opentext™

WHITE PAPER

Drive growth by automating third-party access to enterprise information at scale

Streamline digital transformation initiatives while protecting the enterprise from the No. 1 source of data breaches: “Trusted” third parties

Contents

Executive summary

Digital initiatives are accelerating at record pace. Traditional value chains are looking to transform their external business networks into highly connected digital ecosystems, able to scale growth, efficiency, competitiveness and other business outcomes while lowering operating investment. For example, life insurance companies reduce the time and cost to connect with potential customers by selling through a distributed ecosystem of third-party agents, brokers, advisors, marketing organizations, underwriters and others. Digital product and service providers deliver new value to customers and subscribers by seamlessly incorporating partner services into core offerings.

For these and similar B2B digital strategies, success hinges on the ability to securely and predictably connect partners, suppliers, customers and other third-party organizations to enterprise systems and resources.

Unfortunately, most tools that secure and enforce user access to enterprise systems do so for internal employees—not third parties. When such solutions underpin complex multi-enterprise use cases, delays, additional cost and concessions quickly ensue.

This paper describes the complexities and challenges of securing third-party access and the critical capabilities needed to scale that access. It also introduces a cloud-native, Platform as a Service solution proven to secure access to enterprise systems across global value chains—typically consuming only two to three FTEs.

Third-party access: Introduction

Businesses have relied on collaborative third-party relationships for years to reduce costs through collaborative work. For example, in 2000, the “Big Three” North American automotive manufacturers realized massive efficiencies by working collaboratively with their shared supply base. Suppliers were given access to the manufacturers’ back-end systems to fulfill procure-to-pay processes that were previously performed in house.

The growth of collaborative work is most evident in global value chains, as digitally connecting value-chain partners to the company’s core business processes is essential to introduce efficiency, reduce cost and decrease the risk of disruption. (see Figure 1).

