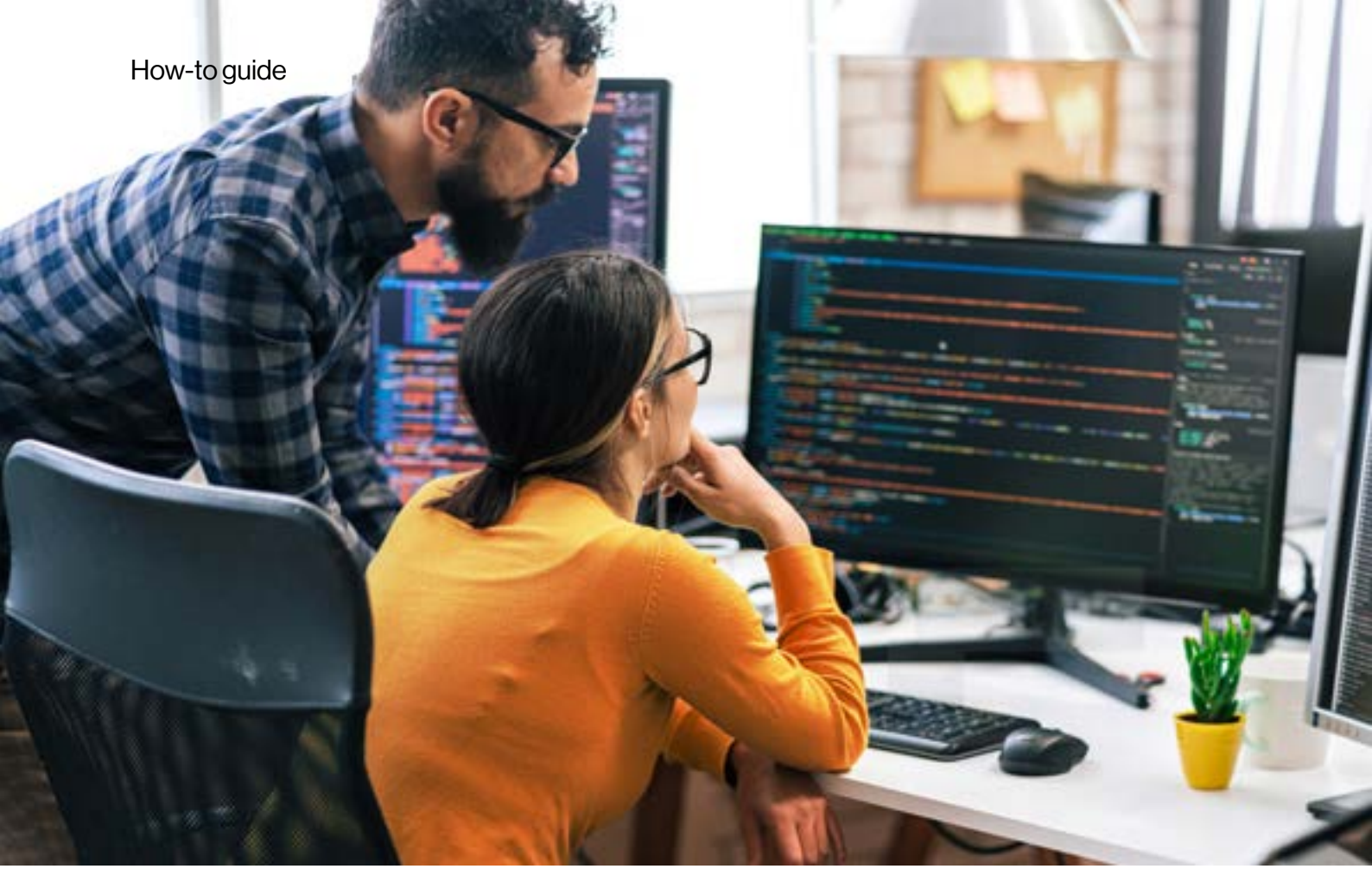
How-to guide

A holistic approach to strengthening cyber resilience

verizon business

Contents

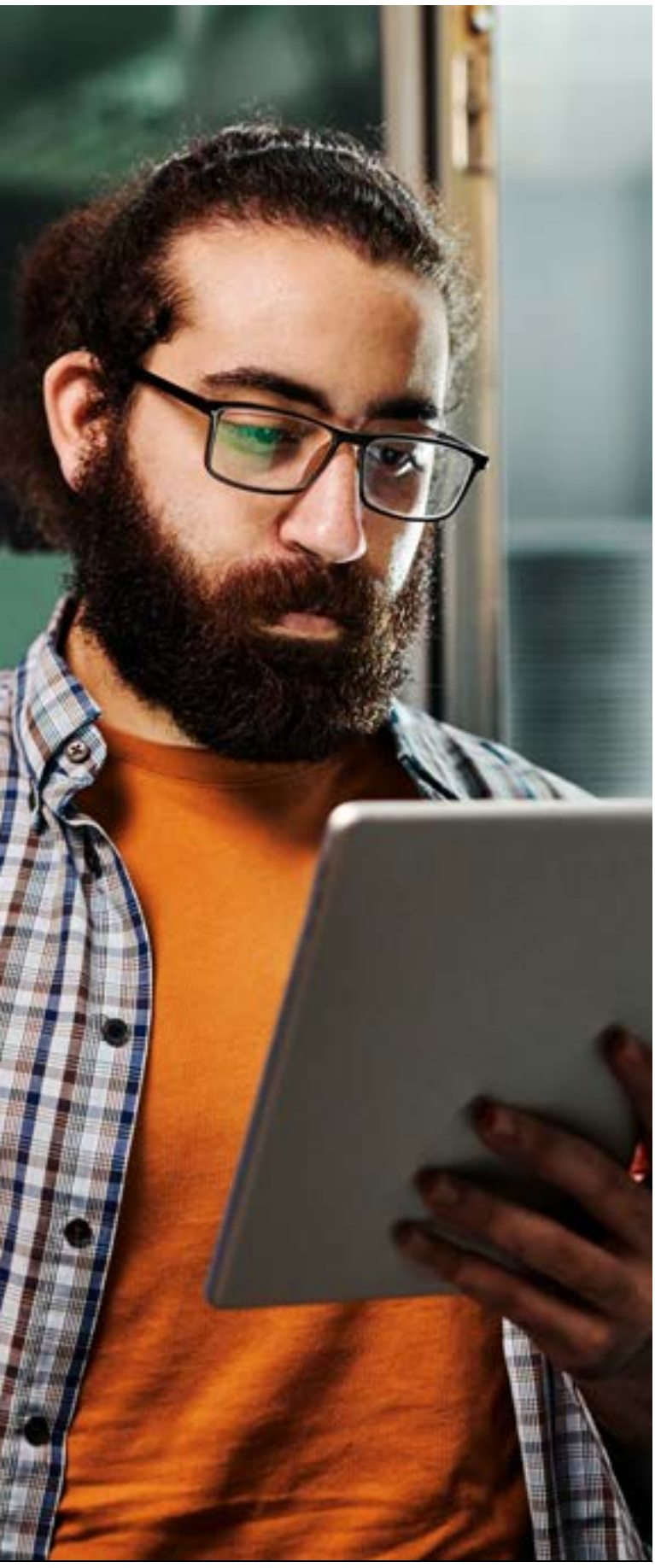


How businesses can boost their resilience in the face of increasing cyberthreats

With the level and sophistication of cyberthreats increasing, how can businesses ensure they remain protected? The key is taking a more holistic view.

As technology advances and businesses in all sectors become ever more connected, the risk of cyberthreats continuously increases, too. Cybercriminals are becoming more sophisticated every day. And with businesses increasing their reliance on digital tools and processes – with greater amounts of data stored and shared in the cloud – each organisation's attack surface also grows.

To keep themselves protected, businesses need a robust cybersecurity program that meets the specific needs of their organisation and the regulatory environment they operate in.



Cyberthreats are on the rise

The Verizon Business 2024 Data Breach Investigations Report[1] analysed:

30,458
real-world security incidents

10,626
of which were confirmed data breaches affecting victims in

94
countries

Managing growing threats

The report shows a substantial growth in attacks involving the exploitation of vulnerabilities – up a staggering 180% compared with the previous year – and the main point of entry for these attacks was web applications.

