

Securing the B2B Ecosystem

The Modern Approach to Managing B2B
Access Control and Third-Party Risk

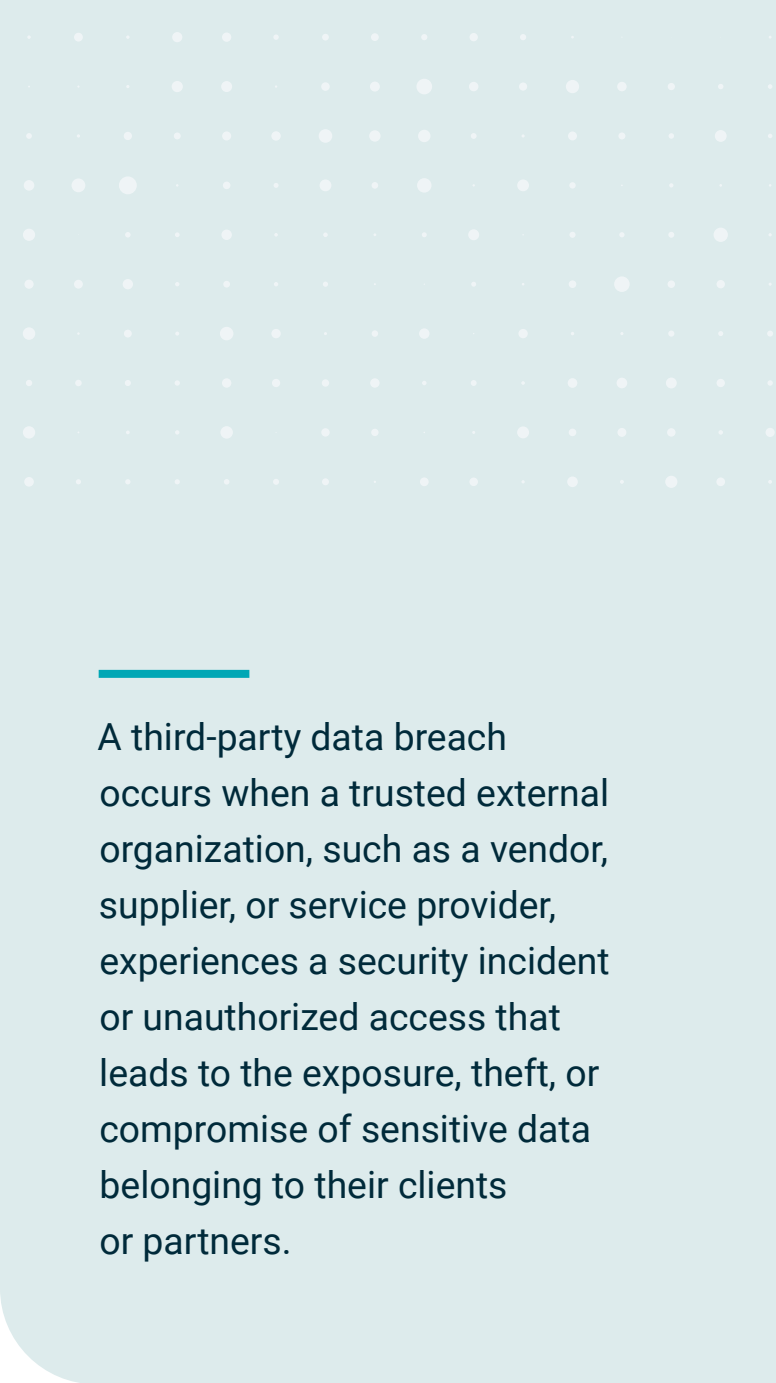


In today's business landscape, organizations are confronted with increasingly complex challenges when it comes to managing risk, particularly in relation to third parties and B2B access. As reliance on external partners continues to grow, businesses must make it a priority to adopt flexible access control systems that effortlessly match their specific business and security models.

