The Logistics of Identity for Building Partner Ecosystems

An IDC InfoBrief, sponsored by OpenText Corporation

Written by: **Jay Bretzmann**, Program Director, Security Products

January 2022

IDC

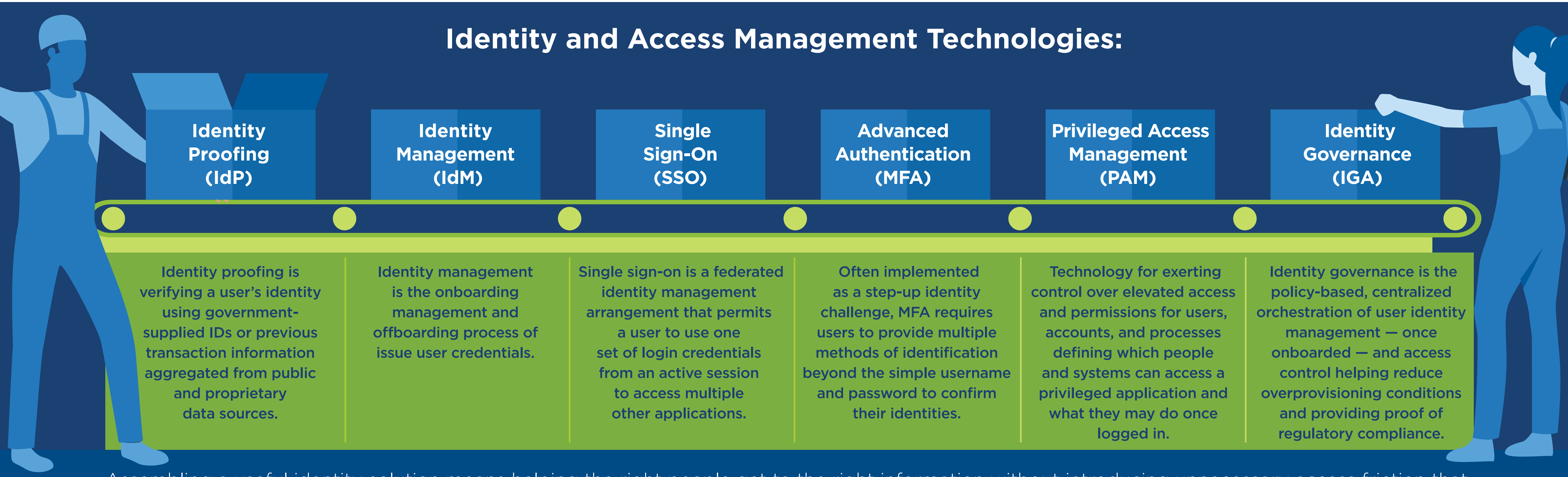
opentext™

Contents

Identity and access management is more than username/password

Identity and access management (IAM) is not one self-contained software program but more a framework of technologies, policies, and business processes that help organizations manage digital identities. It can be a simple database of usernames and passwords — a directory similar to a phonebook — or it can be a more complex solution that proofs a user to a government-issued ID, and includes a call/response challenge program for deeper authentication capabilities, a privileged access component for monitoring and recording user activities, and a governance program for managing a user through a joiner/mover/leaver lifecycle process.

Identity and Access Management Technologies:



Identity Proofing (IdP)

Identity proofing is verifying a user's identity using government-supplied IDs or previous transaction information aggregated from public and proprietary data sources.

Identity Management (IdM)

Identity management is the onboarding management and offboarding process of issue user credentials.

Single Sign-On (SSO)

Single sign-on is a federated identity management arrangement that permits a user to use one set of login credentials from an active session to access multiple other applications.

Advanced Authentication (MFA)

Often implemented as a step-up identity challenge, MFA requires users to provide multiple methods of identification beyond the simple username and password to confirm their identities.

Privileged Access Management (PAM)

Technology for exerting control over elevated access and permissions for users, accounts, and processes defining which people and systems can access a privileged application and what they may do once logged in.

Identity Governance (IGA)

Identity governance is the policy-based, centralized orchestration of user identity management — once onboarded — and access control helping reduce overprovisioning conditions and providing proof of regulatory compliance.

Assembling a useful identity solution means helping the right people get to the right information without introducing unnecessary access friction that reduces user efficiency.

Vast majority of network breaches and data loss are associated with identity credentials compromises

Identity compromises are the number one attack vector for today's cybercriminals. It's just easier, it turns out, to convince some unsuspecting individual to type in their credentials or click on intriguing URLs than to develop worms, trojans or other sophisticated malware. Email phishing leads the pack but there are other techniques like man-in-the-middle attacks that take advantage of telephony protocols never meant to be used for secure communications. Similar to previous years, Verizon's 2021 Data Breach Investigations Report confirms that phishing (36%) and other credentials compromises (25%) are the leading causes of network breaches, and both have accelerated in the past year due to COVID-19 related work-from-home orders.

Forms of deception

Identity fraud preys on ill-prepared organizations and uneducated users urging immediate actions where just one click results in a network compromise.

