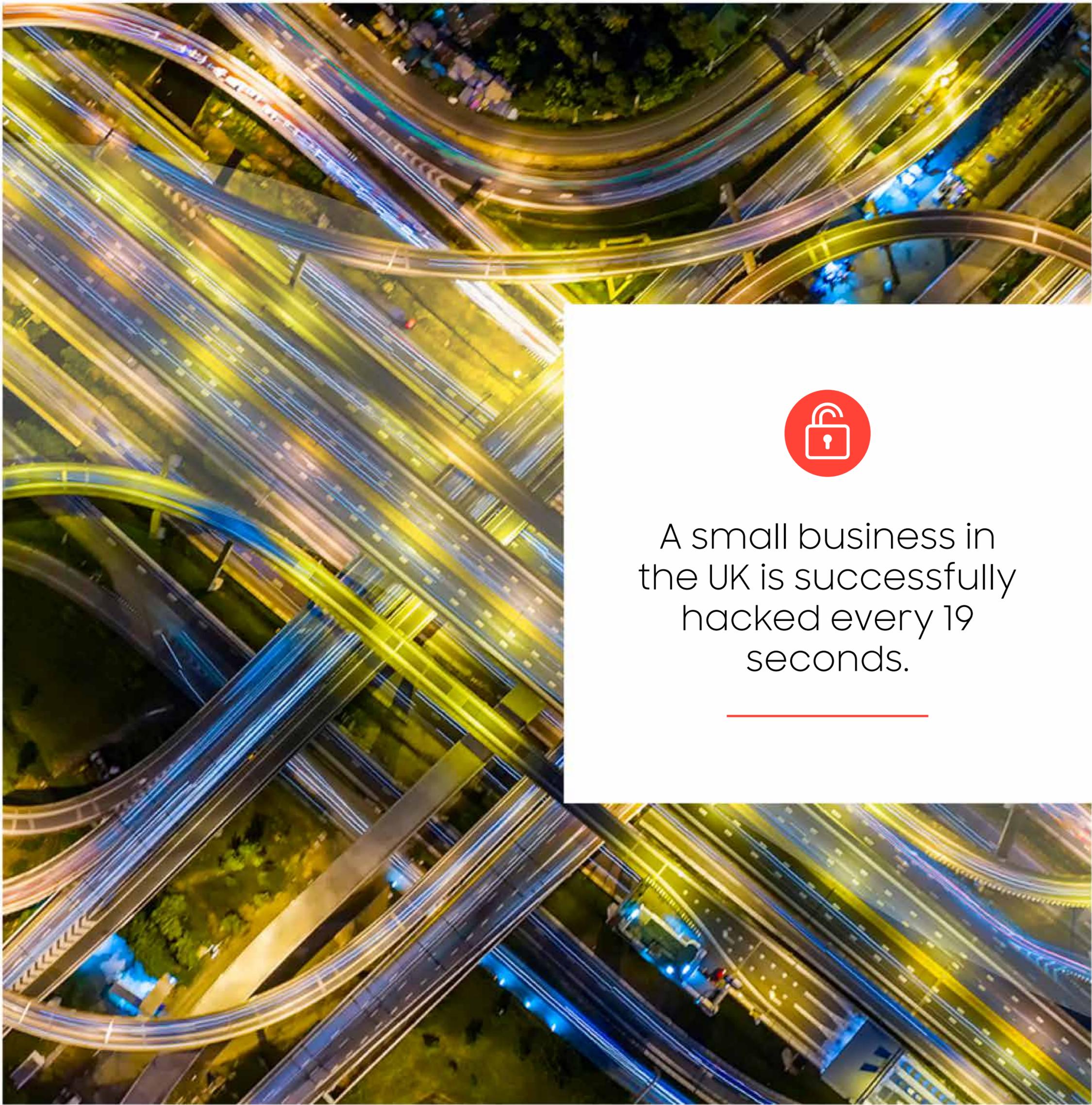
1

2

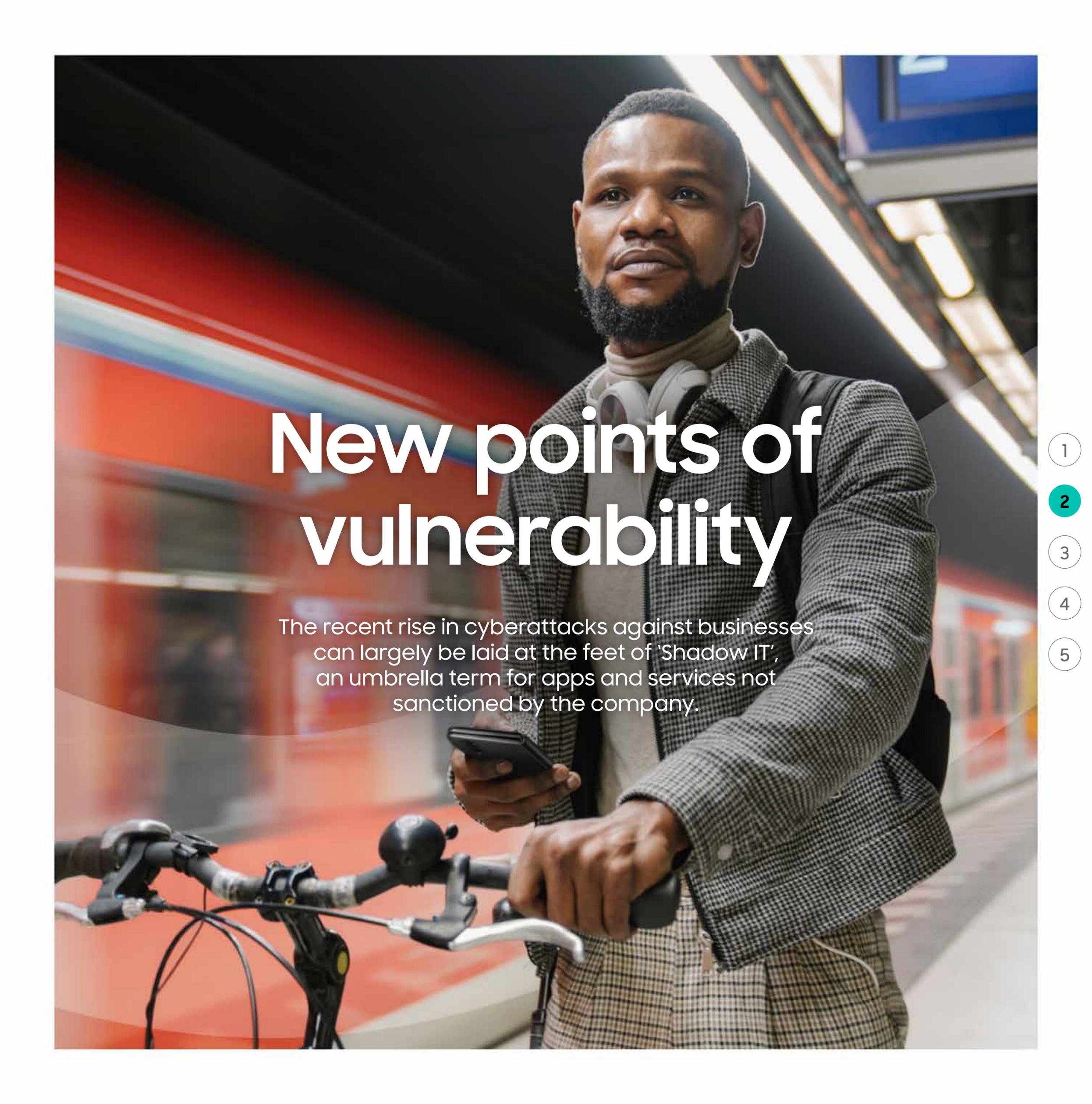
3

4

5



A small business in
the UK is successfully
hacked every 19
seconds.



New points of vulnerability

The recent rise in cyberattacks against businesses can largely be laid at the feet of 'Shadow IT', an umbrella term for apps and services not sanctioned by the company.

1

2

3

4

5



In fairness to employees, the most common reason they download unsanctioned applications is a sincere effort to do their job productively.

Common culprits of Shadow IT include free, downloadable PDF-to-document and JPEG-to-vector converters. While these online tools may offer a quick fix, they are also often laced with malware deep in the code, and so employees unwittingly onboard hackers.

But the risk of Shadow IT has been compounded by the rise of IoT, the Internet of Things.

Today, there are **11 billion** connected devices, and that figure is projected to nearly double in the next five years.

We do not think twice about our work phone connecting to our Bluetooth speaker. But even the most seemingly benign objects—like a toy doll—are potential points of vulnerability when they connect to the internet.

1

2

3

4

5



The sophistication
of cybercrime is not
in the individual.
It's in the platform.

Brett Johnson, a prolific hacker turned white-hat expert, suggests that 90% of all attacks use known exploits, like unsuspecting Bluetooth devices.

There are swathes of instructional how-to guides online. Cyber criminals understand the power of networking. If the data needed to carry out an attack isn't instantly available, they will turn to forums to get what they need.

"You will never plug every single vulnerability that your company has. That's a fact." And for those SME employees using their own unprotected personal devices for work, those risks compound.

