eBook

Third-Party Identity Risk: Closing the Security Gap in External Access

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

Introduction	3
Identity Management: Controlling Access to Minimize Risk	4
The Rising Importance of Third-Party Identities	6
Common Bad Practices to Avoid	7
Regaining Control Over Third-Party Identities	8
How can innovative solutions enhance both the security and agility of your value chain?	14
Conclusion	18
About Thales	18

Introduction

- Third-Party Risk Management (TPRM) helps organizations assess and mitigate risks when working with external vendors, suppliers, and partners. Traditionally, TPRM focuses on contractual compliance, cybersecurity, and operational resilience, but validating the organizations themselves is equally critical.
- Regulatory frameworks such as Know Your Business (KYB) and Legal Entity Identifier (LEI) provide structured approaches to verifying third-party legitimacy and financial integrity. Mandates like the USA PATRIOT Act, the EU's Anti-Money Laundering Directives, and FinCEN's Customer Due Diligence Requirements enforce rigorous due diligence, with non-compliance leading to severe financial and legal consequences.
- While TPRM helps organizations establish trust at the organization level, it does not address who within those entities is accessing systems and data, a challenge best addressed through identity management.
- Identity management ensures that the right individuals within third-party organizations have appropriate access. Each external user, whether a supplier, contractor, or distributor, has unique roles and access needs, requiring clear policies and controls to prevent unauthorized access and security gaps.
- By managing both third-party risk and identity in parallel, organizations gain greater visibility, security, and compliance alignment. A complementary approach to validating both organizations and individuals reduces exposure to supply chain vulnerabilities and regulatory risks, ensuring trusted third-party relationships without compromising security.

Identity Management: Controlling Access to Minimize Risk

- Businesses have long relied on third-party collaborations to optimize operations, reduce costs, expand market reach and drive innovation. Since the Industrial Revolution, manufacturers have depended on suppliers, logistics providers, and distributors to scale production efficiently. Today, digital transformation has further integrated external partners, enabling seamless coordination across outsourced manufacturing, consulting, and global distribution networks.
- A clear example is the Aircraft industry, where manufacturers source components from thousands of specialized suppliers worldwide-from raw material to avionics systems. Each supplier plays a critical role in production, requiring precise coordination and secure access to digital design, inventory, and supply chain systems. This model allows businesses to enhance agility, maintain competitiveness, and adapt to dynamic markets while ensuring efficiency and compliance in highly regulated industries.
- Nowhere is this interdependence more apparent than in global value chains, where organizations must coordinate with a vast network of external entities to ensure seamless production, distribution and service delivery. Digitally integrating these partners into core business processes enhances efficiency, reduces costs, and strengthens supply chain resilience.

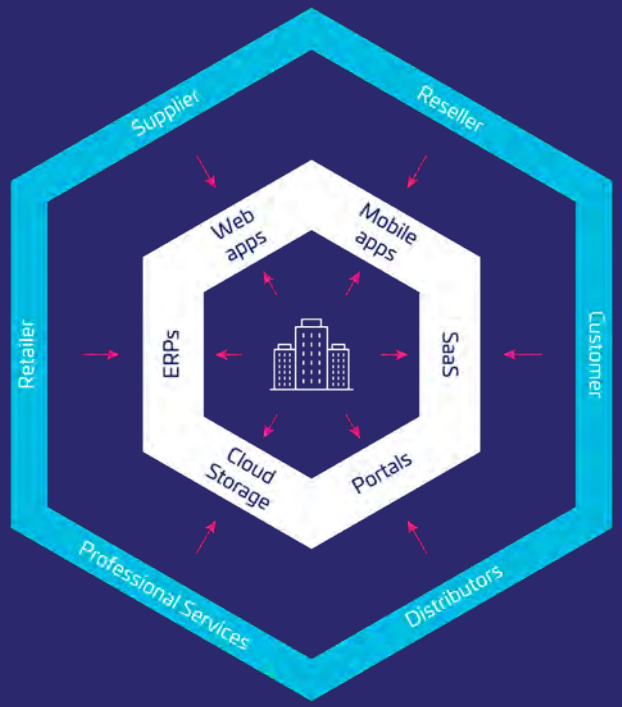


Figure 1: A collaboration ecosystem that connects organizations with suppliers, partners, distributors and customers.