Phishing
Bulk emails not specifically targeted to any one individual

Spear Phishing
Targeted emails using personal information to increase success rates

Smishing
Phone-based, text messaging delivery of deceptive information and links

CEO Fraud and Whaling
Spoofed emails either directed at or coming from senior executives threatening dire consequences for inaction

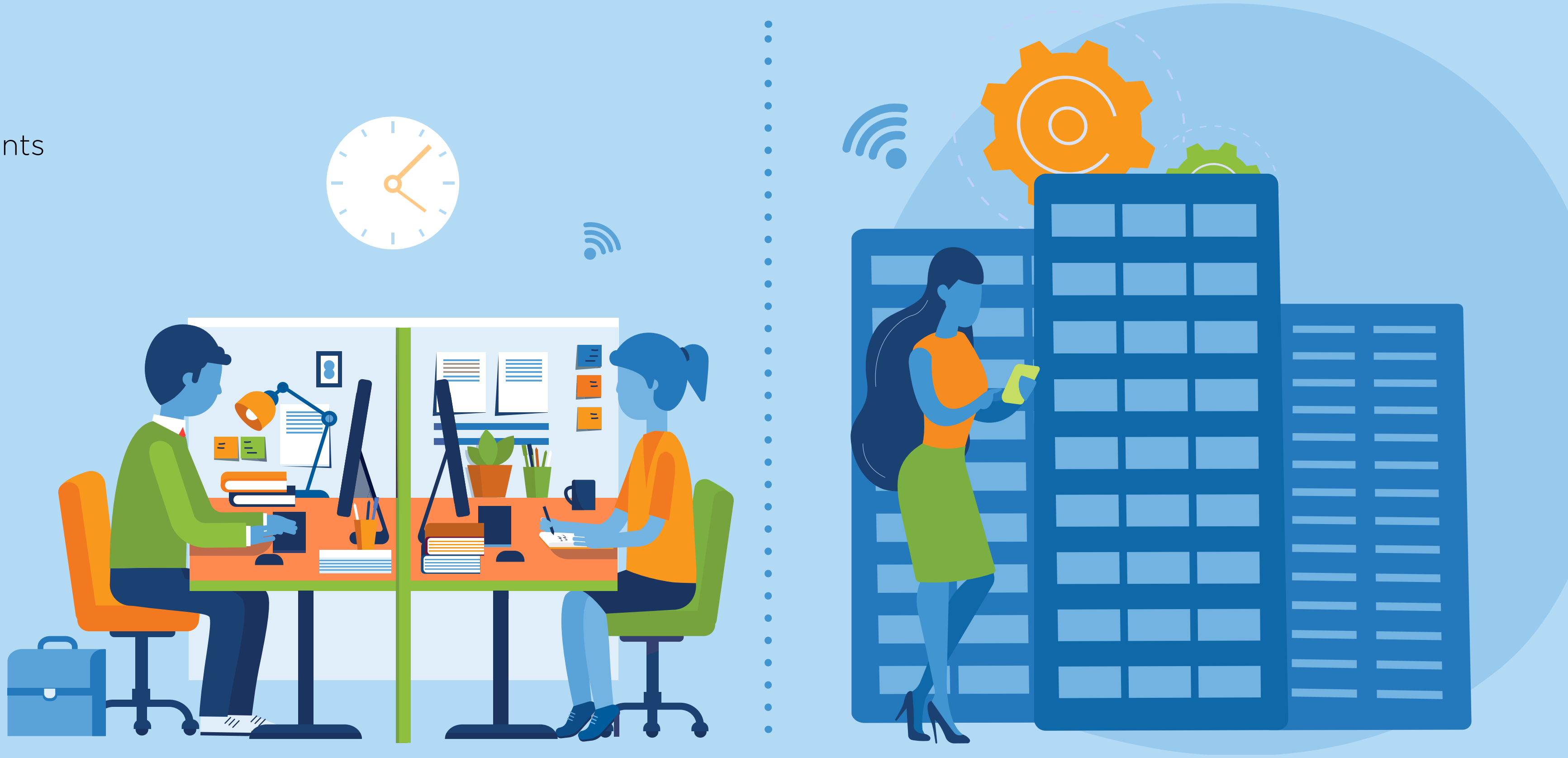
Identity opportunities are on fire due to COVID-19

Nobody save a couple soothsayers in the CDC or Word Health Organization saw the possibilities of a pandemic coming. Almost overnight, it was not safe to gather in crowds or work in close proximities within an office environment. The means to stay safe were to stay home, and that placed an unplanned burden upon both IT management and security staffs. Heretofore, remote access was for the few, the salespeople, the traveling executives, but not for the rank-and-file employees. But all of that changed and created an immediate need for better, safer remote connectivity and positive identification outside the firewall employee access. Work from anywhere became the new survival requirement.

