Microsoft

How to engage customers and partners with

Microsoft Azure Active Directory External Identities

Popular Use Cases for

Azure Active Directory External Identities

Collaborate with Business Partners

Engage with Customers

Customize User Experiences and Brand

Manage and Secure Your Entire Workforce

Organizational success depends on users beyond the enterprise

Now more than ever, organizations drive productivity not just by the work they do internally but by collaborating with external partners and enabling digital engagement with customer.

How external collaboration and access is managed can raise numerous challenges, including greater security threats.

⬆ *Last year saw a 300% increase in identity-related attacks.

Disparate identity management solutions not only create IT complexity but can also put your organization at risk.

** Microsoft internal research, 2019*

Microsoft Active Directory (Azure AD) External Identities helps you secure and manage all your customer and partner identities.

With Azure AD External Identities, external users such as contractors, suppliers, customers, or anyone outside your organization can be approved, managed, and given secure access to Microsoft and thousands of SaaS applications, as well as custom line-of-business applications. Security depends not only on having the right intelligence and controls, but also on enabling seamless access to resources across your organization.

Why are seamless experiences essential? External users round out the success of your organization. Collaboration between your employees and contractors, suppliers, and distributors sustains the productivity and growth of your organization. Additionally, enabling cohesive, frictionless access for customers and clients support greater customer retention and relationships that drive your bottom line.

Just as every organization is unique, so are the ways you can customize Azure AD External Identities for your needs. Below are some of the most common uses cases for how organizations have leveraged External Identities to solve their challenges.

Collaborate with Business Partners

Whether communicating with a consultant, arranging an order from a supplier, or managing processes with a distributor, collaboration with external partners is increasingly built into the framework of every organization. External Identities provides the tools to work quickly and securely with essential external team members.

An external HR consultant has been hired by a large IT company to conduct a culture gap assessment. In order to complete this assessment, the consultant needs access to the internal HR team's Microsoft Teams site where they have been collaborating on related documents and exchanging ideas in the chat.

The internal project owner on the HR team invites the external consultant to join the Teams site as a guest, through an invitation redemption process. The consultant receives an email invitation to the shared Teams site, and redeems the invitation using a corporate Google email address. Now, the consultant can access data in the Teams site and chat with the internal HR team, without having to create a new set of credentials.

Enable B2B collaboration in Azure AD

View demo ›

External Identities enables a variety of identity providers that allow external users to

> "Bring Your Own Identity"

Enable "Bring Your Own Identity" with:

- Any organization with a SAML/WS-Fed based federated identity provider
- Microsoft accounts
- Google federation
- Social IDs such as Facebook and Google
- Email one-time passcodes
- Any email address

Beyond the first invitation to collaborate, the consultant's entire lifecycle can be secured and managed. Admins can utilize Azure AD Identity Governance to define specific policies around user permissions, including access review policies and additional security policies using Azure AD Conditional Access and multi-factor authentication (MFA).

A small produce vendor supplies a regional grocery retailer and wants to be able to manage their invoices and view inventory levels in real-time. The grocery retailer has created a custom line-of-business (LoB) application designed to improve communication with its hundreds of vendors, but the produce vendor doesn’t have access to this custom app today.

Rather than the retailer inviting individual vendors to the application, the app is set up to support **self-service sign-up** so that the produce vendor can independently request access and may be prompted to provide additional profile information during the process. Just like with invitation redemption, the grocery retailer can choose to enable vendors to use a variety of identity providers when signing up and accessing the application. After the produce vendor signs up to request access, the grocery retailer can then approve or deny the request.

Learn more about:

- Invitation redemption
- Bring your own identity (BYOI)
- Identity governance and security policies
- Self-service sign-up

Build experiences that customers and partners love with Azure Active Directory External Identities

