A Secure Foundation

From Zero Trust to AI-powered productivity

Microsoft 365

Table of Contents

Increase in average monthly identity attacks from 2018 to 2022[1]

+1,329%

password spray attacks

+26%

password attacks

+35%

phishing attacks

Today, work can happen anywhere. Whether in the office, at home or in between – employees want to do work when and where it happens, without interruption. Many organisations meet this need for anywhere work with hybrid solutions. But creating the right environment means navigating a slew of continuously evolving challenges.

For many organisations, remote work means connecting employee-owned devices to get work done, while other organisations provide additional devices for remote use. Both scenarios can lead to an increase in unmanaged endpoints and identities. IT workers who are already busy with their existing day-to-day duties often don't have the time or tools to securely manage them all.

With cyberattacks increasing significantly over the past few years, a single unmanaged device can put an entire organisation at risk.

New ways of working need enterprise-wide technology founded in Zero Trust to enable flexible, productive work. Tools built to centrally manage security are critical. But those tools must give employees the foothold they need to work productively, collaborating and innovating from anywhere.

Zero Trust is a security model that assumes no implicit trust in any entity, internal or external, and requires continuous verification of identity, device, data and network.

This eBook explores how and why risks arise from today's hybrid work environments, and what tools organisations can use to secure their technology for productive work from anywhere.

Security risks in today's world of work

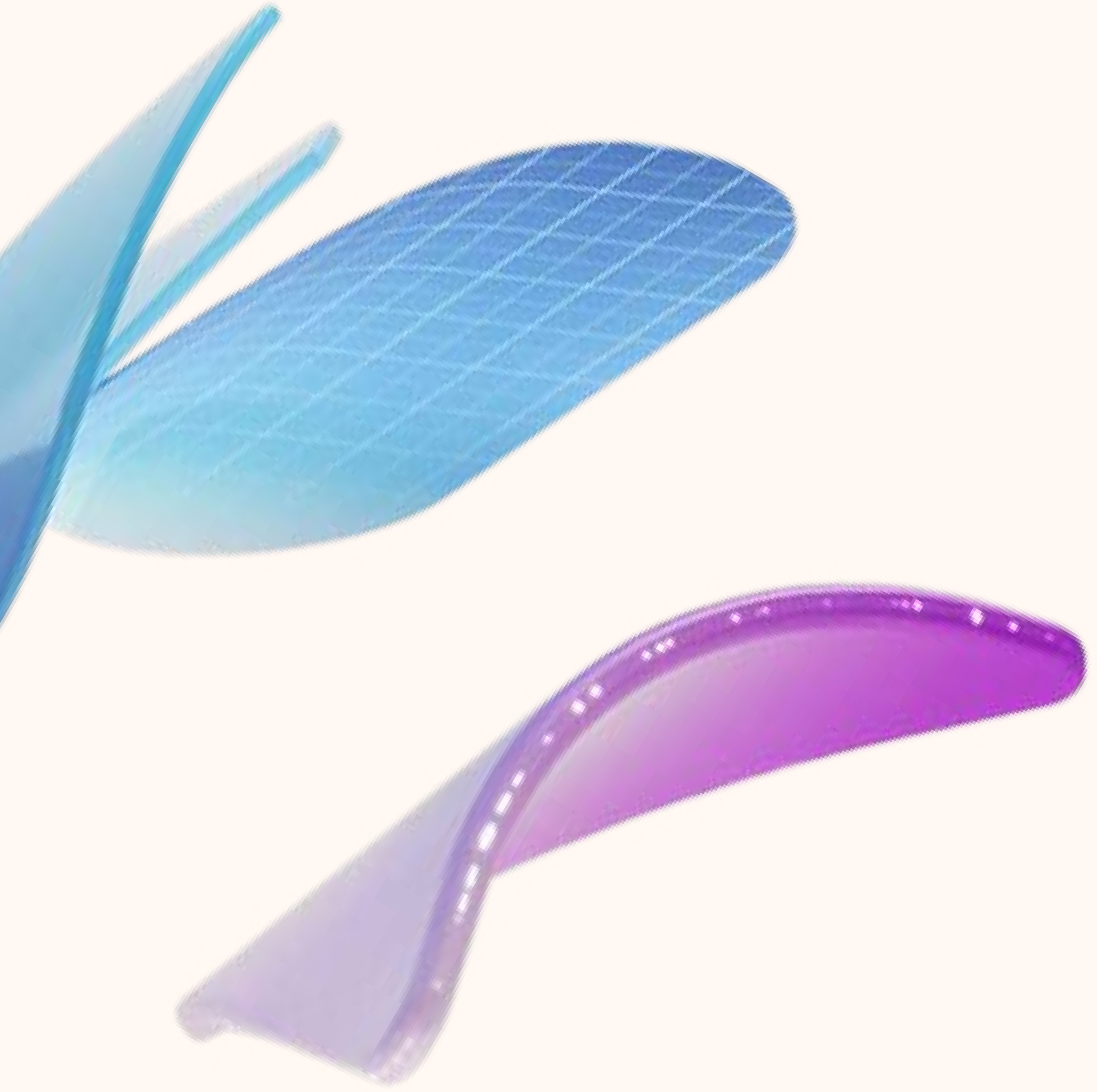
While organisations look to evolve their ways of working, 68% have experienced one or more endpoint attacks that compromised data and/or their IT infrastructure.[2] A single security breach can erode customer confidence for years into the future and cost an average USD 4.45 million.[3] Without proper security, organisations risk more than downtime. And perhaps more importantly, they risk long-term reputational damage.