Enterprises now heavily depend on external entities to drive revenue and facilitate critical business processes, such as data collaboration, distribution, reselling, and brokering. While these partnerships offer immense opportunities for growth and innovation, they also introduce inherent risks. Inadequate security measures among vendors, suppliers, contractors, or business partners can leave industries exposed to third-party data breaches.

To mitigate these risks effectively, organizations need to establish robust access control mechanisms that go beyond the traditional boundaries of their own infrastructure. By adopting a proactive approach to managing access control within B2B interactions, organizations can foster a secure environment that nurtures trust and confidence among their partners.

While enterprises have strengthened their cybersecurity programs over the past decade, many are still neglecting this crucial blind spot. The absence of robust security measures among vendors, suppliers, contractors, and business partners can leave these industries vulnerable to third-party data breaches.



A third-party data breach occurs when a trusted external organization, such as a vendor, supplier, or service provider, experiences a security incident or unauthorized access that leads to the exposure, theft, or compromise of sensitive data belonging to their clients or partners.

THIS PAPER COVERS:

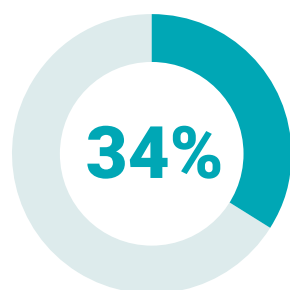
- Security gaps created by third-party relationships in the B2B space
- Proven strategies and solutions to effectively close these critical security gaps
- Key features of PlainID's Authorization Platform that provide these solutions

A Growing Security Problem in the Supply Chain

Recent data shows a troubling lack of preparedness when it comes to managing security with third parties. Only 39% of companies report having adequate protection for data exchanged with strategic partners, and only 34% of organizations are confident that their suppliers would notify them in the event of a breach that jeopardized their sensitive information.

Meanwhile, cybercriminals are increasingly using supply chain vulnerabilities as gateways to private data. A 2022 Ponemon Institute report found that 56% of respondents had experienced a data breach caused by a third party that resulted in the misuse of sensitive or confidential information. 70% of these breaches were the direct result of simply giving too much privileged access to third parties.

These breaches often have devastating consequences. A 2022 IBM report found that the average data breach in the United States costs \$9.44 million. The report also found that almost a fifth of breaches of critical industries were supply chain attacks that used a third-party business partner as the attack vector.



Only 34% of organizations are confident their suppliers would notify them of a breach of their sensitive information

More than half of risk leaders say their company has experienced a breach caused by a third party.

Navigating the Top Challenges in B2B Access Control

Clearly, the problem of insecure third-party relationships demands a solution capable of closing vulnerable gaps in the collaborative workflow. This solution, however, must also address several other issues that frequently plague B2B companies in the midst of digital transformation. When it comes to finding a secure means of accessing and sharing information, many B2B companies get burdened with:

- **Static and weak access controls** that fall short of meeting the stringent security standards required for dynamic and fine-grained access.
- **Lack of a unified approach to managing different types of identities**, which results in a scattered approach to access control.
- **Poor visibility and manageability of authorization policies**, particularly concerning resellers, distributors, and brokers, creating potential gaps in security and governance.
- **Poor user experience** introduces unnecessary friction and impedes efficient collaboration with third parties.

¹ Gartner 2022: [Three Key Trends in B2B Customer/Partner Identity and Access Management](#)

² Ponemon Institute: [The 2022 state of cybersecurity and third-party remote access risk](#)

³ IBM Security: [Cost of a Data Breach Report 2022](#)

Foundational cybersecurity solutions are a perfect fit for managing employee identities, but they leave gaps when it comes to third-party access.

Strong, adaptable access controls form the foundation of a modern cybersecurity strategy. However, existing Identity Governance and Administration (IGA) and Identity and Access Management (IAM) tools often fall short in terms of the depth and coverage of authorization they offer. This limitation, coupled with the lack of visibility, presents a significant challenge.