Expenses related to securing remote business operations:

- VPNs and reverse proxy network access environments
- Stronger authentication measures for untrusted endpoints and users
- Broader-privileged access coverage admins, line-of-business users, developers, and partners
- B2C capabilities to communicate and directly interact with consumers

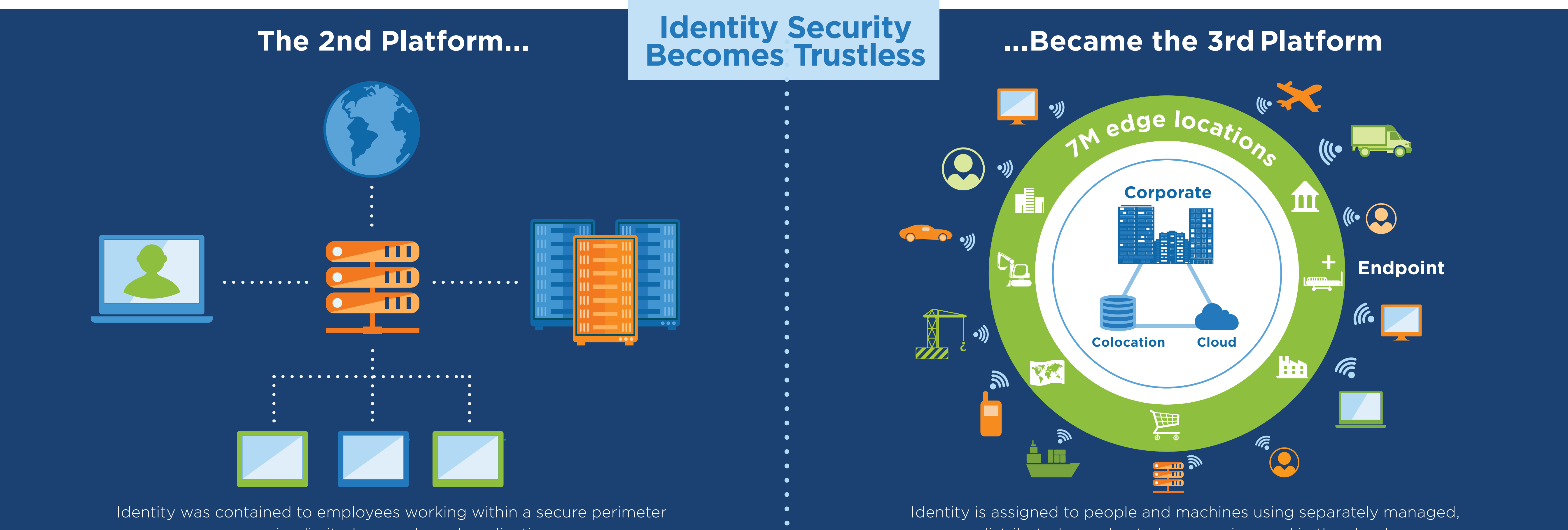
COVID-19 introduced new connectivity and security requirements that wouldn't wait for carefully planned rollouts and methodical digital transformation activities. For many organizations, the challenge was to evolve or perish.



Inside-out identity is yesterday’s model

In the days before anyone could get an IP address, IAM was a simple discipline. The network was something you accessed to share processing capabilities, disk drives, or printers, and eventually trade messages via email systems. Users were either admins or ordinary people and delineated with a single-factor secret we all know as a password. And since no one from outside the organization could possibly connect, it was easy to identify, control, and forecast how many people (not machines) would exist at any one point in time. There has been an ongoing and necessary shift from more simple IAM models based on second platform architectural environments towards IAM in third platform architectural environments, where identity is assigned using separately managed, distributed apps hosted on premises and in the cloud.

Identity Security Becomes Trustless



Identity was contained to employees working within a secure perimeter accessing limited server based applications

Identity is assigned to people and machines using separately managed, distributed apps hosted on premises and in the cloud.

Source: IDC, 2021

Inside-out identity is yesterday’s model

The Internet Effect:

- Unmonitored access to published information
- Unsupervised processing using remote servers and procedures
- Uncontrolled access to organizational resources through open networking ports
- Unforeseen demands for access to publicly exposed data

The legacy of IAM solutions embodies an inside-out approach, meaning it all begins with controlling the internal environment business to employee (B2E) with vendors attempting to extend access rights to external organizations (B2B and B2C). While some solutions were better suited than others, the overall scale, control, and context required compromised the user experience. Enterprise IAM solutions could not adequately serve the requirements of third-party users.

Channel partner delays (service unavailable warnings)

User frustrations (and abandoned shopping carts)

