# OpenText Core Secure Access

Harness the power of business networks to fuel digital services while reducing cost and risk

## Benefits

- Secure enterprise access across global value chains using 2-3 FTEs
- Accelerate and standardize third-party onboarding
- Connect once and go anywhere

Enterprises are racing to add external-facing digital services to scale their businesses. However, opening the enterprise to third-party organizations and their users brings inherent risk: the possibility of security weaknesses at every organization given authorized access. In fact, 93 percent of businesses have experienced a data breach resulting from a security weakness at a "trusted" third party: supplier, partner, B2B customer, provider or vendor.[1]

With the cost of a data breach averaging $4.35M USD[2]—plus financial loss related to reputation and disruption—it is time to embrace B2B identity solutions that scale secure access across enterprise ecosystems.

Unlike workforce identity and access management (IAM) environments with well-defined enterprise constructs and processes to facilitate employee access, B2B environments are unpredictable. A B2B IAM solution worthy of investment must be able to secure access for every new relationship, regardless of IT footprint, involved systems and user experience requirements.

OpenText™ Core Secure Access delivers enterprise-class security for the extended enterprise. The OpenText cloud-based platform includes technologies and innovations that enable customers to predictably secure access across unknown environments without compromising security or experience—all while enforcing zero-trust principles.

1 BlueVoyant, *Managing Cyber Risk Across the Extended Vendor Ecosystem*. (2021)
2 IBM, *Cost of a Data Breach 2022 Report*. (2022)

## Scale enterprise access across global value chains using 2-3 FTEs

Collaborative ecosystems can be comprised of thousands of external organizations and millions of users, most of whom need access to the enterprise. Granting external access at this scale demands automation and knowledge of which external users need access to what enterprise resources, why, for how long, whose approval is needed and whether access is still needed. Unfortunately, ecosystem owners do not typically have this level of visibility into trading partner operations.

OpenText Core Secure Access includes a delegated administration component to create visibility into each organization and eliminate massive user administration costs. Customers delegate day-to-day administration authority to partner administrators closest to users. Delegated administrators use the platform's self-service administrative interface to perform administrative tasks, such as requesting access on behalf of users, adding users and updating profiles. When submitted, requests and changes are automatically evaluated and then trigger identity lifecycle processes as appropriate, e.g., approval workflows, creating users and provisioning resources.

