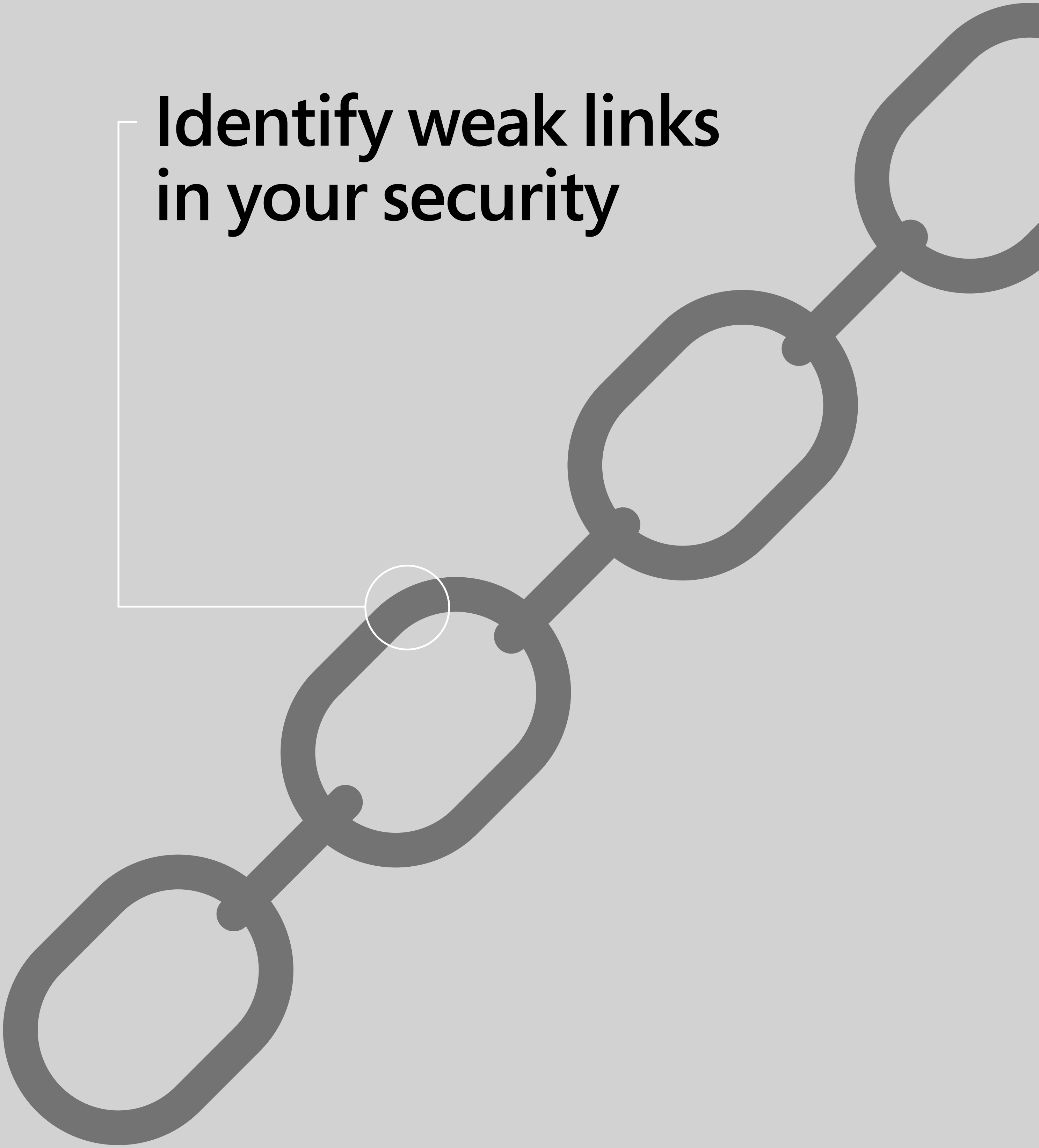
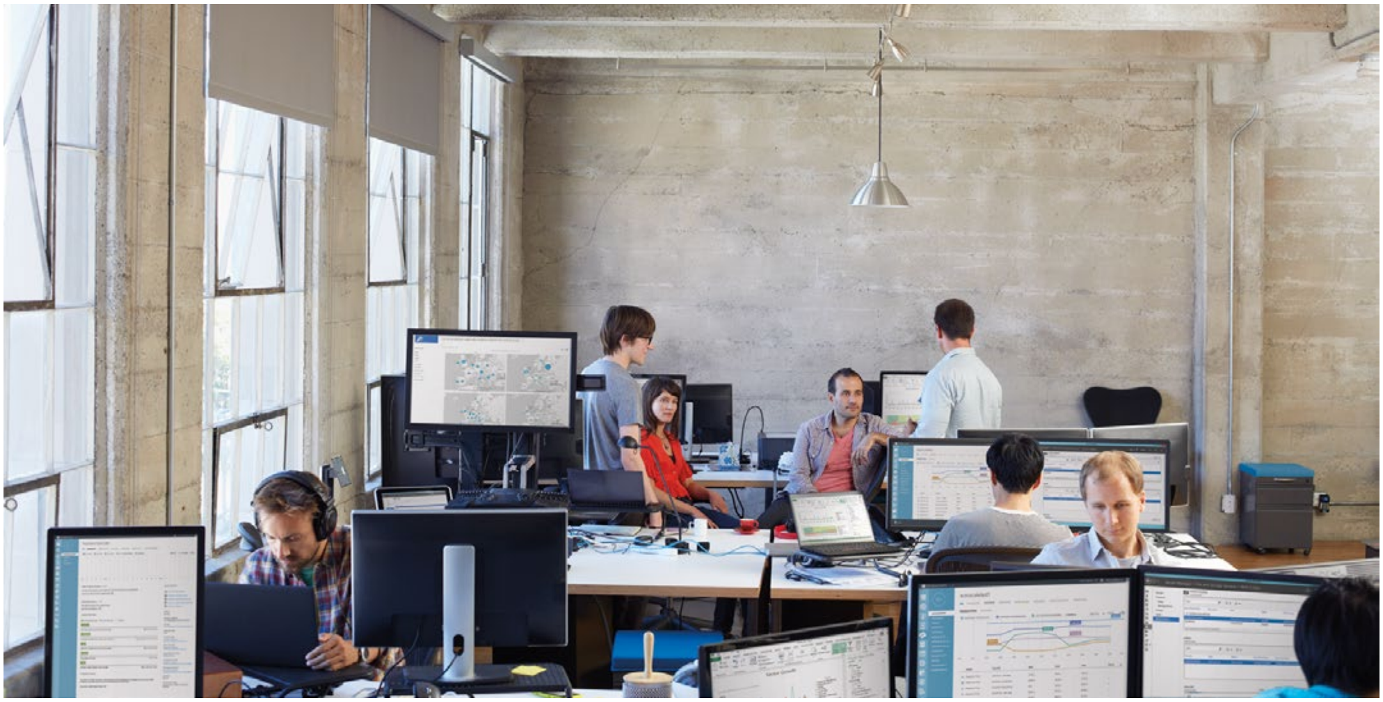
Microsoft