Understanding third-party identity risk

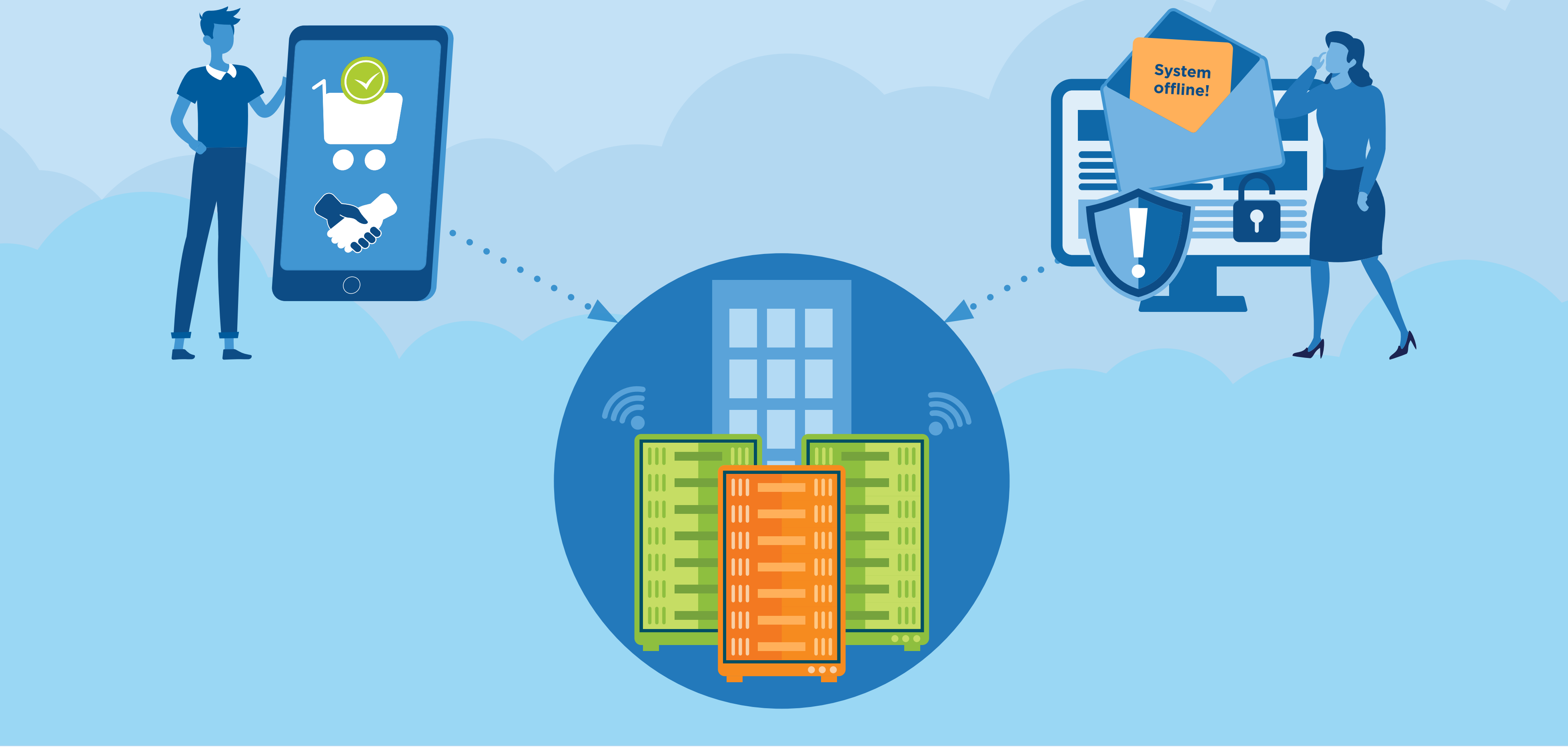
Organizations embracing digital transition projects are increasingly exposing their internal systems to outsiders.

The trickle-down impact of unauthorized third-party access includes:

- Reputational damage
- Adverse audit findings
- Significant costs due to non-compliance

Done properly, giving partners direct access to your ordering and fulfillment systems delivers cost savings based on improved efficiencies.

Done improperly, identity compromises of your partners systems can lead to catastrophic internal data losses and business disruption. Third-party access requires tighter user identifications and access control.



Challenges with third-party identity implementations

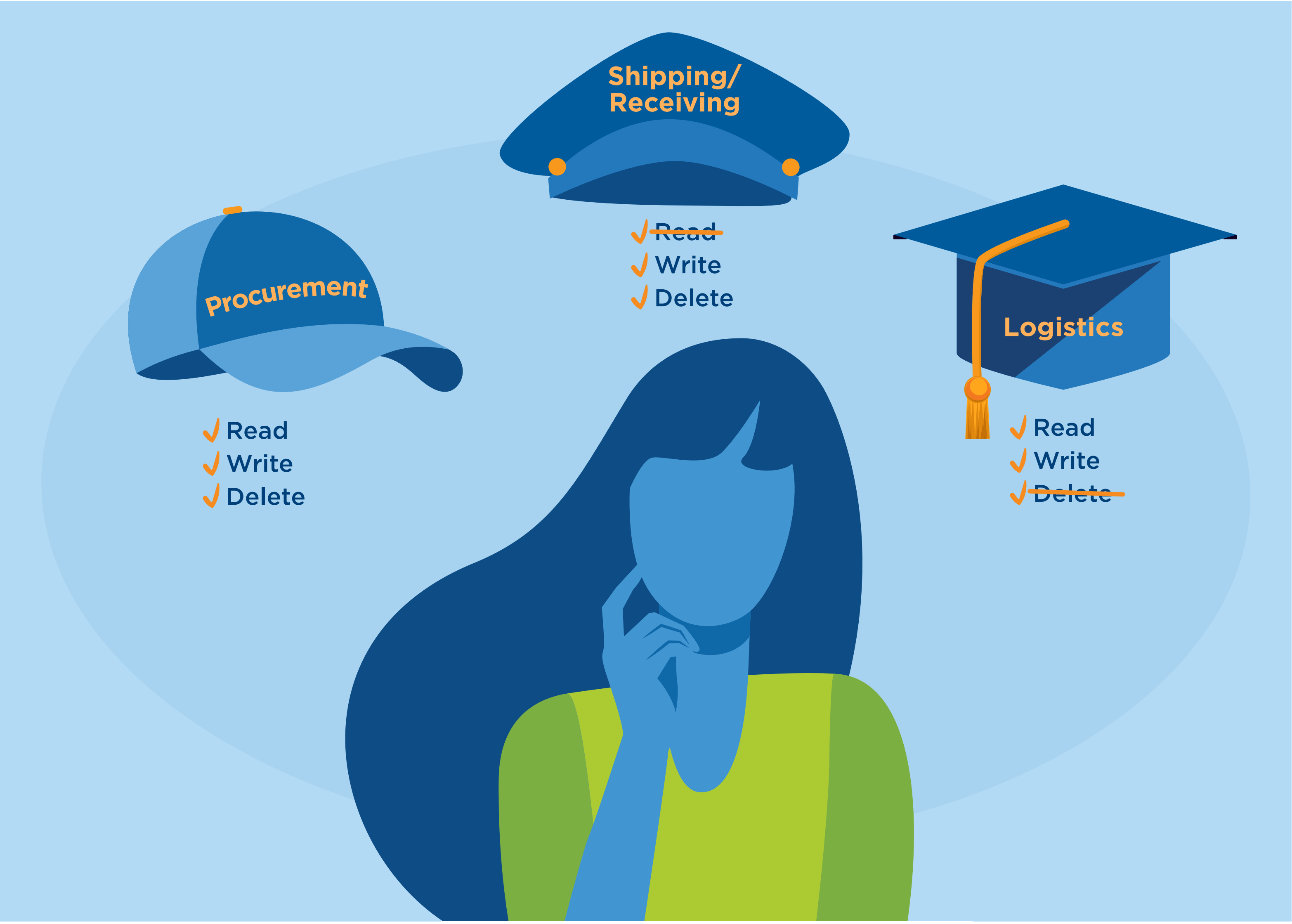
Business network or supply-chain providers face a huge problem managing third-party access rights. Many have hundreds to thousands of partners using applications to get access to their goods and services, but centrally managing such high numbers of users is both cost prohibitive and fraught with high levels of risk. A better model is basically to divide and conquer allowing both the buyer and partner to contribute their respective expertise.

