techaisle

Why Cybersecurity Needs to be an SMB Business Priority

Technology powers SMB business success

89%

SMBs consider technology to be important and integral to business success

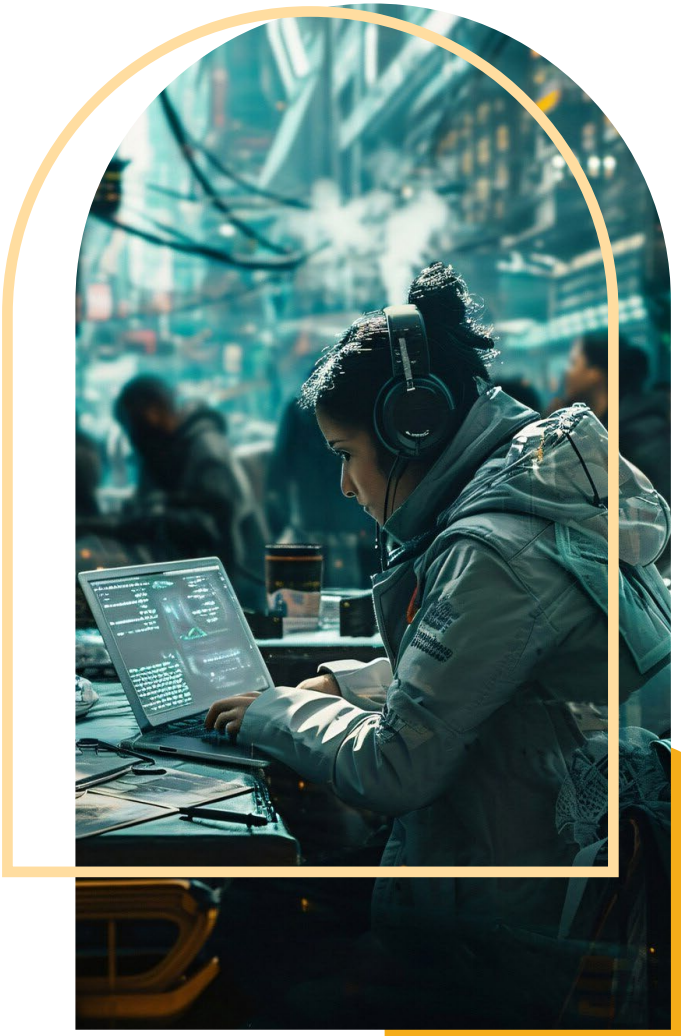
SMBs rely on technology, but cyber threats are a constant risk, therefore...

54%

SMBs consider cyberattacks a business risk

93%

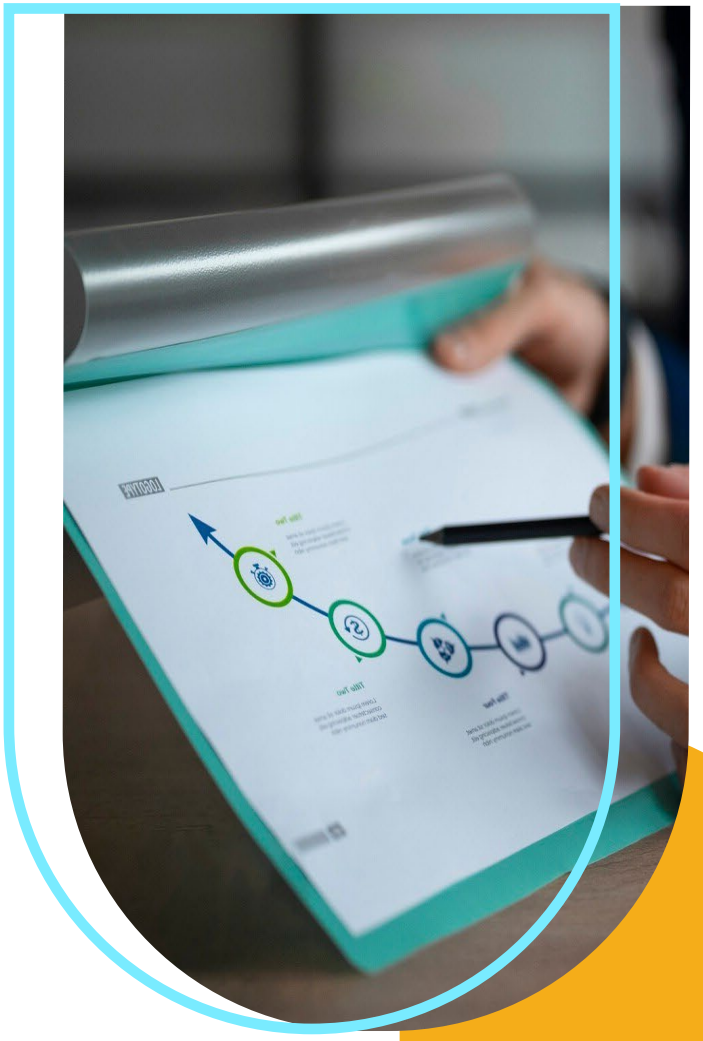
SMBs have prioritized investments in cybersecurity



