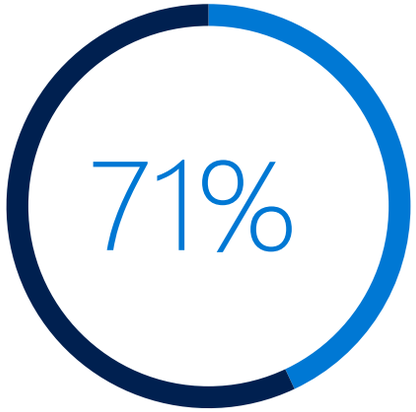
Microsoft

Protect your business against cyber threats and information loss

Author name: Veritech ICT Solutions
Date: June 2021

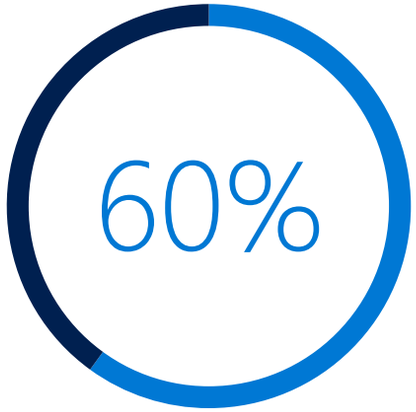
VERITECH
TECHNOLOGY FOR PEOPLE

Threat landscape for small businesses



of cyberattacks target small businesses

Devices are compromised by ransomware every month



of small businesses close their doors after a cyberattack

is the average cyber attack remediation cost for small businesses

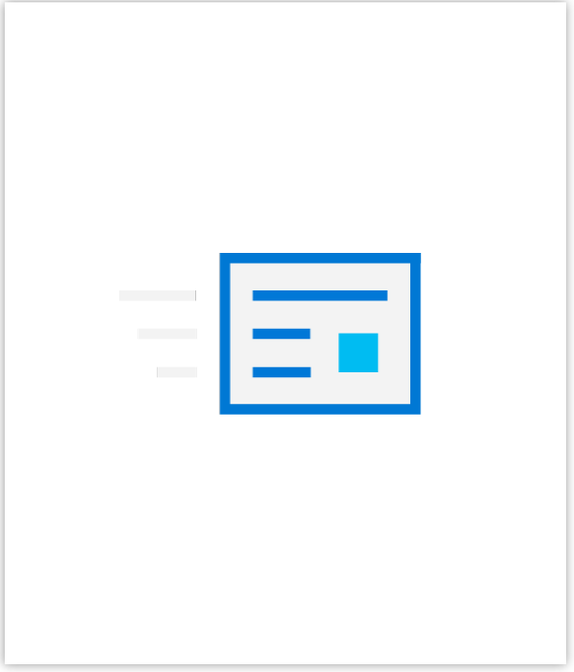
VERITECH
TECHNOLOGY FOR PEOPLE

Why are attacks so successful?

It only takes hackers 4 minutes to get in your network, but 99+ days for businesses to discover they've been breached.

VERITECH
TECHNOLOGY FOR PEOPLE

Where are the biggest security pains for small businesses?

