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 #1 source of data breach: “trusted” third-parties.

opentext™

Contents

opentext™

Executive Summary

Digital initiatives are accelerating at record pace. Traditional value chains look to transform into highly-connected Partner and Supplier ecosystems to increase predictability and efficiency. Financial services companies reimage operating models to get closer to customers through networks of external agents and brokers. Digital product and service providers look to create new value by incorporating partner services into offerings. For these and other digital strategies, success hinges on the ability to securely connect partners, suppliers, customers and other third-parties with your enterprise's digital business processes.

While brilliant on paper, these digital strategies often become side-tracked when trying to secure and scale access for third-parties. Turns out that the vast majority of identity and access management (IAM) products that automate access control and enforcement do so for employees – not third-parties. When such solutions are used to underpin complex, multi-enterprise use cases, delays, additional cost, and concessions quickly ensue.

This white paper describes the complexities and challenges of securing third-party access, details critical capabilities to mange third-party access at scale, and 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, substantially as a way 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 reduce risk of disruption. (see Figure 1).

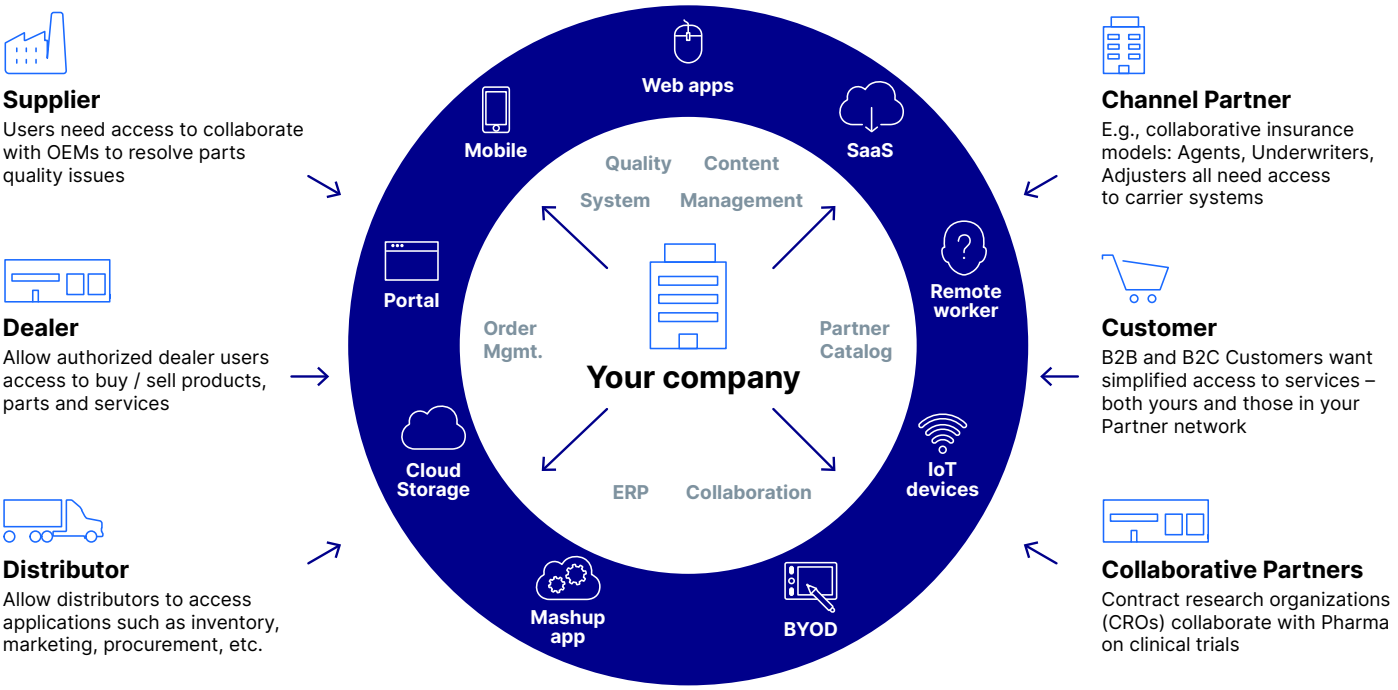