Data is a critical asset in technology-driven business environment, fueling SMB growth

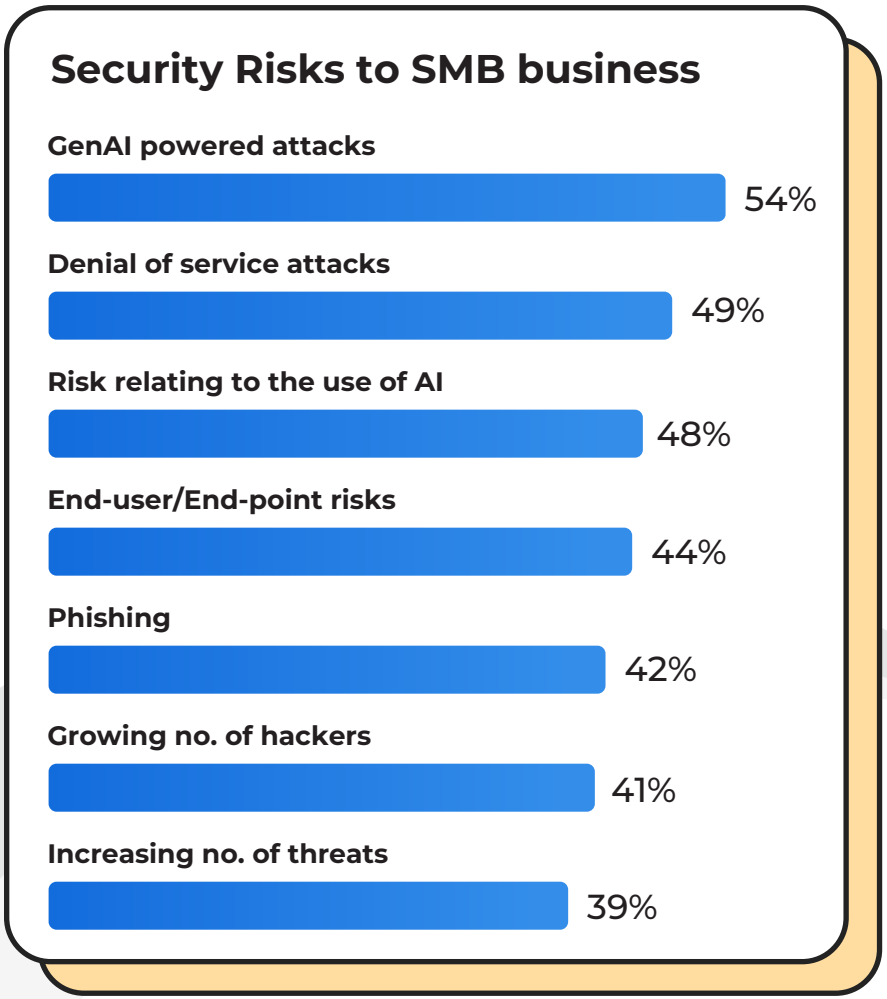
74%

SMBs have increased their reliance on data to improve decision-making, enhance customer experience, and drive operational efficiency



Hence, securing and protecting data is essential

- **AI-powered threats** pose a significant risk to data security, compromising sensitive information
- **Cyber threats are evolving rapidly**, targeting data across various technologies from traditional networks to cloud and mobile platforms
- **New threats emerge constantly,** seeking to exploit vulnerabilities and steal or damage data



But, first, What is Data Security and Data Protection

Prevents unauthorized access to your data.