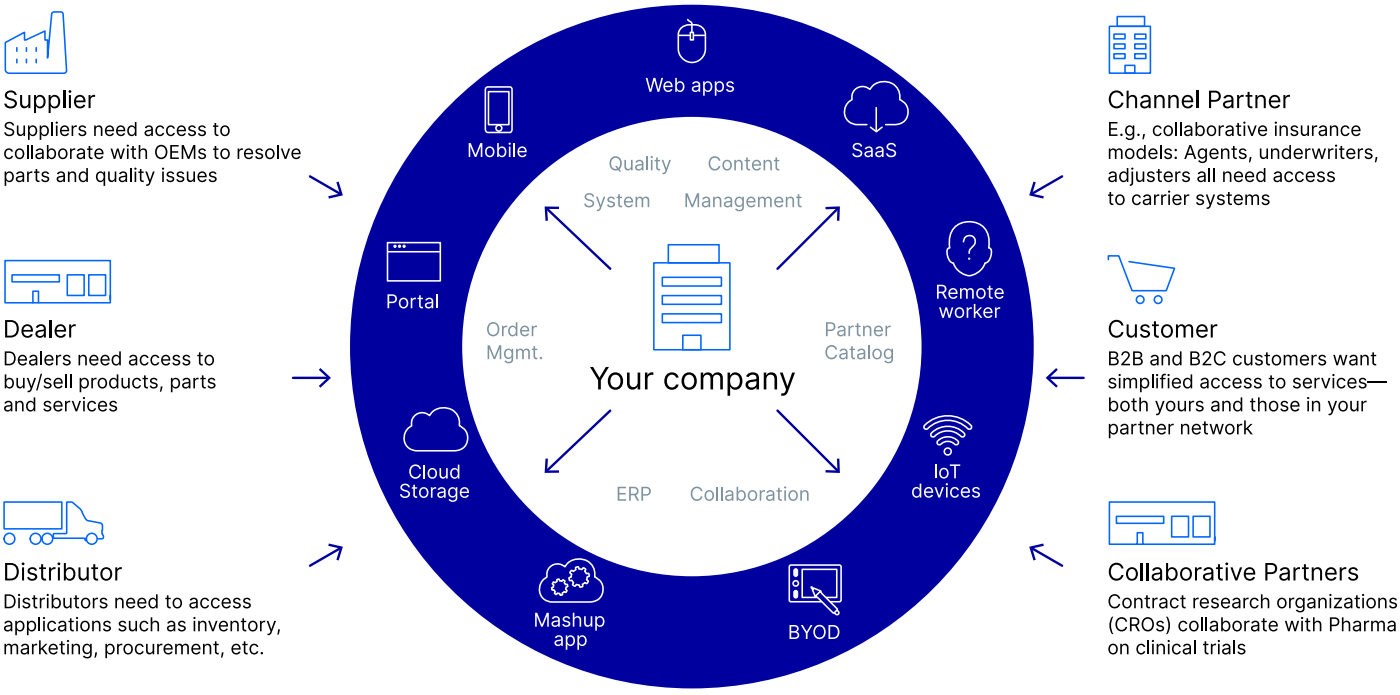

Figure 1. The Collaborative Ecosystem

As value chains expand, digital assets and information previously accessible only to employees need to be made available to an ever-changing community of suppliers, partners, distributors, B2B customers and other third parties. Historically, enterprises instituted ad hoc 1:1 connections to funnel trading partners to internal resources and directly managed identities and access as a mesh network.

However, this approach quickly leads to an untenable situation as each new endpoint represents an exponential increase in attack surface and puts one or more factors of an enterprise architecture to the test: scalability, availability, security and others. (see Figure 2).

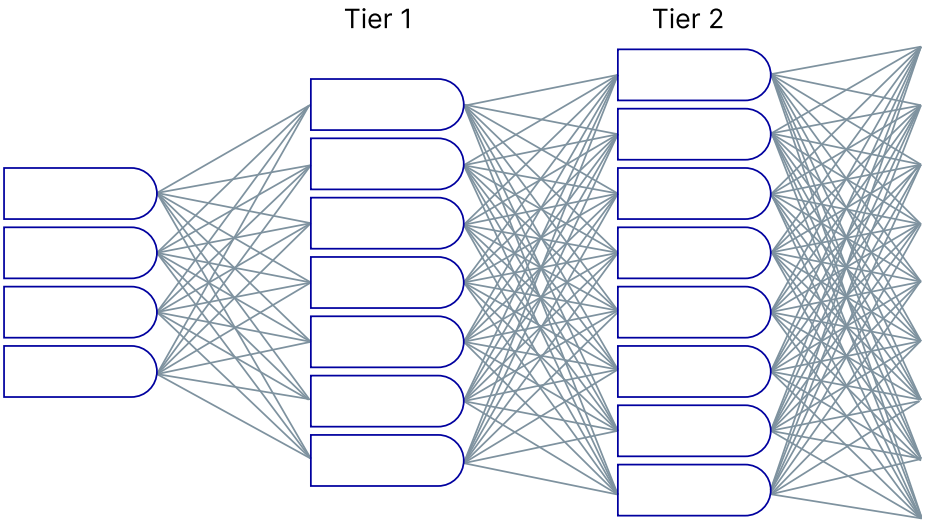

Figure 2. High degree of complexity with multi-tiered partner and user relationships

The current state of third-party access remains far from ideal. The increasing number of third parties given access to back-end systems without orchestrated identity management or governance has led to significant risk and cost.

Opportunities await those able to implement effective controls to overcome risks and harness the power of third-party ecosystems. The reliance on collaborative third-party relationships is only expected to increase, and at a much faster pace, as digital transformation initiatives mature.

- Digital ecosystems will account for ≈ €60 trillion in revenue worldwide by 2030[1]
- 53% of supply chains will continue to make significant changes to their supply base through 2026[2]
- By 2025, leaders will use ecosystem product development to meet new customer expectations[3]

But without effective controls in place to mitigate third-party risk, such initiatives will only increase the risks of a breach.