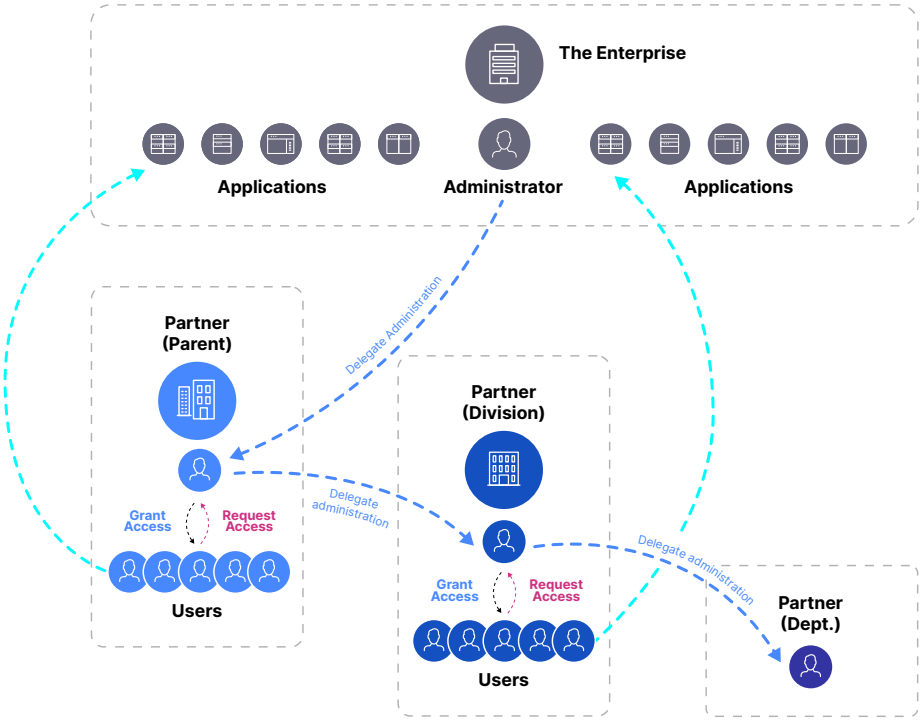



Figure 1. Delegated administration

## Accelerate and standardize third-party onboarding

Onboarding business partners and other third-party organizations is notoriously slow and disruptive. Onboarding collaborative partners, where part of the partner's workforce will need access to customer systems, can add significant time and complexity to an already long and disruptive process. It can also introduce ongoing user support and compliance costs to manage external user access to internal systems.

Some of the world's largest companies use OpenText Core Secure Access to onboard collaborative partners and their users quickly and efficiently. Self-paced, workflow-driven processes combined with comprehensive self-service capabilities minimize onboarding costs and delays while limiting staff involvement until knowledge workers are truly needed.

**Registration:** Invitation-based registration enables authorized staff to invite key partners to register and learn more. Invitations include a code unique to each potential partner and are entered on a public-facing walk-up registration page. If desired, the registration page may allow other organizations to submit inquiries without requiring a partner code.

**Qualification:** Organizations can automate data collection by empowering trading partners to securely create their profile, complete self-assessments and upload required documentation without assistance. Staff can monitor onboarding progress, get notifications when it is time to engage prospective partners, digitize high-touch and high-risk activities and create electronic forms to collect information digitally. OpenText Core Secure Access also allows for verification of submitted data against authoritative sources via external API calls, messaging or other provided integration.

## Automate & standardize onboarding

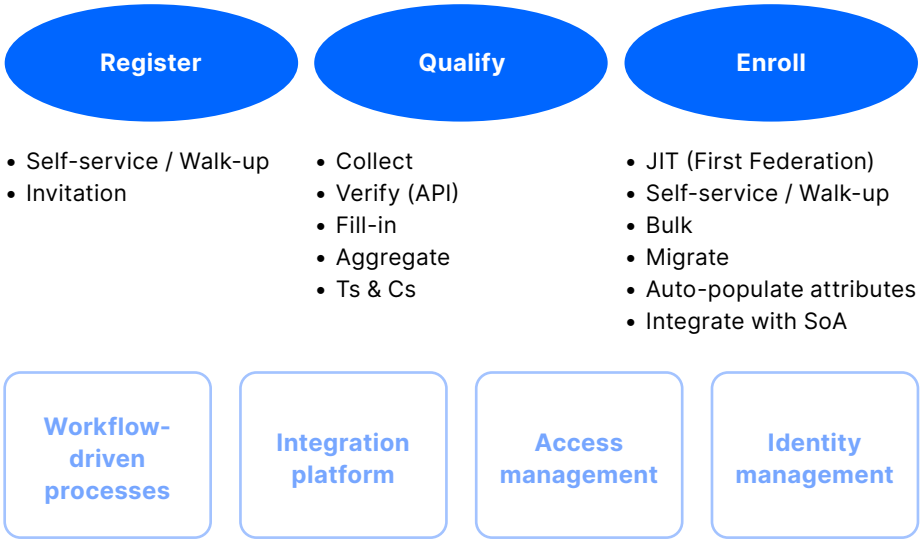



Figure 2. Onboarding for collaborative partners and users

## Connect once and go anywhere

OpenText Core Secure Access allows organizations to provide B2B users with the consumer-like experiences they expect: simple, secure and obstacle-free. When B2B services fail to live up to these expectations it leads to declining user adoption and customer attrition. Simplifying authentication throughout the B2B customer journey increases customer retention, as single sign-on eliminates repetitive log-ins after initial authentication. OpenText Core Secure Access provides multiple authentication options, including risk-based authentication (RBA), MFA, FidoU2F, phone, push and mobile authenticator. A combination of RBA and single sign-on can deliver the personalized and seamless experiences users expect. RBA also dynamically scales authentication strength to mitigate the risk each user presents.