Figure 1. The Collaborative Ecosystem

As value chains expand, digital assets and resources previously accessible only to employees now need to be equally available to an ever-changing group of suppliers, partners, distributors, logistics providers, and other third-party partners. However, each integration or access grant represents a potential point of access for unauthorized users looking to exploit security flaws. Historically, enterprises institute ad hoc 1:1 connections to manage third-party identities. However, the individual, point-to-point integrations result in each new supplier endpoint representing an exponential increase in the threat surface and exposure to risks such as orphaned or easily-compromised accounts, or data integrations with little or no identity or access management controls (see Figure 2).

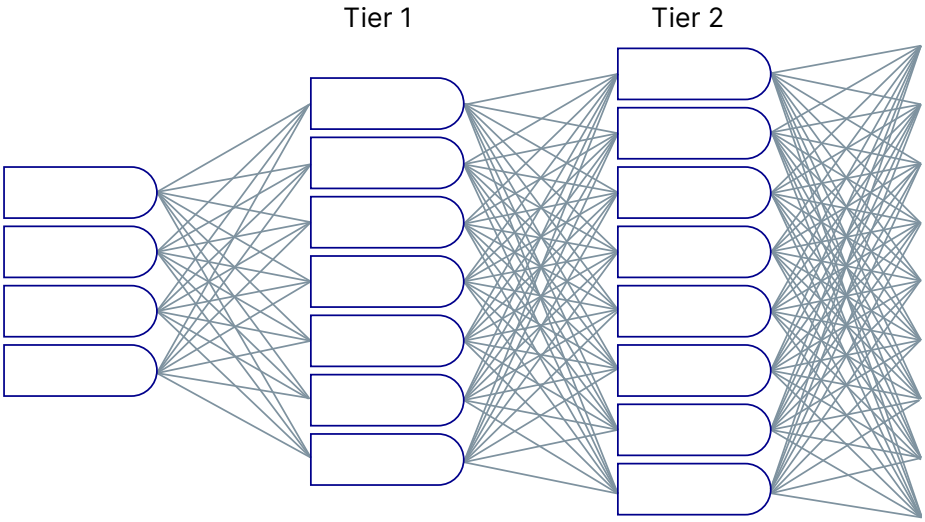

Figure 2. High degree of complexity with multi-tiered partner and user relationships

The current state of third-party access is far from ideal (see Figure 3). The increasing number of third-parties with access to back-end systems, yet without centralized identity management or governance, has led to significant risk and cost.

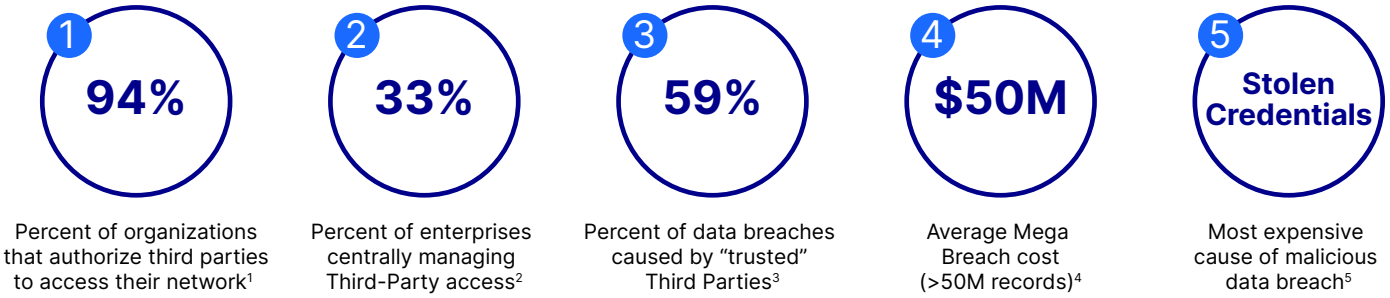

Figure 3: Current state of third-party access

Based on these statistics, opportunities await those able to implement effective controls to overcome these 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. But without effective controls in place to mitigate third-party risk, such initiatives will only accelerate the path to breach:

- Ecosystems will account for 30 percent of global revenues by 2025[6]
- 93% of supply chains are adding new sources and regions[7]
- "Next Gen" [digitally transformed] operating models are expected to increase growth by 20 to 25 percent[8]
- Third-parties include increasing number of startups and business model innovators over incumbent service providers[9]

1 Dimensional Research. Third-Party Access and Compromise. 2020
2 Salesforce. 2019
3 Ponemon Institute. Cost of Data Breach Report. 2020
4 Ponemon Institute. Cost of Data Breach Report. 2020
5 Ponemon Institute. Costs and Consequences of Gaps in Vulnerability Response. 2020
6 McKinsey. Insurance beyond digital: The rise of ecosystems and platforms. 2018
7 McKinsey. Risk, resilience, and rebalancing in global value chains. 2020
8 McKinsey. Turbocharging the next-generation operating model. 2019
9 Gartner. Staying Ahead of Growing Third-Party Risk. 2019

opentext™

Identity and access management defined

Identity and access management (IAM) is a technology that automates alignment of user 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 4, below:

Who has access to what, why, who approved it, and is it still needed?

- Identity (authenticated)
- Authorization
- Resource authorizations (aka):
  - Entitlements
  - Permissions
  - Access rights
  - Role (resource)
- Role/Rule
- Certifier/Sponsor
- Governance, e.g.,
  - Access certification
  - Attestation

Figure 4. 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 before it can be granted, 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, leaves the company and thousands of other events. The end-to-end process of managing identity and access for joiners, movers and leavers is called identity lifecycle management (ILM). Figure 5 below depicts the three identity lifecycle phases and provides sample events that normally trigger IAM processes.

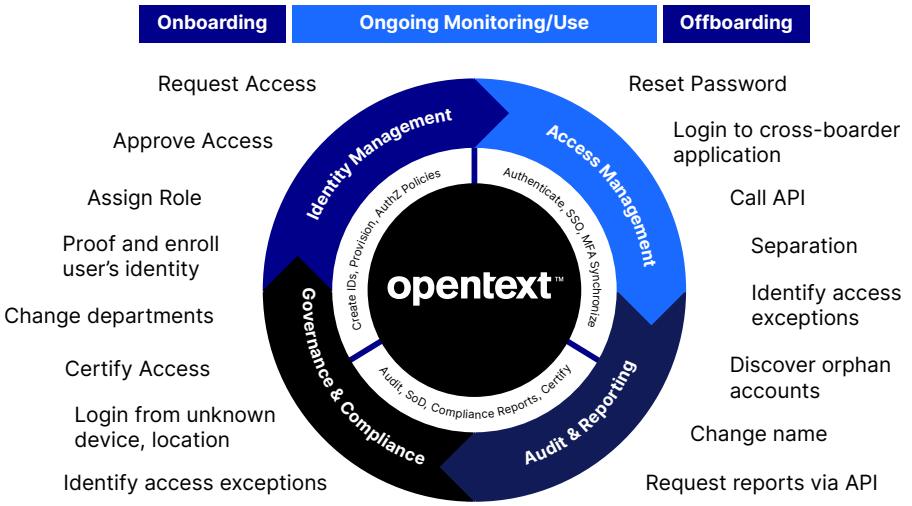

Figure 5. Identity Lifecycle Management

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 (connectors) and can be delivered as a cloud service (IDaaS). However, the primary use case remains the same – securing employee access to on-premises and cloud resources.