1 McKinsey, Digital ecosystems for insurers: No one size fits all. (2021)

2 Ernst & Young, Why global industrial supply chains are decoupling. (2022)

3 Gartner, Rebound Quickly From the Current Downturn by Using Collaborative Ecosystem Product Development (2021)

Identity and access management defined

Identity and access management (IAM) is a technology that automates alignment of user authorizations and access with an organization's security and privacy policies. The simple definition below is ideal for those outside of information security, yet easily connects to underlying IAM frameworks and components as shown in Figure 3, below:

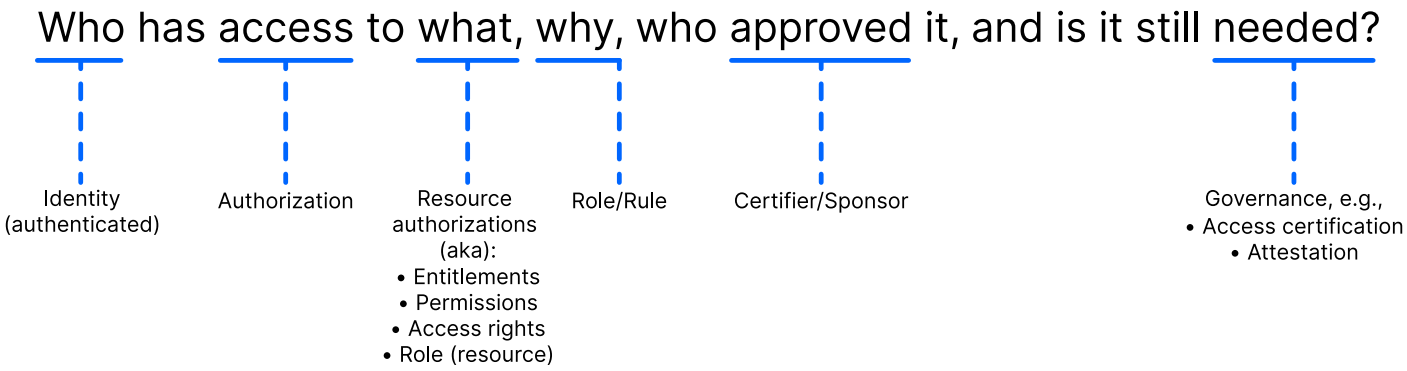

Figure 3. IAM defined

Beyond the most basic function of directory services that maintain the metadata associated with an identity, IAM covers two main functions:

Authentication—the mechanism for establishing the veracity of a user's credentials, effectively determining that a user is who they claim to be, then communicating that authentication across security domains via federated single sign-on or other means.

Authorization—the mechanism for administrating access rights/privileges to protected resources typically related to implementing an information security control point, application access and role management. Authorizations are typically governed via a defined access policy, incorporating workflow and certification.

Authorizations management is the heart of an IAM solution, as it ultimately controls which applications each user is authorized to access, what can be done within the application, who must approve the access and who must recertify that access so it may be retained or revoked. IAM solutions automate these processes by detecting and responding to scheduled or realtime events, such as when a person joins a company, moves to a new job within the company or leaves the company. The end-to-end process of managing identity and access for joiners, movers and leavers is called identity lifecycle management (ILM). Figure 4 below depicts the three identity lifecycle phases and provides sample events that routinely trigger IAM processes.

