

POSITION PAPER

Another portal? What's in it for me?

Why a single-portal infrastructure improves partner and customer engagement and adoption

The proliferation of portals within an enterprise has exceeded acceptable levels of inconvenience and cost for the communities they serve, including suppliers, partners and B2B customers. Portals have become a standard practice to reduce value chain support and administrative costs, but without delivering material value. Partners and customers are pushing back asking—what's in it for me? This position paper examines the cost and business benefits of implementing a single enterprise portal infrastructure.



Contents

Executive summary	3
Connected and collaborative digital ecosystems	3
Enterprise portal infrastructure vs. platform portals	4
Benefits of an enterprise single-portal infrastructure	5
Reduce cost and effort of global partner management	6
Harness collaboration to drive innovation	7
Simplify and strengthen global ecosystem security	9
The Automotive Exchange	10
Digital workflows: Streamline, automate and extend	11
Key features of the infrastructure include:	11
The power of OpenText Active Access	13
OpenText Active Access: At a glance	14

“Since most organizations will have multiple portals, one must decide if a single-portal infrastructure will be appropriate for all portals.”

Forrester

Executive summary

In terms of trading partner management and collaboration, the benefits of implementing portals are clear. A portal provides an integrated online platform shared by organizations and their partners to help streamline processes, share information, improve payment cycles and facilitate improved communication and engagement.

The number of portals within an enterprise continues to rise each year, with most portals being specific to a platform or business workflow. Such portals create headaches for collaborative partners and B2B customers. Users frequently find that they must log in and out of multiple siloed portals to complete a single task. So, it's not surprising that Gartner reports that 43 percent of partners claim that customer systems impede their productivity.¹

Portal fatigue has led Forrester to an insightful observation, “Since most organizations will have multiple portals, one must decide if a single-portal infrastructure will be appropriate for all portals.”²

This paper examines the unique benefits of a single-portal infrastructure, which cannot be achieved within a multi-portal environment.

Connected and collaborative digital ecosystems

The COVID-19 pandemic illustrated the fragility of global supply chains. Research suggests that 93 percent of organizations are looking to build resilience and agility in their supply chains by adding new suppliers in new regions, and even building entirely new supplier communities to explore new business models.³

At the same time, supply chains and other value chains continue to evolve from linear, physical instances to multi-layer digital ecosystems of suppliers, customers and partners. Organizations are seeking to extend their enterprises to leverage external partners to control costs, target better, sell faster and innovate more effectively.

This requires an unprecedented level of connectivity and collaboration across the extended enterprise. Today, 94 percent of enterprises authorize third parties to access their back-end resources.⁴ However, connecting and sharing information with large partner communities is far from an easy exercise. It requires dealing with any number of separate systems and portals and breaking down process, application and information silos.

According to Supply Chain Brain, the industry is moving towards Supply Chain as a Service (SCaaS), which it describes as “an innovative approach that allows companies to generate a four-to-five-times return on investment by partnering with one service partner to support all or part of their supply chain needs, including procurement, production control, manufacturing, quality, warehousing and logistics.”⁵

A single-portal infrastructure is an excellent example of the SCaaS approach. It delivers an enterprise-wide capability that allows for the creation of portals and communities that overcome the major drawbacks of the fragmented platform-driven portal method.

1 Gartner, Supply chain cybersecurity

2 Forrester, Forrester Glossary. (Updated 2022)

3 Alicke, Knut, Gupta, Richa et al. Resetting supply chains for the next normal. McKinsey & Company (2020)

4 One Identity, 2019 State of Identity and Access Management. (2019)

5 Bastin, Gerald, Five Supply Chain Trends to Expect in 2022. Supply Chain Brain. (2021)

“94% of enterprises authorize third parties to access their back-end resources.”

Dimensional Research

“93 percent of breaches originate from a weakness in their supply chains or third-party ecosystems.”

BlueVoyant

Chief amongst these drawbacks is security. Each portal adds more network endpoints that increase the surface area for attack, while a single-portal infrastructure can limit the number of entry points to one. Organizations report that 93 percent of breaches originate from a weakness in their supply chains or third-party ecosystems.⁶

Increasingly, the threat from third-party access is putting CxO jobs at risk. Gartner estimates that as many as 50 percent of CEOs who lack defensible cybersecurity postures will be fired following material breach incidents that impact more than 25 percent of their customer base.⁷ A single-portal infrastructure simplifies and strengthens supplier identity and access management for fast and secure collaboration around information across the extended enterprise.