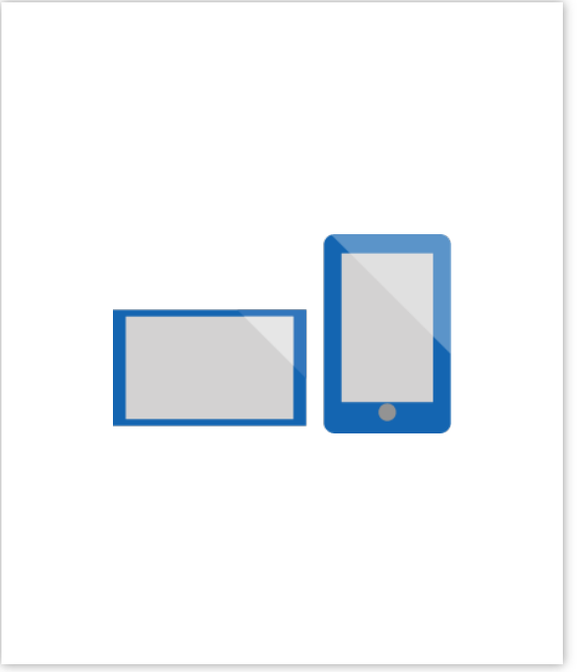


Email

Subpar antivirus antispam doesn't catch attacks

Users click on ransomware and phishing links

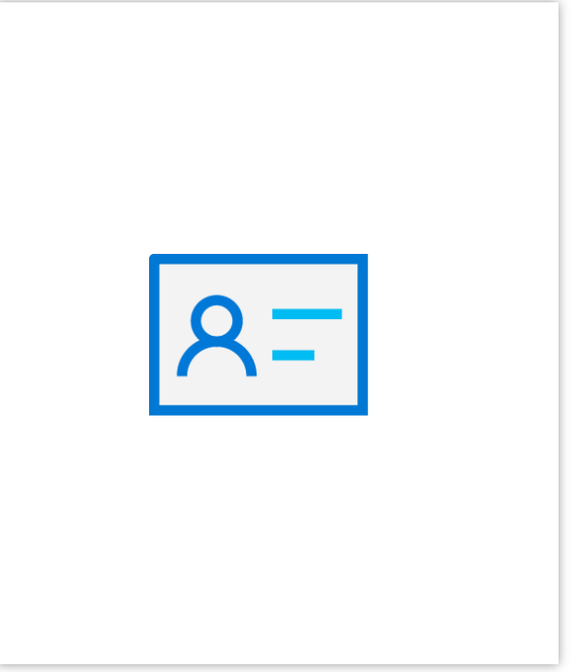
Accidentally send confidential data



Mobility

One extreme: Prohibit use because of security concerns

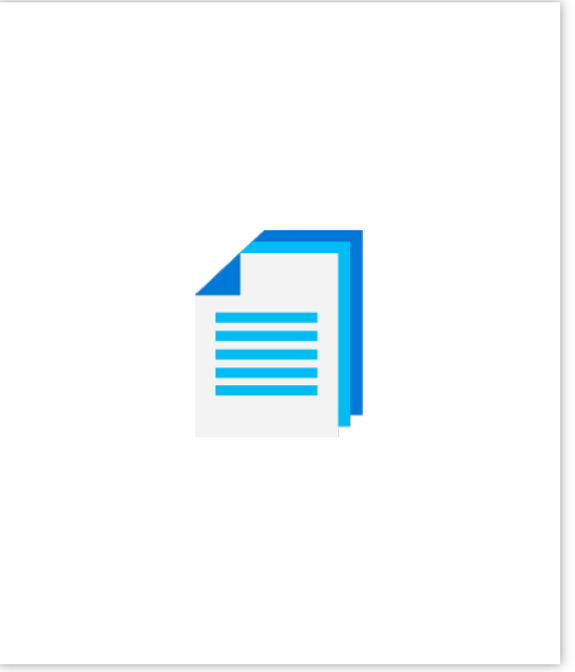
Or the other: Don't provide any protection for data on devices



User credentials

Users have same passwords across all accounts, increasing risk if compromised

Attackers have sophisticated methods to easily steal credentials



Compliance

Standards don't change based on company size

Requirements for GDPR and other regulations are rigorous and complex

Why don’t small businesses have the security they need?

Common misconceptions about small businesses contribute to the problem.

Security is too complex

While SMBs may not have in-house IT departments, that doesn’t mean they can’t implement comprehensive security. Technology and services can radically reduce complexity while also providing strong protection.

Security is too expensive

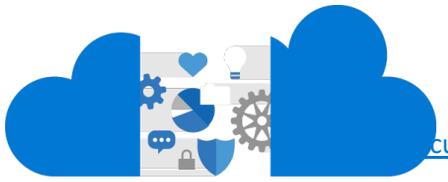
SMBs typically spend about **15%** of their budget on security or **$1,320/user** annually. To increase protection, you don’t need to necessarily increase IT spend – just adjust how you are spending your dollars.

Security is not a business priority

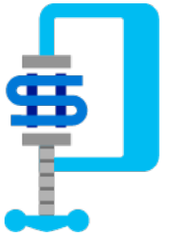
Small businesses that deal with customer information – whether they are retail, financial, health care, or food services – have the same accountability to secure data as big enterprises, so they need enterprise-level protections.