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

Organizations that first consider using their existing enterprise IAM investment to manage third-party users quickly realize that the assumed levels of automation, security and compliance are out of reach due to the solution's reliance on enterprise infrastructure and processes (see Figure 6).

opentext™

Infrastructure or Practice	How leveraged by Enterprise IAM: Managing Employees	How leveraged byEnterprise IAM: Managing Third Parties
Identity Proofing	• Establish Trust • Background checks • In-person verification	• Not available • No visibility into Third-party users organizations to verify user's true identity
System of Record	• Curated HR System • Accurate, verified version of truth • Single version of truth	• Unavailable • Supplier/self-provided information • Multiple versions of truth • Identities stored in LOB apps, spreadsheets
Corporate Hierarchy	• Reliable framework to facilitate assignment of roles to users • Increases automation • Consistent policy application • 360-degree view of access and risk	• Not available • Increases manual administration • Inconsistent policy application: User management siloed by department or LOB application. • Identity silos prevent understanding a user's aggregate picture of risk
Mobile Devices	• Company-issued devices • Standardized security • Monitored	• Assume all devices are BYOD
Origin of Access	• Access typically originates inside firewall	• All access is "remote"

Figure 6: Employee-centric IAM: suitability for managing Third-Party users

IAM solutions for the extended enterprise 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
- 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

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

OpenText IAM provides innovative solutions to simplify and standardize how your enterprise manages access across large third-party ecosystems. Below are a few OpenText IAM innovations that demonstrate our leadership in this space.

Entity Relationship Management

OpenText IAM creates a unique digital identity for every person, system and thing ("entity") it manages. Our Unified Data Model is a canonical representation of identity information for each entity type. The unified data model 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 efficient and secure method for controlling access across large ecosystems (see Figure 7).

Figure 7: Entity Relationship Management Model

The "Extended" Enterprise Directory

The OpenText IAM platform can act as the system of record for all the external organizations and users connecting to your enterprise – providing a Single Source of Truth for third-parties.

Analysts agree that managing third-party identities in the enterprise directory is 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."

10 World Food Programme. Internal Audit of Third-Party Access to WFP Data and Systems. 2020

OpenText IAM easily integrates 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 – eliminate disjointed experiences
- operationalize third-party risk management (TPRM) strategies by aligning OpenText IAM 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 IAM 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 IAM leverages this same construct to represent a logical view of an organization's hierarchy. The platform enables delegated administrators to create and maintain a "digital twin" of the parts of their organization that require access to your enterprise – all without involving your enterprise administrators. Organizational hierarchy also provides a means to detect organizational changes in third-party organizations: see Hierarchy Management & Synchronization, discussed later.

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 IAM tools and manual processes. Additionally, the lack of visibility into the comings and goings of personnel at third-party organizations create 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 of your partner organizations
- 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 your business structure

OpenText IAM includes a comprehensive delegated administration model that creates visibility into third-party organizations and enables 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 your enterprise with a continuous monitoring function for third-party access that operates at effectively zero-cost.

Your enterprise is the top-tier organization within the realm, ensuring you have ultimate control and oversight of all suppliers, partners, customers and other third-parties you authorize to access enterprise systems (see Figure 8). However, day-to-day user administration, help desk support, access certifications and other functions are delegated to administrators, managers, data owners, and others in your third-party partner organization. Multiple roles are provided that determine the activities each delegated administrator may perform.