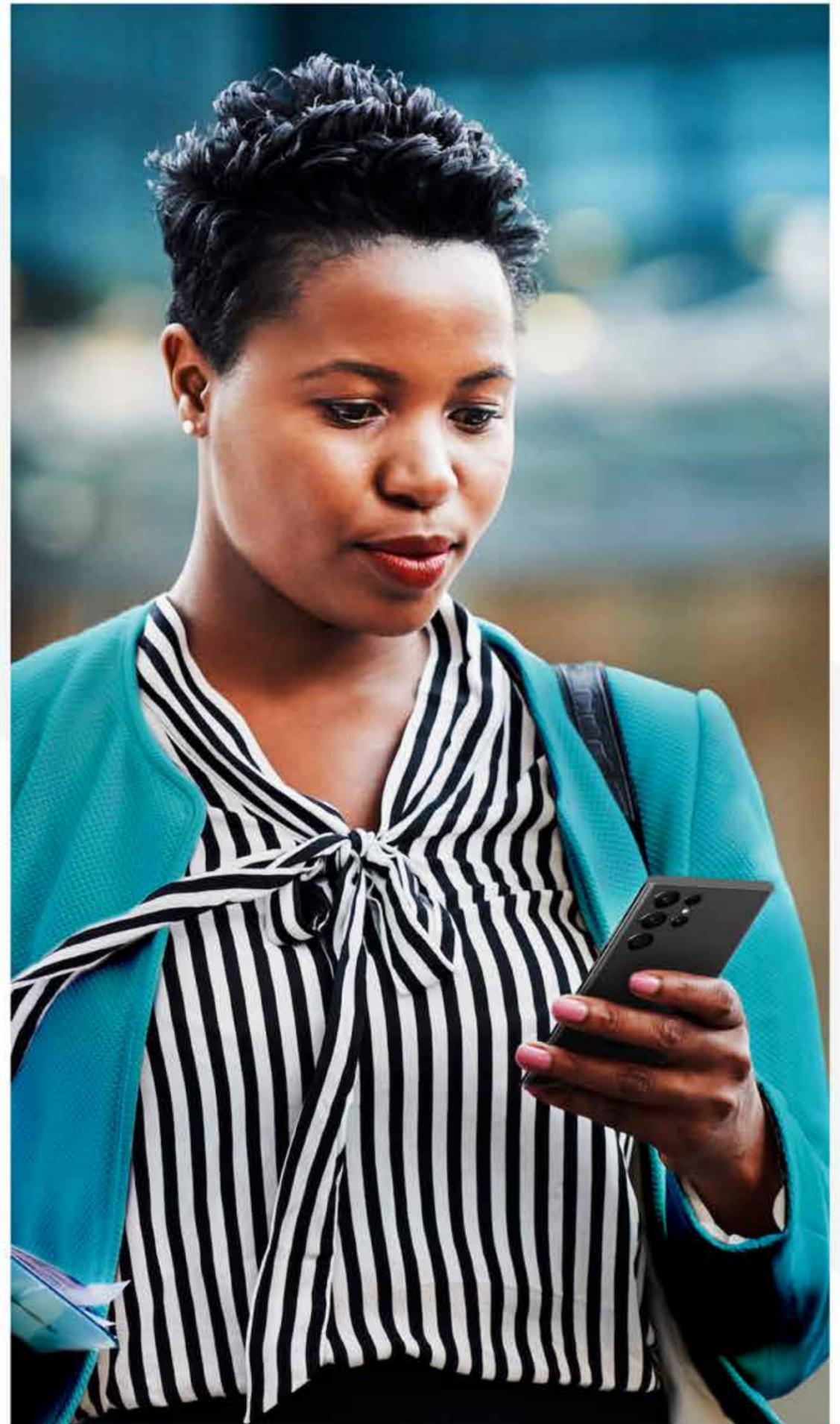
80%

of IT organisations found IoT devices on their networks that they did not install, secure, or manage. There is an attempted hack on IoT devices an average of 5,200 times per month.

So, how likely is it that your business is exposed?

Part of the problem is that this technology is still in its infancy. Without the bandwidth for encryption, most IoT devices are inherently insecure, and so cybercriminals use them to leapfrog into the real target. Without the right protection, something as innocent as connecting your mobile to that new air purifier you bought could cost you.

It could cost you a lot.



1

2

3

4

5



Cyberattacks are more common than you think

Last year, 38% of SMEs reported some form of cyberattack.

1

2

3

4

5



1

2

3

4

5

When calculating the financial impact of a typical data breach, 38% of the total figure (£1.21 million) is down to lost customers, a damaged reputation and technical dysfunction.