Microsoft 365 Business

Business savvy way to reduce risk



curity assessment link



Simple

One solution

Cloud platform simplifies deployment

Use this security assessment link well your business is protected from cybersecurity risks

Reduces costs

Eliminates costs for multiple third-party vendor solutions

Reduces maintenance and management costs

Aligns with business goals

Security built into your productivity platform

Don’t need to make trade-offs to justify security investment

Protect business against risk-related costs

Microsoft 365 Business security benefits

Safeguard your business against external threats and leaks

Protect against security threats

Protect business data against leaks

Control who has access to business information

VERITECH

TECHNOLOGY FOR PEOPLE

Protect against security threats

Protect inboxes against spam and viruses

Block ransomware and phishing attacks

Keep Windows 10 devices safe from sophisticated malware

1 Verizon 2017 Breach Investigations Reort (ref. P11 of Security Playbook)
2 Security Week Survey (ref P35 of Security Playbook)

Protect your business against data leaks

Restrict copying and saving of business information

Block sharing of sensitive information like credit card numbers

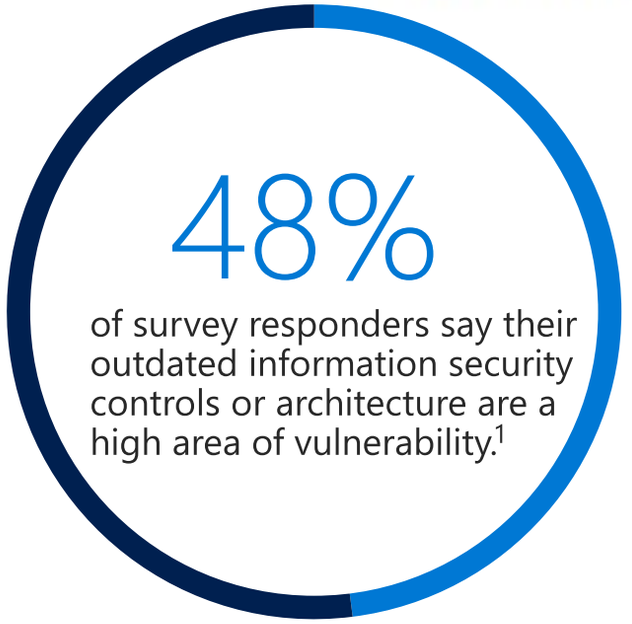
Prevent unauthorized users from opening or viewing sensitive documents

Encrypt data on mobile devices

Wipe data on lost or stolen devices

Back up email in secure archive

[1] 2016 EY Global Information Security Survey http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016.
[2] 2016 Ponemon Institute Cost of a Data Breach Study https://securityintelligence.com/media/2016-cost-data-breach-study/



Control who has access to business information

Only let the good guys in

Know who is accessing your data

Keep credentials safe

Confirm identities with multi-factor authentication

Quarantine compromised devices

Prevent non-compliant devices from accessing your systems

1 Verizon 2017 Breach Investigations Report (ref. P11 of Security Playbook)
2 Security Week Survey (ref P35 of Security Playbook)

Our expertise + Microsoft 365 Business

VERITECH

TECHNOLOGY FOR PEOPLE

Secure the Front Door

Identity-Driven Security

Go beyond passwords and protect against identity compromise, while automatically identifying potential breaches before they cause damage.

- Risk-based Conditional Access and Multi-Factor Authentication
- Advanced security reporting
- Identify threats on-premises
- Identify high-risk usage of cloud apps, user behavior, detect abnormal downloads, prevent threats

Secure Content

Protect content: creation, transit, consumption

Use cloud applications without putting company information at risk by adding protection, ranging from access privileges to data encryption.

- Shadow IT Detection: Discovering Apps and Risk Scoring
- Intelligent Classification and Tagging of content
- Document encryption, tracking, revocation
- Monitoring shared files and responding to potential leaks
- Data segregation at a device/app level

Secure Devices

Workplace Issued or BYOD Devices

Manage company and BYOD devices to encrypt data and ensure compliance, automatically detect suspicious activities, and quickly block, quarantine, or wipe compromised devices.