Identify weak links in your security





Increase your protection by finding and monitoring security issues, fast.

Weak links in your chain of security defences – no matter how small – leave your company open to costly breaches. Information loss is now the most expensive consequence of cybercrime, closely followed by business disruption and loss of employee productivity.[1] The fast-paced nature of today's businesses, paired with the increasing demand for more data and innovation, requires security that evolves as fast (or faster) than the threat landscape.

Robust security relies on the full chain's strength; one weak link could have a significant impact on your business. Explore the most common sources of leaks, what they mean for your business and how you can better protect your entire network.

When your security is compromised from within

Even with the best security systems in place, the unpredictability of end users from within your network often weakens security links. Here's a closer look at end-user activities that can create breaks in your security chain, along with tips for prevention.

42%

Although 42% of data breaches are caused by tech errors, human error is still the leading cause, at 58% internationally.[2]

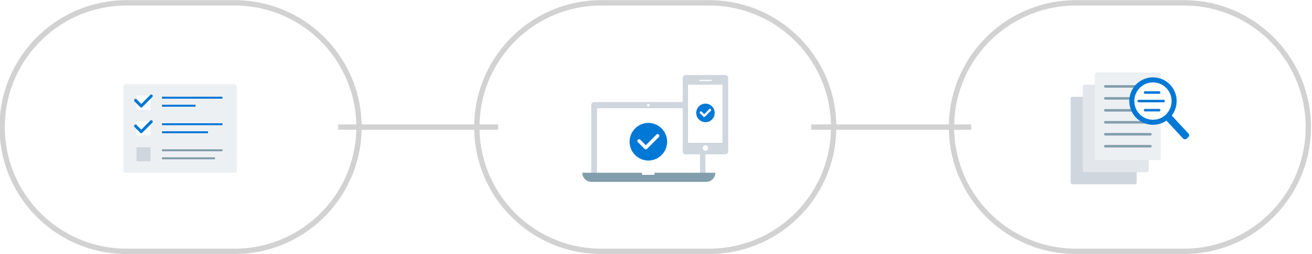
Possible breaches from local and remote workforces

As the number of devices and locations that employees can work from increases, so does the threat potential. Companies are no longer confined to a single space, but rather, spanning countries and time zones, while our systems are connecting full-time employees, vendors and contractors through multiple devices. Each new device and end user connected to your network is another entry point for a potential attack.