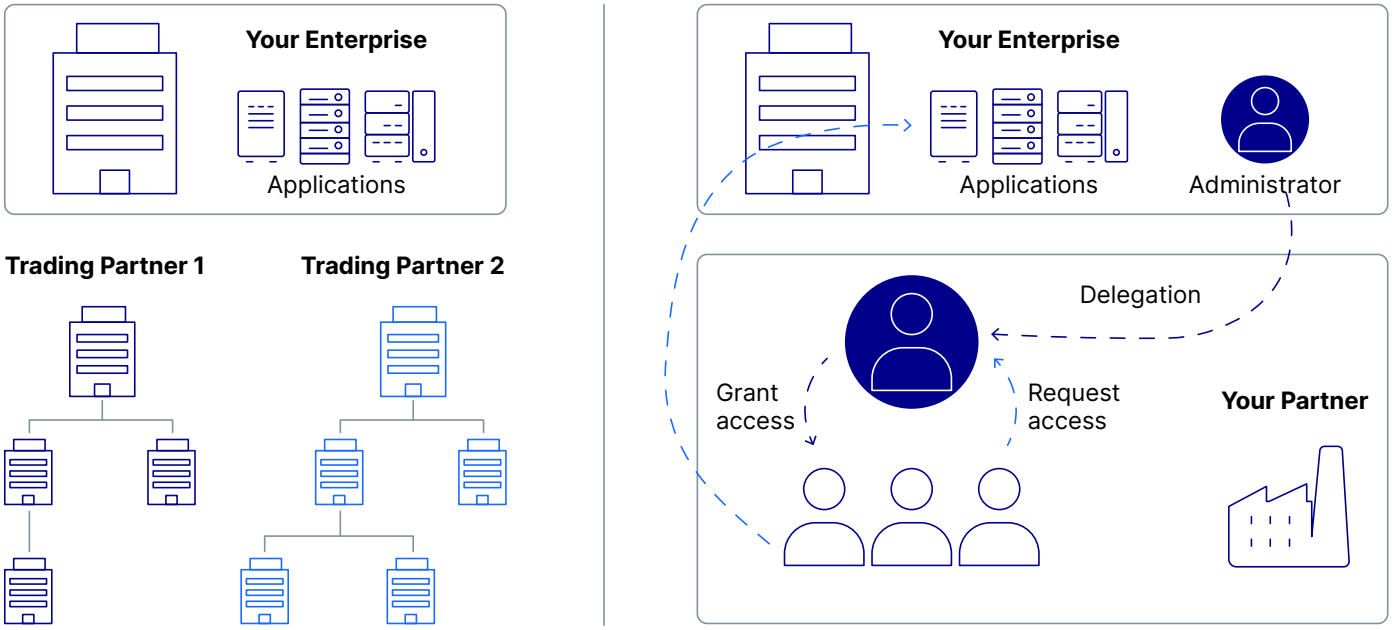

Figure 8. OpenText IAM Delegated Administration Model

The delegated administration model establishes automated, repeatable processes for managing the organization hierarchy, user access & 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
- and others

Note: delegated administration is used in many other OpenText IAM and IoT contexts, such as the connected vehicle use case where the vehicle owner may remove a secondary driver's permission to request a vehicle function.

opentext™

Hierarchy Management & Synchronization

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

OpenText IAM can automatically monitor master vendor data to detect discrepancies in the logical organization being maintained by your partners. Any discrepancies automatically trigger notifications to the partner's appropriate delegated administrator who can then use predetermined workflows to make any necessary user moves, code grant changes or other authorized operations as allowed (see Figure 9).

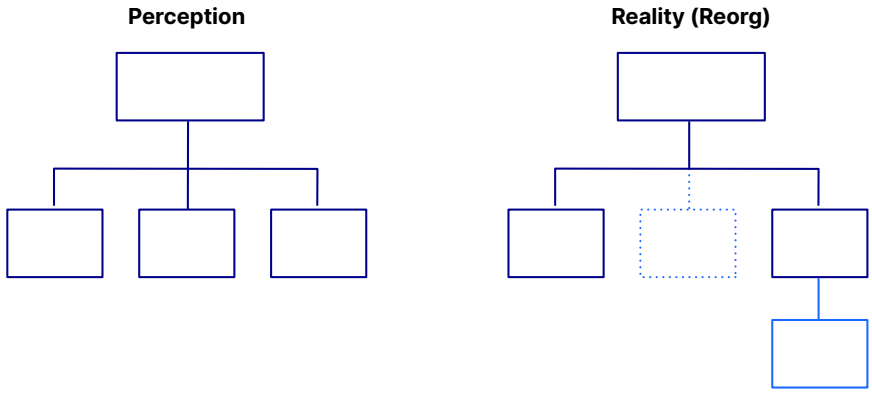

Figure 9. Hierarchy Management & Synchronization

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™

OpenText IAM Platform as a Service

OpenText™ Identity and Access Management (IAM) 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 10). 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.