Watch video ›

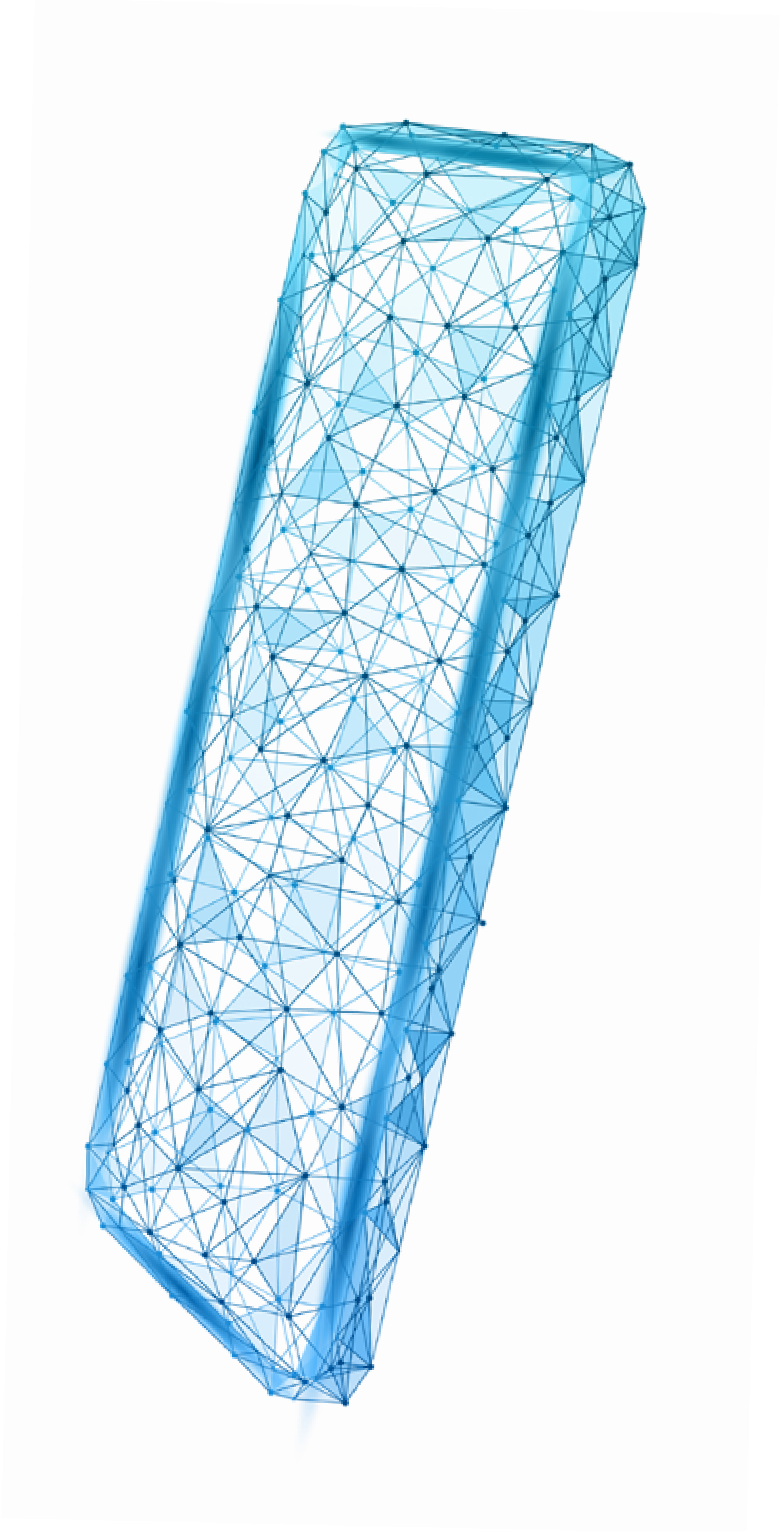
Engage with Customers

Customers depend on a frictionless user experience to connect with your organization in a way that is meaningful and helpful to their personal or professional lives. Seamless access is part of what makes External Identities optimal for engaging and connecting with your customers.

A customer previously visited a hardware store’s physical location but wants to start ordering online from the store, which can be done through the store’s custom application that the customer has not yet accessed.