B2B ecosystems are intended to be dynamic and fluid; they are constantly changing. Enterprises often attempt to use their workforce identity management solution to manage access across their external business partners. Unfortunately, explicit authorizations, 1:1 connections, roles and other workforce identity and access management conventions become impediments in an ecosystem model. The goal should be to enable an ecosystem, i.e., the buy-side and sell-side processes of the business, to automatically absorb large-scale and granular changes, exactly per policy and without staff intervention.

## Leading global Oil & Gas company improves security and revenue

With more than 400 joint ventures annually, this global Oil & Gas company needed an efficient way to provide thousands of globally distributed external partner users with point-in-time and project-based access to critical applications, information and resources.

Leveraging OpenText Core Secure Access, the company was able to securely onboard thousands of joint venture partners, manage access, decommission identities as necessary and then safely dissolve the ecosystem when their energy project was complete.

### Business Issues

- Reduced revenue
- Inability to scale
- Excessive permissions

### Solution

- Rapid onboarding
- Automated secure access
- Policy-based provisioning

### Business benefits

- Reduced JV set-up & end time by 50%
- Scale to millions of users
- Cost avoidance (compliance, breach)

The OpenText data model presumes significant, ongoing change and can secure the entire ecosystem in highly scalable and efficient ways. OpenText Core Secure Access has a unified data model that normalizes information across people, systems and things. Inferential relationships can also be evaluated, enabling this OpenText solution to predictably control access and authorizations without the extra overhead and technical debt of traditional identity and access methods. For example:

- Eliminating the burden of individual, manual and explicit provisioning of users to applications and devices.
- Enabling realtime permissions updates.
- Scaling to handle radically higher volumes of entities, identities and policies.
- Enabling efficient administration with the ability to, for example, change rules to force a step-up authentication when a device talks to a specific person type without having to update every device.

The OpenText model enables zero-trust principles beyond least privilege authorizations. Consider the administrative overhead typically needed to request, approve and provision non-birthright entitlements on an exception basis. Organizations need a more predictable and automated method to provision the exact entitlements an entity is to receive based on policies. OpenText Core Secure Access customers are doing that today.