Enterprise portal infrastructure vs. platform portals

As a community of global partners grows, managing partner process manually leaves room for error, adds delays to the process and makes it difficult to deliver an excellent experience. An intelligent portal solution can automate processes and workflows, improve communication and information sharing and drive supplier management and performance.

However, the buyer and supplier businesses soon find that working with multiple portals is not an ideal scenario. Platform-specific portals are limited to applications and services for a given vendor or platform.

Each of these portals has its own set of tools that are only available to users of that portal. This quickly leads to redundant tools and administrative costs, as well as inconsistent processes for security, onboarding and management and information sharing. Collaboration tools can be limited and not fit for partner communication and engagement.

Line-of-business (LOB) managers are often the primary purchasers of these portals—focusing on the needs of the vertical function rather than a cross-enterprise or end-to-end process. As other LOB purchasers do the same, a series of silos form, and often, it will take various customer portals to perform even a simple activity such as invoice processing. The result is that each business function has its own set of portals distinct and separate from other functions. (See Figure 1)

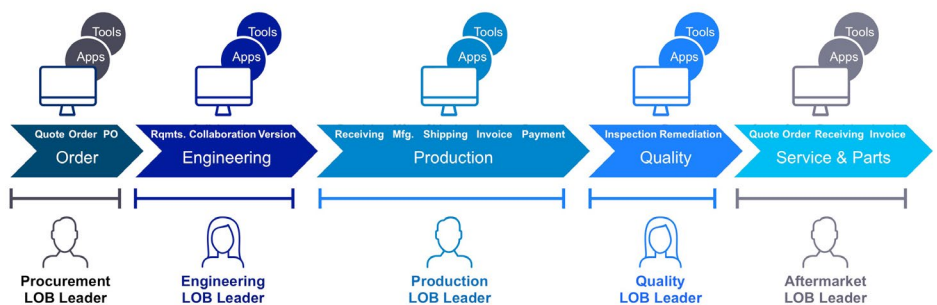


Figure 1: Line-of-business portals create information silos and user frustration

⁶ BlueVoyant. Managing Cyber Risk Across the Extended Vendor Ecosystem. (2021)

⁷ Gartner, 8 Reasons More CEOs Will Be Fired Over Cybersecurity Incidents. (2019)



This fragmented approach decreases the value of collaborative processes by creating silos that hide information, decrease user productivity, increase cost and frustrate users.

A single-portal infrastructure allows an organization to use a single portal technology, providing all communities—both internal and external—with a common set of collaboration tools that expand beyond a specific platform or business processes and support cross-functional processes.

Portals that provide process automation and workflow capabilities streamline information access and cross functional processes by quickly connecting people to needed information. Routine tasks can be automated, driving efficiency, accelerating processes and increasing enterprise visibility while reducing costs. In addition, reporting and analytics on partner and security data is available at the enterprise level to reduce risk and strengthen compliance.

Benefits of an enterprise single-portal infrastructure

Partner relationship management

Automate and simplify supplier management throughout the entire lifecycle, from onboarding to offboarding.

Partner engagement

Increase the value of every trading partner by improving communication and access to information and documentation to drive engagement and productivity.

Collaboration

Enable cross-functional and cross-application processes that improve information sharing and automate key tasks and workflows to facilitate collaboration between all parties in the supply chain.

Security at scale

Drive down the cost and risk of managing external users connecting to an enterprise through advanced identity and access management, including realtime monitoring and dynamic authorization provisioning.

Personalized experiences

Identity-driven security delivers tailored and relevant experiences for each portal user across devices.

“Supply chain managers are currently troubled by a lack of visibility throughout their extended supply chains, as there are so many nodes and participants within the extended chain. Leading organizations are using advanced technologies to significantly improve visibility and thereby become far more responsive to major disruption and variability within their domestic, regional and global supply chains.”⁸

KPMG

Reduce cost and effort of global partner management

A single-portal infrastructure facilitates partner management from an enterprise perspective. As the “front door” to the enterprise for all user communities, a single portal solution can become the “extended” enterprise directory, maintaining all trading partner user and organization profiles and providing a single source of truth. It also facilitates onboarding new partners by streamlining registration, qualification and enrollment. Workflow-driven digital processes accelerate trading partner time-to-value and eliminates thousands of hours spent on inefficient onboarding and monitoring activities.