- It is like guarding your business's most valuable secrets.
- It is about protecting your sensitive information from hackers and cybercriminals.
- This involves using strong passwords, firewalls, and antivirus software to create a shield around your data.

Safeguards your data from loss or damage.

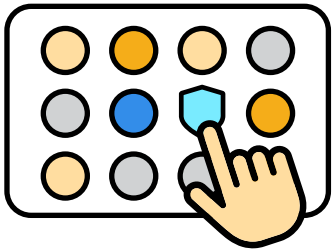
- It is like having an insurance policy for your digital assets.
- It is about ensuring that your important data is safe and recoverable in case of a disaster, such as a computer crash or a ransomware attack.
- This means regularly backing up your data and having a plan in place to restore it quickly.

64% of SMBs, however, consider preventing attacks on Data & developing a Cyber Resiliency Business Strategy a critical challenge

SMB Cybersecurity adoption business challenges

59%

Understanding Risk assessment



50%

Choosing business-relvant security technology

41%

Implementing security cost-effectively

Each of these challenges can be addressed - with a plan.

Data Security is the Essential First Step in the plan for a Comprehensive Cyber Resiliency Strategy

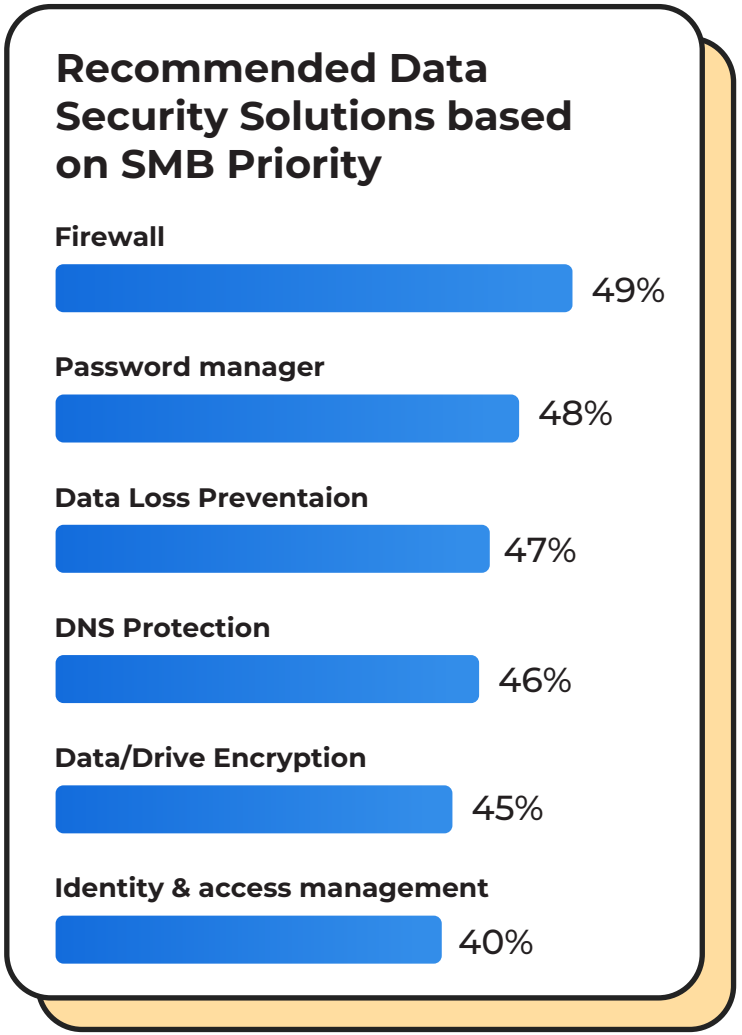
Data security protects the confidentiality, integrity, and availability of information.