67%

of IT security practitioners are unable to detect which employees use insecure mobile devices, which puts sensitive data at risk.[3]

Strengthen your chain:



01

When it's difficult for employees to access information, end users will try to find ways around IT and security policies to get their jobs done quickly and efficiently. Enable your workforce to be compliant by providing them with easy access to approved company data and tools across devices, both in the office and remotely.

02

Leverage multi-factor authentication and mobile application management to help prevent unauthorised access to company information.

03

Give your IT team the tools to monitor and remotely identify and resolve issues or to wipe devices when threats arise.

Intentional breaches from within

Unfortunately, employees sometimes purposefully misuse company data. Even small leaks can lead to significant losses.

60%

of employees who leave with secure data do so in the hope of profiting from it in the future.[3]

71%

of cases of insider misuse target personal and medical information.[3]

Strengthen your chain:

01

Use tools that can monitor suspicious activity within your network and shut down a user account.

02

Personalise access to specific roles and responsibilities within your organisation.

03

Make it easy for IT to give employees access when they need it and to remove it when they don't.

Microsoft 365 E5

Discover the Microsoft 365 Enterprise Solution that's right for your business

- Office 365 Advanced Security Management gives you insight into suspicious activity so you can investigate situations that are potentially problematic and, if needed, take action to address security issues.

- WithCloud App Security, discover all the cloud apps in your network, gain visibility into Shadow IT and assess risk – no agents required.

- Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric system or a PIN.

- Azure Active Directory is a comprehensive identity and access management cloud solution with a robust set of capabilities to manage users and groups. It helps secure access to on-premises and cloud applications, including Microsoft web services like Office 365 and many non-Microsoft Software-as-a-Service (SaaS) applications.

When your infrastructure is threatened by external malicious sources

Attacks from outside your organisation with malicious intent are a common cause of security breaches. Methods such as social engineering have existed as long as mankind – and certainly as long as people have been sending emails and browsing the Internet. With increased awareness comes increased creativity from attackers, and even the savviest end user can fall victim.[5]

3.3

billion credentials were reported stolen in 2016.[6]

23%

of social engineering phishing attacks are successful due to recipients opening the messages.[6]

Here are five common types of social engineering attacks:[7]

Phishing

Redirects users to suspicious URLs that appear legitimate, to steal credentials or other personal information.

Pretexting

Creates a fake scenario to gain user trust in order to steal personal information.

Baiting

Infected USB drives or disks are left in public places, in the hope that someone will insert them into a computer. This tactic can also be found on the web in the form of download links.

Tailgating

Attackers gain access to restricted areas by following an employee with proper authentication.

Quid pro quo

Promises some kind of benefit for the victim's information.

Recovering your data, at a price

Ransomware (attackers holding data ransom for a hefty fee) isn't just increasing in frequency; more victims are also paying to get their data back. Ransomware can be avoided by reverting back to the basics: awareness, education, hygiene, frequent backups, a plan of action and, certainly, software.

6,000%

Ransomware increased 6,000% from 2015 to 2016.[8]

40%

Ransomware was in almost 40% of all spam messages in 2016.[8]

70%

of victims paid hackers to get their data back. Of those who paid, 50% paid £7,500+ and 20% paid £30,000+.[8]

Microsoft 365 E5

Discover the Microsoft 365 Enterprise Solution that's right for your business

- When your PC is protected by Windows Defender Antivirus, you get comprehensive protection for your system, files and online activities from viruses, malware, spyware and other threats.

- Office 365 Advanced Threat Protection protects your company's emails in real time against unknown and sophisticated attacks by securing your Office 365 environment from advanced threats, unsafe files and malicious links clicked within those files.

- BitLocker Drive Encryption works seamlessly with Windows 10 and addresses the threats posed by data theft or exposure from lost, stolen or inappropriately decommissioned computers.

Quickly detect and address security breaches

The cost of a data breach is greatly impacted by the time it takes to identify and contain the breach. Your ability to quickly recover can potentially save millions of pounds.