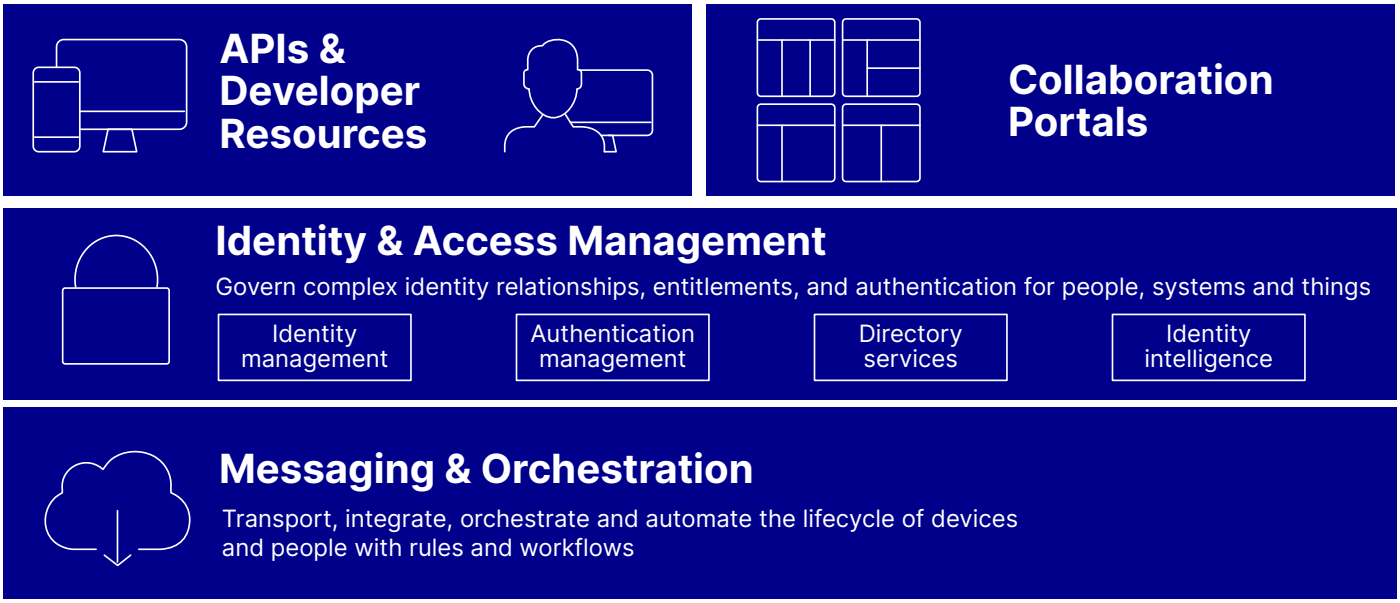

Figure 10. OpenText IAM Platform as a Service

Identity and Access Management. 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.

APIs & Developer Resources. OpenText APIs and developer tools accelerate new solution and application development while increasing security. OpenText IAM 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. 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 the OpenText IAM platform (e.g., create user, update profile, grant service package, update user lifecycle status), then take the appropriate action. Connect any external user to any enterprise system.

opentext™

- OpenText IAM
- Customer IAM
- Supplier IAM
- Supplier Portal Solutions
- Product overview
- IAM Blogs

Conclusion

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

OpenText IAM secures access and risk for some of the world's largest value chains, distribution networks and customer ecosystems. Our cloud service connects over 30 million suppliers, customers, partners, vendors and other third-parties to on-premises and cloud information systems – at scale. Our proven technology and 20 years of innovation in identity and multi-enterprise collaboration create visibility into third-party organizations to achieve the same levels of automation and security as employee IAM solutions, yet at far less cost and complexity.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact