


Guide to strengthen and streamline security

Three strategies to streamline and strengthen security during times of change

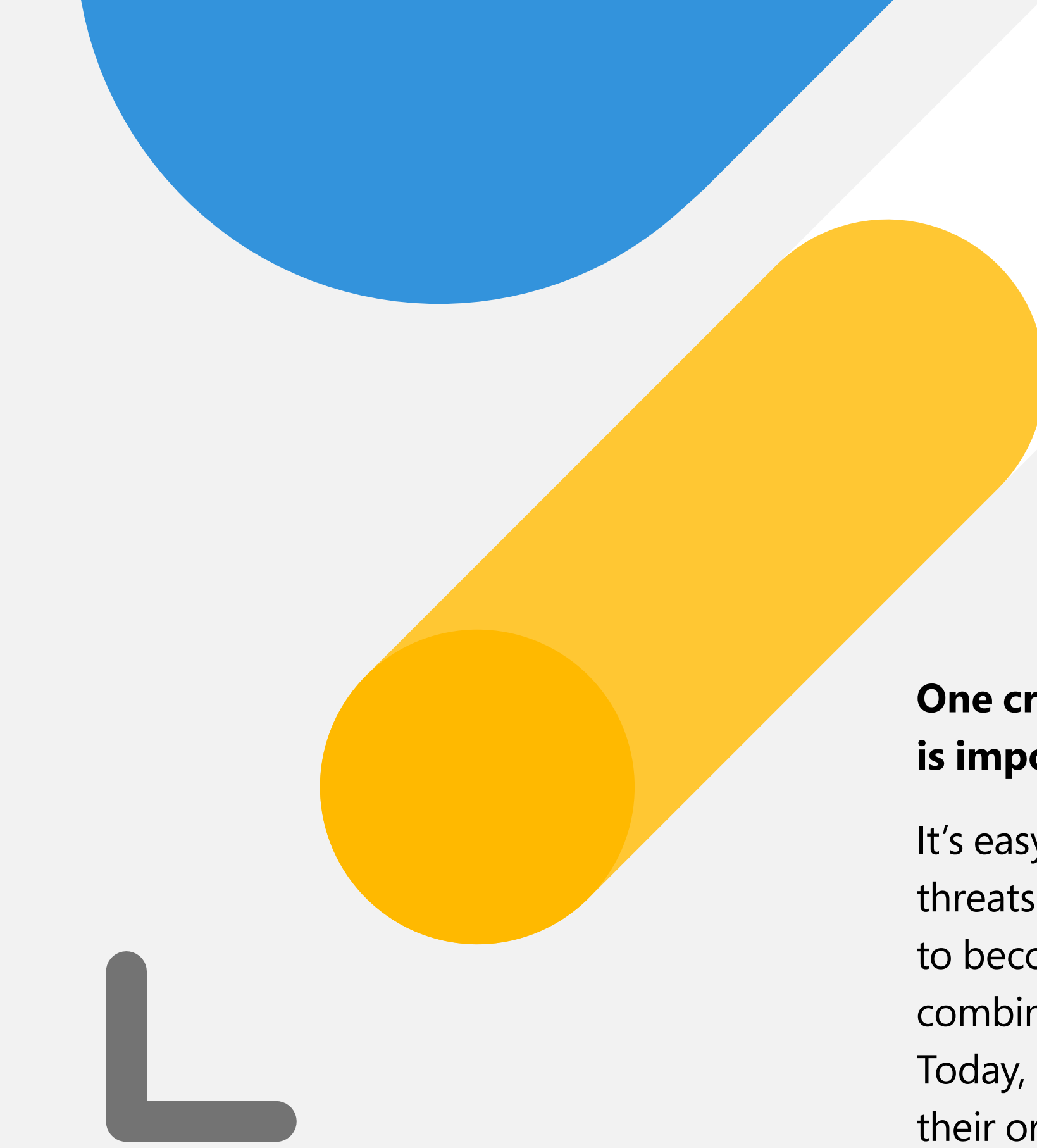
- ✓ Create an efficient, cost-effective approach to security
- ✓ Deliver seamless end-user experiences
- ✓ Reduce cyber-risk with integrated, best-in-class protection



An abstract graphic design featuring a light gray background with several overlapping white rounded rectangular shapes. A prominent blue diagonal bar runs from the bottom left towards the top right. On this bar, there are two blue circles. To the left of the bar, there is a dark gray L-shaped corner element and a dark gray circle. Below the bar, there is a yellow circle. The overall aesthetic is clean and modern.