Moreover, in the realm of third-party relationships, it is crucial to recognize that third parties cannot manage their own access to company data. Instead, they rely on their partnered enterprise to provide delegated authorization capabilities. When this delegation is unclear or poorly managed (or downright unmanageable), all parties suffer.

Businesses that rely on their third-party relationships need a better solution—one that leverages the new functionalities available in modern authorization software.

Advancing Access Management Beyond Traditional IGA and IAM Solutions

Identity and Access Management (IAM) systems serve a central security function: they ensure that the right people are able to access the right resources at the right time for the right reasons. But because IAM and IGA rely on a role-based, coarse-grained approach to access decision-making, its structure and predefined rules can sometimes impede the access request and approval cycle. It can also inevitably lead to the over- or under-provisioning of access rights.

These traditional solutions are a perfect fit for managing employee identities at a coarse-grained level, but they have gaps when it comes to the need for non-employee (e.g. third-party) access and dynamic access decisions. For this reason, managing these systems becomes incredibly complicated as organizations grow and expand their partnerships with third-party vendors. The responsibilities associated with these third-party relationships are scattered across business lines within the organization, and this distributed network of responsibility doesn't fit neatly into the centralized authority of IAM systems. This leads to inefficient workflows that slow down essential functions and create gaps that bad actors can exploit.

Delegated authorization management closes these gaps. By delegating administrative capabilities to partners via self-service access portals, delegated authorization management supports and augments IAM and IGA systems by casting a net of centralized management over the distributed network of third parties and their points of contact within the organization.

SIMPLIFYING B2B ACCESS CONTROL FOR THE ENTERPRISE AND THIRD PARTIES



Delegated Authorization Management: A Key Pillar of Third-Party Risk Mitigation

Modern authorization solutions effectively address gaps in B2B access control, providing comprehensive visibility and control over access policies across various business lines, multiple identity types, and third-party organizations that rely on data access for their operations. This holistic level of control enables enterprises to proactively prevent unauthorized access and minimize the impact of potential breaches, ensuring a robust and secure access control environment. The adoption of modern B2B access control offers the following significant benefits:

MINIMAL RISK AND A SECURE SUPPLY CHAIN

Modern authorization platforms offer tailored access controls and delegated authorization capabilities for downstream administrators, safeguarding the entire supply chain and mitigating risks associated with

sensitive interactions. This feature is particularly valuable for customers, distributors, resellers, brokers, and other third-party identities engaged in B2B collaborations, providing them with enhanced security and reducing the potential for unauthorized access or data breaches.

ENHANCED DIGITAL EXPERIENCES FOR ALL USERS

A seamless and efficient user experience is crucial for consumers, third-party partners, and administrators alike. Modern authorization platforms combine granular access control with user-friendly and low-friction user experiences, accommodating diverse user flows. This ease of administration and use empowers enterprises to manage data at scale without subjecting users to unnecessary complexity, thereby reducing the risk of human error and ensuring a positive user experience.

SIMPLIFIED AUDITING AND COMPLIANCE

As data privacy regulations become more stringent and widespread, organizations face the challenge of complying with intricate data sharing requirements. Modern authorization platforms offer centralized control and robust auditing capabilities that span across business lines, facilitating compliance efforts. By implementing well-developed measures to protect personally identifiable information (PII), enterprises can ensure privacy, avoid regulatory fines, and demonstrate their commitment to compliance.

REDUCED COSTS THROUGH SIMPLIFIED MANAGEMENT AND AUTOMATION

Manual processes drain valuable time and resources. By leveraging automation for policy approval workflows, lifecycle management, and policy deployment, enterprises can significantly reduce administrative burdens. Automation in decision-making processes related to provisioning, certification, deauthorization, and deprovisioning of identities streamlines operations and reduces certification time from days to minutes, resulting in cost savings and increased operational efficiency.

Emerging Compliance Risks and Managing Access Control

Regulatory measures related to data security and privacy continue to evolve on a global scale—and this trend isn’t going anywhere. To stay compliant (and competitive) businesses need to adopt a cybersecurity posture that can meet escalating regulatory standards (e.g. GDPR, CCPA, CPPA, HIPAA, etc).