Flexible workplaces see an increase in unmanaged devices and identities

While employees are ready to work from anywhere, their organisations' security may not be. More than half of organisations do not have visibility or control over at least a quarter of their endpoints.[4] And with more places work can be done, the number of unmanaged devices and identities is likely to increase.

As employees work and collaborate in a hybrid environment, they may find existing tools inadequate. Remote collaboration can be difficult without optimised apps, and software interfaces may vary widely between desktop, laptop and mobile devices. This leads some employees to turn to shadow IT, with a reported 80% using non-sanctioned apps and devices that have not been reviewed.[5]

With the number of unmanaged endpoints that IT teams are left to manually discover and restrict access to, almost 70% report feeling overwhelmed trying to manage remote work.[7]

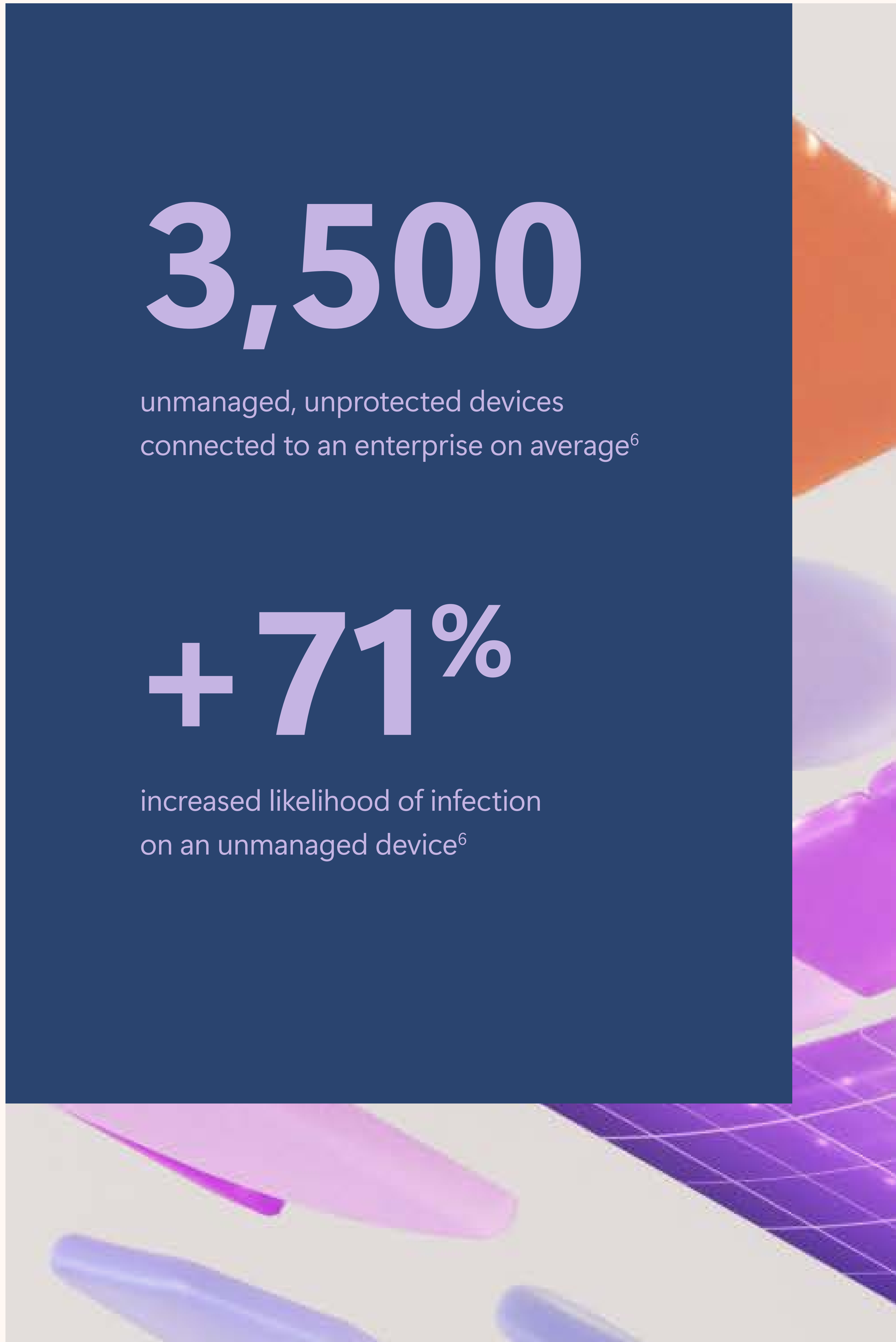


3,500

unmanaged, unprotected devices connected to an enterprise on average[6]

+71%

increased likelihood of infection on an unmanaged device[6]



Outdated, manual endpoint and app management

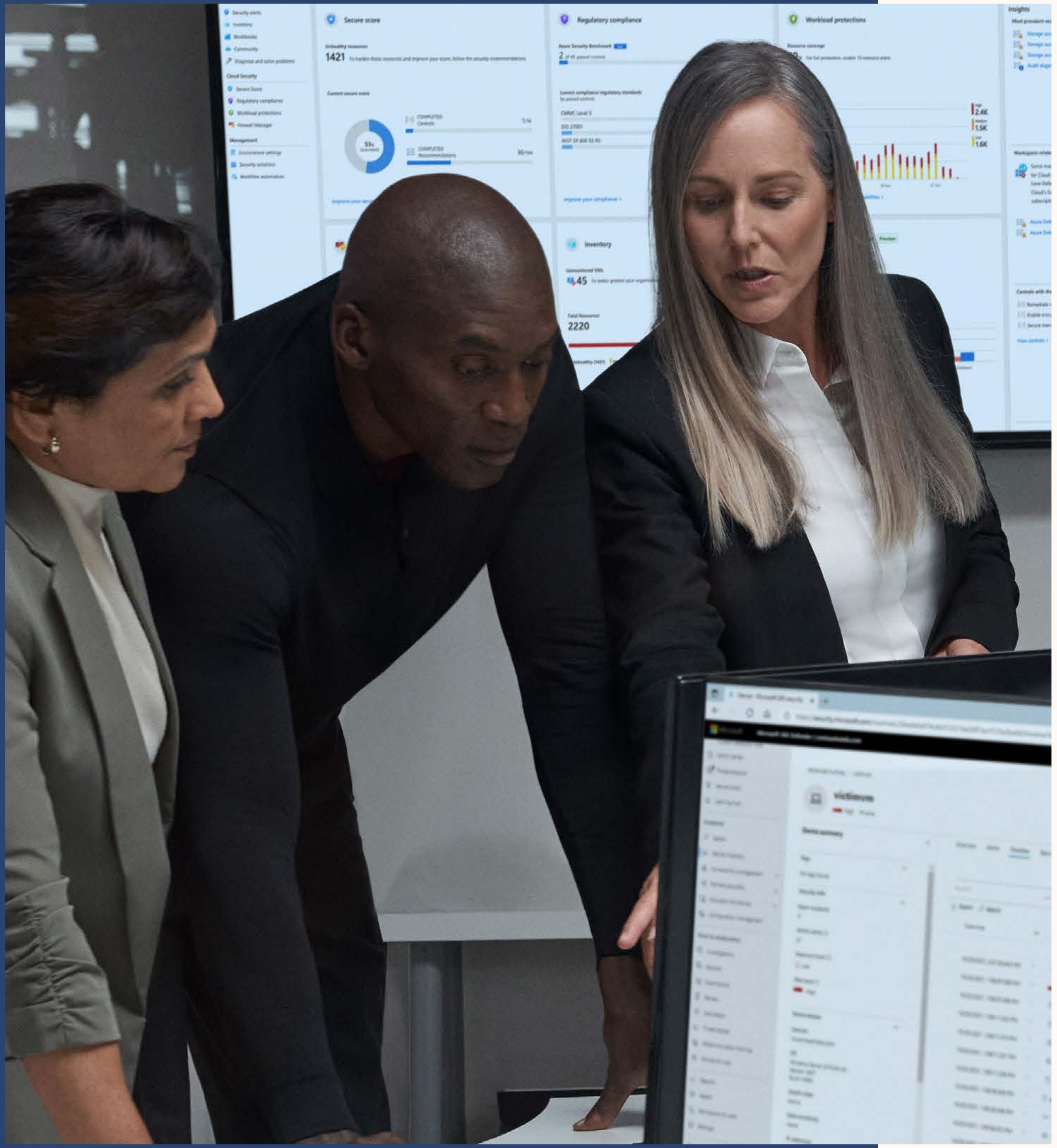
To properly secure the influx of employee-owned devices, and the apps and tools needed for employees to work from anywhere, organisations must address their legacy endpoints, software and apps. Almost 90% of security leaders agree that outdated PC hardware leaves organisations vulnerable to attack, yet reports show a third of most organisations' hardware is outdated.[8] Less than half of organisations update their computers every two years.[8]