Roughly one-third of attacks involved ransomware – something that is still a major concern for 92% of industries, as the cost of an attack can be significant. According to the FBI's Internet Crime Complaint Center (IC3) ransomware complaint data, the median loss associated with the combination of Ransomware and other Extortion breaches is $46,000 (ranging between $3 and $1,141,467 for 95% of cases).[2]

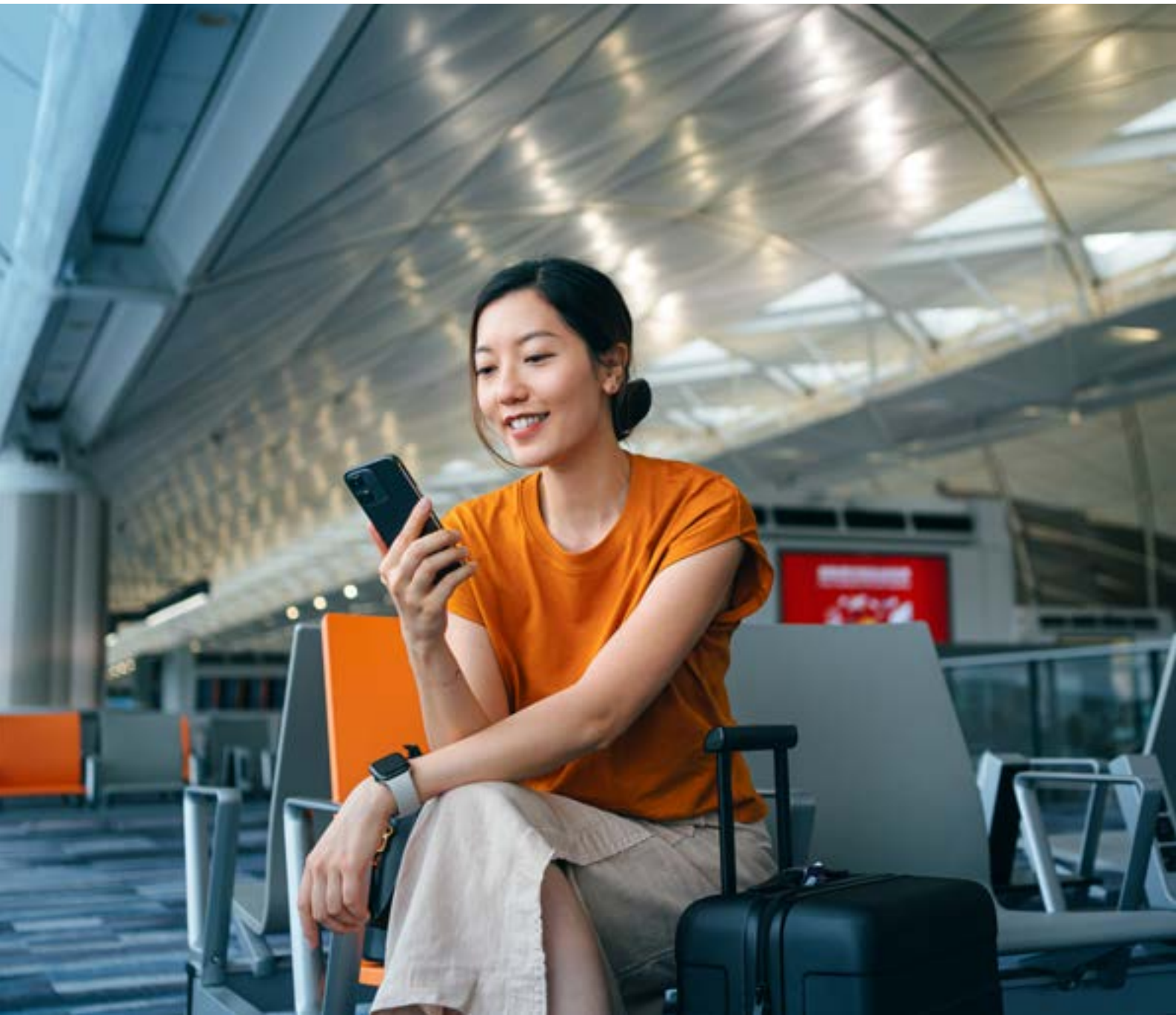
1&2. 2024 Data Breach Investigations report. (n.d.). Verizon Business. https://www.verizon.com/business/en-gb/resources/reports/dbir/

