opentext™

Strengthen your cybersecurity

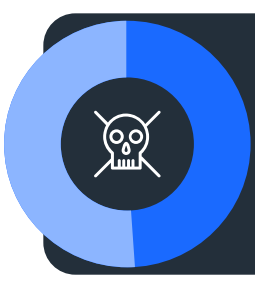
7 reasons for MSPs to act now

As cyberattacks grow in sophistication and frequency, the pressure on Managed Service Providers (MSPs) to ensure digital safety has skyrocketed. Customers don't just need IT support; they want assurance that their business is safe and secure.

Here are 7 reasons why you must enhance your cybersecurity to remain competitive and lock in customer trust.

1 | Cybercrime is constantly evolving

Hackers are getting smarter. You need a security partner with the resources, reputation, technical expertise, and solutions to stay one step ahead of the next attack.



49%
increase in 'living off the land' phishing attacks recorded by OpenText in 2023

Source: OpenText 2024 Threat Report

2 | Cloud requires a new approach

$170b
projected revenue in the APAC public cloud market in 2025

As more businesses migrate to the cloud, traditional on-premises security solutions are falling short. Advanced, cloud-adapted threat intelligence is critical to secure customers on their digital journeys.

Source: Statista

3 | Compliance is getting more complex

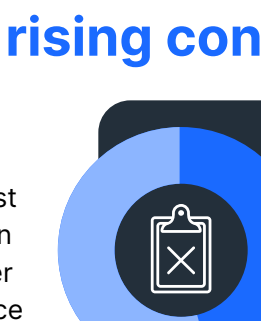
Compliance regulations are tightening. You must provide security solutions that are flexible and compliant with evolving laws to protect your business and your customers from hefty penalties.

US$1-20m
in costs for small businesses that experienced data breaches in APAC over the last three years

Source: 2024 PwC Global Trust Insight Report

4 | Remote working risks run high

72% **of IT leaders are concerned about the security risks of employees working remotely**

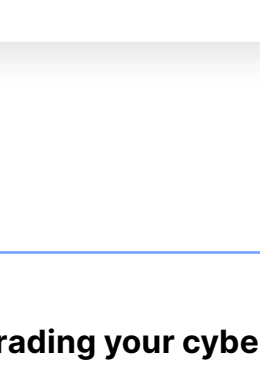


Traditional defences like firewalls and antivirus programs are incapable of protecting remote workforces, especially as hackers get smarter. Your solutions must support remote access, fortify endpoints, and secure teams wherever they work.

Source: Statista

5 | Emerging tech increases attack surface

IoT and AI are game changers, but they also create new risks. To protect your customers, you need to roll out solutions that can communicate across multiple interfaces seamlessly and close the gaps that let bad actors in.



The number of IoT devices is set to reach
29 billion
worldwide by 2030, almost double what it is today

Source: Statista

6 | Supply chains are a top target

Over
30,000
public and private organisations were impacted by the SolarWinds supply chain attack

Disparate technologies in supply chains create cybersecurity vulnerabilities. Your suite must offer holistic cybersecurity solutions that can quickly close these gaps, and identify and quickly mitigate breaches should one occur with a known vendor.

Source: TechTarget

7 | Data privacy is a rising concern

Data breaches can devastate reputations and even put a company out of business. You must partner with cybersecurity solution providers who can fortify customer data against these threats, enhance compliance, and govern data access more effectively.

46%
of MSPs said they lost business or contracts due to cyberattacks

Source: Coleman Parkes Research

Upgrading your cybersecurity offering isn't just a value proposition—it's a necessity. By providing your customers with best-in-class protection and support, you're letting them know that their safety is your primary concern.

Learn how OpenText Cybersecurity can help you deliver trusted, cyber resilient environments for your customers.

Begin your journey

Sign up now

Microsoft Solutions Partner

opentext™