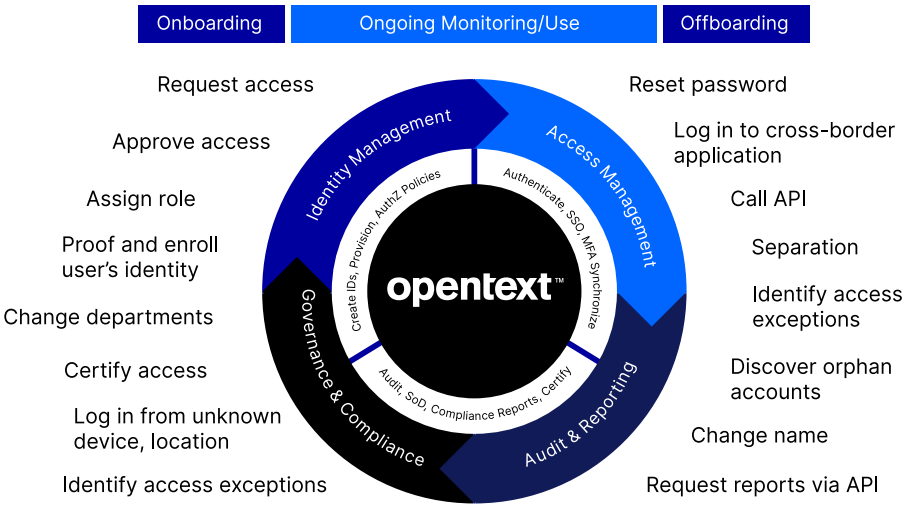

Figure 4. Identity lifecycle management

Enterprise IAM vs. Extended Enterprise IAM

Although IAM is a security technology, its initial value proposition in the early 2000s was reducing the cost to manage employee access—security was more of a "perk." When anti-fraud and corporate accountability regulations were introduced (e.g., Sarbanes Oxley, Graham Leach Bliley, etc.), "Enterprise IAM" was a natural fit as it provided a framework of controls to mitigate the risk of unlawful or inappropriate actions by employees. For example, enforcing Segregation of Duties enabled enterprises to disallow toxic combinations of authorizations that enable fraud, e.g., an employee who is authorized to create a vendor, issue a purchase order and pay invoices.

Enterprise IAM has since grown to automate more lifecycle events, support more systems and be delivered as a cloud service (IDaaS). However, the primary use case remains the same for the majority of vendors—securing employee (workforce) access to on-premises and cloud resources.

Extended Enterprise IAM, on the other hand, focuses on the much larger population of external users—suppliers, partners, vendors, B2B customers, agents, contractors and other users OUTSIDE the enterprise who need access to resources INSIDE the enterprise.

While both IAM varieties are designed to securely manage user authorizations and access, they do so for very different audiences, purposes and environments. For example, organizations that use their enterprise IAM investment to manage trading partner and B2B customer identities typically see an immediate reduction (or absence) in automation, security, compliance and standardization, and an increase in manual operations. Why? Enterprise IAM products are built to leverage internal enterprise processes, conventions and data to work as advertised. For example: a consistent and curated system of record for users and attributes, defined corporate hierarchy to facilitate provisioning and security decisions, company-issued devices, and so on. When enterprise IAM products are pointed at B2B organizations, these prerequisites become unavailable or insufficient to establish trust, provision access or otherwise secure external access and in an automated, scalable fashion.

B2B IAM products worthy of investment bring technologies and innovations that create visibility into external enterprises to simplify and scale managing identity lifecycles for all people, systems and things within the ecosystem: suppliers, customers, employees, citizens applications, devices and operational technology.

Extended enterprise IAM solutions differentiate themselves from employee-centric products by including technologies and digital processes that:

- Create visibility into third-party organizations.
- Secure access across multiple security domains and complex ecosystems.
- Validate credentials using a variety of signals to corroborate identity.
- Protect APIs from public view.
- Create a 360-degree view of every person, system or thing accessing the enterprise
- Enable external organizations to be added without increasing internal resources.
- Present one endpoint for all external access.

What innovations can increase the security and agility of your value chain?

OpenText's IAM product, OpenText™ Core Secure Access provides innovative solutions to simplify and standardize how an enterprise manages access across large third-party ecosystems. Below are a few OpenText Core Secure Access innovations that demonstrate the company's leadership in this space.

Entity relationship management: Unified Data Model

Securing ecosystem access to enterprise information is more than just managing users. Businesses are required to inventory, audit and certify all external access to the enterprise, including people, but also systems, sensors, vehicles and other non-carbon entities.

OpenText Core Secure Access has a Unified Data Model that creates a consistent approach to securing access for all people, systems and things. Each of these entities receive a unique digital identity that reflects all known accounts, authorizations, relationships, profile data and other information. The Unified Data Model is a canonical representation of identity information for each entity type. It describes the entity's relationship with other entities (nodes) to be explicit or derived. These relationship nodes are then used for authentication and authorization, providing a highly scalable and secure method for controlling access across large ecosystems (see Figure 5).