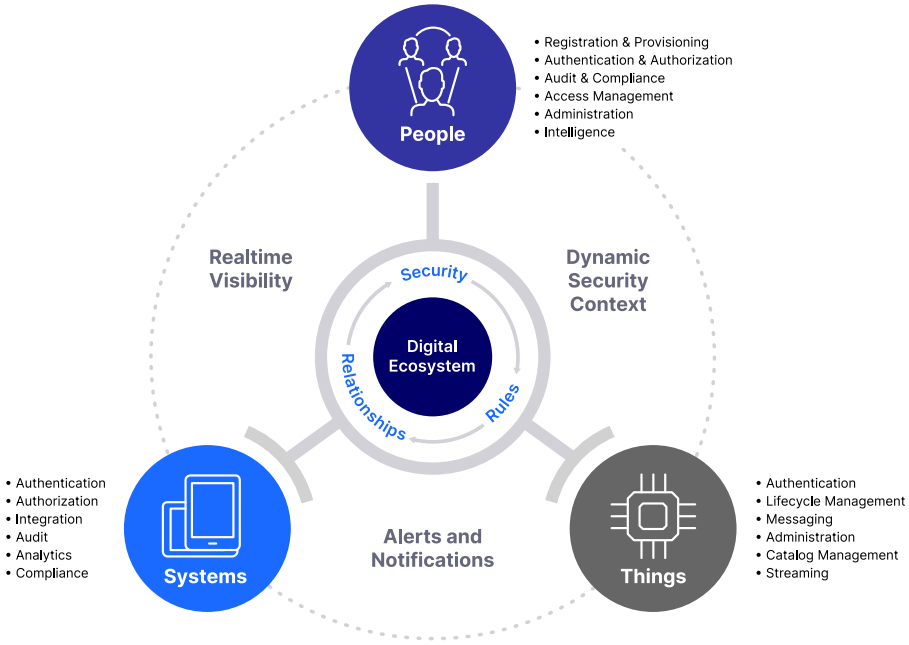



Figure 3: Unified data model encompasses people, systems, things and relationships.

| | Lifecycle Management | Authentication | Authorization | Experience | Integration |
|---|---|---|---|---|---|
| TECHNOLOGY | • Single Global Identity<br>  • People, IT, OT<br>• Onboard / Change / Offboard<br>• Delegated administration<br>• Provisioning & deprovisioning | • Adaptive, risk-based, contextual<br>• Passwordless (2Q23)<br>• MFA, Strong / FIDO<br>• Brokering<br>• Machine-to-machine<br>• Zero trust | • Dynamic personas<br>• Runtime authorization<br>• Hierarchy management<br>• Governance / Attestation<br>• Remote authorization<br>• Service orchestration | • Self-service<br>• Personalized security<br>• Omnichannel experience<br>• Identity-driven journeys<br>• Customized branding | • Identity streaming<br>• Orchestration<br>• Unified messaging<br>• Any-to-any<br>• IoT |
| USE CASES | • Supplier relationship mgmt.<br>• Customer lifecycle mgmt.<br>• Agent recruiting<br>• Contractor management<br>• OT – to – IT lifecycle<br>  • Send data to caring and qualified | • Multi-enterprise access<br>  • Customer service rep (loyalty)<br>• Remote access<br>  • Internal / third-party workforce<br>  • Partner / customer ecosystems | • Secure Ecosystems<br>  • Supply chain<br>  • Insurance<br>  • Distribution channels<br>  • Corporate clients<br>  • Retail | • Portals<br>  • Supplier portal<br>  • Agent portal<br>  • Customer portal<br>  • Distributor portal<br>• Identity-driven journeys<br>  • Connected customers<br>  • Connected agents<br>  • Connected ecosystems | OpenText™ Core Secure Access |

**DISTRIBUTED IDENTITY FABRIC**

| Supply Chain Ecosystems | Financial Services Ecosystems | Manufacturing Ecosystems | Joint Venture Ecosystems | Merger and Acquisition Ecosystems |
|---|---|---|---|---|

| Function | Capability | Description |
|---|---|---|
| **Access management** | Single sign-on | Enable users to authenticate once and access any authorized resource across multiple security domains and enterprises. |
| | Advanced authentication | Establish needed levels of assurance to mitigate risk using the most appropriate method(s): risk-based authentication (RBA), adaptive, multi-factor (MFA), strong authentication (FIDO U2F), token verification, mobile authenticator, third-party and others. |
| | Web access management | Secure access to internal and cross-border web apps without heavy protocols or replicating identity stores. |
| | Single point of entry | Maintain a single connection to the Active Access cloud, no matter how many trading partners connect. Reduce the number of endpoints connecting to the enterprise to reduce attack surface and costs. |