- Confidentiality safeguards sensitive data from unauthorized access. A data breach can lead to catastrophic loss of customer trust, hefty fines, and legal repercussions.
- Integrity ensures data accuracy and reliability. Compromised data integrity can disrupt critical business operations like production, billing, and sales.
- Availability guarantees timely access to data. System outages due to data unavailability can result in lost customers, damaged relationships with suppliers, and operational disruptions.

What can SMBs do about data security?

SMBs employ a range of security measures to protect their data.

- Perimeter defenses like firewalls and identity and access management systems to prevent unauthorized entry.
- Data safeguards such as encryption, password managers, and data loss prevention to protect information from internal and external threats.
- System security measures, such as antivirus software, data encryption, and DNS protection, to fortify corporate systems and virtual environments.



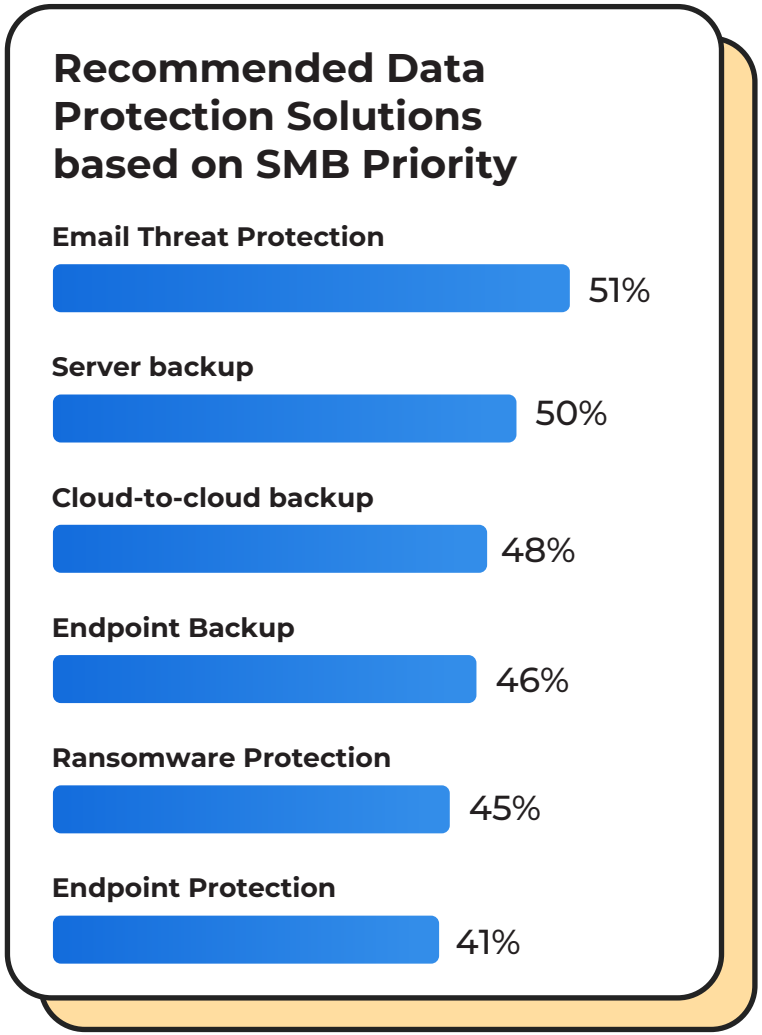
Data protection is the crucial complement to Data security

Data protection safeguards personal and corporate information from unauthorized access, misuse, or loss.

What can SMBs do to establish data protection?