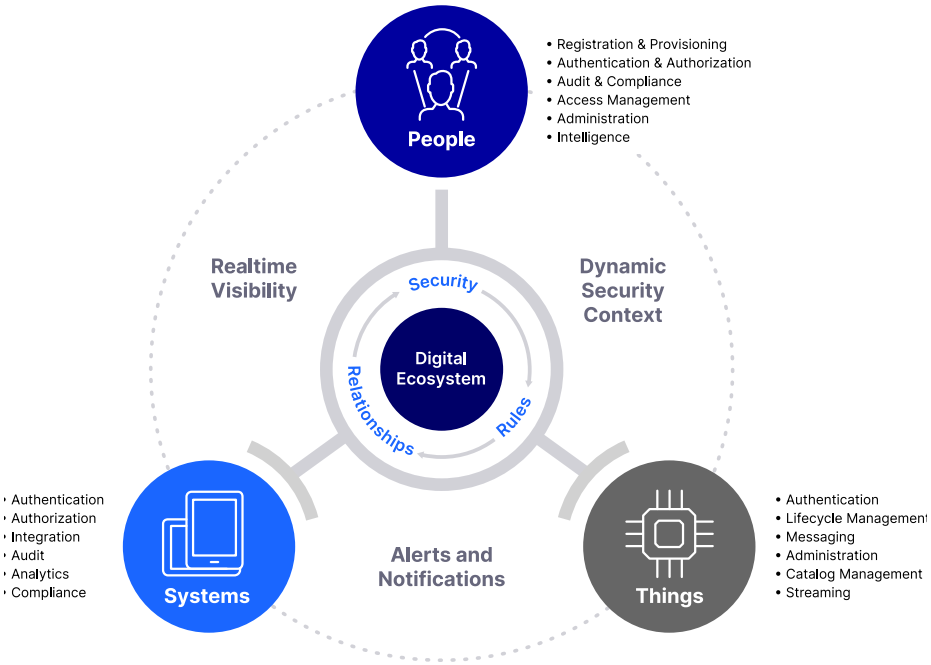

Figure 5: Entity Relationship Management Model

The "Extended" Enterprise Directory

Enterprise directories maintain and manage information that ultimately determines access permissions for each user, creating a "single version of truth" for employee and workforce users. Establishing the same construct for extended enterprise users is equally critical but far more complex.

External user identities are typically created within each system that a user is authorized to access (e.g., ERP, Quality, CRM) and is managed by the owner of the system or the supported business process. This results in silos of identity information that weaken security and undermine operations. For example, the value and protection afforded by risk-based authentication tools is reduced, with only a subset of information for determining risk and the factors to mitigate that risk.

Some organizations opt to store external user data in the enterprise directory. Analysts agree that managing third-party identities in the enterprise directory can be a "worst practice" due to the inherent risk when co-mingling internal and external users. This is evidenced in a 2020 internal audit report concerning third-party access to the World Food Programme's data and information systems.10 Specifically, the configuration of the enterprise directory resulted in providing internal and external users with "the same default access to applications, services and data available through AD including WFP's intranet… virtual private network connections and some shared drives, etc."

OpenText Core Secure Access is the “single version of third-party truth” easily integrating with on-premises and cloud systems to ensure that user profile and authorization information is correct, current and delivered in the right format across value chain systems and devices. Messaging and orchestration, event streaming and other integration layer services simplify connecting and managing identity store and eliminating silos.

This best-practice approach results in a 360-degree view of all third parties to:

- Scale trust during authentication by knowing the true risk a user presents.
- Improve access decisions.
- Personalize journeys across business processes.
- Resolve customer service issues quickly and happily when CSRs understand all relevant customer services and eliminate disjointed experiences.
- Operationalize third-party risk management (TPRM) strategies by aligning OpenText Core Secure Access access policies and controls with TPRM.
- Securely connect remote third-party and employee users with enterprise systems, without requiring VPN.
- Work collaboratively across partner ecosystems with granular access.

Organizational hierarchy concept

A key component in enterprise products is the concept of an organizational structure or hierarchy. An organizational hierarchy provides an efficient means for determining a user’s access rights, administrative authority and other privileges based on their on their placement within the hierarchy.

OpenText Core Secure Access leverages this same construct to represent a logical view of a third party’s organizational hierarchy. The platform enables delegated administrators to create and maintain a “digital twin” of the parts of their organization that require access—without involving enterprise administrators. Organizational hierarchy also provides a means to detect organizational changes in third-party organizations: see Hierarchy management and synchronization, discussed later.

