Navigate IT complexity with boundaryless collaboration

Microsoft Security
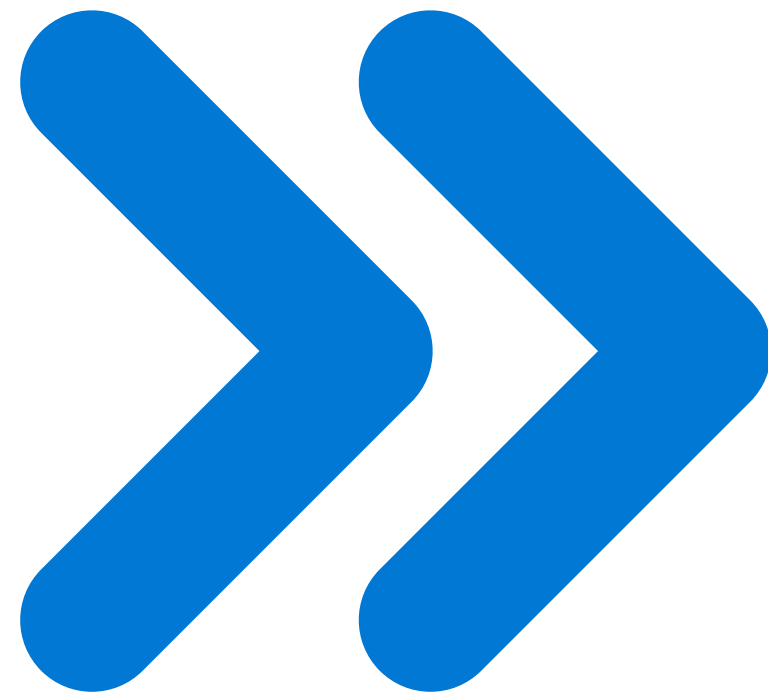
Are you ready for the future of collaboration?

As work becomes more team and project based, the importance of speed, innovation, and relationships are more important than ever. The growth of mergers and acquisition (M&A) activity, multinational companies, and an increasingly globalized and hybrid workforce requires flexible connections between users. IT executives report that **55 percent of all collaboration is with external business partners[1]**. However, the need to improve partnerships can conflict with technology designed to keep people, data, and resources inside security boundaries.

[1] Pulse Research

Organizations need to feel empowered to collaborate across boundaries. With a flexible and secure identity foundation built on Zero Trust, organizations can have more control over who they collaborate with, what resources are shared, and how much access is needed to work productively.

More than 300 midsize to large enterprises identified the two most common elements of collaboration that have risen in importance over the past two years:

○ Effective team communication **(72%)**

○ Fostering collaboration with a wide range of people inside and outside the organization **(68%)**

Discover how Azure Active Directory (Azure AD), Microsoft's cloud-based, universal identity platform, supports secure collaboration without compromising security, user experience, or efficient governance.

Watch this 2-minute video on Azure AD.

Solve three common business collaboration challenges

Organizations need to solve three core challenges to support the future of collaboration.

Balancing security and collaboration

IT admins are responsible for both protecting your organization from external threats and enabling frictionless experiences for employees and business partners. Admins need granular control over access policies to shared resources.

Providing seamless experiences for end-users

Workers in multiple locations drive IT executives to find integrated approaches to access management. Each new access point and login credential required means added friction, security risks, and potential disruptions for your workforce and your customers. Comprehensive tools are essential to integrated, secure, and seamless experiences.

Simplifying collaboration governance

Integrating business units or collaborating with multinational subsidiaries creates manual, time-consuming, and costly processes. Boundaryless collaboration requires greater flexibility and granularity in access controls to make organizations more secure and more productive. These access controls reduce end-user friction, administrative overhead, and allow collaboration to happen on tools that are easy to use and easy to manage.

61% of employees have reported that their teams are siloed because they are using different tools.

- Gitlab 2021 Remote Work Report

Navigate collaboration challenges with Azure Active Directory

Resolving collaboration challenges requires adopting the right identity and access management solution for your organization. Many enterprise businesses are turning to cloud solutions. By 2023, over **55 percent of enterprises will replace outdated operational models with cloud-centric models to foster better collaboration and better business outcomes.**[2]
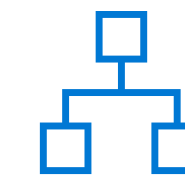
Azure AD is a flexible cloud-centric solution that enables boundaryless collaboration through several principles:
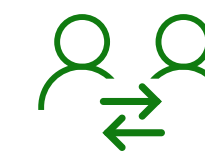
Secure collaboration access:

Start with a Zero Trust foundation and provide user access based on:

- Who you collaborate with
- What resources are shared
- How much access is needed to work productively

Connected organization productivity:

From day one, easily connect organizations and trusted partners disconnected by geographic and IT boundaries

Seamless end-user experiences:

Reduce friction and disruptions by allowing users at trusted organizations to collaborate efficiently.