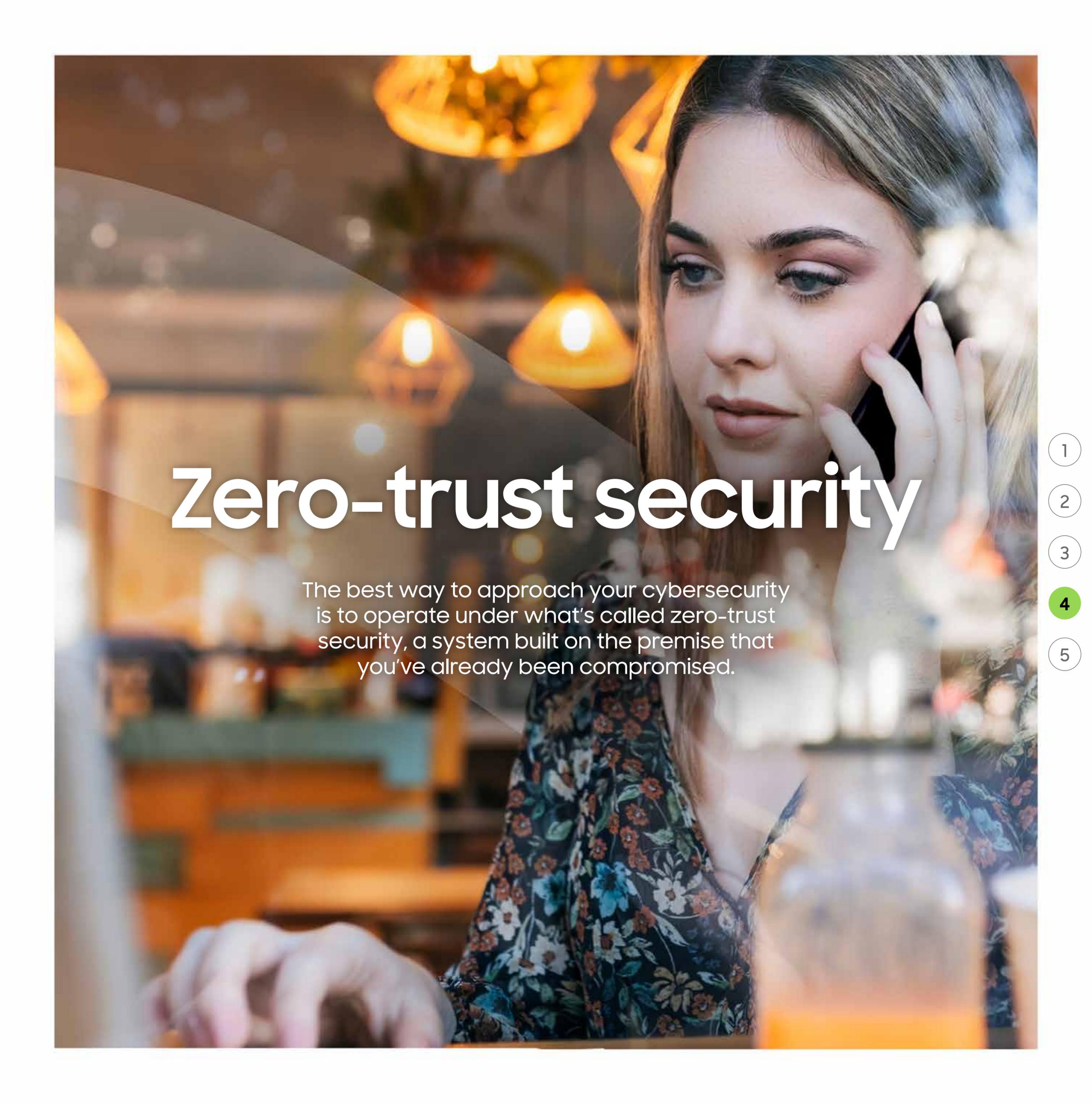
“If you’re deploying ransomware, it typically means some sort of social engineering attack”. Johnson explains, from a black-hat perspective, how easy it can be to break into an organisation.

“Why would I try to brute force my way past an industrially approved firewall, if the only thing I need to do is send an email to someone sitting behind that firewall?”

The hefty expense of security breaches also comes from lost time and resources. Not just business downtime but the time spent investigating the breaches. For SMEs without an IT department, that can be extremely costly and time-consuming.

According to IBM, the average number of days elapsed before a data breach is contained is 287. To put that in perspective, if your business fell victim to a cyberattack on the 1st of January, then it would not be contained until the 14th of October.

This timespan increases when employees work from home. The same IBM report found that businesses with more than half of their workforce working remotely, took 58 days longer to identify and contain breaches than those with most employees in the office.



Zero-trust security

The best way to approach your cybersecurity is to operate under what's called zero-trust security, a system built on the premise that you've already been compromised.