Distributed decisions: Delegated administration

Scalability is the limiting factor when managing third-party users. The time, cost and risk to administrate identity and access for thousands of organizations and millions of users can be cost prohibitive if using a mix of enterprise tools and manual processes. Additionally, the lack of visibility into the comings and goings of personnel at third-party organizations creates significant risk, potentially delaying deprovisioning of departed users until the next contract recertification one to two years out.

Managing identity and access management at scale requires distributed decision-making while maintaining centralized policy enforcement, audit, logging, compliance and reporting. Yet oversight needs to be retained related to high-risk activities, such as:

- Specific applications available to each partner organization.
- Final approval on the applications a user can access.
- Removal of application access by user or customer's partner.
- Monitoring that user audits are performed as required.
- Alignment of partner organizations to business structure.

OpenText Core Secure Access includes a comprehensive delegated administration model that creates visibility into thousands of third-party organizations by tasking external organizations to manage their own user access to authorized enterprise resources. Delegated administrators (e.g., suppliers) have the best knowledge of "who should have access to what" and which users no longer need access. This provides enterprises with a continuous monitoring function for third-party access that operates at effectively zero cost.

The deploying enterprise is the top-tier organization within the realm, ensuring ultimate control and oversight of all suppliers, partners, customers and other third parties given access to enterprise systems (see Figure 6). However, day-to-day user administration, help desk support, access certifications and other functions are delegated to administrators, managers, data owners and others in each third-party partner organization. Multiple roles are provided that determine the activities each delegated administrator may perform.

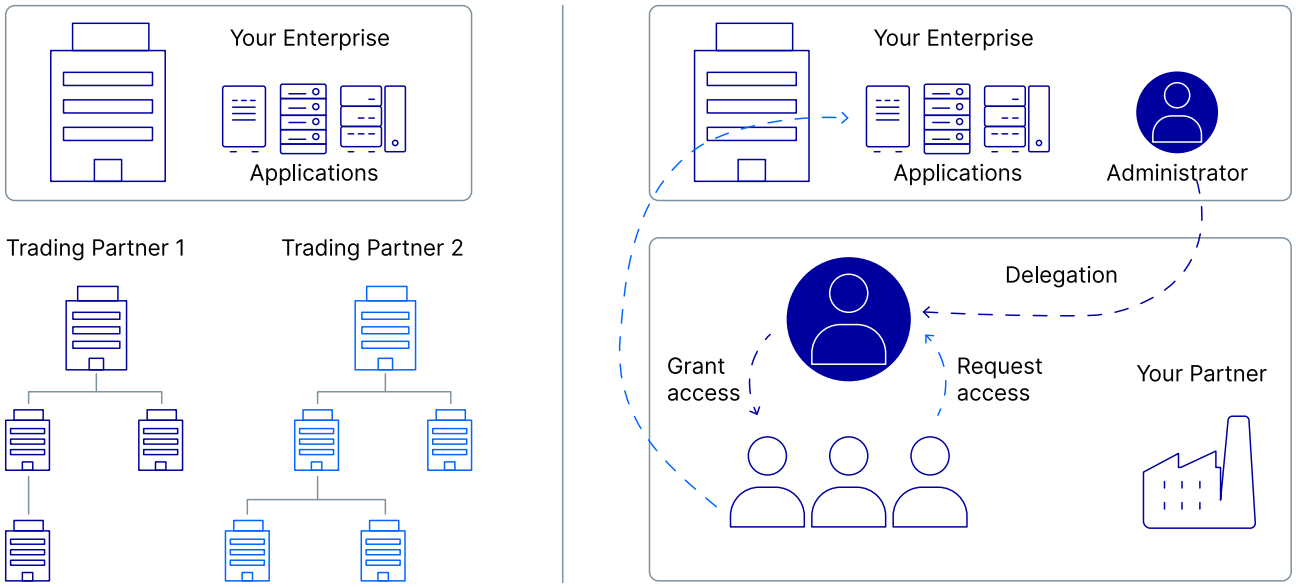

Figure 6. OpenText Core Secure Acess Delegated Administration Model

The delegated administration model establishes automated, repeatable processes for managing the organization hierarchy, user access and requests, support, governance and other functions. For example:

- Invite new users and administrators.
- Update external organization information (e.g., change location, change parent).
- Request access.
- Approve requests.
- Assign administrative roles.
- [Re]certify roles and user authorizations.
- Manage authorizations.
- Manage profiles.
- Reset passwords.