All ecosystem users managed by the portal have access to a common set of services and tools for use across the entire ecosystem to avoid redundant administration and inconsistent or siloed processes and provide the following benefits:

Minimize the administrative burden of partner user management

A single-portal infrastructure centralizes control of all core operations and security policies for all users and organizations connecting to the enterprise. However, day-to-day user administration can be distributed to each partner to improve security and avoid costs, providing “eyes on the ground” to continuously monitor partner users, modify access as users come and go and recertify access per buyer’s governance schedule.

Onboard new trading partners quickly and efficiently

Organizations can remove manual onboarding processes and regain thousands of hours spent on inefficient onboarding and monitoring activities. Self-service, workflow-driven processes streamline registration, qualification and enrollment to accelerate trading partner time-to-value.

Standardize digital processes across the partner lifecycle

A single-portal infrastructure increases efficiency and drives predictable outcomes with consistent and automated digital processes for partner onboarding, ongoing change, offboarding, access request and approvals, authorization management, authentication management, access certification and more.

Enable self-service user administration

By providing self-service capabilities to trading partners, an organization can significantly reduce internal cost and resource requirements while improving the quality of data held on its trading partners. Partners can handle many of the user management functions to ensure that all business and product data is valid and correct. Self-service access speeds procurement, work-in-progress and payment processes.

Simplify security and access management

A single identity and access management platform spanning all ecosystem users and enterprise systems dramatically reduces the amount of administration. Users are provided with a single digital identity to control access to any authorized system within the ecosystem after a single login. Policy management and administration is centralized, facilitating effective authorization and authentication and ensuring authorization is withdrawn immediately to reduce the risk of ghost accounts.

⁸ KPMG, Six key trends impacting global supply chains in 2022.

Automatically detect and react to organizational change

Undetected changes in master supplier and vendor data can send operations sideways—delayed delivery, unnecessary cost and increased risk of a data breach from unauthorized access. Using a single-portal infrastructure, such as OpenText™ Active Access, allows an organization to automatically monitor master vendor data to detect discrepancies and take the appropriate action. An organization can automatically re-apply access policies to align access with master data updates or notify the internal stakeholder(s) along with a list of pre-defined workflows to make any necessary changes. The organization can use its portal capabilities to ensure a single source of the truth for master data where appropriate.

Gain enterprise visibility and insight

Organizations gain visibility into supplier activities to help improve supplier performance and decision-making. Transparency of data across the enterprise breaks down process and information silos to feed analytics systems, which creates business insight and agility.

While platform-driven portals create friction and cost, a single-portal infrastructure centralizes administration and leverages suppliers to work collaboratively and reduce expense to the enterprise.

Harness collaboration to drive innovation

Collaboration across the extended enterprise of trading partners, suppliers and customers is a pivotal element of business today. McKinsey reports that companies that regularly collaborate with suppliers demonstrate higher growth, lower operating costs and greater profitability than their industry peers.⁹

However, collaboration efficiency is eroded by platform-specific portals that create information silos, duplicate administration costs and lack cross-functional collaboration. To generate value from changes in manufacturing methods, quality-assurance regimes or supply-chain processes, representatives from the respective functions on both sides of the partnership need to work together through seamless communications and information sharing.

Cross-functional, cross-application collaborative processes require that suppliers and other trading partners be continuously engaged, informed and productive. A single-portal infrastructure delivers advanced collaboration capabilities including:

Increasing supplier adoption

Suppliers can be deterred by the complexity, effort and digital nature of portals. With simplified and streamlined onboarding and single sign-on access to all needed resources, organizations lower the barrier to entry and make it easier for suppliers to connect and start collaborating.

⁹ Gutierrez, Agustin, Kothari, Ashish et al. Taking supplier collaboration to the next level. McKinsey & Company. (2020)

"Companies that regularly collaborate with suppliers demonstrate higher growth, lower operating costs and greater profitability than their industry peers."

McKinsey

Improving margins and productivity

Organizations can easily create portals that span business processes and communities. The supplier has a single place to go for all content and communications—with a single security credential for all resources. Users can quickly surface the information they need and complete key tasks, such as identifying RFTs, checking inventory levels or submitting invoices. The organization can monitor all supplier activity as a basis for supplier performance management.