To build a robust Data Protection strategy and safeguard their business, SMBs are prioritizing these essential data protection measures:

- **Comprehensive Backups:** Implement regular, reliable backups for all data, regardless of location (servers, cloud, endpoints).
- **Automated Protection:** Employ email and endpoint protection tools to prevent data loss through malicious attacks.
- **Threat Vector Defense:** Strengthen your defenses against cyberattacks by implementing Secure Access Service Edge (SASE) and Network Access Control (NAC) solutions.
- **Ransomware Resilience:** Invest in dedicated ransomware protection to safeguard critical data.

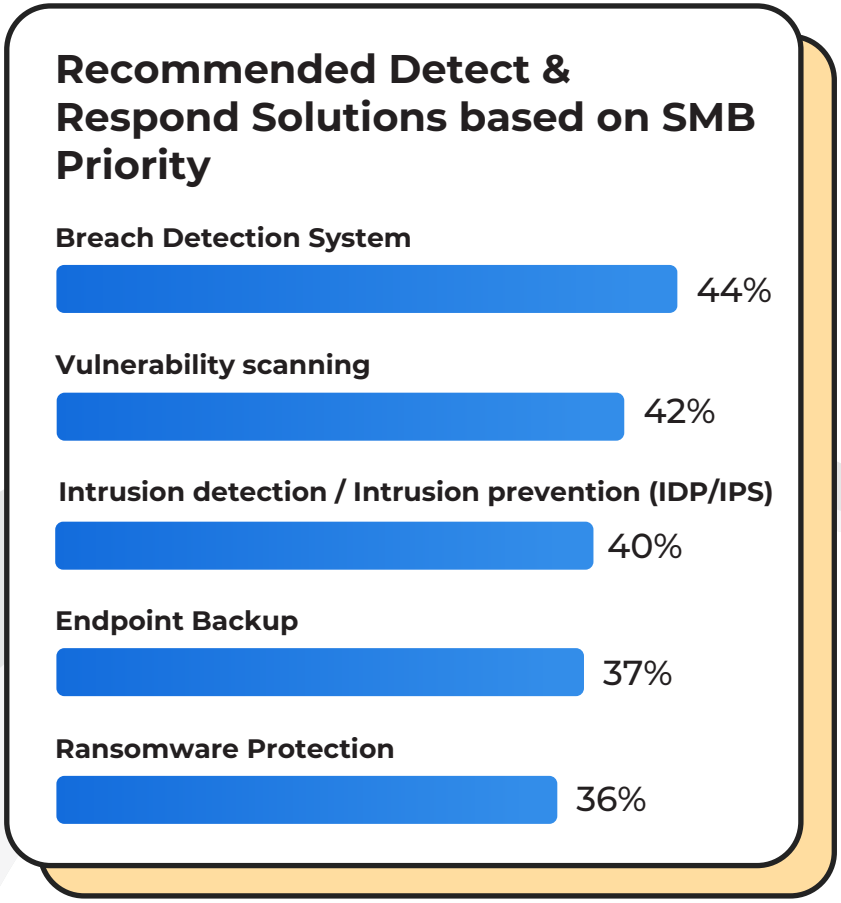


Detection and Response is the active shield that builds on the data security and data protection foundation

Complementary to data security and protection is a robust cyberinfrastructure that empowers SMBs to detect and respond to threats proactively. Given the complexities of threat detection and response, many SMBs rely on specialized third-party providers.

What should SMBs do to build detection and response capabilities?

- SMBs typically employ a combination of technologies to detect and respond to cyber threats. This includes tools for identifying vulnerabilities, recognizing attack patterns, and automating defensive actions. Breach detection systems and vulnerability scanners are widely used to identify potential risks.
- Managed detection and response (MDR) services offer an alternative approach, providing comprehensive threat detection, investigation, and response capabilities. Additionally, threat intelligence can enhance an organization's ability to anticipate and defend against emerging threats.



85%

SMBs say that data security and protection enable cyber resiliency and reduce business risk

In today's interconnected world, data flows freely between devices, users, and applications. SMBs prioritizing the recommended security solutions will be better positioned to thrive in the digital age, minimize business risk, drive a sound cyber resiliency strategy

Each business needs to chart a cyber strategy.