It is hard to fathom the amount of change most organisations have faced over the past year. This change required organisations to digitally transform quicker than originally planned. Whether that be quickly transitioning people to remote work, evolving financial models and business strategies or trimming budget or forecasts to adapt to the new world of work:

Business and technology leaders are under pressure to make decisive decisions, in order to become more resilient.



One critical area where operational resilience is important is with cybersecurity.

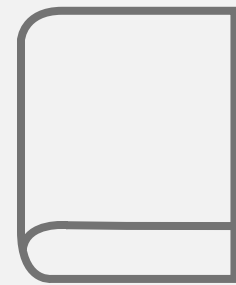
It's easy to fall into a reactive mode in responding to new threats or quickly changing business needs but in order to become resilient you need to develop a strategic combination of planning, response and recovery. Today, only 42% of global executives are confident their organisation can recover from a major cyber event without impacting their business.¹ To maintain cyber resilience, one should be regularly evaluating their risks and risk thresholds and their organisation's ability to operationally manage those risks through a combination of human efforts and technology products and services.

It is important for leaders to take the time now to assess security environments and develop an approach that can accommodate change while being efficient with resources, enabling user productivity and reducing cyber- risk with best-in-class security. Here we take a practical approach to exploring how you can streamline and strengthen your security, drawing from third-party research that Microsoft commissioned to Forrester and real-world results from our customers.

Several topics we will explore include:

- ✓ Savings on automation and process improvements
- ✓ Reduced total cost of risk
- ✓ Security vendor cost consolidation
- ✓ IT administration and deployment savings

¹ Forbes Insight Study, 'Perception Gaps in Cyber Resilience', August 2019.



Resource guide

This guide provides you with practical steps you can take to streamline and strengthen your security with Microsoft 365 E5 to protect against new security threats while managing the rising costs to the organisation. Refer to the below list to identify areas of interest for you and use the links to jump directly to that information.

Challenges

Security landscape cost and complexities

Procurement and IT management of multiple security vendors is difficult, time-consuming and expensive.

Our IT team spends too much time trying to make our estate of security products connect to each other, and to our internal systems.

Maintaining a diverse set of security products to protect across multiple fronts is costly.

End-user productivity and security

Our employees cannot remember every unique password for each business app, burdening our help desk with calls and added costs.

We are concerned that by having a multi-vendor approach to security, we deliver an inconsistent security experience for users and introduce new performance and support challenges.

We lack a consistent way to enforce security for sensitive data, from how it's accessed, to how it's shared.

Increasing cyber-risks

We're worried about the patchwork of expensive domain specific security tools that don't understand incidents from a holistic end to end perspective leaving us vulnerable to new threats.

Our security team is overwhelmed by the high volume of security alerts we receive.

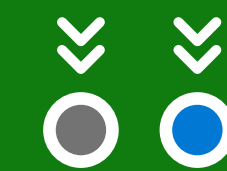
We're too slow when responding to threats – we have too many tools, making it hard to get end-to-end visibility and prioritise actions.

Start with



Create an efficient, cost-effective approach to security.

Microsoft can help you streamline your security vendor landscape so you can realise savings with an integrated, large-scale security solution.



Deliver seamless end-user experiences for greater security.

Microsoft can help you streamline your end-user experiences so they can be more productive, and your IT teams more efficient.



Reduce cyber-risk with integrated, best-in-class protection.

Microsoft can help you reduce your cyber-risks with an integrated, best-in-class protection for your organisation.