Personalizing user experience

Organizations can customize content by user type, leveraging integrated identity and access management, attribute-based security and alerts and notifications. The portal personalizes the user experience and access based on the user's authorizations and accelerates collaborative work processes. The organization can easily create identity-driven journeys to dynamically expose capabilities, choices and information based on the user's authorizations, profile, preferences and relationships.

Enhance content management

The portal can integrate content and document management with social collaboration, page creation and collaboration tools. Advanced search functionality allows content to be easily and securely retrieved and shared across functions and with external partners. For some portal solutions, such as Active Access, realtime alerts and notifications keep trading partners informed on new or updated content, published bulletins, exceptions, community messaging and other critical information.

Connect the right trading partners with the right information.

With a single portal infrastructure, organizations can quickly publish bulletins and other communications to highly-targeted recipients. They can identify suppliers based on granular recipient information, such as location, manufacturing, performance or quality data and deliver realtime communications and alerts to the recipient's device of choice. The most advanced portal solutions provide omnichannel communications and personalized security to enable a bi-directional flow of information to increase collaboration and trust.

Simplify and strengthen global ecosystem security

According to a recent survey, 79 percent of organizations have formal programs in place to manage third-party risk but only 14 percent are highly confident that suppliers are meeting their security requirements.¹⁰ Platform-specific portals create a range of security inconsistencies with manual user administration across thousands of external users who each have multiple user IDs and passwords.

This approach is expensive and virtually impossible to scale. It also results in each new supplier endpoint representing an exponential increase in the threat surface. The organization is exposed to risks such as ghost, orphaned or easily compromised accounts, or data integrations and application access with little or no identity or access management controls.

A single-portal infrastructure leverages a single security and identity and access management (IAM) platform to secure all users, systems, operational technologies and devices. It allows administrators to automate and control identity for individual users, specific groups and entire communities throughout its lifecycle.

The business benefits from the ability to quickly create identity-driven journeys that dynamically expose capabilities, choices and information based on the user's authorizations, profile, preferences and relationships. The user benefits from a single point of access, with one set of credentials, to access all authorized resources. Vitally, the attack surface is reduced from potentially hundreds of thousands of endpoints to one.

Deploying a single-portal infrastructure, such as Active Access, delivers secure access at scale for large ecosystems of suppliers, partners and other third parties, based around the following capabilities:

Identity management

An organization can manage identities and authorizations for the millions of people, systems and things accessing its enterprise using an innovative and scalable solution, far beyond what platform-specific portals provide.

OpenText™ Identity and Access Management (IAM) is the security platform for Active Access. Securing B2B user access to enterprise resources for nearly 20 years, OpenText IAM uses a distributed model that centralizes control of the “keys to the kingdom”—authorization and authentication policies, approval and provisioning workflows and access governance—but decentralizes control of identity administration activities to those who best know “who needs access to what, why and if it’s still needed.” This model improves security decisions and avoids massive costs by enabling partner administrators to perform day-to-day activities, such as adding and removing users, updating user access (request, add, modify, revoke), resetting passwords, and other activities as authorized by the customer.

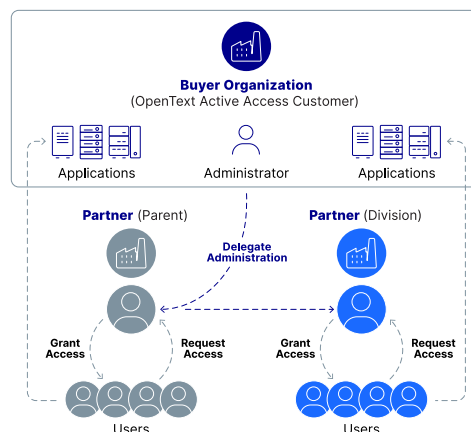


Figure 2: Distributed IAM model improves security decisions while eliminating costs

¹⁰ RiskRecon, The State of Third-Party Risk Management. (2021)

The Automotive Exchange

World's largest automotive manufacturers rely on OpenText

OpenText™ Active Access has roots tracing back to 2000, when the “Big Three” US automakers formed an independent company (Covisint; acquired by OpenText in 2017) that would enable the OEMs to dramatically reduce the cost and administrative overhead of partner-related business processes.

The Covisint Supplier Portal was introduced to enable OEMs and their suppliers to collaborate electronically and securely, providing direct access to the applications that underpin procure-to-pay, quality, engagement and other end-to-end processes.