- **SUPPLIER:** Exchange of data for procurement, inventory updates, and production planning. Requires controlled access to manage orders and supply chain logistics.
- **RETAILER:** Engages with supply and demand systems, needing access to stock levels, pricing updates, and transaction management for omnichannel sales.
- **PROFESSIONAL SERVICES:** Provides consulting, support, and integration services, necessitating controlled access to project management and client-specific data.
- **DISTRIBUTOR:** Manages large-scale logistics, requiring efficient access to inventory, fulfillment systems, and demand forecasting tools.
- **CUSTOMER:** Expects frictionless interaction with services, whether purchasing products, tracking orders, or accessing support resources.
- **RESELLER:** Needs secure access to pricing, promotions, and inventory details to facilitate product sales and enhance customer service.

Identity Management: Controlling Access to Minimize Risk

- As value chains expand, digital assets once restricted to employees must now be accessible to an ever-changing network of suppliers, partners and logistics providers. But each new connection creates a potential security risk, exposing systems to unauthorized access.
- Historically, enterprises managed third-party identities through one-off, point-to-point integrations, but this approach scales poorly, with each new supplier exponentially increasing risk exposure.

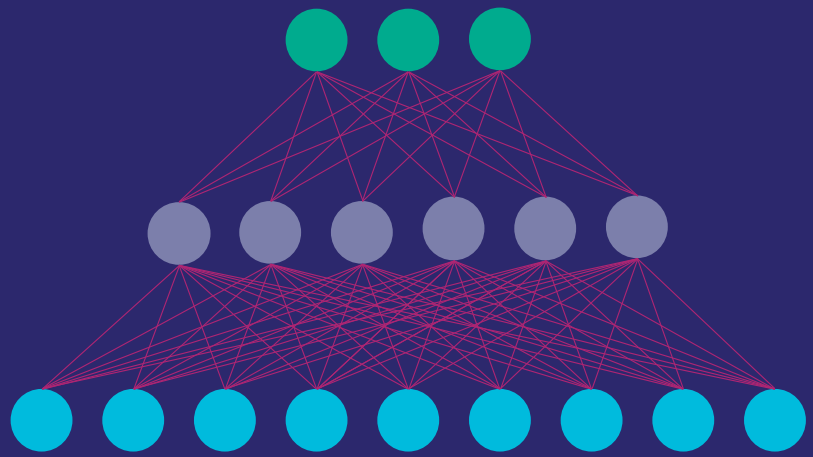


Figure 2: The Challenge of Scaling Third-Party Access

The growing complexity of multi-tiered partner and user relationships as point-to-point connections expand, increasing security risks and operational overhead.

The Rising Importance of **Third-Party Identities**

Represent non-customer external identities

Source: S&P Global, 2024. B2B IAM – the hidden value of third-party identities

of organizations grant third parties deep access to their systems

Source: Gartner, 2023. Reimagining Third Party Cybersecurity Risk Management Survey

of companies feel confident that their cybersecurity strategies adequately protect data shared with third parties

Source: Gartner, 2022. Three Key Trends in B2B Customer/Partner Identity and Access Management

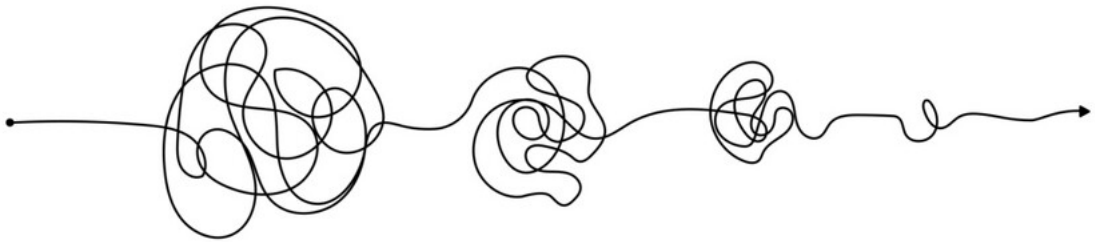
of large organizations, IAM solutions must evolve to address these vulnerabilities