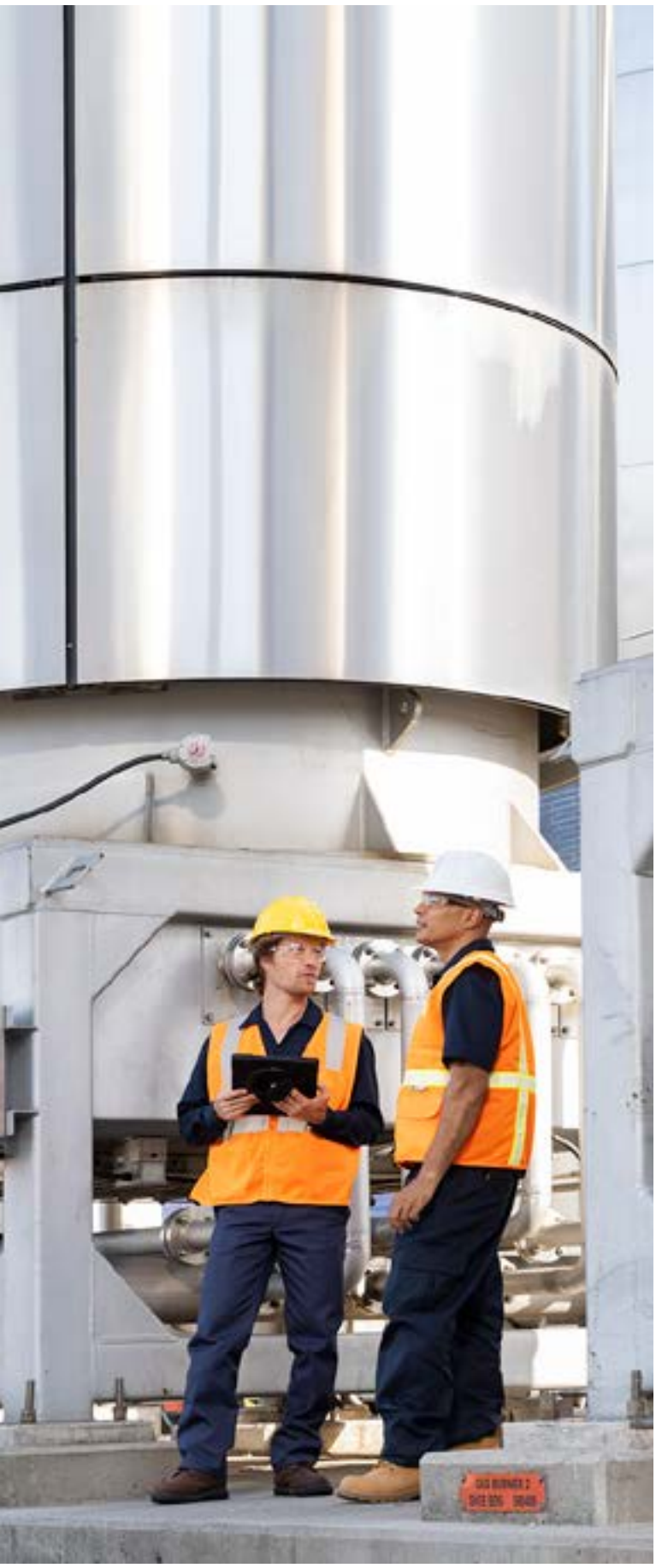
However, it's not just the number of threats that businesses should be concerned about. Cybercriminals are also increasing their capabilities, devising more sophisticated attacks to beat the latest technologies that thwart attacks and prevent data loss, and regulations that increase an organisation's diligence. As ANSSI's Panorama of Cyberthreats 2022 says, "malicious actors are continuously improving their capabilities for financial gain, espionage, and destabilisation. This improvement is illustrated in particular in the targeting of attackers who seek to obtain discreet and permanent access to their victims' networks."[3]

Increased vulnerabilities

Advances in technology, network capabilities and working practices have meant organisations need to be aware of the increased vulnerabilities that cybercriminals can exploit. "The key element to consider is the development of remote working and the hybridisation of organisations, which has redefined the contours of information systems security," says Steven Gevers, Associate Director, Security Consulting Services for Verizon Business.