Here is a checklist to help you navigate the journey:

Organizational Commitment:

- [ ] We have identified cybersecurity as a top business risk and a strategic priority with significant investment and executive support
- [ ] We recognize the potential losses from cyber incidents and align our investments accordingly
- [ ] We use risk frameworks, train staff, have response protocols, and are confident in our recovery capabilities
- [ ] We measure cyber investments against business outcomes and demonstrate their value

Security Posture:

- [ ] We have implemented the recommended security solutions and frequently prioritize them in line with industry norms
- [ ] We formally assess risks, prioritize protections, and identify constraints
- [ ] We aim to recover quickly and continue operating during a cyber incident
- [ ] We study best practices from similar organizations and integrate them into our strategy

Count the number of check marks. If you scored:

1-3: you are behind the curve; 4-6: is typical, but you could improve; 7-8: shows you are ahead of the curve

Having a sound cyber strategy is not enough. Identifying the weakest link - the area where cyber defenses are not deployed or cannot stop breaches – is essential, too.

Here is a checklist to help identify your “weakest link”

Defend against intruders looking to access data

- [ ] Our firewalls are up-to-date, strong, and well-managed, effectively blocking unauthorized access
- [ ] We use a company-wide identity and access management system to ensure only authorized users can access our systems and data

Prevent disclosure of data by employees or devices

- [ ] We enforce strong password policies and regularly require password changes
- [ ] We use data loss prevention tools to prevent sensitive data from being accidentally or maliciously leaked

Protect data in corporate systems from theft or corruption

- [ ] We protect our virtual environments, both internal and cloud-based, with data security and antivirus solutions
- [ ] We encrypt data both at rest and in transit to prevent unauthorized access and data theft
- [ ] DNS security protects our environment from distributed denial of service attacks, which can lead to data loss

Automate defenses against common vulnerabilities

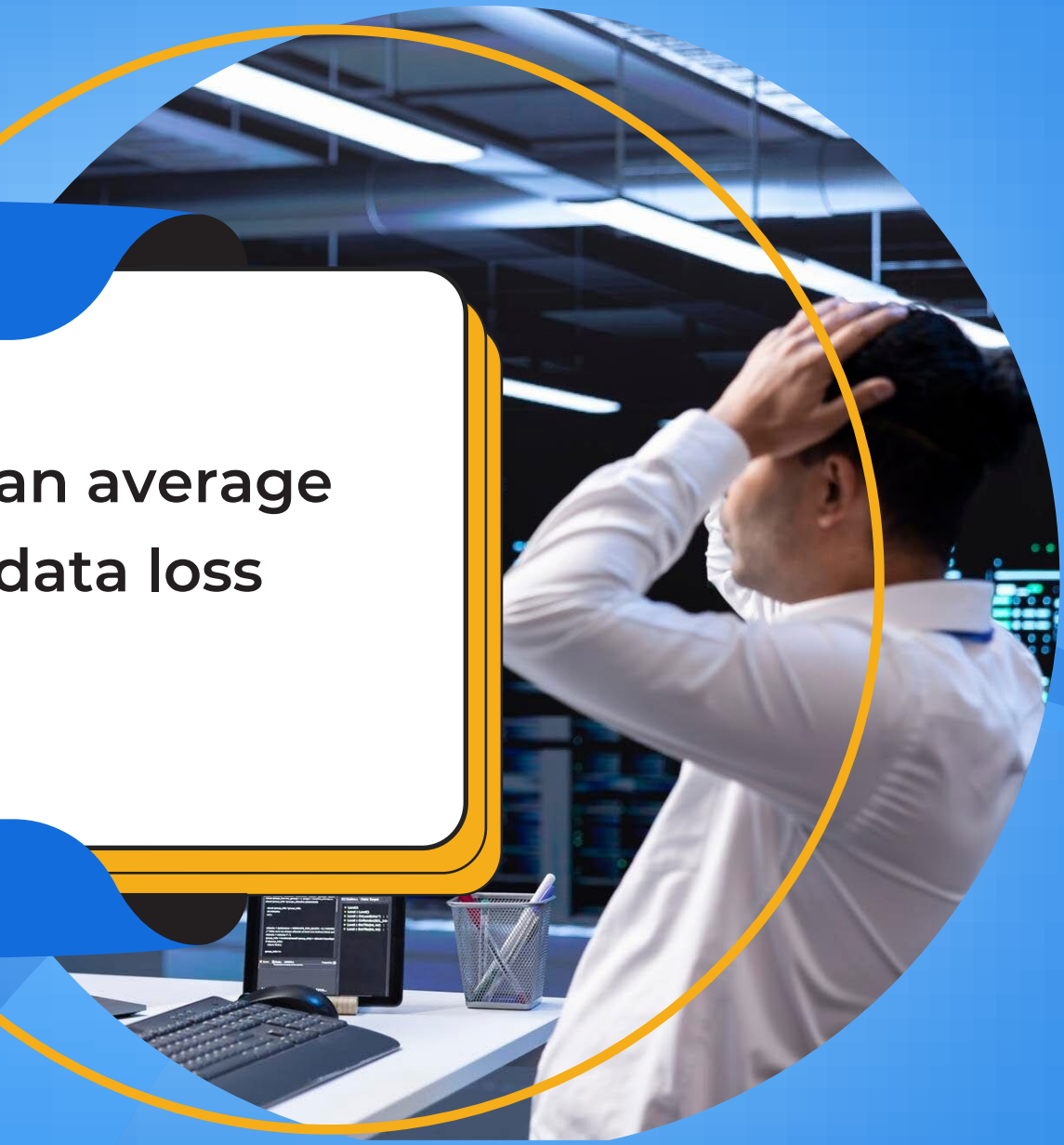
- [ ] We use business email compromise prevention measures, including internal training, to reduce the risk of phishing attacks
- [ ] Our endpoint protection platform allows our IT team to manage devices and apply security patches and policies centrally