A buyer offers a technology framework and core services with rich self-service capabilities; a partner contributes local expertise using that framework to define who within its user community can do what. The partner assigns local administrators to create its organizational structure, identify users needing access to specific buyer resources, responding to access requests and removing people as they leave the organization. This model allows partners to access to key resources, and buyers to improve security decisions while retaining access audit and control and eliminating external user administration cost across a global value chain.

Tapping into the value of an extended-roles model built upon attributes and access rules

Even within a single organization, assigning accurate user roles without resorting to the overprovisioning of resource accesses is both a difficult and unending task. On the flip-side, many attempts to define roles more narrowly can result in lost productivity as users are denied access to the resources they require. A better model — in context of external user populations that can dwarf internal populations — is to enable the resources themselves to determine who gets in and who doesn't.

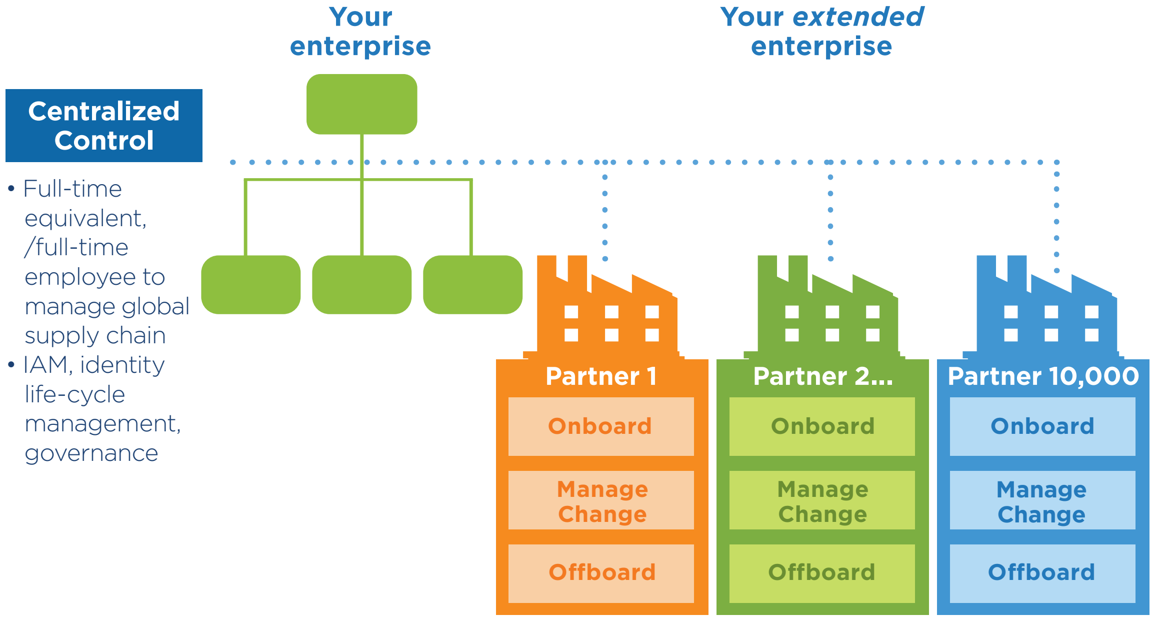
The best practices for these scenarios is to offer predefined service bundles (e.g., templates specifying provisions and access rights to applications, workflows, dashboards, data aggregation/analysis, and other industry-specific logistical capabilities) tailored for common partner and internal communities such as procurement, shipping/receiving, sales, buyers, and others — all of whom require access to multiple enterprise and cloud systems to get their job done.