Source: Gartner, 2023. Reimagining Third Party Cybersecurity Risk Management Survey

- Businesses are becoming increasingly reliant on third-party relationships, with many engaging a substantial number of external entities. As this trend accelerates, organizations are granting third-parties deeper access to their systems, raising critical security considerations. However, confidence in existing cybersecurity measures remains limited, underscoring the need for IAM solutions to evolve in response to these challenges.
- Security measures alone, if not designed to facilitate structured collaboration, do not scale effectively. Organizations must recognize that security and collaboration are not opposing forces but interdependent components of a resilient operational model. The ability to enable third-party access in a controlled and well-governed manner is fundamental to strengthening security posture and ensuring sustainable growth.

Common
bad practices to avoid

- **Ad hoc processes:** Disjointed or manual onboarding lacking consistent and contextual data.
- **Trust by proxy:** Granting access based on a user's employer alone.
- **Inattention after onboarding:** Failing to manage identity throughout the user's lifecycle.
- **Shared access:** Multiple users logging in with a single shared account.
- **Shortcuts:** Relying on inactivity instead of business rules for access termination.



Regaining **Control Over Third-Party Identities**

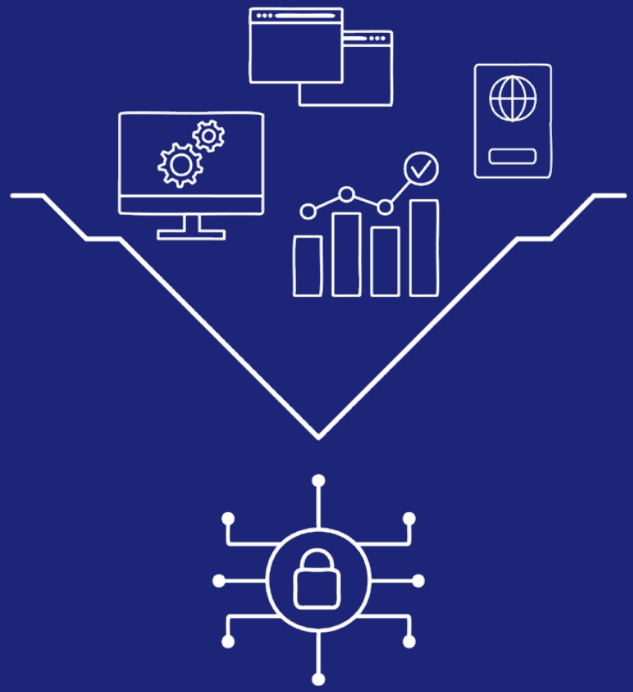
Vendors, suppliers, and contractors need access to critical systems, but without strong security controls, organizations expose themselves to credential misuse, unauthorized persistence, and insider threat. Security teams must ensure third-party users enter with verified identities, maintain only necessary access, and removed when no longer needed. This framework delivers a practical, security-first approach to managing third-party lifecycle events without unnecessary complexity.

1. Identify and Remove Unnecessary Third-Party Access

Security teams cannot control what they can't see. The first step is to map all external accounts and eliminate unnecessary credentials.

- **Discover and document third-party access.** External accounts often exist across multiple systems, making visibility difficult. Security teams must centralize access records to ensure no unmanaged third-party credentials persist.
- **Identify how and why access was granted.** Determine who onboarded each third-party user, what permissions were assigned and which internal sponsor approved it.
- **Immediately revoke orphaned or stale accounts.** Unmonitored third-party credentials are a major attack surface. If an account has no clear owner or hasn't been used in months, it must be removed.
- **Standardize how third-party access is granted.** Security teams must enforce clear, repeatable procedures for onboarding new external users, ensuring each request follows a security-controlled process.

OUTCOME: A full inventory of third-party access, inactive accounts revoked, and a structured process for how external users enter the system.



Regaining **Control Over Third-Party Identities**

2. Restrict Access to Active Business Relationships Only

Once access is mapped, security teams must ensure that external users still have a valid reason for access.