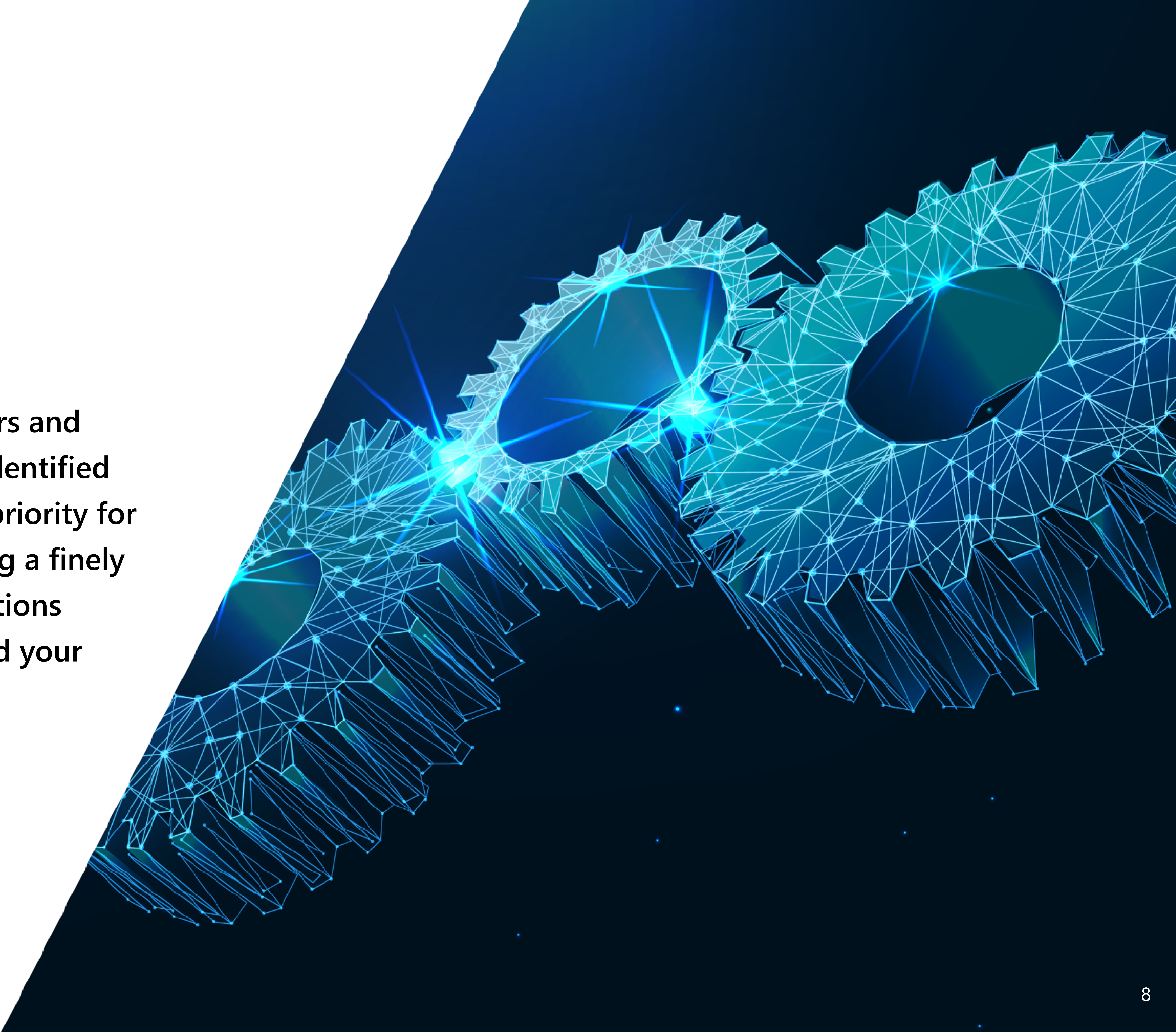
The customer finds the hardware store app and sets up an account, using a one-time passcode sent to their phone number via SMS. Once authenticated, the hardware store’s application prompts the customer to link the account to an existing loyalty account card they previously used in the store, as well as requesting additional information that will inform a more customized customer experience.

In addition to phone sign-up and sign-in, the hardware store can also configure the app to allow any SAML or OIDC provider including social IDs, email, local accounts, or business or government identity providers to sign into the store’s app.



Customize and Brand the User Experience

A seamless user experience is necessary to maximize your relationships with customers and partners. *Identity decision makers have identified investing in user experiences as their top priority for the next 12 months. A large part of creating a finely tuned user experience relies on customizations according to your organization’s brand and your users’ needs.



* *Microsoft internal research, 2020*

At a large wholesale company, a member of the operations team wants to make it easier for the company's merchandising team to track and analyze orders from all their external suppliers.