Example use cases

Distributed identity management example:

> *Delegated identity administration provides local experts the ability to define and manage their organizations and access.*



Your enterprise

Your *extended* enterprise

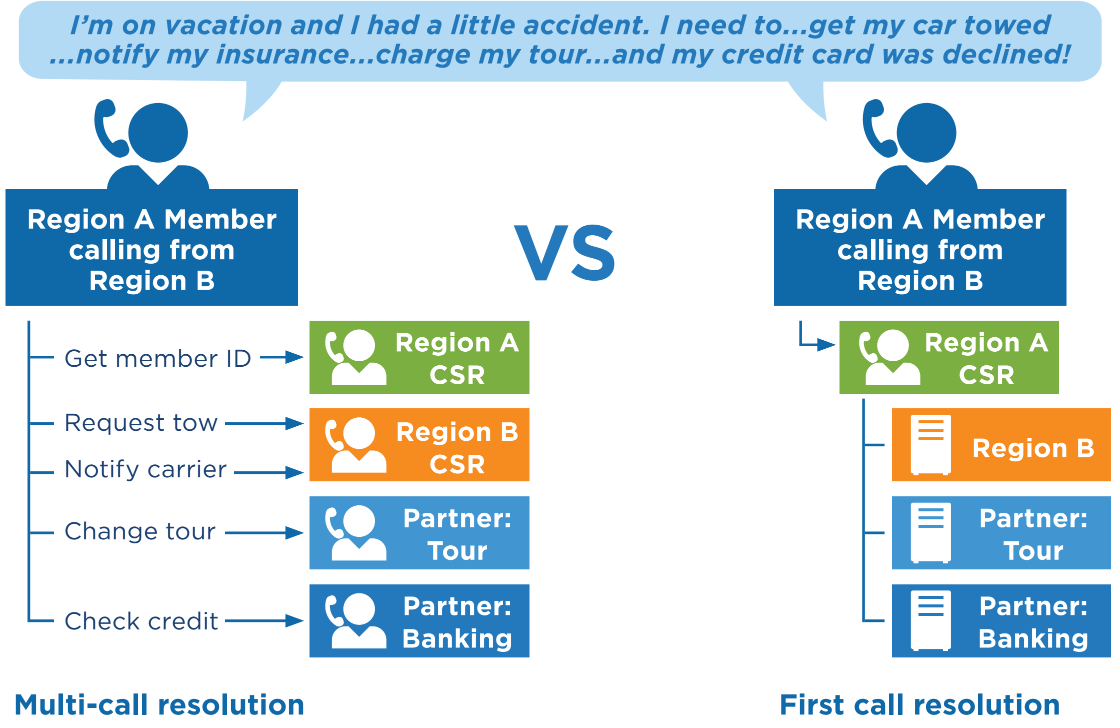
Centralized Control

- Full-time equivalent, /full-time employee to manage global supply chain
- IAM, identity life-cycle management, governance

Partner 1	Partner 2...	Partner 10,000
Onboard	Onboard	Onboard
Manage Change	Manage Change	Manage Change
Offboard	Offboard	Offboard

Automotive insurance example:

> *Taking the burden off the end user with authorized access to customer information distributed across multiple enterprise partners.*



I'm on vacation and I had a little accident. I need to...get my car towed ...notify my insurance...charge my tour...and my credit card was declined!

Region A Member calling from Region B

- Get member ID → Region A CSR
- Request tow → Region B CSR
- Notify carrier → Region B CSR
- Change tour → Partner: Tour
- Check credit → Partner: Banking