Today, Active Access is the power behind the Automotive Exchange, connecting more than 125,000 supplier organizations and OEMs.

Access management

Having a 360-degree view of risk posed by every human and non-human login enables organizations to establish the appropriate level of trust and reduce friction. Every person, system and thing authorized to access an enterprise receives a single digital ID that reflects all known accounts, authorizations, relationships, profile data, history and other information. Organizations can leverage this ledger-like capability to improve authentication and authorization decisions that facilitate secure, low-friction experiences; improve risk-based authentication (RBA) scores; dynamically adapt authorization; and scale multi-factor authentication (MFA) trust factors.

Access governance

Delegating access certification to partner administrators improves compliance posture and reduces its related cost and disruption. Designated partner administrators review and attest to the accuracy of users and application entitlements, enabling customer administrators to monitor, certify and audit all trading partner access and synchronize changes across all relevant internal and external systems. Changes made by supplier administrators are quickly surfaced to ensure compliance or activated approval where required.

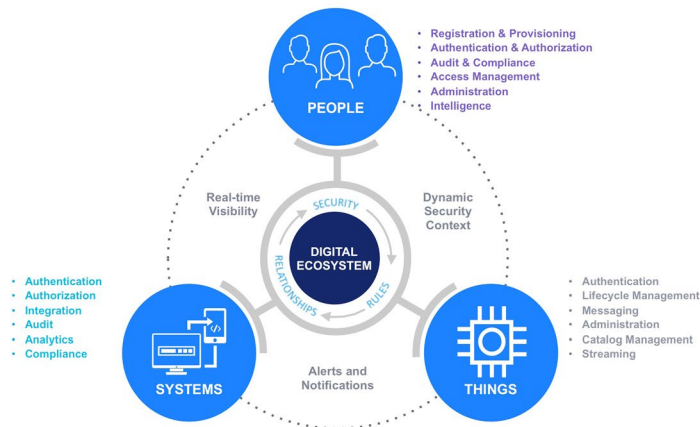
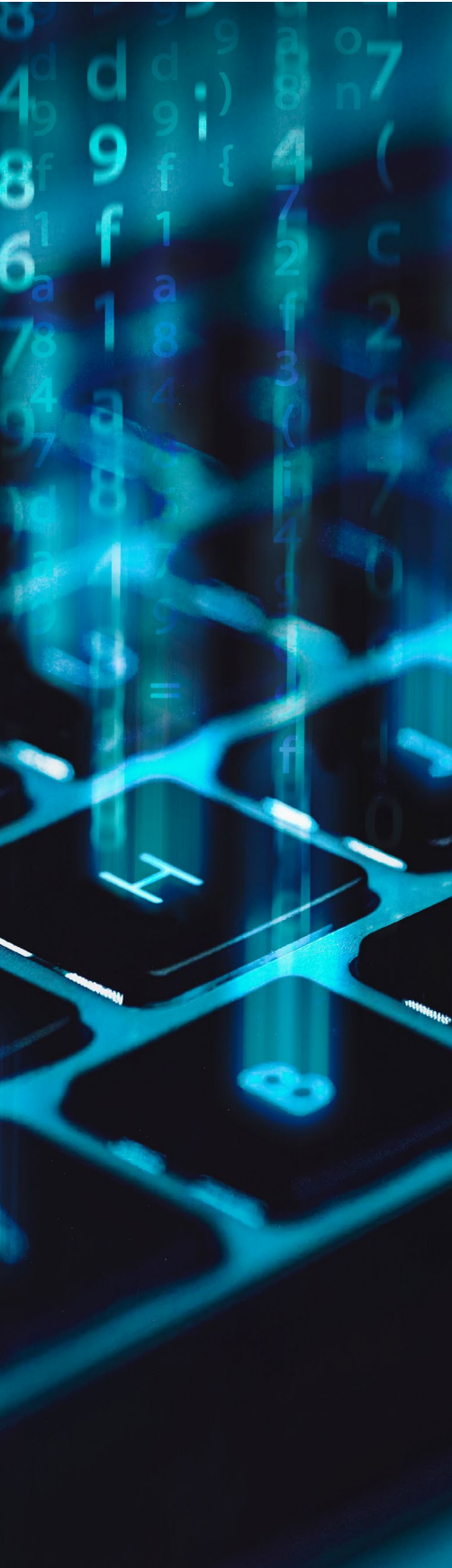


Figure 3: Securing the digital ecosystem of people, systems and things

Digital workflows: Streamline, automate and extend

Delivering secure, multi-enterprise digital processes can be complex and expensive. Platform-driven portals lack enterprise integration, creating silos that reduce productivity and increase risk. For instance, employees and suppliers often improvise collaborative and information-sharing solutions, such as email or file repositories, that are unmanaged and insecure.