3. ANSSI. (2022). PANORAMA DE LA CYBERMENACE 2022.In ANSSI. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf





As discussed in the DBIR, breaches caused by vulnerabilities have tripled recently – driven, largely in part, by the impact of Zero-day attacks. So, it's essential for businesses to remain on top of basic security hygiene. It also shows how important concepts such as Zero Trust and Defense in Depth continue to be.

> It's critical to have a consolidated view on which parts of your organisation expose you to the biggest risk, so you can spend your security budget where it brings most value.
>
> **Steven Gevers**
> Associate Director, Security Consulting Services for Verizon Business

Problems can also arise when employees try to take matters into their own hands. Today's workers are used to operating in a fast-paced, digital way. If they can't quickly find solutions to a problem, they can often be tempted to – perhaps unintentionally - breach security protocols and use unsanctioned and unprotected applications, software or hardware. A study by Harvard Business Review showed that 67% of respondents had failed to fully adhere to cybersecurity policies at least once.[4] This so-called shadow IT can open up extra vulnerabilities, giving the criminals another potential point of entry.

4. Verizon. (2023). 2023 Mobile Security Index whitepaper. https://www.verizon.com/business/resources/T19d/reports/mobile-security-index-report.pdf

Finding the right fit for security

Faced with this increase in cyberthreats, many businesses have adopted Zero Trust and SASE solutions. And while this is great for strengthening network security, it's important to also step back and look at how everything works together.

"Different business units have their own business applications; they have their own processes, their own needs," says Stephen Young, Director, Cyber Defense Consulting Services for Verizon Business. "Security has multiple dynamics, impacting the environment to deal with the various types of attacks. There is no single solution that fits all. Security resilience therefore has to go further than just Zero Trust and SASE."

> There is no single solution that fits all. Security resilience therefore has to go further than just Zero Trust and SASE.
>
> **Stephen Young**
> Director, Cyber Defense Consulting Services for Verizon Business

Getting the basics right

Sometimes, businesses are looking so closely at the bigger security threats that they lose sight of the simple, fundamental elements of their setup. “The more complex the situation, the greater the threat, the more companies tend to neglect the fundamentals,” Young says.

> It is the fundamental principles that constitute the relevance of an effective security policy.
>
> **Stephen Young**
> Director, Cyber Defense Consulting Services for Verizon Business

While businesses need to take a wider look at the security of their overall infrastructure and find solutions to the big problems, it’s essential not to forget the basic security steps – like updating systems and correctly setting up firewalls. By keeping these bases covered, IT teams may not only prevent small security threats creeping in, but they may also avoid wasting money on unnecessary security tools.