The wholesale operations team decides to build a custom application for external suppliers to update order statues for the merchandising team. When building the app, they choose what information needs to be collected from the suppliers using custom user attributes, as well as which identity providers suppliers can use to access the app.

The operations team also leverages company branding capabilities to apply lightweight customization to the user interface, so the authentication flow reflects the organization's logo and brand style. This provides a consistent experience for suppliers through every communication and interaction with the wholesale company.

A financial institution customer has created a savings account in the past but hasn't accessed their account with this institution through their new mobile banking application.

At the same time, this financial institution wants to vastly improve the application's user experience, including the data they're collecting, the UI/UX layout, and even integrating with a third-party identification service to increase secure access.

The financial institution updates the app so that the users first step in accessing the app prompts them to add their existing account number to their profile. By using their account number, their essential profile information is already linked. The app admin also creates unique progressive profiling so that on their next visit to the app, the user adds additional account information.

Learn more about:

- Company branding
- Custom attributes
- Advanced customization (B2C)
- Progressive profiling (B2C)
- Partner integrations (B2C)

App admin also make a user's driver's license upload a part of **progressive profiling**, integrated with an identity proofing service. The driver's license helps confirm the customer's identity and their authorization to use that account number, adding an additional layer of security.

Manage and secure employee, customer, and partner identities

With workforces more dispersed than ever, external partners and customers need to rely on secure access no matter where they are. Your extended team is not only working from multiple locations but may also be using numerous devices.

Microsoft's trusted security infrastructure combined with the agility and flexibility of Azure AD provides users with a secure but also seamless experience when accessing essential applications from anywhere, on any device.

An external consultant temporarily working for a multi-national franchise is used to working at client headquarters with a dedicated computer. However, a new project requires the consultant work from a specific store.

The consultant needs to work and transmit data securely while at this new location. Fortunately, the IT team has already put in place automatically security controls that verify the consultant is accessing data from a secure device and location before granting access.

*Azure AD Identity Protection and Conditional Access together helps Fortune 500 organizations prevent over

10 million attacks each month.

The IT admin has already established Conditional Access polices powered by Azure AD Identity Protection, so that the consultant is prompted to complete an additional MFA after signing in at a new IP address despite still being logged in at HQ.

Powerful APIs and an intuitive and integrated UX provides IT with a risk dashboard, including advanced reports, so they can easily monitor any suspicious activity without adding friction to the consultant's experience.

Because the consulting project is only temporary, a custom timebound access review established with Azure AD Identity Governance and Entitlement Management is triggered, revoking access for the consultant at the end of the project.

** Microsoft internal research, 2020*

Zero trust for all your users – employees, partners, vendors and customers

Watch video ›

The holiday season is a booming time for a retailer, but they know this influx of traffic means greater potential for fraud and other security vulnerabilities. They need to heighten app and data security without introducing complexity to the user experience.

