

# Welcome to today's network-enabled business world.

From an observation drone to a manufacturing robot or an autonomous decision made in response to a driver's licence enquiry—every imaginable human-to-thing, thing-to-thing, or human-to-human transaction is now a complex web of digital relationships, underpinned by the network.

But as networks evolve, so do the cyber threats that businesses face from different fronts.

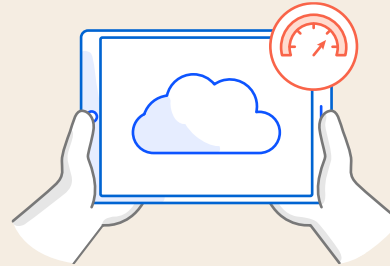


# The security threat landscape is changing



## Accelerated digital transformation

Many organisations struggle to deliver consistent security as services shift to the cloud.



- By 2024, more than 60% of SD-WAN customers will have implemented a secure access service edge (SASE) architecture, compared with about 35% in 2020.

Source: Gartner, Magic Quadrant for WAN Edge Infrastructure, Sep 2020.

## Widespread remote working

Securing employee data becomes all the more critical as staff working remotely increases.



**Two challenges** security and risk management leaders facing in 2021:

- Acceleration in digital business is outstripping cybersecurity investment.
- Cybersecurity knowledge gap.

Source: Gartner, 2021 Top Priorities for Security and Risk Management Leaders, April 2021.

## Increasingly sophisticated cyber threats

Lack of skills to deal with current threat landscape whilst maintaining compliance standards.



- Remote working and online shopping are fertile ground for **cybercrime**.
- Cybersecurity is perceived as the **key to aid recovery** from the COVID-19 pandemic downturn.

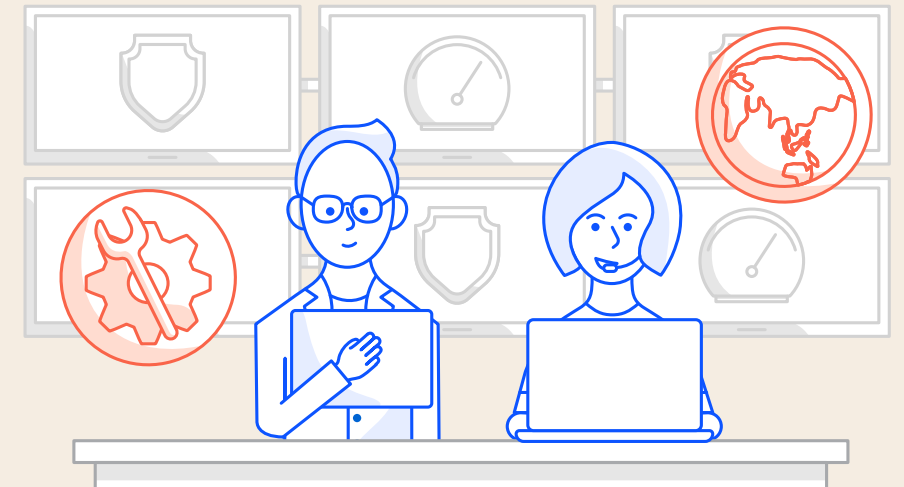
Source: GlobalData, Emerging Technology Trends Survey 2020.

# Something to think about when it comes to security

[Essential Eight Framework](https://www.cyber.gov.au/essential-eight) by [cyber.gov.au](https://www.cyber.gov.au)

While no set of mitigation strategies are guaranteed to protect against all cyber threats, it's recommended to implement eight essential mitigations strategies from the ACSC's strategy to mitigate cyber security incident as a baseline.

This base line, known as Essential Eight, makes it much harder for adversaries to compromise systems



The mitigation strategies constitutes the Essential Eight are:

- **Application Control**
- **Configure Microsoft Office Macro setting**
- **Restrict administrative privileges**
- **Multi-factor authentication**
- **Patch Applications**
- **User application hardening**
- **Patch operating systems**
- **Regular backups**



Thank you.