- **Cross-check third-party access against partner records.** If a company no longer has a contract or partnership with a vendor, their accounts should be removed immediately.
- **Disable accounts for disengaged vendors and expired contracts.** Many third parties retain access simply because no one disabled their credentials. This is a major security risk.
- **Strengthen security for high-risk third parties.** External users must have additional controls, such as session timeouts, location-based restrictions, or mandatory security reviews.
- **Ensure access is revoked when business relationships end.** Security teams must enforce strict offboarding rules, ensuring access removal is a required step when contracts expire.

OUTCOME: External access is limited to active business partners, while expired third-party credentials are automatically removed.

Regaining **Control Over Third-Party Identities**

3. Enforce Strong Authentication and Identity Verification

No external account should be granted access without authentication and verified identity proofing

- **Require identity proofing during onboarding.** Third-party users must verify their identity through business validation, internal sponsor approval, or other credential verification methods.
- **Mandate internal sponsorship for all third-party accounts.** No external user should receive access without an internal employee vouching for them.
- **Enforce phishing-resistant multi-factor authentication for all third-party access.** Passwords alone are insufficient. Every third-party user must authenticate using MFA, preferably FIDO-based methods.
- **Limit session persistence and enforce re-authentication**. Persistent sessions allow third parties to maintain continuous access without security checks. Security teams should enforce session timeouts and re-authentication for high-risk actions.
- **Standardize how third-party access is granted.** Security teams must enforce clear, repeatable procedures for onboarding new external users, ensuring each request follows a security-controlled process.

OUTCOME: Only verified third-party users gain access, and strong authentication prevents unauthorized persistence.

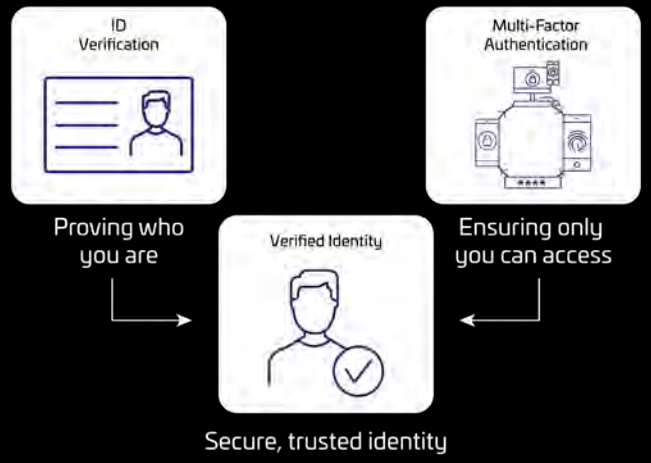


Figure 3: Establishing a Secure and Trusted Identity

This diagram illustrates the two essential steps for securing digital identities:

- ID Verification ensures that users prove who they are through document validation, credential checks, or identity proofing.
- Multi-Factor Authentication (MFA) guarantees that only the verified user can access systems by requiring additional authentication factors, such as mobile devices, biometrics, or security keys.
- By combining identity verification with strong authentication, organizations can establish a secure and trusted digital identity, reducing the risk of unauthorized access and identity fraud.

Regaining **Control Over Third-Party Identities**

4. Limit Privileges and Minimize Third-Party Exposure

Over-provisioned identities increase risk exposure and create unnecessary attack paths. The objective is to minimize access while ensuring third parties can still perform their work.

- **Enforce least privileged access.** Third parties should never be granted broad access privileges. Their permissions must be scoped only to what they need for their task or contract.
- **Eliminate long-term access.** No third party should have permanent credentials. Security teams must implement expiration-based access that ensures credentials are disabled when no longer needed.
- **Use dynamic access rules based on risk.** Static permissions do not account for evolving risks. If a third party is connecting from an unknown device, unapproved network, or exhibiting unusual activity, access should be automatically restricted.

OUTCOME: External users only receive the access they need, for the time they need it, with additional controls for high-risk scenarios.

Regaining **Control Over Third-Party Identities**

5. Implement Secure Lifecycle Management for Third-Party Users

As third-party access expands, security teams cannot manually manage every identity change. B2B IAM enables self-service and delegated administration so that business units or external administrators can handle day-to-day identity tasks within a security-controlled framework.