Whether it’s cross-border compliance or a general privacy ruling like the EU’s General Data Protection Regulation (which is designed to protect data from unauthorized processing, accidental loss, damage, or destruction) or an industry-specific regulatory development, strong access control provides a means of achieving necessary compliance goals.

DELEGATED AUTHORIZATION MANAGEMENT FOR THE B2B MODEL



How PlainID Helps With Fine-Grained B2B (And B2C) Access Control

Addressing the security complexities that come with third-party relationships begins with three important actions: **externalizing authorization, centralizing policy management, and distributing its enforcement**. This strategy enhances the enterprise's security stance while also enabling security experts to maintain comprehensive visibility into access control pertaining to multiple types of identities and digital assets.

PlainID empowers enterprises to accomplish both goals simultaneously. PlainID's Delegated Authorization Management makes it easy for security professionals to create, manage, and enforce access control policies for B2B access, which in turn makes it easy for third parties and other lines of business to access key enterprise data without compromising either party's security framework.

By incorporating dynamic risk indicators from multiple sources (network, device, identity, etc.) the PlainID Authorization Platform continuously verifies trust during each digital interaction and prevents unauthorized access. PlainID delivers dynamic, fine-grained authorization essential for identity-first security throughout various technologies and third parties in the supply chain.

KEY BENEFITS

- **Increased access protection** that enables the secure, customizable, and scalable management of complex third-party relationships
- **Better compliance** with data residency requirements (along with flexible delegated administration for B2B customer administrators)
- **Visibility into multiple lines of business** that allows them to remain separate structurally

- **Coarse- and fine-grained access controls** that accommodate the growing need for nuanced data sharing between internal and external teams
- **Consistent user experience** for both users and administrators through a single platform
- **Ease of auditing** for policy creation, management, lifecycle, and approval workflows

CASE STUDY

A Smoother, More Secure Approach to Access Control in Financial Services

CLIENT – A major provider of tax services that serves over 29k clients across 6,000 firms and generates billions of dollars in annual revenue

PROBLEM – The client's tax offering hinges on powerful data management technology that supports data collection and reuse for the end-to-end delivery of tax services, but their legacy system was fraught with manual processes and security gaps—plus it cost too much. The client needed a better way to provide secure, flexible, and agile customer access to sensitive proprietary data.

SOLUTION –

The PlainID Authorization Platform

RESULTS –

- Seamless customer experience
- Faster time to market
- Simple platform integration with new applications and data
- Tighter, centrally managed security and control with externalized and standardized authorization



A Better, More Secure Future for Third-Party Relationships

It's no secret that the digital landscape is changing at lightspeed, and this period of dramatic transformation is changing the way businesses work together. To keep up and protect their data, enterprises need an effective authorization platform that helps them manage and grant access to third-party identities. The PlainID Authorization Platform helps enterprises rise to the challenge by mitigating risk, improving user experiences, and supporting compliance in a shifting regulatory landscape.

To learn how PlainID can help you be confident in the completeness of your Zero Trust environment, we invite you to reach out to us for a free trial.

[REQUEST A DEMO](#)



ABOUT PLAINID

PlainID, the Authorization Company, simplifies the complexity businesses face when securely connecting identities to digital assets. Powered by PBAC, PlainID provides a SaaS-based, centralized policy management platform with decentralized enforcement to manage who can access what across the enterprise technology stack; including applications, data, API, microservices and more. [Visit PlainID.com for more information.](https://PlainID.com)

© 2023 PlainID Ltd. All rights reserved. All intellectual property rights in, related to or derived from this material will remain with PlainID Ltd. Reproduction, modification, recompilation or transfer in whole or in part without written permission is prohibited. This material is made available as-is, without any implied warranties, all of which are hereby disclaimed, and PlainID Ltd. shall have no liability in relation hereto. All brand names, product names and trademarks are the property of their respective owners.