| Function | Capability | Description |
|---|---|---|
| **Identity management** | Single digital identity | Provide one identity for every person, system and "thing" connecting to the enterprise. Create granular policies leveraging identity profile data: authorizations, grants, attributes, history, and other information. Automatically verify identity authorizations at the moment resources are accessed, providing greater flexibility and protection. |
| | Lifecycle management | Establishes consistent and repeatable processes for identity creation, provisioning, change management and deprovisioning for internal and external users. |
| | Advanced authorizations | A flexible authorization and approval framework centralizes policy administration and control while decentralizing authorization request and validation activities to trading partner local administrators. |
| | Directory services | Cloud-based directory with comprehensive capabilities to synchronize identity and access management data across on-premises and cloud directories and user stores in multi-enterprise environments. |
| **Identity governance and administration** | Governance and attestation | Automates access certification campaigns (attestation) to verify the efficacy of identity and access management program and comply with applicable regulations. |
| **Cloud access security broker (CASB)** | Identity broker | Secure complex cross-domain authentication scenarios, connect IdPs and SPs in a many-to-many relationship model, verify authenticity, enrich and remap tokens to required protocol. |
| **Integration and Interoperability** | Platform as a Service | An API-first, auto-scaling microservices architecture enables customers to rapidly develop applications and custom solutions in a DevSecOps environment. |
| | Messaging and orchestration | Secure and streamline data transport and integration across devices, applications and machines. |
| | Identity streaming | Use a reliable, production-class approach to synchronize directories and identity data across the ecosystem by streaming identity events using a pub/sub model. |
| | Cross-domain synchronization | Synchronize identity data across on-premises and cloud applications and systems. |
| **Intelligence and analytics** | Reporting and dashboards | Provide actionable insights to internal and partner stakeholders via highly visual dashboards and ad hoc and API-driven reports. |
| | SIEM adapters | Stream threat indicator-related identity events to security information and event management (SIEM) systems to support threat detection and response. |
| | Hierarchy management and synchronization | Quickly detect and respond to out-of-sync trading partner master data. Use supplied workflows to make any necessary user moves, code grant changes or other authorized operations to avoid disruption. |

| Function | Capability | Description |
|---|---|---|
| **Customer community and support** | Developer community | Build and run applications on a highly scalable, low-code infrastructure. Access a comprehensive suite of APIs covering identity, portal and messaging to rapidly develop and deliver custom solutions. |
| | Global customer support | Support includes 24×7×365 service, nine supported languages, online tutorials and ticket generation, online chat support with agents and a user-accessible knowledgebase. |
| | Trading partner support | Help Desk role is provided to enable trading partner support staff to handle routine incidents without customer intervention. OpenText is also available to provide Tier-1, Tier-2 and Tier 3 support. |

## Resources

**Drive growth via third-party access**

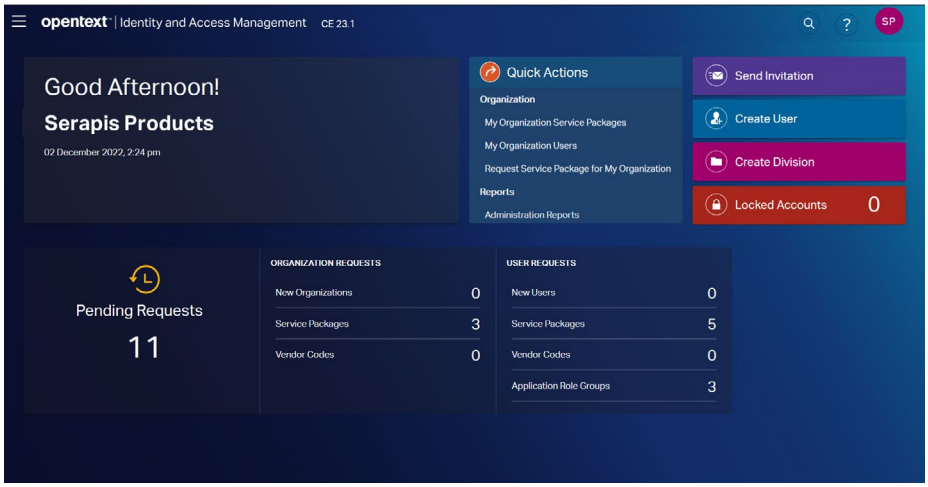
Read the position paper ›

**How to secure Third-Party identity and access at scale**

Watch the explainer video ›

**Addressing cyber resilience gaps across key infrastructure assets**

Read the blog ›




Learn more: OpenText Core Secure Access ›