Devices that rely on manual patching and updating present a considerable risk. The gap between when an update or patch becomes available and when it's implemented leaves organisations vulnerable. And the time it takes to manually update devices may delay more important strategic IT work. Reports show more than half of IT teams don't spend enough time on strategic work, like defending against the increasing sophistication of cyberattack techniques. Instead, they're often preoccupied with everyday issues like software and firmware patches.[7]

When organisations do implement new technology, they must be sure to sunset redundant solutions. 72% of organisations reported increased complexity within their IT environment over the past two years.[9] This complexity represents not only complications in the computing environment, but also increased complexity of IT teams' jobs.

68%

of organisations that suffered ransomware attacks had a high dependence on manual patching and updating[7]



Creating a Zero Trust foundation

Turning your organisation into a modern environment where employees can work from wherever they need to can be a significant undertaking, and security must be at the forefront. Left unaddressed or under-addressed, your organisation may be exposed to risk of large losses. Your IT teams may already manage many different small-scale issues to keep your security posture intact. They need a solution that will allow them to focus on higher-order security risks to combat the rising number of attacks. The right solution must deliver productivity tools with security baked in.

A secure solution from Microsoft

Microsoft 365 E3 is a comprehensive, cloud-based productivity and security solution for building a strong, Zero Trust foundation for modern work. Through identity management, threat protection and data security measures, Microsoft 365 E3 secures your enterprise while allowing your teams to collaborate effectively and eliminate redundant solutions.

Secure all your organisation's identities

With Microsoft 365 E3, you can implement simple and effective identity security measures at scale.