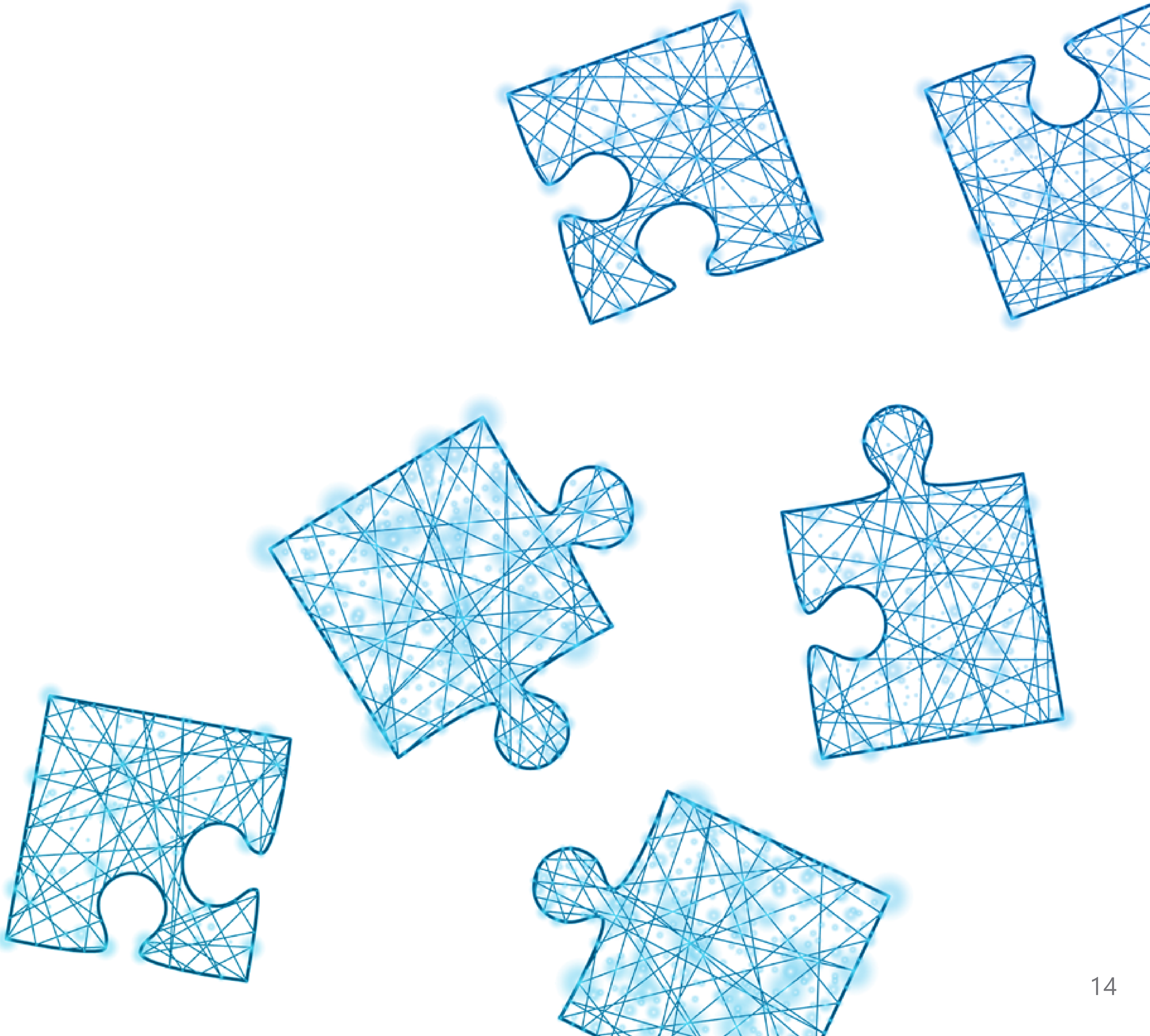
The retailer is looking to integrate an extra layer of fraud protection and Azure AD integration capabilities make this possible. There are multiple third-party fraud protection services to choose from, but the retailer decides to integrate Dynamics 365 Fraud Protection with Azure AD External Identities.

With this integration in tandem with Conditional Access policies coupled with Identity Protection, the retailer can monitor potential security issues more efficiently and leave some monitoring to ML and AI capabilities. ML eliminates the guess work from many of these scenarios by flagging authentications as low, medium, or high risk, using learnings from these scenarios to get smarter over time.

Risks such as users completing a transaction from multiple locations or logging in from a device with a malware-linked IP address can also be more easily detected. By enabling MFA through Conditional Access, these riskier scenarios can trigger MFA authentication so that the user needs to verify they are a legitimate customer looking to make a purchase.

With these automated security policies in place, the retailer spends less time monitoring and making sense of large amounts of data and more time focusing on the busy holiday season.

A gaming company wants to release a new mobile game to its customers. Because the content targets older teens and adults, the company wants to make sure that children are not able to sign up as users without an adult guardian’s supervision. With age gating enabled, the gaming company can now identify minors based on information collected during the sign-up process and either require parental consent status, or block the minor from gaining access or sharing data. This helps protect minors and keeps the gaming company compliant with child privacy regulations in the countries where they operate.



Learn more about:

- Conditional Access
- Azure AD Identity Protection
- Multi-factor authentication (MFA)
- Azure AD Identity Governance
- Entitlement Management
- Age gating (B2C)

Moving forward with

Azure AD External Identities

> Between customers, suppliers, distributors, consultants, and more, your organization is constantly growing and requires tools and solutions that can scale with your business. Azure AD External Identities supports your journey by providing your users with the flexibility and seamless they have come to expect, while keeping your users and business secure.

To dive deeper into the breadth of Microsoft Azure Active Directory External Identities, visit aka.ms/externalidentities

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.