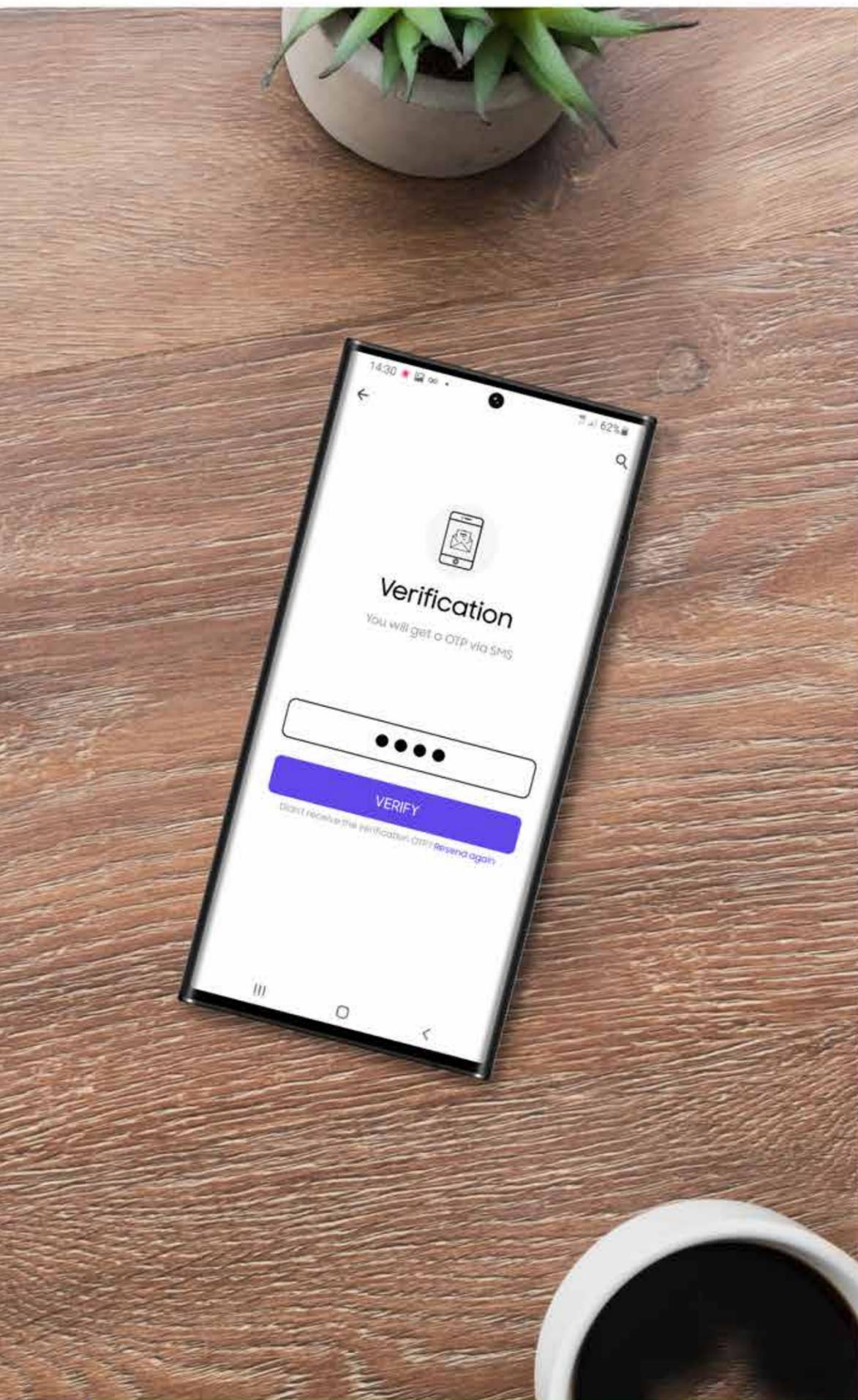
1

2

3

4

5



If you've ever used two-step verification, then you're familiar with the basic tenant of the zero-trust approach, which allows for a remote workforce to securely connect to their business from anywhere.