Multi-call resolution

VS

Region A Member calling from Region B

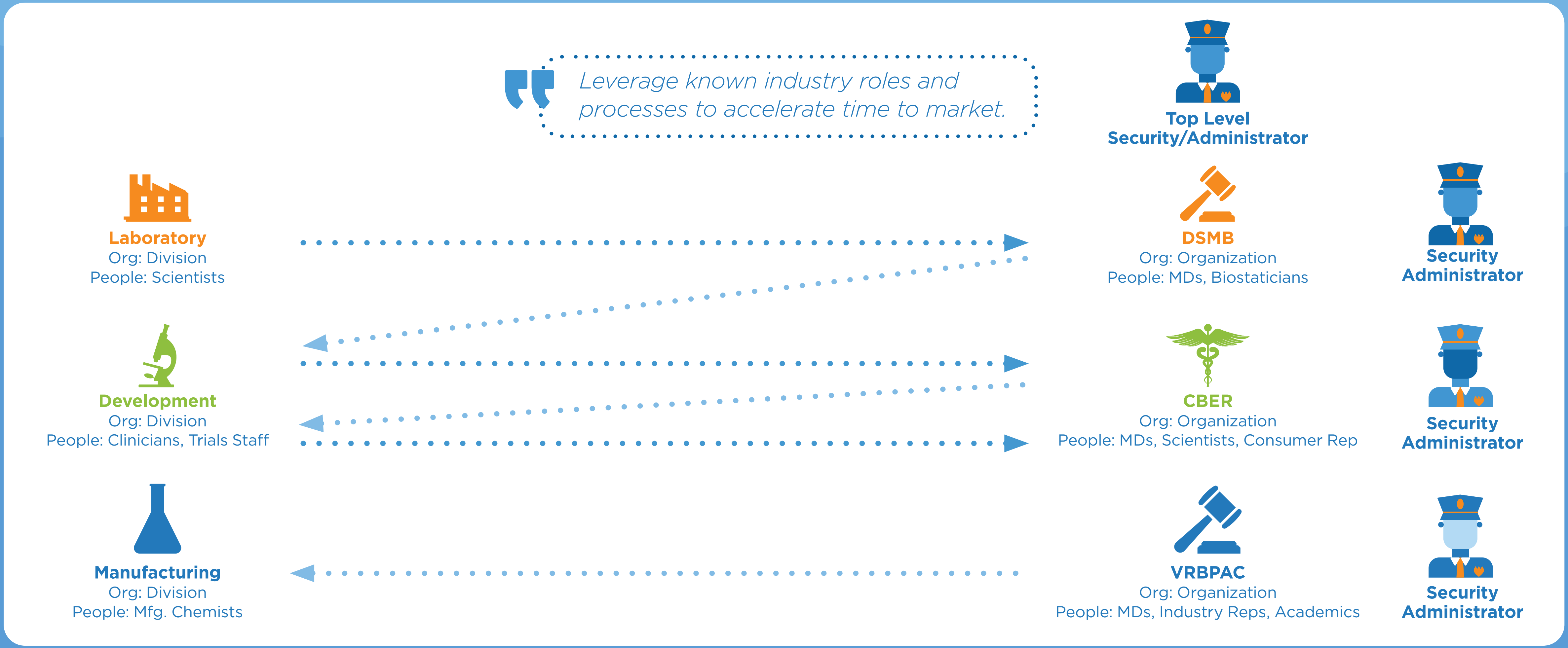
→ Region A CSR

- Region B
- Partner: Tour
- Partner: Banking

First call resolution

Example use cases

Life sciences example:



Leverage known industry roles and processes to accelerate time to market.

Top Level Security/Administrator

Laboratory
Org: Division
People: Scientists

Development
Org: Division
People: Clinicians, Trials Staff

Manufacturing
Org: Division
People: Mfg. Chemists

DSMB
Org: Organization
People: MDs, Biostaticians

CBER
Org: Organization
People: MDs, Scientists, Consumer Rep

VRBPAC
Org: Organization
People: MDs, Industry Reps, Academics

Security Administrator

Security Administrator

Security Administrator

Benefits of an outside-in identity approach

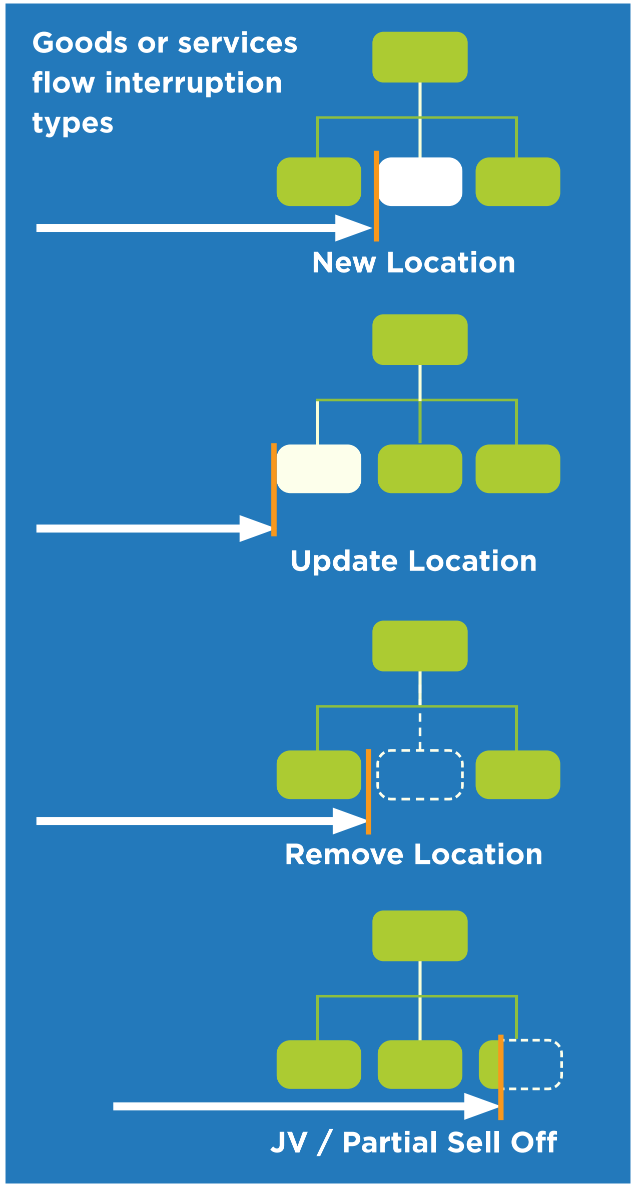
Extending an inside-out model of identity to incorporate third parties places an enormous burden and liability on the buyer organization's security team. The ask is that they apply a technology developed for a different purpose — workforce identity — to an extended enterprise ecosystem and use it to control the actions of external participants. More than that, the buyer is challenged to manage these third-party supply chain partners without disrupting business operations even when organizational or locational changes occur due to unreported partner activities.

