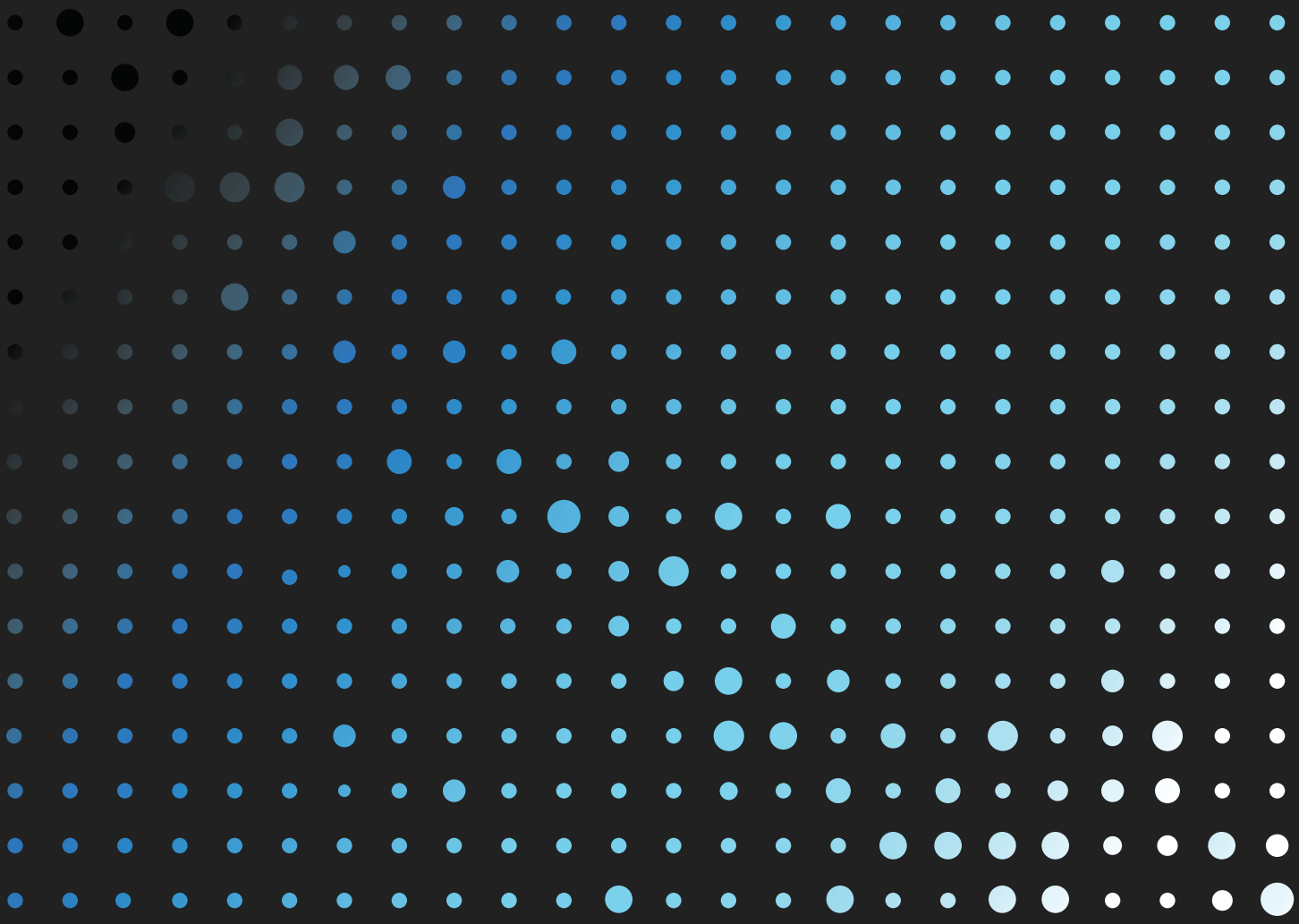
Microsoft

The endpoint is the enterprise

How endpoint modernization enables secure and productive hybrid work

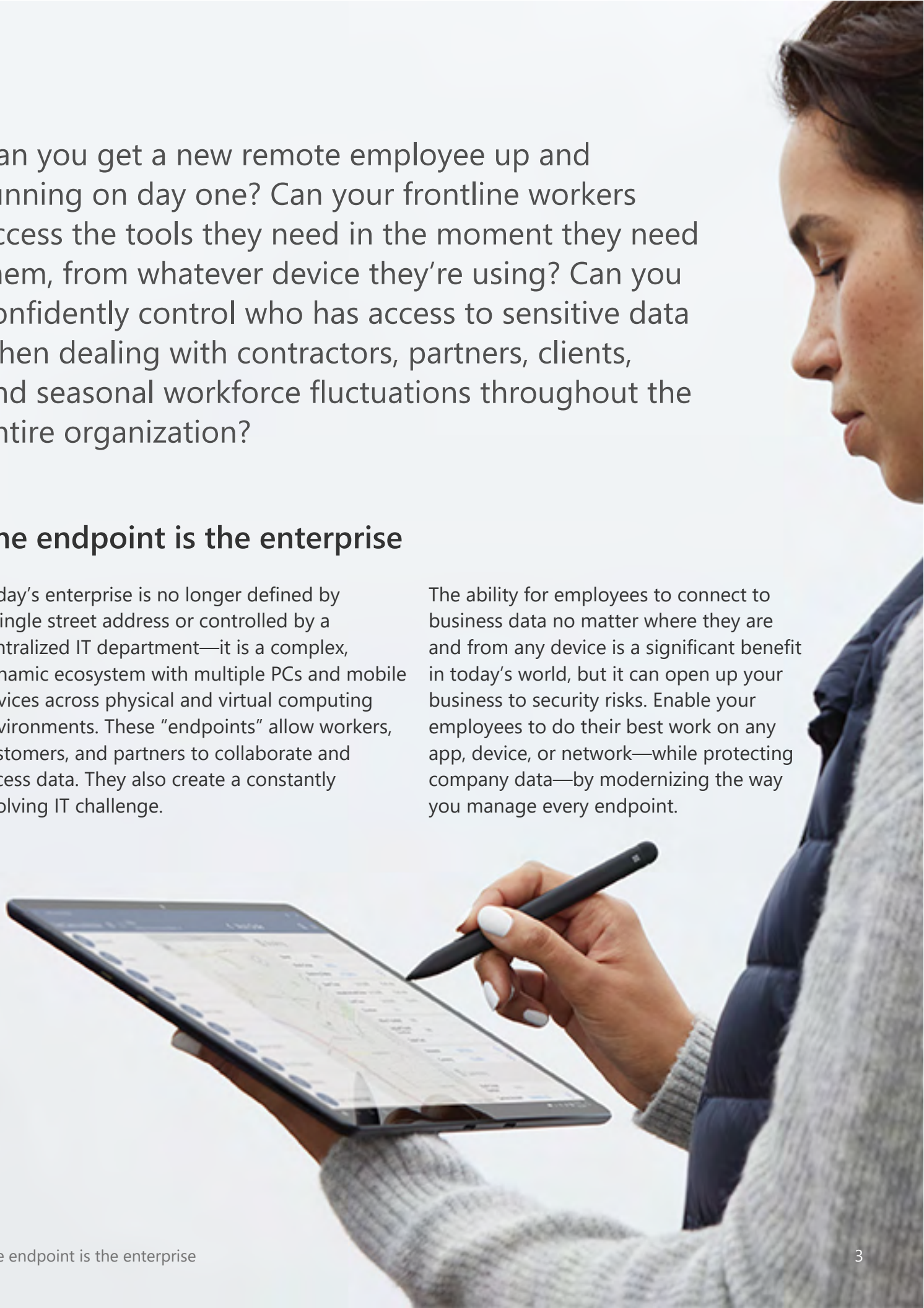


Can you get a new remote employee up and running on day one? Can your frontline workers access the tools they need in the moment they need them, from whatever device they're using? Can you confidently control who has access to sensitive data when dealing with contractors, partners, clients, and seasonal workforce fluctuations throughout the entire organization?

The endpoint is the enterprise

Today's enterprise is no longer defined by a single street address or controlled by a centralized IT department—it is a complex, dynamic ecosystem with multiple PCs and mobile devices across physical and virtual computing environments. These "endpoints" allow workers, customers, and partners to collaborate and access data. They also create a constantly evolving IT challenge.

The ability for employees to connect to business data no matter where they are and from any device is a significant benefit in today's world, but it can open up your business to security risks. Enable your employees to do their best work on any app, device, or network—while protecting company data—by modernizing the way you manage every endpoint.



Section 1

Empower employees with modern technologies

The modern workplace is increasingly hybrid and remote, which means employees need to be able to stay connected to the enterprise from anywhere. Without the right tools—and secure support for those laptops, mobile devices, and other endpoints—projects stack up, deliverables get pushed back, and critical opportunities get missed.

These setbacks can also affect team morale. When technology gets in their way, employees can become frustrated, unproductive, and restless. On the other hand, when empowered with tools that are optimized for modern workloads, their experience, wellbeing, and productivity improve.

Whether in the office or on the front lines, remote or on-site, your employees show up to do a job. They're expecting a modern workplace approach that encompasses a range of work styles and provides the tools they need to get the job done: laptops, mobile devices, productivity tools, collaboration apps, and more. A workplace that's optimized for what employees need to do every day, wherever they're working and however they need to work, is quickly becoming a competitive differentiator in attracting and retaining top talent as well.

BRIDGEWATER

> “Our employees can fulfill their company duties from anywhere in the world while maintaining tight control over core security needs.”

Igor Tsyganskiy
Chief Technology Officer, Bridgewater Associates

Learn how Bridgewater Associates invests in secure remote work →

5X

Increase in remote job postings on LinkedIn since the pandemic

73%

of workers want flexible remote work options to continue

41%

of the global workforce is likely to consider leaving their current employer within the next year, with 46 percent planning to make a major pivot or career transition

Read the 2021 Work Trend Index to learn how businesses are preparing for the shift to hybrid work →

Section 2

Simplify device management and oversight

Today's IT department is faced with managing an ever-increasing mix of corporate-owned and personal devices. Meanwhile, seasonal fluctuations, project updates or sudden shifts in the business lead to heavy workloads for the IT department.

During the pandemic, organizations scrambled to equip their employees to work remotely whether they were ready for it or not. Some employees were using company and personal devices, dated hardware, and logging in on unsecured networks. This highlighted the need for the IT department to quickly image hundreds or even thousands of personal devices with a company's proprietary applications and collaboration tools, and to ensure that critical security features were installed.

In order to onboard, manage, and secure every one of those devices—no matter what network they're connecting on—you need a modern endpoint strategy that lets you:

Easily manage who has access to what by controlling devices from a single tool

Automatically push updates to apps, so that everyone is getting the best, most secure experience

Take advantage of analytics to continuously improve user experience

With the right endpoint modernization strategy, employees get a secure experience on every mobile device, tablet, or laptop they're using. All while eliminating major IT administration headaches such as managing dated hardware, software and device deployment, as well as reducing costs for support, setup, and training.

Rabobank

> “Our business case showed we could save millions of euros, but we mainly emphasized the workplace improvements we could achieve with a move to the cloud.”

Abe Boersma
Global Head of Workplace Services, Rabobank

Learn how Rabobank is achieving its One Digital Workplace vision →

Section 3

Secure your hybrid work environment

Your employees want to connect to the enterprise from anywhere: their work computer in the office, their personal mobile on a public network, or even their roommate's laptop. This modern workplace reality of working anytime, anywhere—on personal devices, company computers, applications, virtual desktops, and more—can expose your company to significant security risk. And the rapid pace of business has often meant sacrificing security for productivity.

In the past, when the enterprise was more-or-less constrained to a physical location, it was simpler for IT to manage and deploy devices and how they connect to corporate resources. Now, securing the organization means additional layers to verify users, limiting access based on specific business scenarios, and proactively assuming a breach could happen. These security principles—known as Zero Trust—are nearly impossible without modern endpoints.

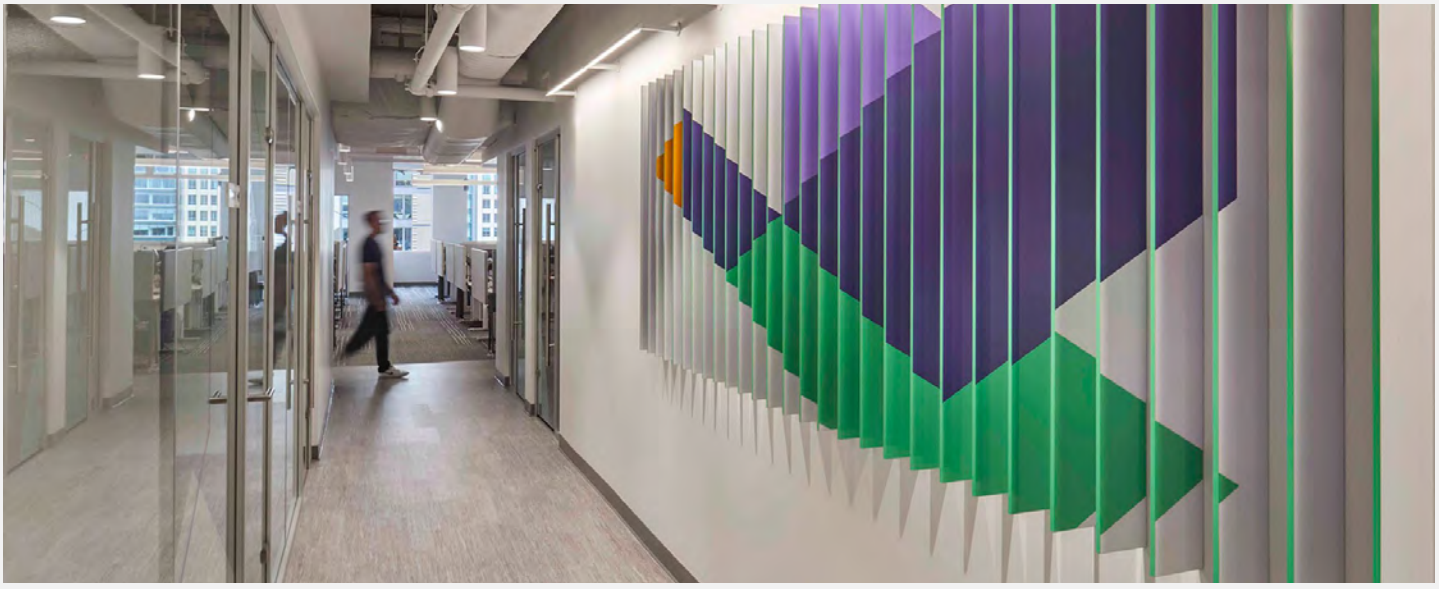
With modern endpoints, you can feel more confident about the security of personal and company-issued devices, no matter where and how they're connecting. You can control who has access to what, apply security settings to devices that are dispersed across the country or the world, and remove sensitive data when an employee leaves the company. Having centralized control and visibility also means your IT team can take system-wide action within minutes if there's a breach.

Duck Creek Technologies

> “I can’t afford to wait for a manual response to an incident, because attackers are moving way too fast. They might be in and out before we even get the alert. That’s why we’re focusing more on security orchestration, automation, and response. We need to have automated responses built into the entire infrastructure of the SaaS environment that we offer our customers.”

John Germain
Vice President and Chief Information Security Officer, Duck Creek Technologies

Learn how Duck Creek Technologies is increasing security and visibility across all endpoints →



Section 4

The path to a connected, secured workplace

Empowering your teams and streamlining your IT oversight through modern endpoints does not have to be a complicated journey. The key is to understand your current security exposure and the steps you're taking to close those gaps, optimize those security workflows to meet the demands of hybrid work, and push them out to every endpoint.

Phase 1

Secure your current workflows

Identify and document your current workflows, such as document sharing, internal messaging, email access, remote access, and data syncing. Modernize what you can by using secure versions of applications or taking advantage of UX and analytics tools to get critical insights before making dramatic change.

Phase 2

Expand to new endpoints and workflows

Once you have modernized your current workflows, identify new places and business scenarios to expand security. Find the most optimal solutions for managing all devices—personal and company-owned—no matter where they're connecting from.

Phase 3

Achieve the endpoint enterprise

Offer every employee—from the front lines to the home office—the ability to do their best work and stay connected from anywhere while maintaining the highest levels of security with completely modern endpoints including virtual desktops and connected cloud applications.

> “Instead of spending days traveling, I can be online in minutes with a subject matter expert to provide technical support or install a new piece of equipment.”

Taylor Davis
Electrical Engineer at the Process Development Center at Goodyear headquarters

Learn how Goodyear is driving secure, remote collaboration as an Endpoint Enterprise →

Secure and productive hybrid work achieved

With modern endpoints, you enable a dynamic enterprise that can react quickly to challenges and opportunities while attracting the most skilled talent. Every employee should be able to connect virtually with other team members, customers, and partners, as well as to the data and tools they need to do their jobs whether they're remote, hybrid, or simply accessing applications on the go. All while reducing burdensome and time-consuming IT oversight—such as onboarding, management, and updates—while enabling you to implement Zero Trust practices across your entire organization.

Welcome to Endpoint Enterprise.

> “In moving to Microsoft 365, we gave our employees a more flexible, secure workplace that allowed them to use whatever device or combination of devices they want.”

Ralf van Houtem
Global Manager Digital Workplace, Atos

Read the case study →

Modernized endpoints within reach

As you modernize endpoints in your enterprise, we recommend looking for a solution that is:

Built-in, not bolted on

Microsoft offers best-in-class solutions within the ecosystem of apps, devices, and software you're already using. Using an integrated solution lets you benefit from trillions of signals that allow the platform to adapt to protect every customer better, then push that protection down to the last mile of devices.

Secure

Microsoft supports Zero Trust security architecture on every endpoint within your enterprise. Cloud-based authentication secures devices based on factors you control, granular access privileges secure both data and productivity, and real-time analytics and threat protection give you the visibility and speed you need to address threats immediately.

Interconnected

Workers can do their best work when they're plugged into a coherent ecosystem of applications, file sharing, and communication tools—regardless of what device they're using. Microsoft gives users a first-rate experience anywhere and everywhere they connect to your business.

Learn more about Microsoft Endpoint Manager →