Create an efficient, cost-effective approach to security.

The reality for most organisations when it comes to their security landscape is one of complexity and high costs. Many organisations have upward of 100 security products across a multitude of security vendors.² Managing all of this complexity and protecting against new and existing threats isn't easy. A recent study found that 88% of organisations that consolidate their security portfolio diminished their risk of breach.³

Lower cost of ownership

Microsoft's unified approach to security can help reduce your security landscape total cost of ownership. Organisations can identify ways to consolidate security vendor licensing costs where Microsoft 365 E5 Security provides comparable solutions across key security categories as:

- ✓ Identity and access management
- ✓ Threat protection
- ✓ Cloud security
- ✓ Data protection
- ✓ Unified endpoint management

With Microsoft E5 Security, you get a leading solution while reducing security costs and complexity through consolidating.

That's because Microsoft is recognised as a Leader by Gartner and their Gartner Magic Quadrants across all five categories with Microsoft Security: access management; cloud access security brokers; enterprise information archiving; endpoint protection platforms; unified endpoint management tools.

Click below for more information on Microsoft's recognition in Gartner's Magic Quadrants.

[Learn more](#)

² BizTech Magazine, 'RSA 2019: Most Organisations Use Too Many Cybersecurity Tools', March 2019.

³ Forrester Consulting, 'Achieve greater security through simplicity', December, 2018.



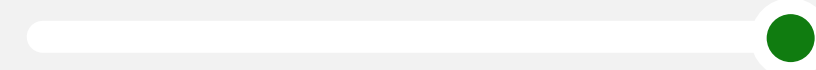
On average, you can save 60% with Microsoft Security

Save 60% with Microsoft Security

With Microsoft Security, you can replace up to 40 disparate products with integrated, end-to-end security, across the five security categories. On average, you can save 60% with Microsoft Security by consolidating security capabilities like cloud security, email protection, endpoint protection, endpoint detection and response and identity management.

For example, an average multi-vendor security strategy can cost USD 30 per month (based on published prices across disparate security solutions based on typical use). You can lower that cost by consolidating those security capabilities, adding Microsoft 365 E5 Security to your existing Microsoft 365 E3 subscription for only an additional USD 12 per user, per month.

Average multi-vendor security



Microsoft security solutions

USD 30
per user

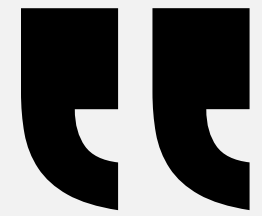
USD 12
per user

- USD 6** Cloud access security broker
- USD 5** Email protection
- USD 7** Endpoint protection platform
- USD 7** Endpoint detection and response
- USD 5** Identity Governance and Protection

Microsoft 365 E5 Security add-on to Microsoft 365 E3

+

Microsoft 365 E3



We recognised the best-in-suite value of Microsoft 365 E5 not just from a security perspective. We realised we could get everything we needed with one licence... If we had used separate vendors, it would absolutely have cost more, in addition to the complexity of managing multiple products and contracts.”

Doug Howell

Director of IT, The Little Potato Company

Driving operational efficiencies with a unified approach to security

Microsoft Security is designed to work seamlessly across your employee identities, devices, apps, data and cross-cloud infrastructure. This unified approach streamlines security management tasks through automation and process improvement opportunities that are built around holistic end-to-end visibility rather than a series of domain specific silos. Your IT and Security teams will be spending less time sifting through hundreds if not thousands of security alerts and multiple consoles – freeing them up to focus on the most important security, and compliance matters.

Lower cost of ownership data points⁴

Lower cost of ownership

Annual value

Vendor licence cost consolidation:

USD 4,300,000

Reduce licence cost by

⁴ Rounded estimates based on Forrester TEI reports and Microsoft Total Cost of Risk calculator and illustrate first-year savings for a 20,000 employee organisation. Contact your Microsoft representative for estimates for your organisation.