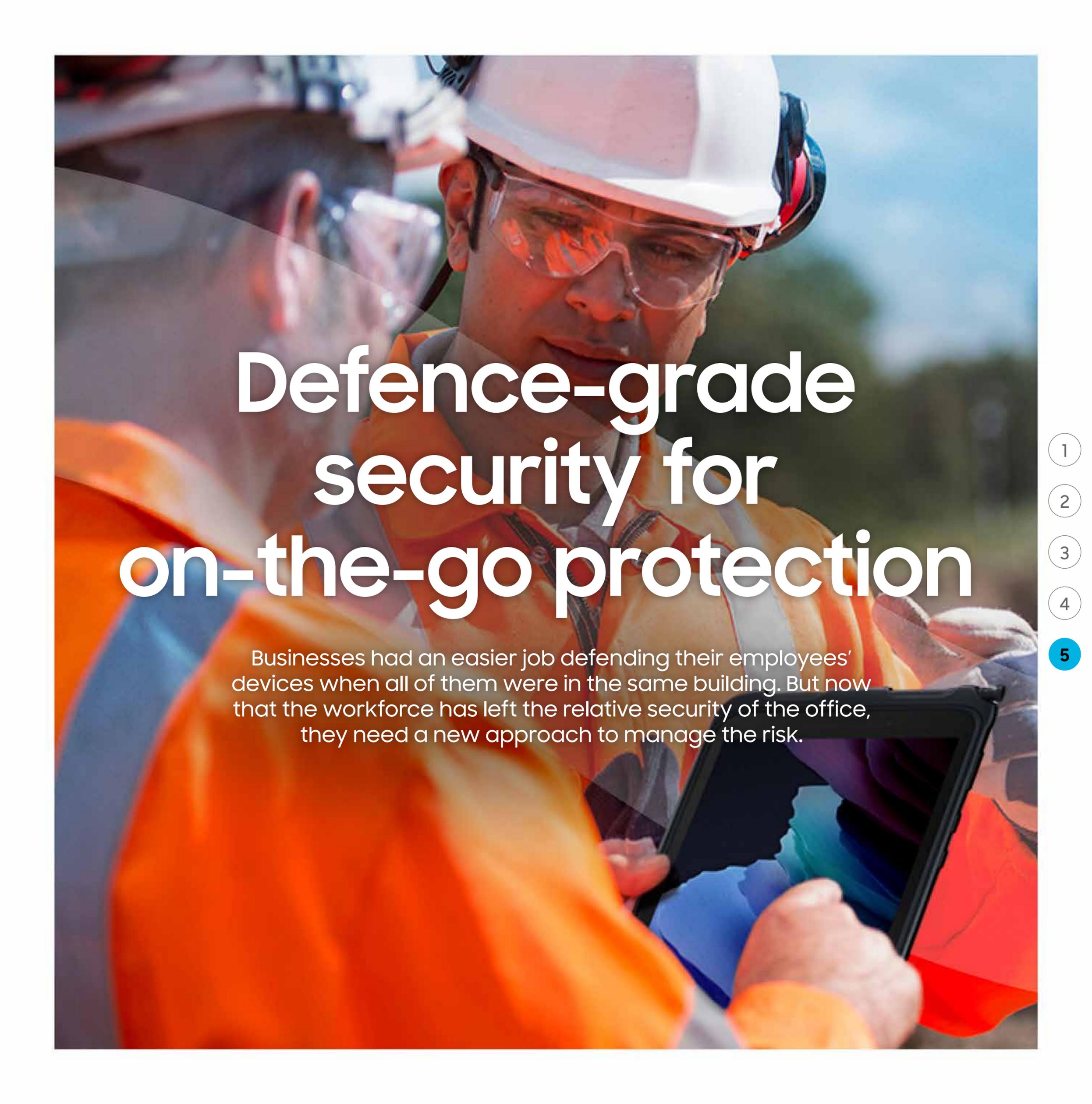
Each time a user attempts to access company resources, the employee needs to verify their identity in some way, such as acknowledging the login on a mobile device.

This is the default mode in zero-trust security: access to applications and services is strictly conditional. The burden of proof is on the user to confirm their identity. This process also picks up other useful information for cybersecurity, such as the state of a device, its location and the time of day.

This improved visibility throughout the network makes it easier to spot—and stop—breaches resulting from malware. According to a Forrester report, by preventing the exfiltration of data by malicious actors, the zero-trust method also reduces security expenses.

These facts explain why three in five business leaders say that their zero-trust security approach has enabled better digital transformation.

- 1
- 2
- 3
- 4
- 5

A construction worker wearing a white hard hat, safety glasses, and an orange high-visibility vest is looking at a tablet device. The background is a blurred outdoor construction site.

Defence-grade security for on-the-go protection

Businesses had an easier job defending their employees' devices when all of them were in the same building. But now that the workforce has left the relative security of the office, they need a new approach to manage the risk.

1

2

3

4

5

You can help to protect your critical business data and applications by employing a few basic security measures—such as biometric authentication, zero-trust, and secure hardware and software. But that’s not all you can do.

Samsung x Android security tools



Privacy Dashboard: This tool lets users manage application permissions, and see which apps have accessed your location, camera, or mic over the past 24 hours.