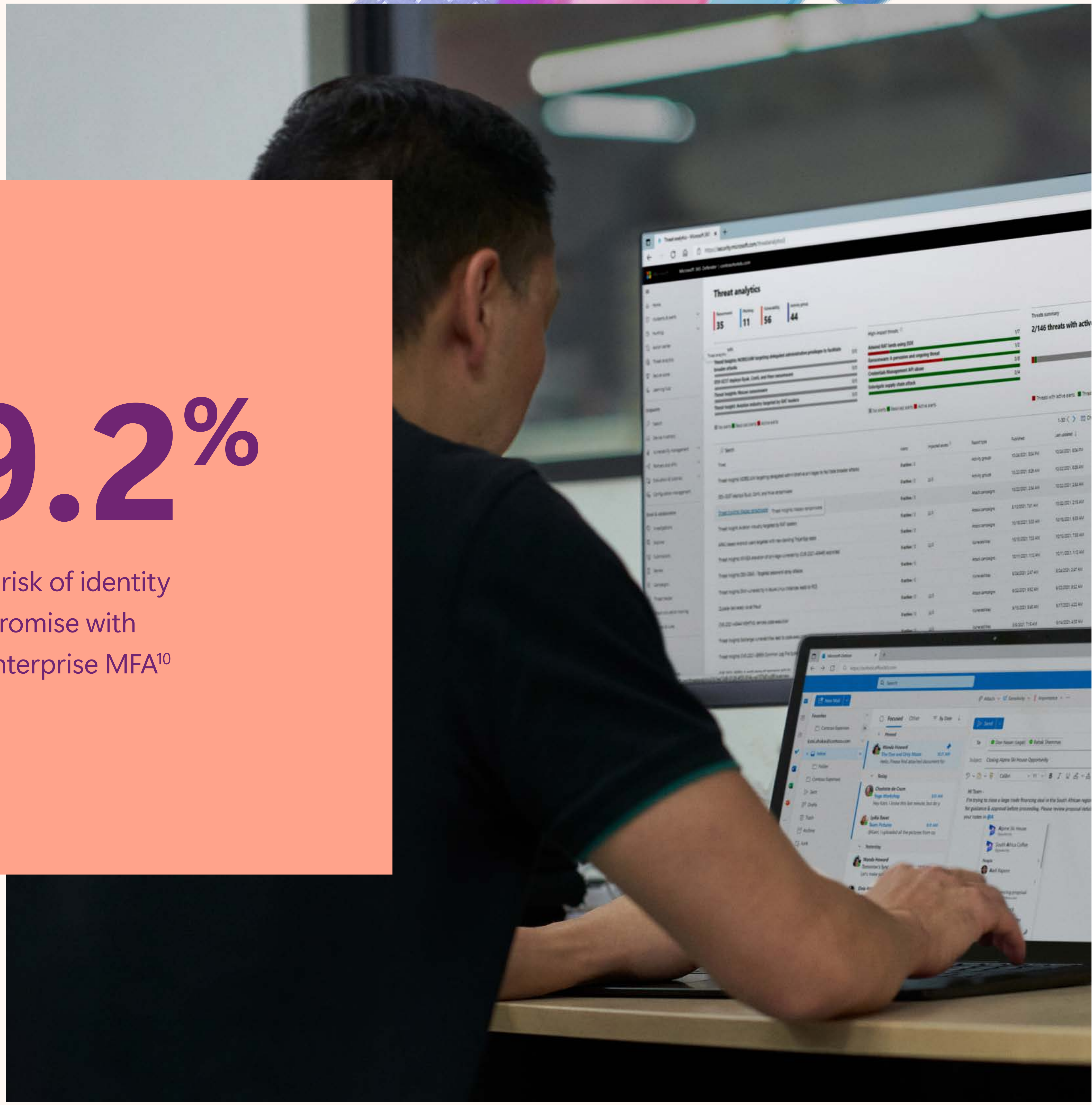
By rolling out multi-factor authorisation (MFA) and passwordless sign-on throughout your organisation, you reduce the risk of compromise significantly. Coupled with continuous access evaluation, you can ensure that all sign-in attempts are within normal geographical areas and working hours. This creates a sign-in process that's both highly protected and easy for workers to use.

Once identities are logged into your organisation, Microsoft 365 E3 provides a powerful tool for risk-based Conditional Access management in the form of Microsoft Intune.

With Intune, IT teams can set up access to apps and tools by role, and employees can use self-service options for common issues like password resets. This can save your organisation up to USD 79 per user over three years* as employee issues are resolved more quickly.[11]

↓ 99.2%

reduced risk of identity compromise with whole-enterprise MFA[10]



Organisations save

USD 55

per user per month* by consolidating suppliers with Microsoft 365[11]

97%

of survey respondents report efficiency gains for IT teams in deploying endpoint updates*[11]

Cut through endpoint management complexity and protect against threats

With Microsoft 365 E3, your organisation gets modern, unified endpoint management and visibility into all endpoints. A single solution, Microsoft 365 can also reduce the number of dedicated solutions and corporate devices in your organisation, saving you money and empowering your IT teams to focus on larger tasks, like strategic security planning and updating your device estate.

Security, deployment and software update automation capabilities are also included in Microsoft 365 E3 to take the load off busy IT workers and keep enterprise endpoints up to date.