We no longer have to worry about what security product we'll use. With Microsoft 365, we're covered."

Itzick Menashe

VP IT and Information Security, Telit

Guide to strengthen and streamline security

Operational efficiencies

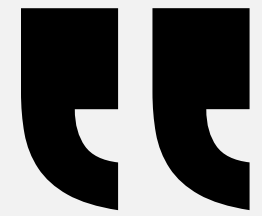
Microsoft, working with customers and research organisations like Forrester, has created a total cost of risk calculator that returns cost-savings opportunities based on your organisational parameters (e.g., number of employees, device, etc.). Here we look at a composite company with 20,000 employees that can benefit from the operational efficiencies that Microsoft Security provides.

Operational efficiency benefits ⁴	Annual value
Integration efficiency gains	USD 126,000
Lower costs to support third-party solutions	USD 150,000 ⁵

⁴ Rounded estimates based on Forrester TEI reports and Microsoft Total Cost of Risk calculator and illustrate first-year savings for a 20,000 employee organisation. Contact your Microsoft representative for estimates for your organisation.

⁵ 'The Total Economic Impact™ Of Microsoft FastTrack', Forrester, October 2017.





With the deployment of Microsoft 365 E5, Threat Intelligence supports organisations as they consolidate security solutions onto a single platform, reducing licensing costs on a myriad of third-party solutions.”

Forrester

Faster time to value

Another challenge organisations face is the time, cost and complexity required to deploy new security solutions. Microsoft understands this challenge and provides resources to accelerate time to value, including **Microsoft FastTrack**, which, on average, reduces the time to onboard Microsoft security capabilities by one month.⁵

- ✓ Gain faster elimination of costs associated with the previous environment
- ✓ Get faster access to value with increased security and productivity

Faster time to value data points⁶

Faster time to value	Annual value
Deployment cost reduction with Microsoft FastTrack	1,300,000 USD

⁵ 'The Total Economic Impact™ Of Microsoft FastTrack', Forrester, October 2017.

⁶ Rounded estimates based on Forrester TEI reports and Microsoft Total Cost of Risk calculator and illustrate first first-year savings for a 20,000 employee organisation. Contact your Microsoft representative for estimates for your organisation.

Create an efficient, cost-effective approach to security

Microsoft Security enables you save through consolidation of your security capabilities and through IT admin and deployment efficiencies. For a 20,000-employee organisation, that can mean savings of nearly USD 6 million per year.

Summary of estimated cost savings⁶

Operational efficiency benefits	Annual value
Integration efficiency gains	USD 126,000
Lower costs to support third-party solutions	USD 150,000
Deployment cost reduction with Microsoft FastTrack	USD 1,300,000
Vendor licence cost consolidation: Reduce licence cost by	USD 4,300,000
Total estimated annual savings	USD 5,900,000

Microsoft Security enables you save through consolidation of your security capabilities and through IT admin and deployment efficiencies.

Deliver seamless end-user experiences for greater security.

With large numbers of employees working remotely, it's more important than ever for organisations to provide their people with the right resources for securely accessing apps and data, from anywhere. A recent Gartner survey found that **82% of leaders** intend to allow remote working some of the time as employees start to return to the office.⁷

While some organisations have taken this as an opportunity to modernise how they deliver user experiences to their workforce, many others struggle with a mixture of legacy applications and infrastructure that is siloed and hard for employees to navigate.

“If you make security hard, people may work around it. With Microsoft 365, we get native capabilities, visibility into our operational environment and simplicity for all employees.”