Taking a more holistic approach

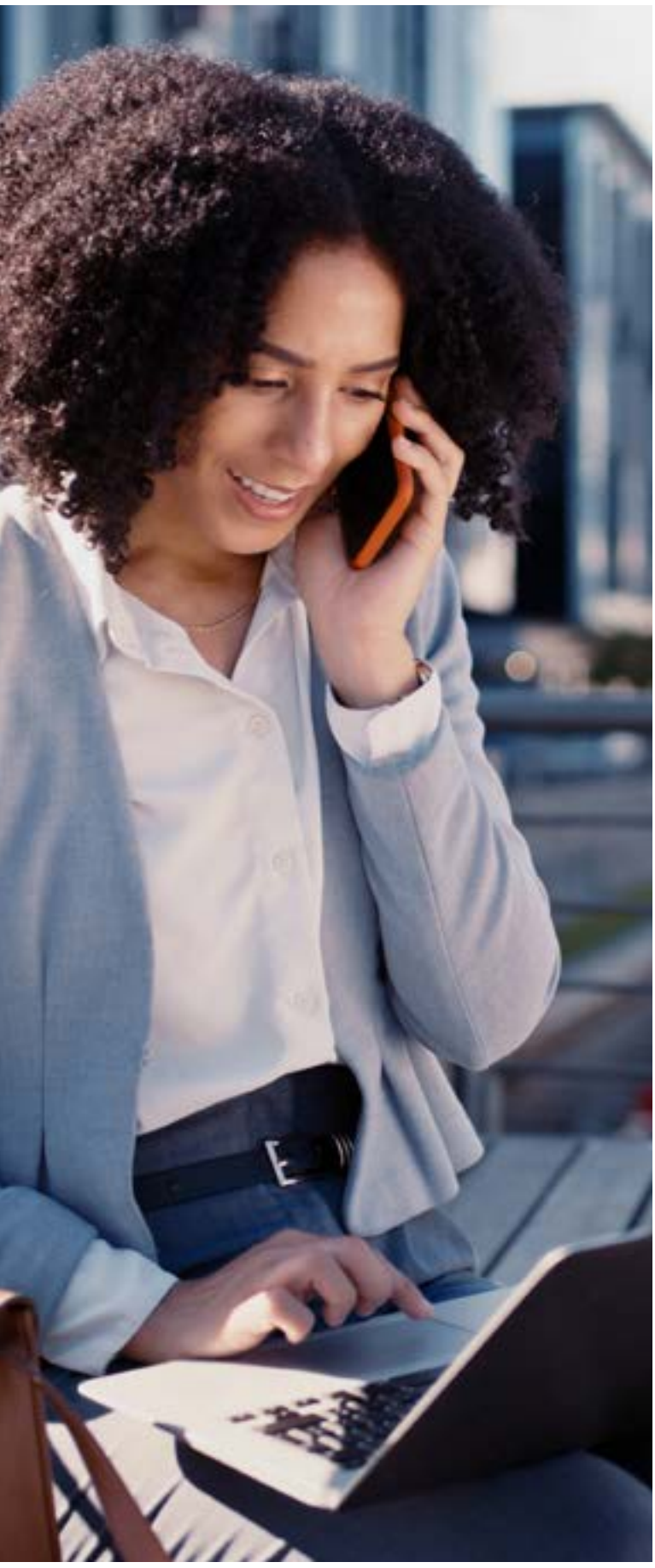
The temptation for many businesses is to increase security by adding multiple extra layers. But this can actually be counterproductive, creating even greater complexity and cost. Instead, it's better to look at the whole picture and evaluate what's needed, where and for what reasons. That's why Verizon takes a more holistic approach based on an in-depth understanding of a business – looking at everything from the organisation's operational ecosystem down to the needs of its individual users.

To do this, Verizon aligns to the National Institute of Standards in Technology's (NIST) security framework, which is based on five key axes.[5]

Verizon can conduct detailed security evaluations to understand a company's specific needs. Then we help them deploy customised security measures to meet those needs.

- Identification
- Protection
- Detection
- Response
- Recovery

5. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. In NIST CSWP 29[Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf



> Every organisation has its own culture and risk appetite, resulting in a different approach to security.

Steven Gevers
Associate Director,
Security Consulting for Verizon Business

"Some organisations might find technologies such as Generative AI an intellectual property risk that needs to be blocked; others think it's a business enabler that requires some coaching. We help our customers improve their security maturity; focusing on the biggest threats – but keeping in mind business requirements. Adopting defense in depth – using multiple security measures to protect an organisation's assets – is key to this. Organisations can have flexibility on one level while keeping risk acceptable with controls at another level. If one layer is compromised, the additional layers may stop the attack or reduce its impact."

Not only does this approach help to create the most robust set of IT defences, but it also enables businesses to manage costs more effectively, investing in the right solutions for their needs and managing their budgets more wisely. “When you have a global vision of the needs of the business and provide tailor-made solutions, it avoids the multiplication of redundant security solutions,” Young says. “A rationalisation that allows better cost control.”

With this more holistic approach to security, businesses can better achieve the right security setup that meets their needs and their budget. And they can be better prepared to keep the cybercriminals at bay.

Find out how Verizon can help you mitigate cyberthreats with the right holistic security solution for your business at Verizon.com/business/en-gb. Sign up for emails to learn more about our security and SASE solutions here.