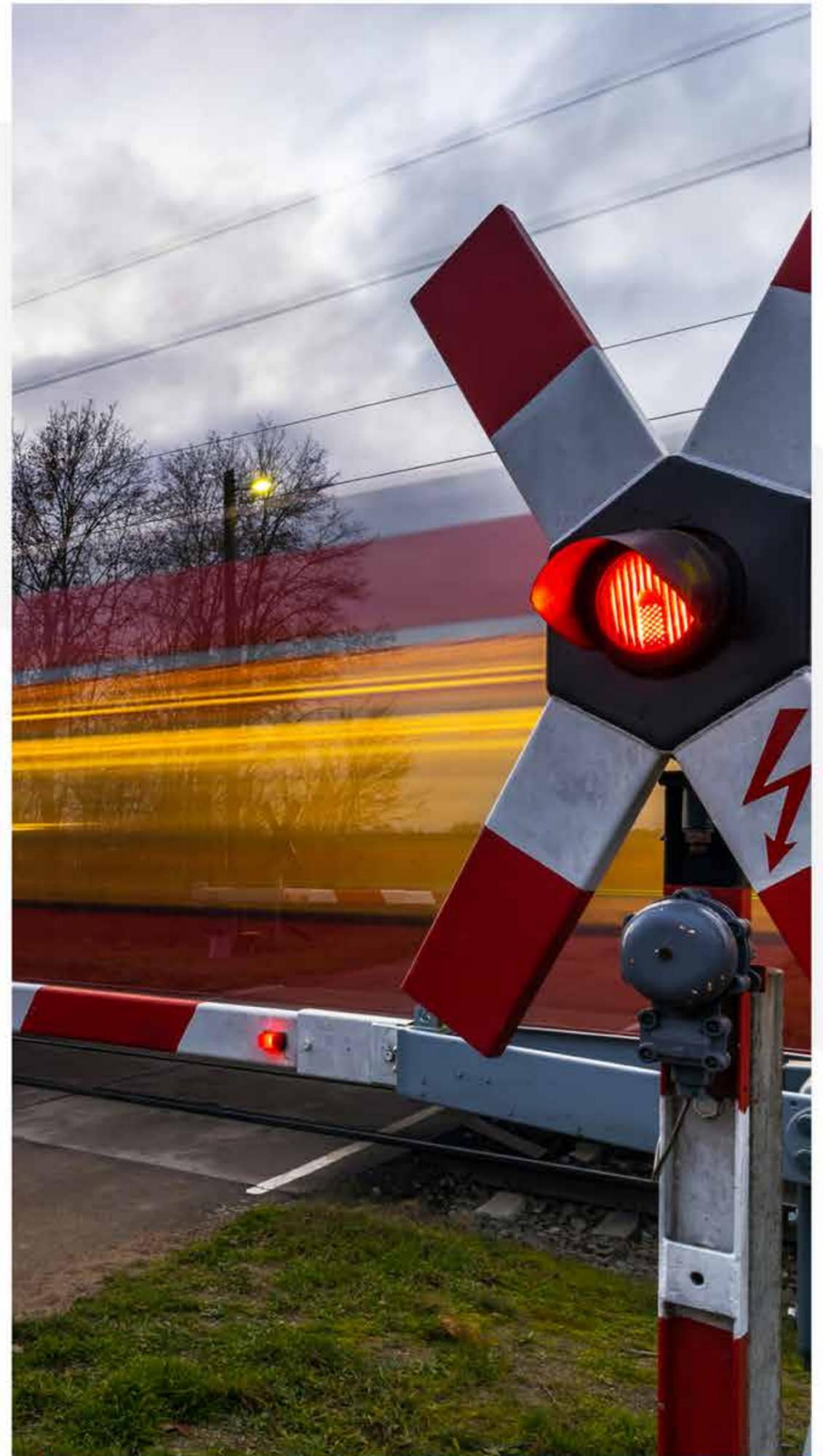


Google Play Protect: Always-on protection that scans all apps on the device to detect malware and harmful apps. SafetyNet Attestation API and Safety VerifyApps API can be used to check if a device has been rooted, as well as whether or not malware is present.