Simon Hodgkinson
Group Chief Information Security Officer, bp

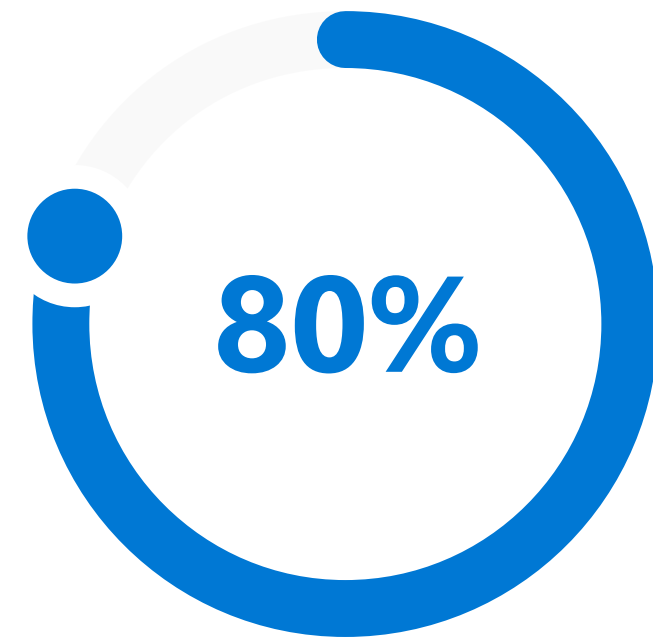
⁷ Gartner press release, 'Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time', June 2020.



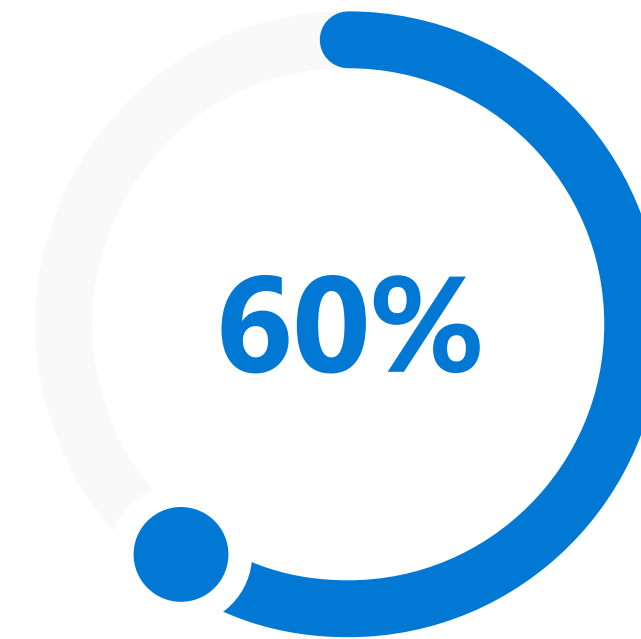
Microsoft's integrated approach helps you deliver seamless user experiences that keep your people both productive and secure.

When user experiences hamper rather than hinder employees' productivity, it can leave an organisation open to more security risks and higher costs. Weak or lost passwords, unsecured access via personal devices or unfettered sharing of sensitive data are just some of the challenges.

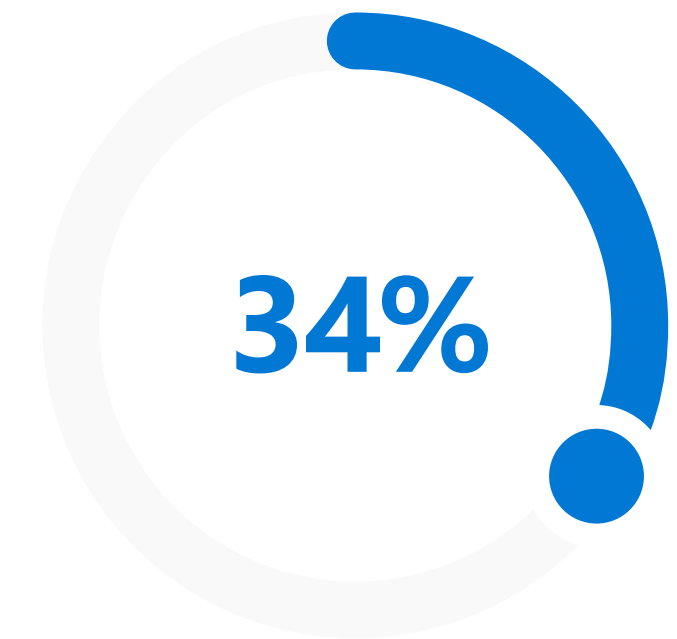
Microsoft's integrated approach helps you deliver seamless user experiences that keep your people both productive and secure across all facets of your employees' daily experiences.



of breaches involve the use of lost or stolen passwords.




of bring your own devices are not secured by IT.



of all data breaches are caused by insider threats.⁸

⁸ 'Verizon 2020 Data Breach Investigations Report.'