A single-portal infrastructure allows an organization to introduce powerful digital processes— and automate existing manual processes—across the extended enterprise to increase the efficiency and effectiveness of working with trading partners. Users receive a highly personalized experience while the new processes encompass all the users, systems and things required to create a fully collaborative business.



Key features of the infrastructure include:

Digital process development

Take an enterprise-wide approach to create new digital processes across disjointed applications and information stores. Organizations can design and deliver cross-application and cross-enterprise workflows that include features such as dashboards, custom web interfaces, forms and governance to speed and simplify operations. New digital services can be created and rolled out incrementally to meet business needs.

Application and device integration

Organizations are not tied to the applications stack of a particular portal but can integrate all back-end business systems and provide access to them. Realtime integration with enterprise systems improves accuracy and speed and eliminates errors when working with enterprise data. The business has the flexibility to choose the best approach for sharing and exchanging information across disparate systems, processes and functions.

Enhanced, cross-cutting workflows

All users can quickly locate documents across information silos. Targeted search allows them to retrieve the documents they need and omnichannel communication allows effective sharing and alerting and notifications when content changes.

Streamlined journeys

Organizations can onboard new trading partners using extreme self-service capabilities that drive down the cost and disruption to register, qualify and enroll partners. This includes digitizing evidence collection, verifying data against authoritative sources and notifying staff when decisions need to be made. Streamlined end-to-end multi-party journeys minimize delays and keep processes moving, such as agent onboarding use cases involving applicants, recruiters and carriers.

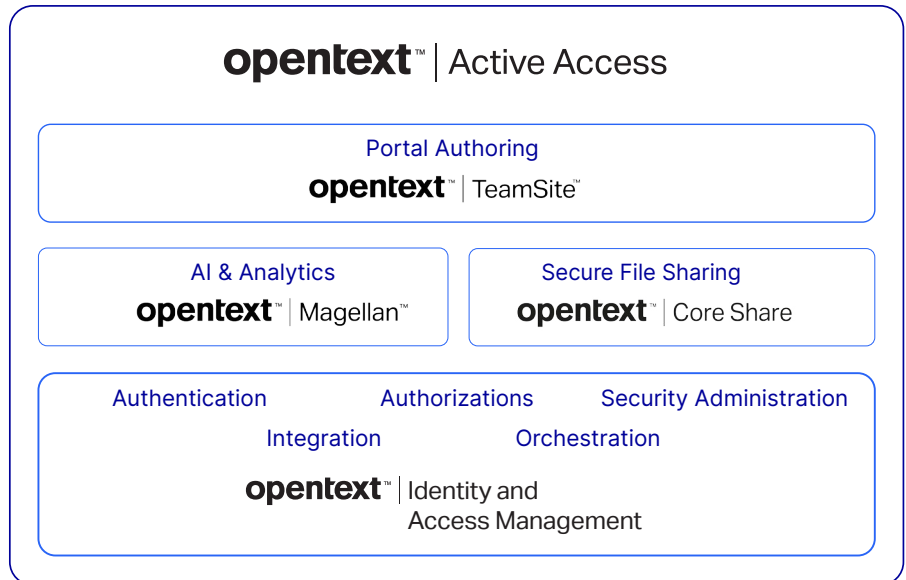
A contemporary architecture to secure business ecosystems

Active Access is built on a cloud-native platform encompassing a contemporary, auto-scaling micro-services architecture with API-first design. The platform simplifies connecting ecosystems across complex, uncertain environments, yet is easily extended to meet the future needs of any value chain.

The digital platform is backed by best-in-class technologies for security, experience, analytics and information access:

- OpenText™ Magellan™: Provide analytics and appealing visualizations, reports and dashboards to deliver insights and information on any device and empower employees, customers and partners to act.
- OpenText™ TeamSite™: Create individualized, omnichannel portal experiences securely at scale with a future-proof, headless web content management system. Empower business users to easily create, modify and publish content—without relying on IT.
- OpenText™ Core Share: Provide a connected collaborative space where documents can be shared externally with customers, partners and other ecosystem participants.

