

Building the foundation for the Frontier Firm

By 2028, businesses are projected to deploy **1.3 billion** agents across their operations¹. The organizations that figure out how to orchestrate human-agent teams effectively will have a significant competitive advantage. As large-scale AI adoption accelerates, we are seeing a new kind of organization emerging - one that brings human expertise and intelligent agents together to help move faster, work smarter, and achieve more. These organizations are building flexible teams that include people and AI with shared goals and measurable outcomes. They are known as **Frontier Firms**.

What defines a Frontier Firm?

A Frontier Firm isn't just a company that uses AI. It's an organization that has fundamentally reimagined how work gets done. Humans set the strategy. Intelligent agents help handle the execution. Think of it as the next evolution of the enterprise: human-led, agent-operated. According to the [2025 Work Trend Index Annual Report](#), Frontier Firms are defined by a new role for every employee: the agent boss. These organizations share several defining characteristics.

- **Security is built in.** Governance and compliance are woven into the tools that people use to get work done from day one. Data protection isn't an afterthought. It's foundational.
- **AI is organization-wide.** Frontier Firms have moved beyond pilots and experiments. AI deployment is scaled across the enterprise and embedded into core workflows rather than siloed in innovation labs.
- **Employees are agent bosses.** People don't just use AI tools. They lead teams of intelligent agents, delegating tasks, evaluating outputs, and focusing their own energy on uniquely human work like creative thinking, relationship building, and strategic decision-making.
- **Outcomes are measured and optimized.** Leaders actively track AI investments and ROI, with clear evidence of realized returns driving continued adoption.



1.3
billion

agents projected to be deployed across business operations by 2028.¹

The journey to becoming a Frontier Firm

On the way to becoming a Frontier Firm, organizations progress through three phases.

Phase 1: AI as assistant. Individuals use AI to work faster on discrete tasks like drafting, summarizing, and generating content. AI augments individual productivity but doesn't change how teams operate.

Phase 2: Human-agent teams. Agents join the team as digital colleagues with specific responsibilities, whether that's triaging tickets, managing projects, or preparing materials. They amplify productivity at the team level and enable humans to focus on higher-value work.

Phase 3: Human-led, agent-operated. This is the Frontier Firm. Humans define strategy and assign goals. Agents execute, working together to execute complex operations and escalating to humans when judgment calls are needed.

The data tells the story

Organizations that have embraced this model are already seeing results. According to the 2025 Work Trend Index Annual Report, Frontier Firm leaders surveyed reported feeling more optimistic than other leaders:

- **Over 70%** reported that their company is thriving, compared to 39% of other leaders.²
- **Over 90%** reported feeling optimistic about future work opportunities, versus 80% of other leaders.²
- **Over 50%** surveyed reported they're able to take on more work, versus 25% of other leaders.²
- **Over 80%** reported they expect agents to be moderately or extensively integrated into their company's AI strategy within 12 to 18 months.²

The gap between Frontier Firms and others is widening. In the very near future, many organizations will be on this journey. The question is whether you're leading or catching up.

Why this matters now

The [2025 Work Trend Index Annual Report](#) surveyed over 31,000 knowledge workers across 31 countries and analyzed trillions of Microsoft 365 signals. The findings are clear: **over 80%** of leaders surveyed reported that 2025 was a pivotal year for rethinking key aspects of strategy and operations².

Organizations are feeling stretched thin while more traditional approaches to scaling (hiring more people, adding more tools) aren't keeping pace with demand. **80%** of knowledge workers surveyed reported feeling they lack enough time or energy to do their work². This emerging productivity capacity gap has accelerated the need for new approaches.

Frontier Firms have found another way. By pairing human expertise with intelligent agents, they're expanding capacity, helping accelerate execution, and unlocking innovation by giving their employees the tools to achieve more.

Success starts with a solid, secure foundation

So how do you enable AI, strengthen security, and reduce complexity at the same time? Transitioning into a Frontier Firm demands a distinct strategy. Scaling AI on legacy infrastructure - systems not originally designed for AI - can present obstacles. An integrated platform can help organizations expand AI capabilities efficiently with security and productivity working together. Your organization is enabled with AI-ready business protection tools to help you proactively address a shifting threat landscape, while productivity solutions amplify impact without compromising security. This is about unifying what you already have and scaling it for what's ahead.

The pressures you're facing

The threat landscape has changed. According to the [Microsoft Digital Defense Report](#), identity-based attacks surged **more than 30%** in the first half of 2025³. Ransomware attacks targeting hybrid environments jumped from **less than 5%** in 2023 to **40%** in 2025³. AI-driven phishing is now **three times** more effective than traditional campaigns³. This ever-evolving threat landscape has made security a strategic imperative.

Today's environment encourages organizations to adopt more dynamic approaches built into the way they operate. Work has never been more flexible - people connect from the office, at home, in coffee shops, or on the go with their favorite devices and cloud apps. This freedom adds to the complexity IT teams already face to keep company data protected, secure a variety of devices, manage access to company resources, and so much more - all while enabling employees to stay productive.

Leaders are embracing this environment, turning to AI to expand their teams' capabilities and drive productivity - adopting smart solutions that empower employees to get their work done safely. **Over 80%** of leaders surveyed in the 2025 Work Trend Index Annual reported feeling confident that they'll use digital labor to expand workforce capacity in the next 12 to 18 months.²

The opportunity is clear: those who harness technology to balance performance and protection will lead the way, while others risk falling behind in a world that's moving forward fast.

More
than **30%**

increase in identity-based attacks in the first half of 2025³.

3x

effectiveness of AI-driven phishing compared to traditional campaigns³.



The security-first foundation

Organizations need more than just a set of tools when adopting AI and agents at scale. A complex, disconnected tech stack may not only limit the power and promise of AI but introduce security risks. When AI is scaled from a foundation that includes robust data governance, strong security, and integration capabilities, it can help amplify impact. It's about allowing productivity and security to work together rather than competing. The foundation you build from can unlock productivity gains while keeping your data protected. That means security is integrated from the start, not layered on after the fact.

Start by evaluating your foundation against the following four pillars for to understand your readiness to scaling AI adoption:

- **Prepare.** Evaluate your security posture, identify data assets, understand regulatory requirements, and establish governance policies to assess your organization's readiness.
- **Discover.** Gain visibility into AI usage across your enterprise. Identify what AI applications are in use, understand data flows, and catalog sensitive information that AI may access.
- **Protect.** Put controls in place to prevent data leakage, unauthorized access, and misuse. This includes data loss prevention policies, sensitivity labels, encryption, and threat detection.
- **Govern.** Maintain ongoing compliance, auditability, and continuous improvement. Manage agent lifecycles, monitor performance, stay compliant, and regularly assess risks.

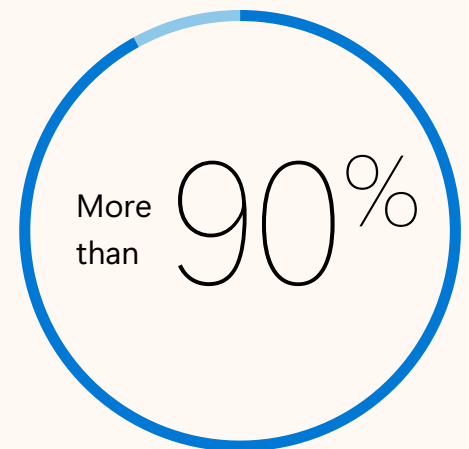
Microsoft 365 - an integrated, secure solution

The right solution delivers value that grows over time. An integrated approach helps you ensure technology investments build a secure, scalable foundation for both current needs and future innovation. Fragmented systems may create barriers to progress while a well-integrated tech stack becomes a platform for transformation.

Microsoft 365 provides an integrated security and productivity solution purpose-built for the AI era. Leverage a unified platform where governance, security, and AI capabilities work together to drive business impact.



The right solution delivers value that grows over time.



of CIOs and CTOs surveyed reported that generative AI has already driven or will drive greater cybersecurity investments in their organization⁴.

Microsoft 365 Apps

Microsoft 365 Apps include familiar productivity tools like Word, Excel, PowerPoint, Outlook, and Teams⁵, among others. Your people already use these tools every day, and now AI is built directly into them with Microsoft 365 Copilot chat. There's no new interface to learn because Copilot shows up right where work happens.

Microsoft Purview

Microsoft Purview⁶ helps organizations govern, protect, and manage data, wherever your data lives in the era of AI. Purview enables visibility into data across your org, safeguards sensitive data across its lifecycle, and protects against oversharing and sensitive data leakage in generative AI.

Microsoft Defender

Microsoft Defender⁶ enables organizations to get ahead of threat actors. Defender empowers organizations to prevent, detect, and respond to attacks across devices, identities, apps, and more. Security Copilot extends these capabilities with dozens of built-in agents that automate security operations while keeping humans in control⁸.

Microsoft Entra

Microsoft Entra⁶ provides identity and access management controls to secure resources for your workforce, customers, and agents. It helps you enforce least privilege access, unify access controls, and improve user experiences.

Microsoft 365 Copilot

At the center is Microsoft 365 Copilot – AI built for work. Copilot helps you turn data into insights, streamline tasks, uncover insights, amplify productivity, and give everyone access to agents all in the flow of work. Secure by design, Copilot is built on enterprise-grade security and responsible AI that empowers you to move faster without compromising the safeguards your business depends on.

Start your Frontier Firm Journey

Becoming a Frontier Firm is more than a technology shift. It's an opportunity for leaders to redefine value, resilience, and innovation. The main barrier isn't technology, it's imagining a new way to work and figuring out how to execute that transformation.

Microsoft 365 provides the security-first foundation that enables your organization to make this transformation possible. With integrated tools for identity, data protection, threat detection, and governance, all built for the AI era, you can move confidently from experimentation to enterprise-scale adoption.

Take the first step →

Complete the Security for AI Assessment to see where your organization stands.

Connect with Microsoft to discuss your path to becoming a Frontier Firm.

Sources

1. [Introducing Microsoft 365 Copilot Tuning, multi-agent orchestration, and more from Microsoft Build 2025](#).
2. [2025 Work Trend Index Annual Report](#) Microsoft analyzed survey data from 31,000 full-time employed or self-employed knowledge workers across 31 countries between February 6, 2025 and March 24, 2025, LinkedIn labor market trends, and trillions of Microsoft 365 productivity signals.
3. [Microsoft Digital Defense Report 2025](#).
4. "Second Annual Generative AI Study: Business Rewards vs. Security Risks", Information Security Media Group (ISMG), February 7, 2025. A global study surveyed over 360 business and cybersecurity professionals during the third quarter of 2024 regarding their understanding of regulations, security challenges, and business opportunities related to generative AI.
5. Microsoft 365 Suites are available with and without Microsoft Teams.
6. Features may vary, explore plans and pricing to learn more.