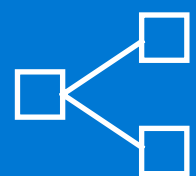
Microsoft helps you drive stronger authentication by offering multi-factor authentication.



Self-service password reset can reduce help desk calls by 20%¹⁰



Microsoft IT reduced hard and soft costs by 87%¹²



26% reduction in IT support costs with Microsoft Endpoint Manager¹³



USD 176,000 is the average cost for a mobile security incident¹¹

Simplify authentication

The moment an employee logs in to start their day represents one of the biggest security challenges organisations face – that of verifying user identities in order to grant access to internal systems and data. Most companies use passwords for this initial authentication. Yet passwords are easily forgotten – they represent a sizeable percentage of all helpdesk costs. Microsoft 365 removes this burden from your team by providing IT admins with the ability to offer self-serve password resets, reducing the number of help desk calls by 20%.⁹

Microsoft helps you drive stronger authentication by offering multi- factor authentication. Just by introducing this step, organisations can reduce the risk of a user account getting breached by 99%.¹⁰ You can also eliminate passwords altogether by adopting passwordless authentication with Windows Hello for Business.

⁹ Microsoft study.

¹⁰ Forrester Consulting, 'The Total Economic Impact Of Microsoft 365 E5 Solution', 2018.

¹¹ Check Point: 'Check Point Capsule: 2014 Mobile Security Survey Report', 2014.

Unify management across devices and apps

With employees working from home in record numbers, organisations have needed the use of more personal devices. Yet that new reality makes more difficult the challenge of managing and securing access to sensitive data, something that is quickly becoming a top concern for security and compliance teams. A study found that on average, the cost for a mobile security incident was USD 176,000, making protecting against these threats paramount for organisations.¹¹

Microsoft streamlines this effort through unified management with Microsoft Endpoint Manager (MEM), providing a single place from which to control all devices, whether corporate or personal.

¹² ZDNet: 'Microsoft: 150 million people are using passwordless logins each month', Catalin Cimpanu, May 7, 2020.

¹³ IDC: 'A First Look at How Windows Intune Can Lower Costs and Raise Productivity' by Randy Perry et al, March, 2011.



Seamless SSO experience saves each worker eight hours per year¹⁵



97% of high-risk login attempts are automatically blocked¹⁴



64% of data theft incidents could be prevented¹⁵



Built in information protection for better end-user experience

Secure access to apps

As employees access productivity apps through their workday Microsoft Azure Active Directory enables you to provide single sign-on (SSO), so your people are not tasked with remembering passwords for every single app. On average, SSO saves workers eight hours per year, and protects your helpdesk staff from additional support calls. In a 20,000 employee organisation, that equates to 160,000 hours saved per year.

Microsoft also helps you verify your users' access to specific apps through Conditional Access, which enables you to confirm which devices and users are allowed access to your corporate resources. Microsoft Conditional Access can block 97% of high risks login attempts.¹⁴

¹⁴ Microsoft internal security research data.

¹⁵ McAfee: 'Grand Theft Data: Data exfiltration study: Actors, tactics, and detection', 2017.

Protect sensitive data

All organisations have segments in their employee base that must work with highly sensitive data on a recurring basis. With workers more distributed than ever, and using a medley of BYOD and corporate devices, how can organisations ensure that sensitive data stays protected?

Microsoft 365 E5 offers built-in information protection for better, and safer, end-user experiences.