Note: Delegated administration is used in many other OpenText Core Secure Access and Internet of Things contexts, such as the connected vehicle use case where the vehicle owner may remove a secondary driver's permission to request a vehicle function.

Detect and absorb change: Hierarchy management and synchronization

Organizations constantly change: new shipping locations, labor disputes, organizational restructuring, sell-offs, acquisitions, personnel changes and other events. If undetected, such changes can result in operations disruption, security incidents and other unwanted outcomes caused by out-of-sync partner or supplier data.

OpenText Core Secure Access automatically monitors master vendor data to detect discrepancies and take the appropriate action. Customers may set the solution to automatically reapply access policies based on the new master data and modify access as needed, or alert the appropriate staff member who can then use predetermined workflows to make any necessary user moves, code grant changes or other authorized operations as allowed (see Figure 7).

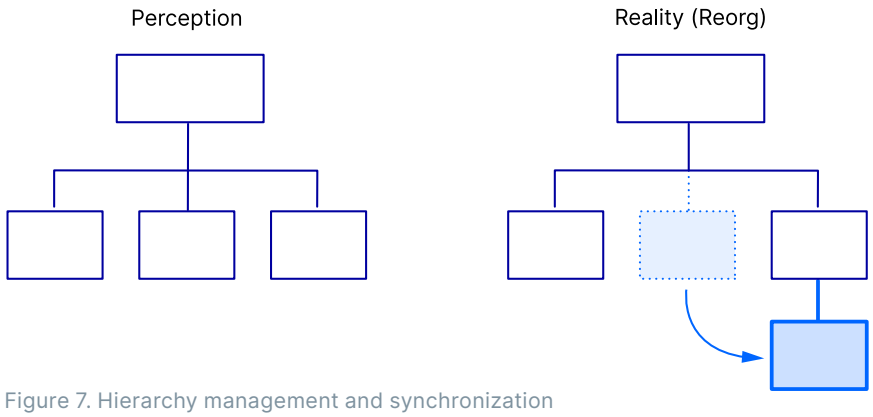

Figure 7. Hierarchy management and synchronization

This critical capability increases the health and predictability of value chains by enabling OpenText customers to:

- Quickly respond to organizational changes in value chain partners.
- Scale identity and access management for thousands of third-party organizations and millions of users.
- Eliminate thousands of menial tasks to update partner and supplier data.
- Always be using the most current partner and supplier information.

OpenText Core Secure Access as a Service

OpenText Core Secure Access is a purpose-built Platform as a Service solution that enables secure, efficient engagement and collaboration across large third-party ecosystems—at scale (see Figure 8). The platform is comprised of cloud-native technologies, built-in security frameworks and digital processes to scale third-party access in a non-linear fashion.