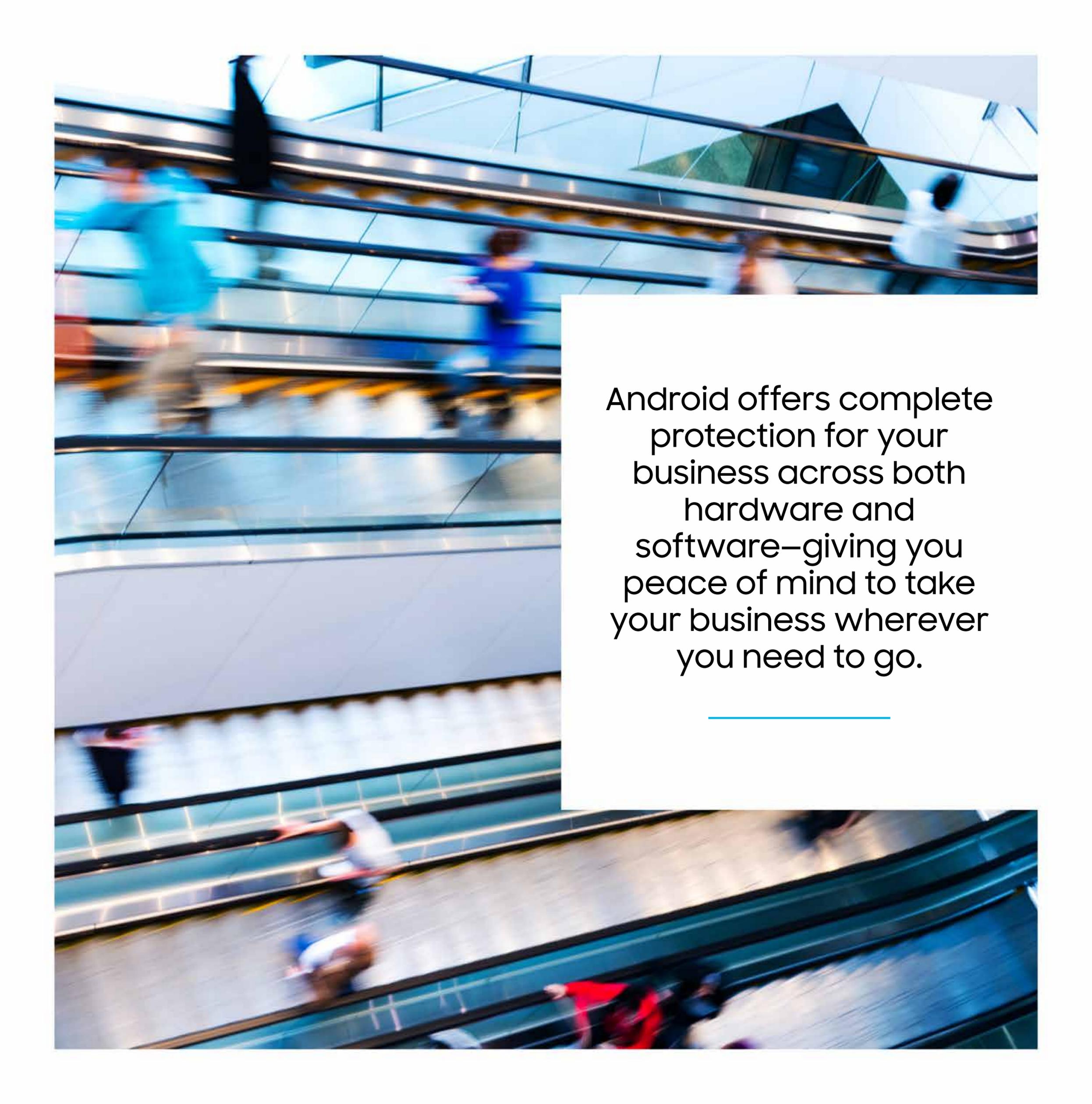


Android Work Profile: Allows employees to work securely on their own mobile devices. Work and personal profiles separate apps with no data sharing, ensuring user privacy as well as security for company data.

Android has expanded the role of identity providers, such as ForgeRock and Okta, helping cultivate a zero-trust work environment. By encouraging employers to move away from using WebView for user authentication, and enabling identity providers to gather device trust signals, Android is improving user security. With Android, it’s possible to enable single sign-on across native apps and the web, improving security and the user experience.



- 1
- 2
- 3
- 4
- 5



Android offers complete protection for your business across both hardware and software—giving you peace of mind to take your business wherever you need to go.



- 1
- 2
- 3
- 4
- 5

Samsung devices are Android Enterprise Recommended, exceeding the strict requirements set by Google. Devices receive regular security patches along with guaranteed major updates, ensuring outstanding security, efficiency and productivity.

With an Android OS-equipped Samsung device, you can feel **confident** that your data is **protected**—wherever your people are working.

You can also take control of your security updates with Knox E-FOTA, which lets you customise how and when updates are delivered across your fleet. You can even force critical updates across all devices—without users taking any action. That way, you can ensure all devices have up-to-the-minute security measures to safeguard against present threats. And you can restrict employees from downloading anything that might leave their mobile device exposed to attacks.

Samsung Knox, along with the Android OS, deliver best-in-class security for your business.*

*Independent advisor, Gartner, awarded Samsung Knox 'Strong' ratings across 27 of 30 categories in its 'Mobile OSs and Device Security' report, May 2019.



Enterprise Edition from Samsung offers further ways to keep your devices protected. You'll receive up to five years of security updates, meaning your devices always have the most up-to-date Android and Samsung security and maintenance patches. And with flexible app control with managed Google Play, as well as real-time app protection with Google Play Protect, your workforce can deploy and download the apps they need without compromising your business security.

There's no doubt internet-connected devices make life easier. But working remotely has opened up a whole new threat landscape for British businesses. Organisations need perception-challenging approaches to threats from mobile tech and IoT devices. It's likely your IT department never expected the coffee machine to be infected with malware.

The best way to view the post-pandemic world of online security is to look at it through a zero-trust lens—by assuming that your data has already been compromised.

With an increasing mobile workforce, cybersecurity hygiene is more important than ever. That means embracing zero-trust, biometric authentication, and the encryption of customer data.

With these measures in place, cyber criminals are faced with increased friction. And that could be enough to keep your growing business safe.



The multi-layered Android approach to security

Security Management: Knox Management-enforced policy controls.

Google Security Services: Google Play Protect app analysis, scanning, remediation, and Google Safe Browsing anti-phishing.

OS Platform: Complete platform security ensures device and data integrity.

Hardware: Mandatory hardware-backed security protects critical tasks and operations.

Allow your business to work both openly and securely. To find out more speak to your Samsung Account Manager, or [visit our website](#).

1

2

3

4

5