Shadow IT Detection: Discovering Apps and Risk Scoring

- Conditional Access
- Device and App access level controls: PIN
- Device and App encryption at rest
- Save-As, Copy, Paste restrictions
- Device and App level data wipe

Microsoft 365 Assessment

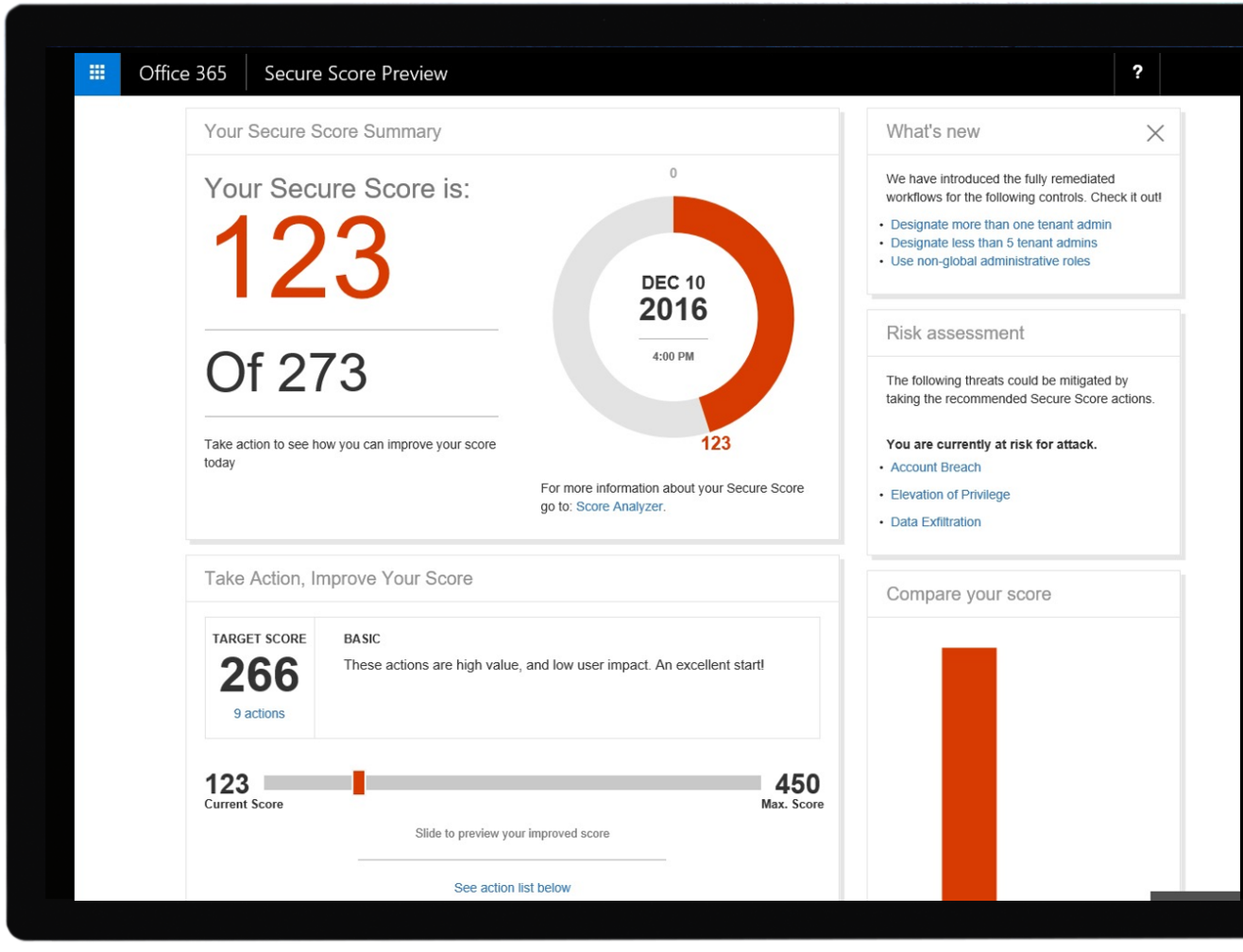
How secure are you today?

- Identify security objectives
- Assess current security state
- Provide customized recommendations and best practices
- Create an actionable security roadmap

Security monitoring service

Get daily insight into your security risk profile

- Establish security baseline
- Continuous monitoring and reporting to reduce risk
- Integrate data into compliance or cybersecurity apps to improve overall protections