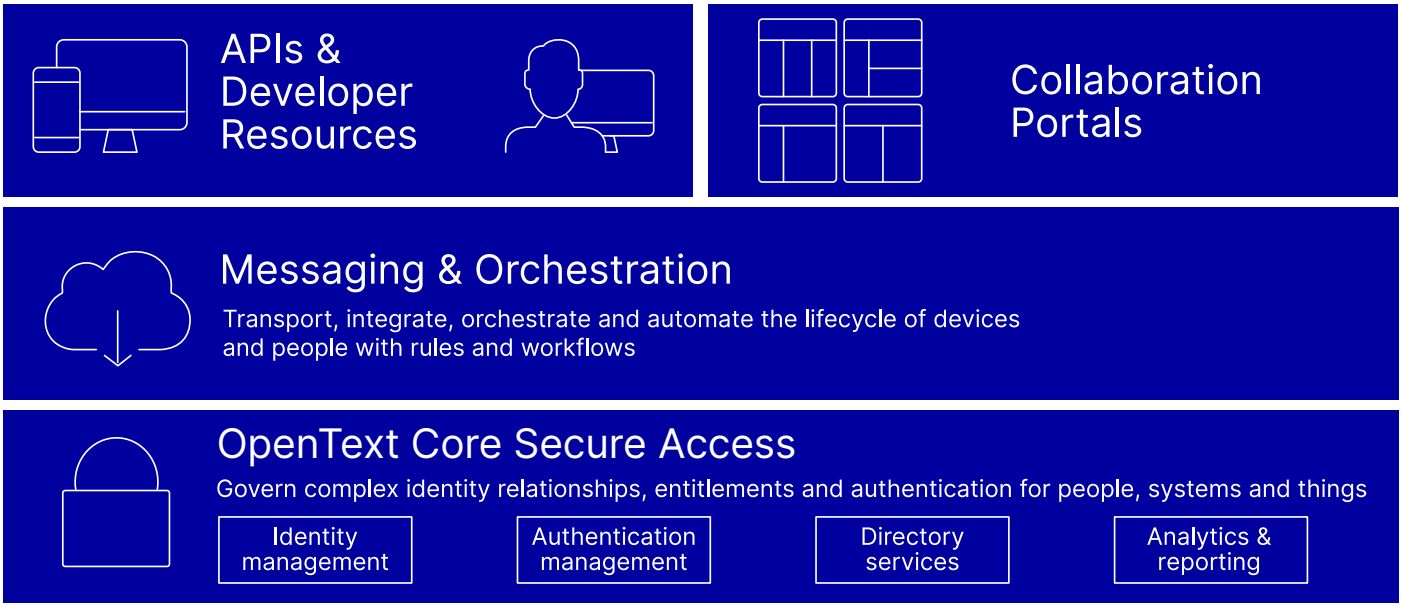

Figure 8. OpenText Core Secure Access as a Service

Identity and Access Management
OpenText Core Secure Access delivers a comprehensive platform of capabilities spanning access management, provisioning, identity governance and administration, identity brokering, verification and other areas to secure remote and third-party access to enterprise on-premises and cloud systems.

OpenText Core Secure Access Admin
A self-service administration and configuration experience makes it easy to create, grow and manage digital ecosystems without costly professional services. Enterprises can reduce time and talent requirements to add new systems, organizations and users to ecosystems, while enforcing zero-trust principles across any-sized value chain.

Learn more:

Solution overview: OpenText Core Secure Access ›

Product Page: OpenText Core Secure Access ›

Explainer video: How to Secure Third Party IAM ›

Blog: Addressing cyber resilience gaps across key infrastructure assets ›

Product overview: OpenText™ Core Collaboration Access ›

APIs & Developer Resources
OpenText APIs and developer tools accelerate new solution and application development while increasing security. OpenText enables enterprises to create frameworks for managing the complex relationships between identities and critical business resources.

Collaboration Portals
Portals enable secure and efficient multi-enterprise collaboration. OpenText Portals include intelligent, flexible capabilities to increase value chain speed and output while driving-down the cost and delays inherent to collaborative work processes, such as P2P, O2C, WIP and others.

Messaging & Orchestration
Enterprises can facilitate automated, event-driven identity lifecycle management throughout the ecosystem. Systems and applications subscribe to a stream of event-based messages triggered by actions within OpenText Core Secure Access (e.g., create user, update profile, grant service package, update user lifecycle status), then take the appropriate action. OpenText enables enterprises to connect any external user to any enterprise system.

Conclusion

OpenText Core Secure Access front ends most every digital product, service and business process. As enterprises widen their digital focus beyond internal efficiencies to increase growth and create value, mainstream OpenText Core Secure Access solutions become the limiting factor: time to value, scalability, cost, ability to integrate with unknown systems and many others.

OpenText Core Secure Access secures access and risk for some of the world's largest value chains, distribution networks and customer ecosystems. Our cloud service connects more than 30 million suppliers, customers, partners, vendors and other third parties to on-premises and cloud information systems—at scale. OpenText's proven technology and 30 years of innovation in identity and multi-enterprise collaboration create visibility into third-party organizations to simplify and automate IAM and governance across complex ecosystems.

opentext™