- **Enable self-service for external users.** Third parties should be able to request access, update credentials, or reset MFA without engaging IT, while still requiring security-controlled approvals.
- **Delegate identity management to business owners.** Instead of security teams manually provisioning and deactivating accounts, business sponsors or partner administrators should be responsible for managing their users' access.
- **Use workflow-driven automation for onboarding.** Rather than relying on IT tickets, access approvals, identity validation, and authentication enforcement should follow structured, automated workflows.
- **Introduce controlled self-service for access modification.** If a third-party user needs additional access, they should be able to request it through a security-enforced self-service portal, with automatic routing for approval.

OUTCOME: Security teams offload identity lifecycle management tasks through self-service and delegated administration, ensuring enforcement at scale without operational bottlenecks.

How can innovative solutions enhance **both the security and agility of your value chain?**

Thales' OneWelcome Identity Platform offers an advanced B2B IAM solution to simplify and standardize access management across large third-party ecosystems. Designed to address the complexities of external identity management, it enables organizations to securely collaborate with partners, suppliers, and customers at scale. Below are a few innovations that can help set your organization up for success.

Single Source of Truth for Third-Party Identities

The B2B IAM solution serves as the centralized system of record for all external organizations and users connecting to your enterprise, providing a single source of truth for third-party identities.

Designed to seamlessly integrate with both on-premises and cloud systems, B2B IAM ensures that user profiles and authorization data remain accurate, up to date, and consistent across value chain systems and devices. Its API-first approach to user journey orchestration simplifies identity management and eliminates silos.

Organizational Relationship Management

Organizations are required to onboard and manage not just individual users, but entire entities -such as partners, suppliers, or subsidiaries- within a structured relationship model. These relationships, whether explicitly assigned or dynamically derived, serve as the foundation for authentication and authorization decisions. By leveraging entity-based relationships, access control extends beyond static roles, allowing permissions to be dynamically adjusted based on real-time factors like business partnerships, contractual status, and contextual attributes. This ensures that third-party organizations and their users receive the right level of access at the right time, without compromising security or operational agility. With this approach, enterprises can efficiently govern complex external ecosystems, enforce fine-grained security policies, and enable seamless collaboration, all while maintaining centralized oversight and security compliance.

Hierarchical Management

A key advancement in modern Identity and Access Management (IAM), compared to traditional flat-group authorization models like those introduced in UNIX, is the use of hierarchical organizational structures. Unlike static, role-based group assignments, an organizational hierarchy dynamically defines a user's access rights, administrative authority and entitlements based on their position within the enterprise structure. This evolution enables context-aware access control, delegated management, and automated policy enforcement, reducing the inefficiencies and security risks associated with rigid, manually maintained access groups.

Our B2B IAM vision extends this concept by mirroring an organization's hierarchy within the platform. This allows delegated managers to replicate and manage the specific parts of their organization that require access to your enterprise - without requiring direct involvement from your IT administrators. Additionally, organizational hierarchy tracking provides a structured way to detect and respond to changes within third-party organizations, ensuring that access remains aligned with evolving business relationships.

How can innovative solutions enhance **both the security and agility of your value chain?**