The ideal solution is to automatically detect these and other changes, then re-validate security across the network to identify corrective actions, e.g., remove access, move users, update master data, etc. Actions can be applied automatically or be sent to buyers and partners to correct using supplied tools, workflows, or APIs. Software should help avoid supply chain disruptions and security incidents when a partner company moves, sells a division, or acquires a new business unit.

Organizations should consider an outside-in model of identity, which encompasses the following elements:

- Pre-defined identity roles and relationships congruent with the needs of specific vertical market requirements
- Access liability reductions for supplier presence and activities
- Improved management and control over active vs. expired identities and specific data access rights
- Scale and reliability exceeding any limits of internal IT resources

IAM is the new security perimeter and a considerable challenge for organizations to appropriately implement for themselves save any third parties. It's an identity problem ripe for an outsourced solution leveraging a supply chain expert that understands the ins and outs of specific industries. The wheel here has been invented, but the rims and tire treads might need a few adjustments.



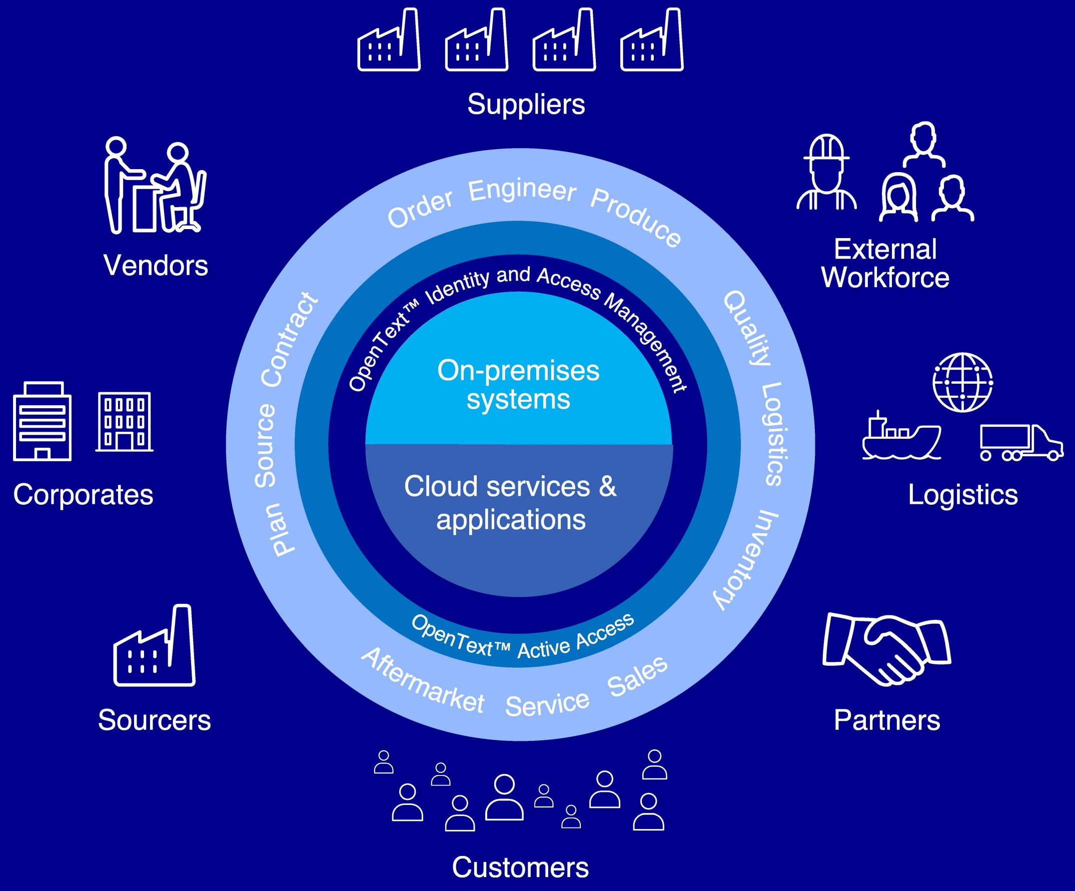
Message from the Sponsor

The OpenText Business Network provides business to anything (B2A) integration solutions that securely connect over 1 million trading partners, exchanging 26 billion transactions with a collective value of $9 trillion dollars.

opentext™

OpenText™ Identity and Access Management (IAM) enables organizations to drive top-line growth and gain bottom-line efficiencies by enabling business networks to quickly and securely access enterprise and cloud systems — at scale. Innovative security frameworks, automated digital processes, and advanced authentication, lifecycle management and governance tame extended enterprise costs, complexity and risk.

OpenText™ Active Access accelerates collaborative work by keeping partners engaged, informed and productive. Using a single portal technology, organizations can connect any external community to any business process or application, streamline communications between buyers and sellers, and enable external users to connect once and go to any authorized resource in the ecosystem.


Suppliers
Vendors
External Workforce
Corporates
Logistics
Sourcers
Partners
Customers
Order Engineer Produce
Quality Logistics Inventory
Sales Service Aftermarket
Plan Source Contract
OpenText™ Identity and Access Management
OpenText™ Active Access
On-premises systems
Cloud services & applications