Cloud endpoint deployment means employees can securely stream Windows desktop, apps, settings and content from the Microsoft Cloud to a Cloud PC. In addition to quickly setting up employees to work from anywhere without the costs of a secondary solution, significant time savings in deployment can translate into an average USD 15M in savings over three years.*[11]

Automatic threat protection and remediation across all apps and environments lets IT teams configure conditional responses to common cyber threats that would otherwise take up valuable time. Additionally, automatic software updates allow employees to stream the most up-to-date versions of apps, settings and content quickly and securely from the Microsoft Cloud.

Govern and protect your organisation’s sensitive information

A fully integrated solution, Microsoft 365 E3 allows IT teams to discover and classify sensitive information at scale. Information protection can even extend between Microsoft and non-Microsoft apps. Features like sensitive data tagging and loss prevention, end-to-end encryption, eDiscovery and compliance managers help IT Teams classify, monitor and control data – both in transit and at rest.

With Microsoft 365,
organisations can expect up to

USD 1.2M

in reduced risk of data breach
over three years[11]

Modern work with a secure foundation

Once your organisation's foundation is secured and your data and teams connected, Microsoft 365 E3 can enable the productivity needed to meet the new era of work. With Microsoft 365, your workers can access the apps, tools and data needed to do their work from anywhere, securely.

Microsoft 365 E3 can help your organisation achieve its digital transformation goals and empower your workforce to work together. With connection through best-in-class productivity apps, your employees can collaborate and drive productivity together, no matter where they work.

Elevate productivity with a powerful AI tool

Microsoft Copilot for Microsoft 365 elevates productivity even further, working as an agile assistant to help employees streamline their work and accomplish more every day. Copilot integrates with your organisation’s data and works alongside Microsoft 365 applications to automate routine processes, create presentations, design data visualisations, write documents and more. Copilot gives employees an AI tool capable of turning their ideas into one of the most powerful productivity tools on the planet.

Copilot works in three distinct ways. First, to unleash your employees’ creativity by creating first drafts for employees to iterate on, generate professional-looking data visualisations and analysing trends. Second, to unlock productivity by intelligently cutting down on busywork by summarising emails, messages and to-dos. And third, to uplevel your employee’s skills with thousands of natural language AI commands that make the work they do easier.

Microsoft 365 for enterprise

Build a secure foundation for flexible work with Microsoft 365 E3.

Learn more >

Sources:

[1] 'Microsoft Entra: Five identity priorities for 2023.' Microsoft Security Blog, Jan 9, 2023.
https://www.microsoft.com/en-us/security/blog/2023/01/09/microsoft-entra-5-identity-priorities-for-2023/

[2] 'The 3rd Annual Study on the State of Endpoint Security Risk', Ponemon, Jan 2020.

[3] Cost of a Data Breach Report 2023, IBM, July 2023.
https://www.ibm.com/reports/data-breach

[4] Gruber, Dave; Knuth, Gabe, 'Managing the Endpoint Vulnerability Gap: The Convergence of It and Security to Reduce Exposure.' Enterprise Strategy Group, February 2023.
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWXwKT

[5] 'Discover and Manage Shadow IT – Microsoft Defender for Cloud Apps.' Microsoft Learn, May 24, 2023.
https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-shadow-it

[6] 'Anatomy of a Modern Attack Surface.' Microsoft Security Insider, May 2, 2023.
https://www.microsoft.com/en-us/security/business/security-insider/threat-briefs/anatomy-of-a-modern-attack-surface/

[7] Microsoft, 'Microsoft Digital Defence Report 2022: Illuminating the threat landscape and empowering digital defence.'
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

[8] 'Security Signals Boost SDM Research Learnings' Microsoft Security, Sept 2021.
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWP0mz

[9] Gartner Survey Shows 75% of Organisations Are Pursuing Security Vendor Consolidation in 2022, Press Release, Sept 2022.
https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-survey-shows-seventy-five-percent-of-organizations-are-pursuing-security-vendor-consolidation-in-2022

[10] 'Microsoft Digital Defence Report: Building and improving cyber resilience.' Microsoft Threat Intelligence, Oct 2023.
https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[11] The Total Economic Impact™ of Microsoft 365 E3, a commissioned study conducted by Forrester Consulting, Oct 2022. Results based on a single composite United States-based organisation with global operations and 30,000 employees using Microsoft 365 E3.
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5970p

Microsoft 365