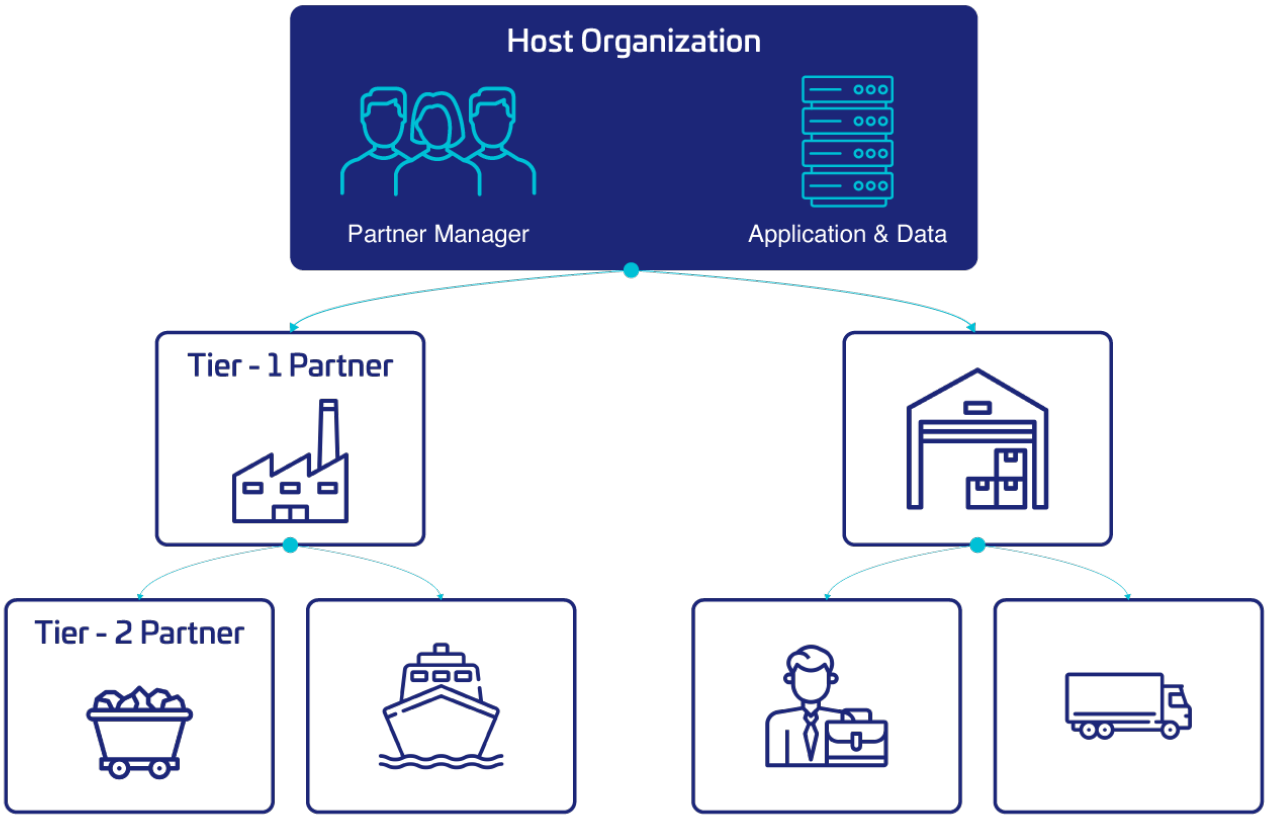


Figure 4: Hierarchical partner ecosystem.
The Host Organization governs access and interactions with Tier-1 Partners, such as manufacturers and warehouses, who, in turn, manage Tier-2 Partners, including suppliers and logistics providers. It ensuring that each entity has the right access to applications and data while maintaining security and efficiency in a multi-tier partner network.

How can innovative solutions enhance **both the security and agility of your value chain?**

Delegated User Management

While B2B IAM serves as the single source of truth for external identities, effective management also requires systems of engagement, interfaces and processes that enable seamless delegation, structured access management, and enforcement of policies across a vast third-party ecosystem. Without these mechanisms, organizations face operational bottlenecks, security blind spots, and excessive administrative burdens that hinder scalability. Another key consideration is the degree of delegation an organization is willing to establish with third parties. Traditionally, delegation has focused on identity onboarding and access provisioning, but a more sophisticated model recognizes that delegation exists on a spectrum. This means:

- **Application onboarding delegation** – Allowing third-party administrators to manage access to specific applications, but only within defined sub-entities.
- **Policy definition delegation** – Enabling third-party managers to enforce access policies within their scope, such as regional offices, subsidiaries, or specific operational tiers.