- OpenText™ Identity and Access Management: Drive top-line growth and bottom-line efficiencies by securely connecting suppliers, partners, customers and other third-party organizations and users with collaborative processes.



OpenText Active Access key components

The power of OpenText Active Access

OpenText Active Access gives diverse supplier networks simplified and secure access to enterprise information. It's a cloud-native service that delivers collaboration throughout the extended enterprise, with a secure, single point of entry for all suppliers, partners, distributors, customers and other communities, and the flexibility to create digital process flows.

Active Access combines:

- **Robust collaboration capabilities** to keep trading partners engaged with realtime communications and secure content sharing.
- **Ecosystem creation and management** to empower customers to securely build and connect integrated business networks to enterprise services and collaborative processes, irrespective of industry and geography.
- **Application and device integration** to distribute critical information, notifications and alerts wherever needed, and collect device and sensor data.
- **Governance and lifecycle management** to keep large ecosystems secure and compliant, and allow them to scale without increasing internal resources.
- **Identity and access management**, which underpins the entire platform by securely connecting any person, system or thing to any authorized enterprise resource.

For more than 20 years, Active Access has helped organizations manage and engage thousands of trading partners and millions of users while reducing cost, effort and risk. Active Access creates value for organizations in any industry by simplifying and securing access to end-to-end collaborative business processes and applications (see Figure 4).

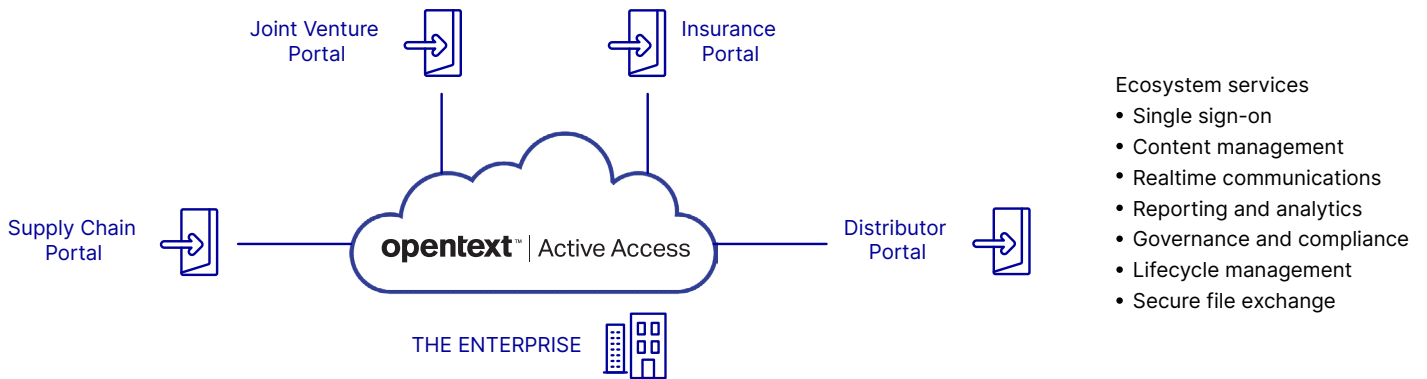


Figure 4: Standardize collaboration: one portal for all ecosystems and applications (use case: end-to-end procure-to-pay)

OpenText Active Access: At a glance

- A single portal infrastructure for 123,000 supplier companies and 725,000 supply chain professionals
- A single portal technology that supports any number of applications, processes or partner communities
- A single secure entry point for all external access
- A single point for supplier engagement, communication and collaboration
- A single standardized process for onboarding, offboarding, authentication and authorization, lifecycle management search and retrieval, and other security and collaborative functions
- A single identity and credential for all resources a user is authorized to access
- A single platform for reporting, auditing, analytics and compliance
- Global, multi-language support for global supplier portals

As global organizations rely more heavily on digital ecosystems of suppliers, customers and partners to ensure supply chain agility and resilience, the vulnerability of line-of-business based, platform-driven portals becomes more pronounced. The cost, risk and complexity of managing hundreds of portals with hundreds of thousands of users rise almost exponentially. Active Access provides a single infrastructure, with powerful and unique security and collaborative features, which connects global supply chains while reducing costs and internal resources.

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](#)