Efficient collaboration governance:

Easily apply policies through unified application management, delegating management to project owners, and enabling end-user self-service.

The need for these principles stems from two complex collaboration scenarios organizations commonly face:

The need for these principles stems from two complex collaboration scenarios organizations commonly face:

1. Separate companies collaborating as joint venture partners or interdependent supplier, contractor, or vendor relationships.

2. Multinational and conglomerate companies seeking better connection to subsidiaries or integrating recently acquired business units post-M&A.

61%
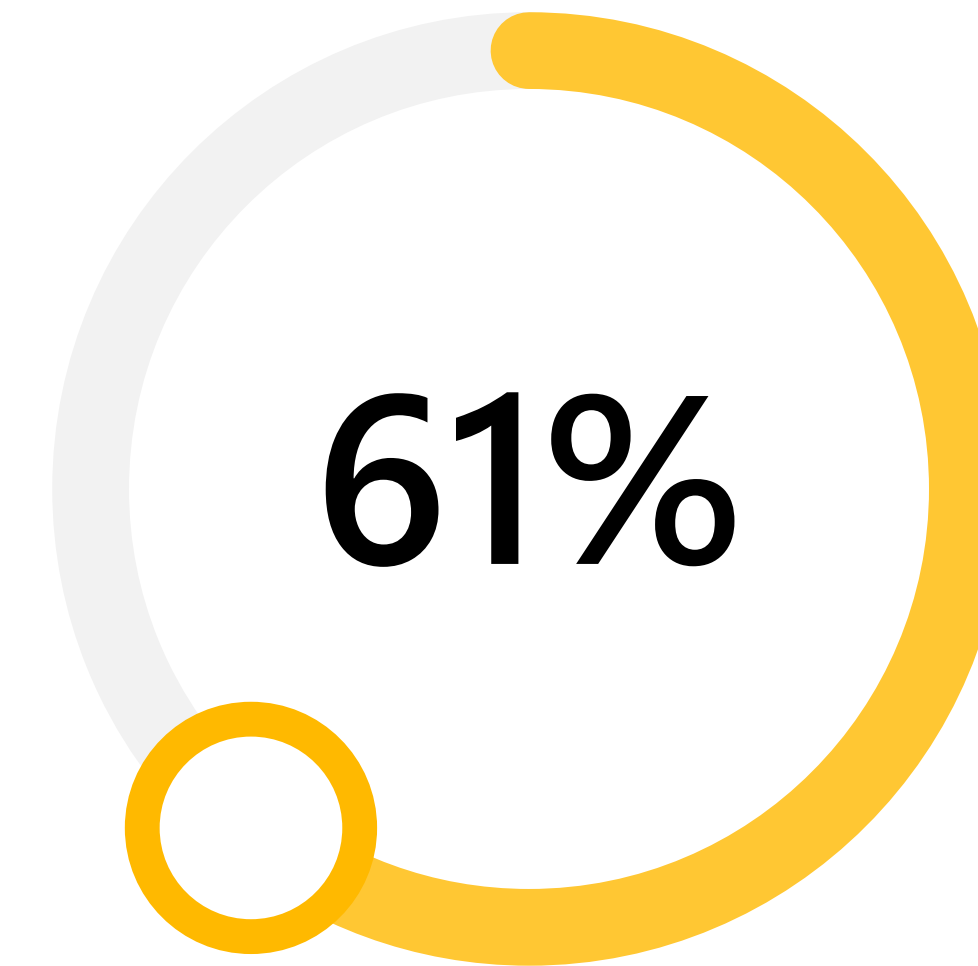
61% of dealmakers expect US M&A activity to return to pre-COVID-19 levels within the next 12 months

 - M&A Trends Survey: The future of M&A

We will dive deeper into these by examining fictional scenarios based on real Microsoft client experiences.

Collaborate with trusted
partners and organizations

To bring a new electric vehicle model to market, a car manufacturing company collaborates under a joint venture partnership with a company that produces batteries for electric vehicles. The car manufacturing company needs to make sure the battery company project team can be easily onboarded and receive the appropriate amount of access to the applications integral to project success, while having a frictionless experience.

IT admins use Azure AD to manage external partners' access in several ways:

- The manufacturer company admins use Azure AD B2B collaboration to efficiently invite and onboard users of the battery company. The Azure AD admin portal provides visibility of internal employees, external employees grouped by department, and key points of contact throughout the network of suppliers.

IT admins specify Conditional Access policies for people in each external organization, such as choosing to trust the existing multi-factor authentication (MFA) to avoid employees authenticating twice.