Managed Identity Service

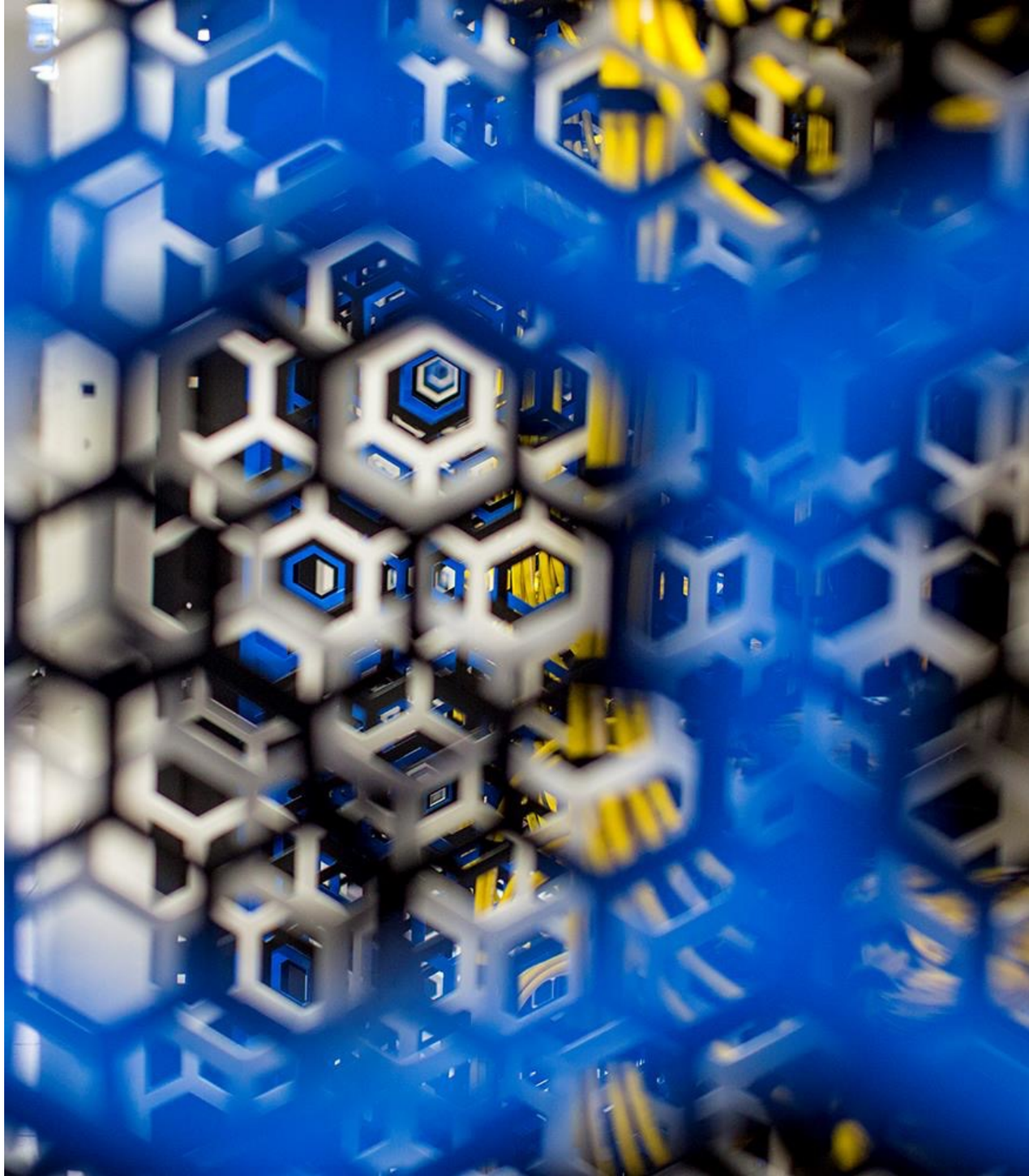
Ensure that only your employees are accessing your systems.

Keep bad guys out	Threat monitoring and prevention to block viruses, malware, ransomware, phishing, and spam attacks
Only let the good guys in	Identity & access management for limiting access to business apps and servers
Show how you stopped them	Power BI automated dashboards to show incidents logged and threats prevented.

Secure content service

Prevent customer and business data from falling into the wrong hands.

Enforce who can open documents	Document encryption monitoring and remediation
Don’t accidentally share confidential information	Monitoring and enforcement for access to shared files in email and team sites
Encrypt corporate data on mobile devices	Separation of personal information and business information on phones and tablets
Prove that you’ve kept information safe	Archiving and compliance reporting for email and/or backup and disaster recovery



Managed Identity Service

Ensure your employees can safely work on their smart phones and tablets.

Secure every employee device	Endpoint security monitoring and remediation for laptops, PCs, tablets, and phones
Create ready-to-use secure devices	Device as a service offering that includes hardware support
Don’t let corrupt devices talk to your systems	Corrupt device quarantining and download prevention
Lock down lost or stolen devices	Remote wipe