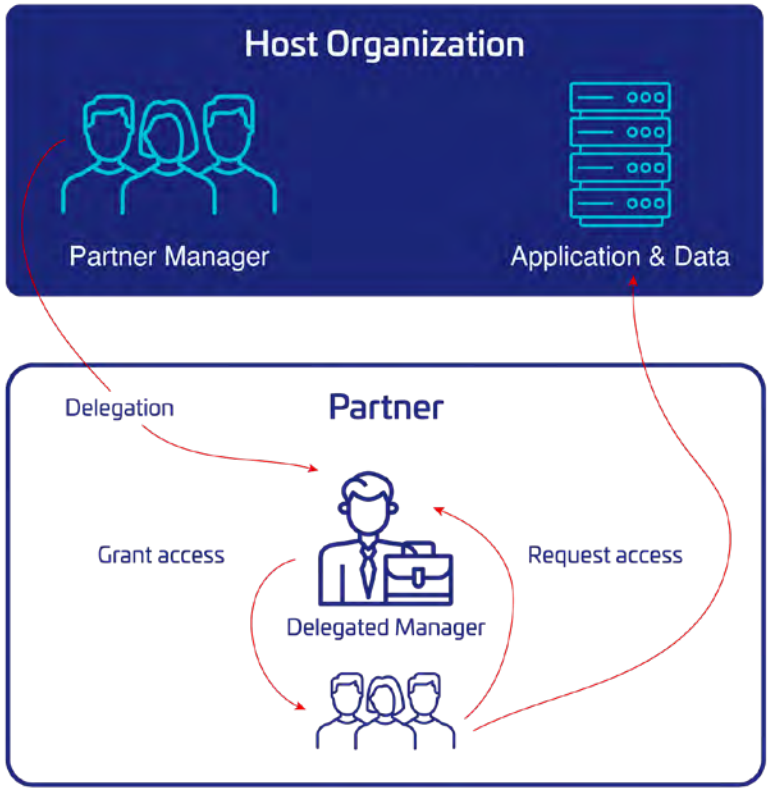
Beyond structured delegation, identity self-service and authorization intersect in new ways. While authorization traditionally defines user permissions within applications, in a third-party context, it expands to empowering external users to manage others through delegated management. This represents a distinct self-service model, focused not on individual users but on delegated managers who govern access within a controlled framework. A structured delegation model ensures that third-party administrators handle identity management tasks while security teams retain critical oversight of:

- **Application Access Management** – Defining which applications each partner organization can use.
- **Approval Workflows** – Implementing structured approval processes to ensure traceability and compliance.
- **Automated Access Removal** – Promptly revoking access when users or partners disengage.
- **Context-Aware Access Control** – Aligning permissions based on business relationships, risk levels, and role-specific requirements.

By shifting routine identity administration to those closest to third-party users while maintaining strict authorization controls, organizations can scale efficiently, minimize risk, and retain control over external access, without compromising agility.

How can innovative solutions enhance **both the security and agility of your value chain?**

Figure 5: Delegated User Management
This diagram illustrates how Delegated User Management enables **efficient third-party access management**. The **Host Organization** assigns a **Partner Manager** to oversee access to applications and data. Instead of managing individual users, access is **delegated to a designated manager within the partner organization**, who is responsible for **granting access to their users** while ensuring requests are handled efficiently. This approach reduces administrative overhead, improves security oversight, and ensures that access remains aligned with business needs.



Conclusion

- No Third-Party Risk Management program is complete without taking identity in the mix. Security teams are not just managing risk, they are actively securing the business while enabling trusted external collaboration. As third-party ecosystems grow, manual processes alone cannot keep up. Without self-service, delegated administration, fine-grained authorization and workflow automation found in B2B IAM solutions, external identities become a persistent attack vector rather than a controlled access model.
- By leading this transformation, security teams:
  - Define and enforce the policies that make external access secure from day one.
  - Ensure every external user is verified, onboarded securely, and granted only the necessary permissions.
  - Prevent permission creep by enforcing least privilege and context-aware access controls.
  - Empower external users with self-service capabilities - without sacrificing security oversight.
  - Shift operational control to business owners through delegated management, reducing IT bottlenecks while keeping policies intact.
  - Drive efficiency by automating identity workflows, making onboarding, access changes, and deactivation seamless.

With security-first policies and implementing scalable B2B IAM controls, IT and Security teams become the architects of trust, ensuring third-party identities are controlled, monitored and adapted as the business evolves.

About **Thales**

In today's digital landscape, organizations rely on Thales to protect what matters most - applications, data, identities, and software. Trusted globally, Thales safeguards organizations against cyber threats and secures sensitive information and all paths to it — in the cloud, data centers, and across networks. Thales offers platforms that reduce the risks and complexities of protecting applications, data, identities and software, all aimed at empowering organizations to operate securely in the digital landscape. By leveraging Thales's solutions, businesses can transition to the cloud with confidence, meet compliance requirements, optimize software usage, and deliver exceptional digital experiences to their users worldwide

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com