64% of data theft incidents could be prevented with Data Loss Prevention technology, a built-in protection in Microsoft Security that ensures data gets to the right recipients and is blocked from accidental, unsanctioned sharing, such as with external parties.¹⁵

Microsoft also helps you verify your users' access to specific apps through Conditional Access.



20,000
employee
organisation
can see
estimated
savings of
USD 15 million on
an annual basis.

Deliver seamless end-user experiences for greater security

With Microsoft Security, you can deliver great user experiences for your people while also gaining savings through automation and process improvements, IT admin and deployment efficiencies, as well as reduced cost of risk. A 20,000-employee organisation can see estimated savings of USD 15 million on an annual basis.

Summary of estimated cost savings¹⁶

Seamless end-user experiences	Annual value
Annual user productivity gains	USD 9,000,000
Reduce help desk spends by	USD 620,000
Annual BYOD hard cost avoidance	USD 3,900,000
Reduce cost of mobile security incidents	USD 1,900,000
Total estimated annual savings	USD 15,000,000

¹⁶ Rounded estimates based on Forrester TEI reports and Microsoft Total Cost of Risk calculator and illustrate first-year savings for a 20,000 employee organisation. Contact your Microsoft representative for estimates for your organisation.



Reduce cyber-risk with integrated, best-in-class protection.

In a recent Microsoft survey to security leaders in large organisations, the number one priority for those leaders is to improve threat protection to reduce the risks of a costly breach. Many security leaders face headwinds in achieving this priority. Cyberthreats continue to evolve and take advantage of our current and continually evolving conditions.

How CISOs are navigating the challenges of COVID-19

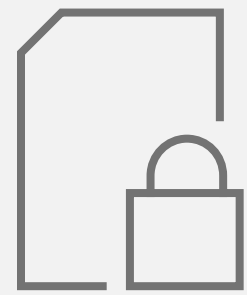
- 82** % feel pressured to lower costs.
- 67** % identified pandemic-themed phishing attacks.
- #1** priority to reduce cost is improved threat protection.¹⁷

To protect against threats, organisations rely on a complex collection of disparate security solutions to help them protect, detect and respond across full attack kill chain. Finally, security teams are often overwhelmed with the sheer volume of security alerts – wasting time trying to discern the difference between a real incident and false positives.

Microsoft 365 E5 Security was built to address these challenges with integrated, best-in-class and breed protection across each stage of the attack kill chain to reduce cyber-risk and reduce the number and cost of breaches. It enables organisations to streamline the security solutions required to protect against cyber-attacks while empowering their security teams to focus on the important activities by automating mundane tasks through artificial intelligence.

It enables organisations to streamline the security solutions required to protect against cyber-attacks

¹⁷ 'Microsoft Pandemic CISO Survey', 2020.



The result found that Microsoft provided nearly 100% coverage across attack kill chain stages.

Integrated protection across the attack kill chain


A major challenge organisations face today is the complexity that exists to detect, respond and remediate cyber-attacks across the kill chain. Many companies rely on a collection of security products provided by different security vendors to protect specific steps in the kill chain. To create connection and across this collection requires complex and costly integration and ultimately it fails to provide the desired level of visibility and improved efficacy.

With Microsoft Security, organisations benefit from an integrated approach across the entire attack kill chain. Using built-in AI and automation, Microsoft Security solutions reduce the signal to noise ratio enabling them to better protect you from attacks before they become incidents – and then remediate quickly when they do.

In fact, Microsoft recently participated in a MITRE ATT&CK evaluation to evaluate how Microsoft Threat Protection performs against an advanced attack simulation. The result found that Microsoft provided nearly 100% coverage across attack kill chain stages.¹⁸

¹⁸ Microsoft blog, 'Microsoft Threat Protection leads in real-world detection in MITRE ATT&CK evaluation.' May 1, 2020.





Microsoft Security solutions reduce the signal to noise ratio enabling them to better protect you from attacks before they become incidents – and then remediate quickly when they do.

Let's explore how Microsoft Security protects across the common steps of an attack.