ESTIMATED AVERAGE COST OF BREACH[9]

<100 days

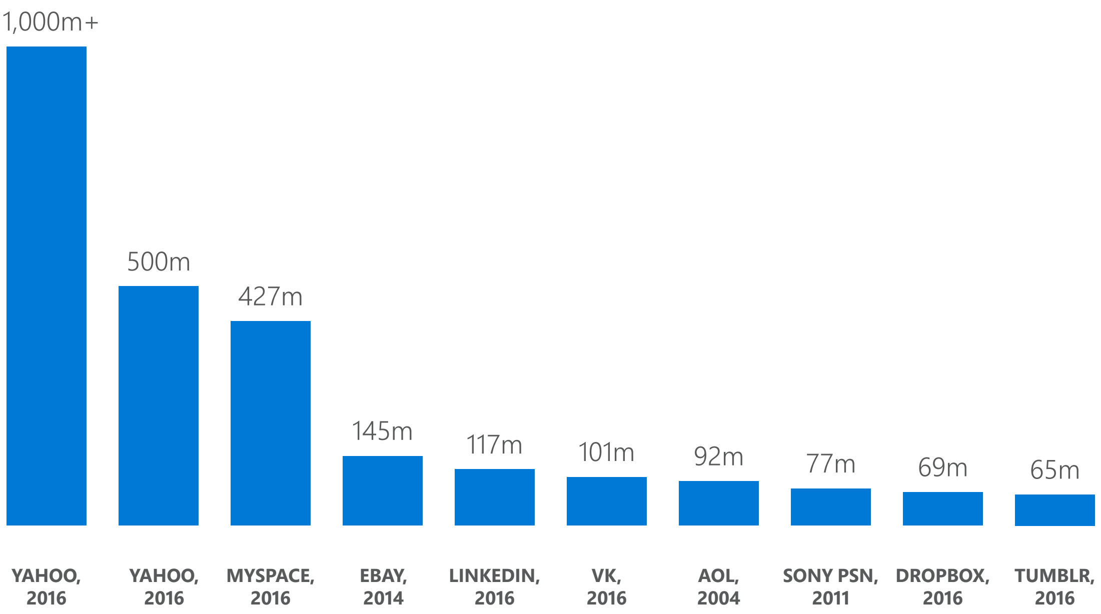
£2.14 million

>100 days

£2.93 million

Data breaches are costly, especially without the proper groundwork for early detection. Here's how some top companies have been affected by costly breaches.

As we think about security as a chain, it is important to make sure every link is strong. Rushing to implement solutions that are inadequate may compromise your security, and you might not realise the consequences until it's too late.


Largest data breaches, 2004–2016[10]

Globally, organisations were able to reduce the days to identify a data breach from approximately 201 days on average in 2016 to 99 days in 2017. The average days to contain a data breach decreased from 70 to 66 days.[9] The faster a data breach can be identified and contained, the lower the costs. Therefore, it's important to make sure your business is equipped with the right tools to quickly identify and contain breaches.

Microsoft 365 E5

Discover the Microsoft 365 Enterprise Solution that's right for your business

- Windows Defender Advanced Threat Protection helps you detect, investigate and respond to advanced attacks and data breaches on your networks.

- Advanced Threat Analytics reduces your risk of costly damage and gives you all the information you need in a succinct, real-time view of the attack timeline. Plus, all the intelligence to learn, analyse and identify normal and suspicious user or device behaviour is built in.

- Office 365 Threat Intelligence enables broad visibility into the threat landscape, removes the noise, then provides rich insight into how these threats impact your organisation. Ultimately, this visibility and insight enables organisations to proactively update security policies and services to mitigate incidents.

Take a holistic approach to address weak links and strengthen your entire security chain.

Microsoft 365 provides a fully integrated, end-to-end toolkit of defences and addresses every component of your chain of security measures. Choose a trusted, secure and productive way to work that brings together the best of hardware, software and network security.

Discover how Microsoft 365 Enterprise can protect your business with intelligent solutions that empower everyone to be creative and work together securely.

Sources:

1. "Cost of Cyber Crime Study & the Risk of Business Innovation", 2016, Ponemon Institute
2. "International Trends in Cybersecurity", 2016, Comptia
3. "The Cost of Insecure Mobile Devices in the Workplace", 2014, Ponemon Institute
4. "2017 Data Breach Investigations Report", 2017, Verizon
5. "2017 Credential Spill Report", Shape Security
6. "Anatomy of a Social Engineering Attack: Exploiting Human Behavior", 2016, PricewaterhouseCoopers
7. "5 Social Engineering Attacks to Watch Out For", 2015, The State of Security
8. "Ransomware: How Consumers and Businesses Value Their Data", 2016, IBM
9. "2017 Cost of Data Breach Study", Ponemon Institute
10. "Latest Yahoo Attack is the Largest Data Breach to Date", 2016, Statista

© 2017 Microsoft Corporation. All rights reserved. This document is provided "as is". Information and views expressed in this document, including URLs and other Internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal reference purposes.

Microsoft