- The manufacturer admins use the flexible controls of Azure AD Entitlement Management to assign permissions to the battery company's project managers to approve self-service sign-up requests to Microsoft 365 groups, Teams, and SharePoint sites through a simple invitation and redemption process using their existing credentials.

  - This delegation removes the overhead of managing new and protecting additional accounts and passwords. Admins can have peace of mind that single sign-on (SSO) access is being managed securely and users are gaining the seamless access they need to stay productive no matter where they are.

Create an integrated
collaboration hub with
external partners

8

Create an integrated collaboration hub with external partners

In addition to the partnership with the battery company, the manufacturing company also needs to connect individual partners and project-based teams throughout its supplier network via Microsoft Teams. The manufacturing company must avoid poor end-user experiences for the suppliers so they are not tempted to turn to shadow IT that can put the organization at risk.

- To get started, the manufacturing company and each individual supplier configures cross-tenant access settings between their businesses in the Azure AD portal. They specify the inbound and outbound policies, including which of their partner organization's Conditional Access policies should be enforced before granting access.

- Now, channel owners at the manufacturing company can search for employees or groups in the supplier's organization and add them to a shared channel in Microsoft Teams using a valid company email address.

- The individual at the supplier company will then receive an email invitation to join the Teams shared channel and can start collaborating on files within a dedicated SharePoint site.

Direct access to shared channels within their own Teams environment means that suppliers have seamless access to only what they need. The organization providing this access can also cut down on time-consuming management processes and allow project leaders, not just admins, to manage the Teams shared channel membership and update shared channel members throughout the lifespan of the project. Everyone benefits from a frictionless experience that doesn't involve navigating between accounts.

"We need to connect approximately 25,000 employees in 200 locations as a unified organization, bringing awareness of our global network so people can find the colleagues and information they need to develop their best ideas for customers in 90 markets. To achieve this level of cohesive teamwork, we're taking advantage of the communication and collaboration solutions in Microsoft 365.

– Chief Information Officer, Wunderman Thompson
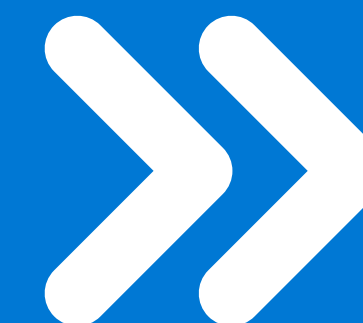
Read the full customer story.

Work productively as one organization

A multinational conglomerate specializing in medical supplies is headquartered in Hamburg, Germany and wants to foster stronger partnerships between the on-premises infrastructure at the company headquarters and:

- 40 international subsidiaries

- A recently acquired US medical supplier

For the conglomerate to realize the value of its acquisition on day one, it must enable boundaryless collaboration to better integrate existing and acquired business units. They need a solution that easily mitigates workforce disruptions and prevents the subsidiaries and acquired business units from feeling siloed. A large part of ensuring these groups don't feel disconnected from the headquarters requires providing secure, seamless access to the same set of Office 365 and line-of-business applications.

IT admins use Azure AD to manage the merger in several ways:

- All partners use the Azure AD admin portal to specify their relationship with the company headquarters and other subsidiaries.