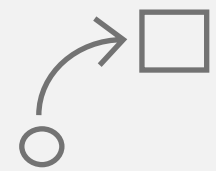
Email protection

Protects users from malicious links and files in email, SharePoint, OneDrive, Teams and Office applications.

Provides real-world phishing and training simulations to help security teams drive secure employee behaviours.

'89.3% reduction investigation and remediation time with Office 365 ATP.'

Forrester¹⁹



Endpoint protection

Prevent, detect, investigate and respond to advanced threats on endpoints.

Accelerate response and remediation, at scale, with automation.

'Automatically contain and remediate on 97% of post-breach detections. This eliminates many of the manual tasks associated with attack response.'

Forrester²⁰



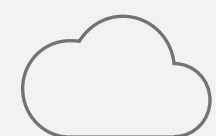
Identity protection

Detect threats early in the kill chain before identities are compromised and used to move laterally.

Protect user identities through sophisticated access capabilities like conditional access.

'Customers who use risk policies have 96% less compromise.'

Microsoft internal security research data



Cloud app protection

Protect cloud-based apps and data while reducing shadow IT.

Protect your sensitive information anywhere in the cloud.

'75% of threats automatically eliminated with Microsoft Cloud App Security due to automated processes.'

Forrester²¹

¹⁹ Forrester, 'The Total Economic Impact™ of Microsoft Office 365 Threat Intelligence Cost Savings and Business Benefits Enabled by Threat Intelligence as Part Of Office 365 E5', September 2018.

²⁰ Forrester, 'The Total Economic Impact™ of Microsoft Defender ATP Cost Savings And Business Benefits Enabled By Microsoft Defender ATP', April 2019.

²¹ Forrester, 'The Total Economic Impact™ of Microsoft Cloud App Cost Savings and Business Benefits Enabled By MCAS', May 2020.



3M

annually for a
20,000-employee
organisation.

Reduce cyber-risk with integrated, best-in-class protection.

Microsoft Security not only helps you reduce your cyber risk across the kill chain, it can also enable savings through IT automation, process improvements and reduced total cost of risk from breaches. In total, that can mean over USD 3 million annually for a 20,000-employee organisation.

Summary of estimated cost savings²²

Reduce cyber-risk	Annual value
IT and SecOps efficiency gains	USD 1,200,000
Reduced end-user downtime cost reduction due to faster remediation	USD 1,760,000
Reduce data loss from breaches by	USD 289,000
Total estimated annual savings	USD 3,250,000

²² Rounded estimates based on Forrester TEI reports and Microsoft Total Cost of Risk calculator and illustrate first-year savings for a 20,000 employee organisation. Contact your Microsoft representative for estimates for your organisation.





We have identified potential cost savings that organisations can see.

Summary of value

Through the Forrester Total Economic Impact studies, we have identified potential cost savings that organisations can see with Microsoft Security. Below illustrate the annual cost savings opportunity across different sized organisations.

Summary of estimated cost savings²²

Cost savings categories	20,000 users	1,000 users	50 users
Vendor licence cost consolidation	USD 4,300,000	USD 220,000	USD 11,000
IT administration and deployment savings	USD 6,100,000	USD 300,000	USD 41,000
Reduce total cost of risk	USD 2,200,000	USD 390,000	USD 290,000
Save on automation and process improvements	USD 12,000,000	USD 600,000	USD 30,000
Potential cost savings per year	Up to USD 25M	Up to USD 1.5M	Up to USD 380K

²² Rounded estimates based on Forrester TEI reports and Microsoft Total Cost of Risk calculator and illustrate first-year savings for a 20,000 employee organisation. Contact your Microsoft representative for estimates for your organisation.

Contact a Microsoft representative or partner to:

Continue the conversation

We can help you get started in streamlining and strengthening your security so you can achieve a stronger posture while saving on costs.

- ✓ Get a customised Total Cost of Risk report for your organisation.
- ✓ Request a Microsoft Security Workshop to learn how Microsoft can help improve your security posture.