Strengthen the network defenses

- [ ] We have implemented network access control to limit unauthorized access and prevent lateral movement
- [ ] We use SASE to protect against external attacks, including those targeting cloud-based connections
- [ ] We enforce least privileged access and other critical network defense policies to prevent lateral attacks

Backup the data your business cannot lose

- [ ] We have a comprehensive backup program for our internal servers, cloud data, and end-user devices



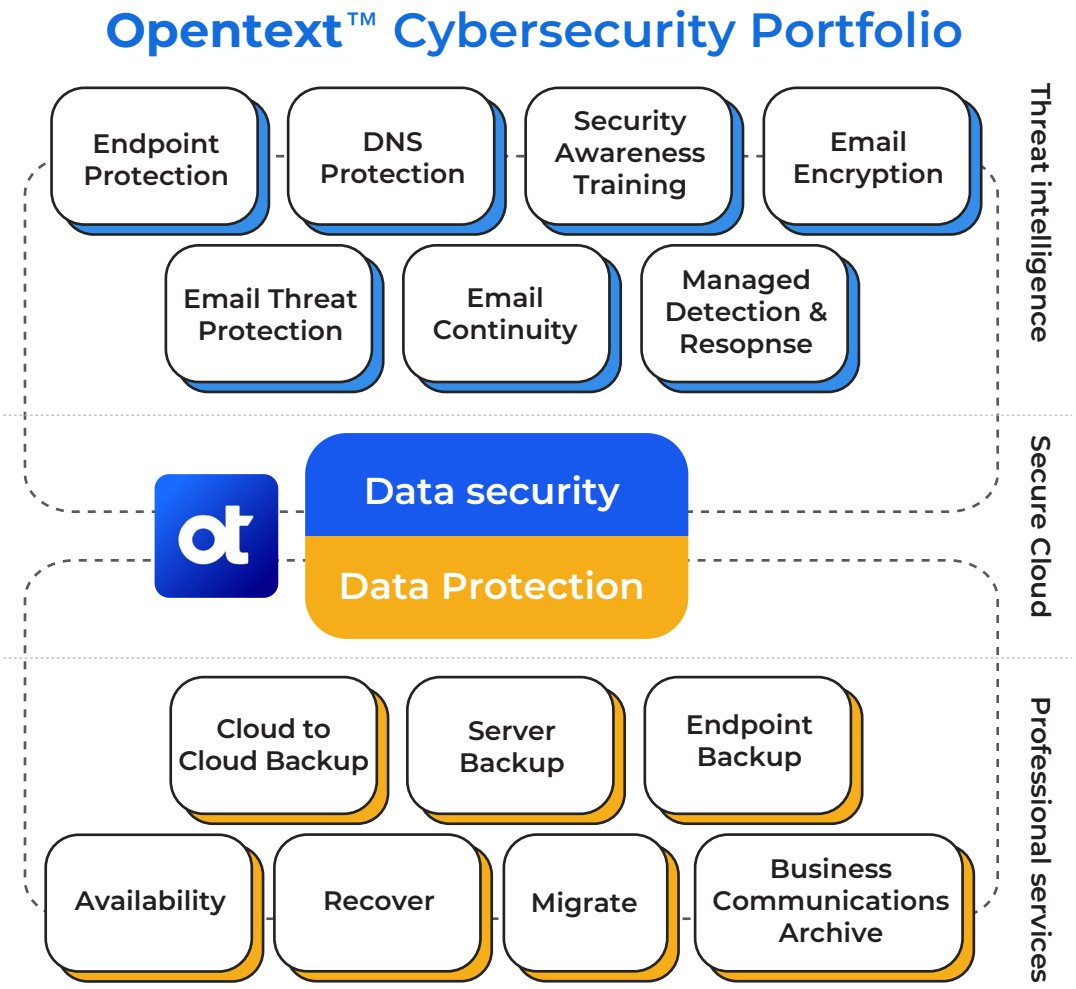
In 2023, SMBs lost an average of US$1.4M due to data loss and breach

The OpenText platform spans vital data security and data protection capabilities

Why OpenText?

The OpenText cybersecurity portfolio addresses critical SMB cybersecurity business requirements identified as priorities in Techaisle's survey of 2,100 SMBs:

- It is an integrated platform approach, combining products with critical services, which reduces the complexity that can derail SMB cyber defenses.
- OpenText also has strong relationships with MSSPs who can manage and augment the platform's capabilities.
- It addresses cloud security, which is critical for SMBs, who know that native cloud security is insufficient to protect their businesses.
- It is positioned to meet current SMB cybersecurity requirements and is designed to adapt to emerging needs. This adaptability ensures that the SMB business will be prepared for future cybersecurity challenges.



Next five steps to take to safeguard data as a business priority

1

Define cyber strategy in business terms:

Identify your most critical digital assets and assess the potential impact of a cyberattack on them.

2

Develop data security and protection as a core competency:

Data security is most effective when combined with data protection. Automated protection against vulnerabilities and well-managed backups can safeguard your high-value data and business viability.

3

Bolster detect and respond capabilities:

If you are not seeing cyber attacks, you need better threat detection. Once aware, you need to react quickly to stop or recover.

4

Increase effectiveness – reduce complexity:

Platform-based security and strong partners can overcome integration challenges for cyber success.

5

Don’t fall behind the cyber curve:

Cybersecurity is not a ‘set it and forget it’ endeavor. Consider adopting always-on, up-to-date security solutions and managed services to stay ahead.

techaisle

Contact:

www.techaisle.com

Ph: 408-2534416

Email: inquiry@techaisle.com

Techaisle is a top global market research firm focused on SMB, midmarket, upper midmarket, and partner ecosystems. We offer insights to help clients grow their market share through data-driven research and analysis. Our surveys of customers and channel partners reveal market trends and technology priorities across various topics like cloud, generative AI, managed services, mobility, analytics, PCs, collaboration, IT services, cybersecurity, and digital transformation. Our channel partner research provides deep insights into MSPs, VARs, SIs, and consultants. Techaisle's services include advisory and consulting, syndicated research, custom primary research, and competitive intelligence.