- Admins choose their desired level of visibility and access policies.
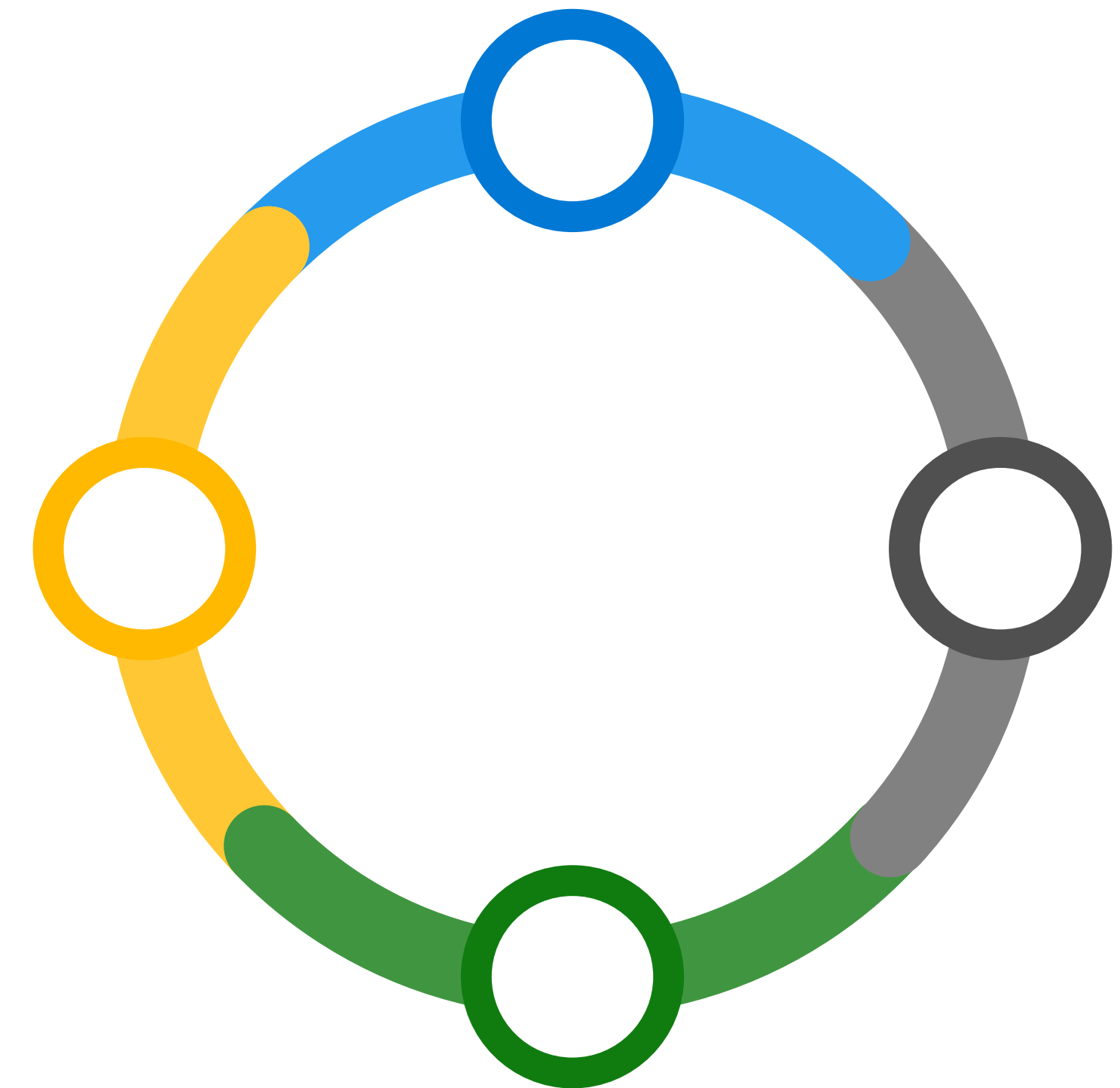
Let's look at the "day one" experience for a sales representative in the recently acquired company. On day one the sales rep can:

Send emails using the conglomerate's email domain, while still receiving emails sent to their previous email in a separate email mailbox.

Complete MFA for SSO access to the conglomerate's apps such as Salesforce so they can collaborate with sales executives on an upcoming client meeting.

Log into the conglomerate's Human Resources applications to update a benefits selection available after the acquisition.

Access Microsoft 365 resources like Microsoft Teams and SharePoint to easily chat, share files, and virtually meet employees across the merged organization.

Take advantage of search capabilities within the Microsoft Exchange global address list, allowing them to view information such as employee calendars and meeting availability.

These capabilities break down communication and collaboration silos. The merged organization and network of subsidiaries are connected through centralized controls so they can mutually benefit from increased collaboration, built-in security and compliance, and reduced IT management.

Azure AD's growing set of boundaryless collaboration capabilities make it easier to customize collaboration and resource sharing in way that matches the relationships and realities of your organization.
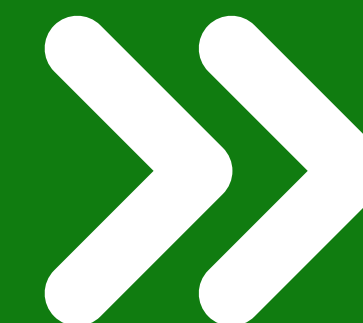
Learn more about auditing and reporting a B2B collaboration user.

[Azure AD] proves valuable both to our IT teams and all the users who are trying to collaborate. The solution is easy, quick, and agile, all while requiring minimal involvement from our IT team and being properly (if not better) controlled.

- Senior Solutions Architect, Centrica

Read the full customer story.

Trust Microsoft for secure and seamless collaboration across boundaries

At Microsoft, we are focused on not only identifying ever-evolving collaboration complexities but also innovating to help prepare you for success today and futureproofing solutions to evolve as your organization evolves.

By enabling Azure AD as your cloud-based solution for secure collaboration across boundaries, members of your entire organization – whether that's internal employees, IT admin, contractors, vendors, or acquired employees – get closer to no longer compromising on either security or experience. Adopting Azure AD helps your organization stay ahead of the curve and collaborate seamlessly no matter what.

Next steps

> **Learn more about [Azure Active Directory External Identities](#) and how to [enable boundaryless collaboration](#) for your organization.**

Microsoft Security