FrontierZero

CISO Guide: Third-Party Breaches

When someone else's risk becomes your own

Most organizations today manage internal security with a high degree of maturity. Identity and access controls are well established. MFA is widely enforced. Endpoint protection and monitoring are standard. Logging, audit trails, SIEM, and SOAR workflows support ongoing detection and response. In short, visibility **within** the internal environment has improved significantly across most sectors.

However, modern organizations do not operate in a closed perimeter. Business processes are distributed across **external parties**: SaaS platforms, infrastructure providers, outsourced IT, contract developers, payroll services, logistics partners, BPO support teams, marketing agencies, analytics vendors, and more. These external entities authenticate into internal systems or process internal data, often with the same level of trust as direct employees. Yet they do not fall under the same lifecycle management, policy enforcement, or behavioral oversight.

According to IBM's Cost of a Data Breach Report 2025,

- 14% of breaches originate through third-party or supply chain access.
- The average cost of a breach was $4.91M.
- They take the longest to detect and contain, averaging 267 days.

This is not due to the absence of internal controls. **It is because third-party access operates outside the core identity perimeter, where visibility is reduced and assumptions of trust remain largely unchallenged.**

Recent Incidents Illustrate the Pattern

Several recent breaches show that the point of compromise often sits outside the organization's core environment, even when internal security practices are mature.

Jaguar Land Rover experienced a major production disruption in 2025 after attackers used compromised credentials belonging to a third-party contractor. The breach stopped manufacturing operations across multiple facilities for several weeks. Although JLR's internal systems were not directly compromised, the operational impact was extensive. Industry estimates place the total financial impact at approximately **£2 billion**, primarily due to production downtime and supply chain delays.

Qantas was affected when a loyalty program services provider experienced a compromise that exposed approximately 5.7 million customer records. Qantas's internal infrastructure remained secure, but the airline still faced reputational response, customer communication demands, and regulatory obligations. The total cost associated with incident response, legal proceedings, and customer support has been widely estimated at **over $100 million**.

Marks & Spencer faced business disruption and data exposure following an incident involving outsourced IT services. The breach resulted in customer and employee data being affected and contributed to temporary e-commerce interruptions. The overall impact, including recovery and operational costs, is estimated at **over $100 million**.

Allianz Life experienced unauthorized access to policy and customer data through a Salesforce-managed CRM environment operated by an external provider. Access was gained using stolen OAuth tokens and targeted social engineering. Allianz's internal systems remained secure, but the exposure of customer records and the associated regulatory response has been estimated to cost **up to $100 million** when accounting for notification, legal review, and remediation.

Workday-related exposures across several organizations were tied to compromised external CRM and identity integrations rather than Workday's core platform. Attackers leveraged credential reuse and existing trust relationships between SaaS systems to retrieve business contact and account records. These incidents typically resulted in **over $10 million** in combined investigation, remediation, and continuity-related costs across affected organizations.

These examples reflect a shared trend: Organizations with strong internal controls can still face significant risk when external entities have trusted pathways into their environment. A **breach may occur without the organization itself being breached, simply because external access was not monitored with the same level of visibility and context as internal activity.**

Why the supply chain remains a blind spot

Although these external identities play an essential role in day-to-day operations, they often sit outside the organization's direct identity oversight. Their access is granted based on operational need, but the ongoing management of that access is rarely reviewed with the same rigor applied to internal accounts.

As a result, visibility into how these identities authenticate, what they can access, and how their behavior evolves over time is often incomplete. **This creates an area of exposure that is not immediately obvious but becomes significant when these accounts are misused or compromised.**

In practice, external identities behave differently from internal ones in several very important ways:

- They are not tied to HR or internal onboarding workflows
- Permissions are often broader than necessary to reduce operational friction
- Accounts may remain active after projects conclude
- Authentication may occur through federated identity, SSO, or OAuth rather than direct domain credentials
- Long-lived tokens may grant access without generating ongoing login events
- Vendors and suppliers vary widely in their own security posture

As a result, the organization may not have answers to fundamental questions such as:

- Which external identities are currently active
- What systems can they access
- How their access is authenticated
- Whether their behavior aligns with normal operational patterns
- Whether their credentials have been exposed elsewhere

This is where risk is introduced without being observed.

A Common Misconception

It is often assumed that attackers focus primarily on large, high-profile enterprises. However, the supply chain incidents referenced earlier did not begin inside those organizations. **They began in smaller vendors, outsourced service providers, and external platforms that held trusted access.**

The determining factor was not the size of the organization but the **ease of access**. If a smaller supplier has a weaker security posture but is connected to a larger company, then the supplier becomes a more efficient entry point.

As a result, the question is not whether an organization is “big enough” to be targeted, but whether it **connects to environments that are valuable targets**. Any organization with access to another becomes part of that organization’s attack surface, regardless of its own scale.

Establishing a pattern of life

To gain control, organizations must move beyond static access lists and periodic vendor reviews. What is required is an ongoing understanding of how external users and integrations **actually behave** in practice.

This involves establishing a **Pattern of Life:**

- Typical timeframes during which access is used
- Usual geographic and network origins
- Expected applications and permissions used in day-to-day activity
- Device or browser characteristics linked to stable usage
- MFA or strong authentication consistency
- Typical frequency and scope of administrative or privileged actions

When these patterns are understood, **deviation becomes recognizable**. External access that is technically valid but operationally irregular becomes visible in a way that does not rely on malware detection or signature matching.

This approach does not introduce friction or reduce productivity. It simply provides context that allows security teams to distinguish **routine vendor activity from potentially harmful access.**

Patterns of Life convert external access from a zone of assumed trust into one of **observable behavior.**

Common situations where baseline monitoring can change the outcome

Continuation of access after project completion
Contractors and service providers often retain access longer than necessary. This extended access can be unknowingly misused or compromised.

Shadow integration adoption
Business units adopt SaaS tools that request OAuth access into core systems. These connections often remain unreviewed and persistent.

Cascading dependencies
A supplier may depend on another service provider. Access may be indirect and difficult to trace.

Token persistence
Many integrations authenticate once, then operate indefinitely using session tokens that do not require reauthentication.

Regulatory responsibility
Data protection regulations assign responsibility to the data controller even when the breach originates externally.

Reducing exposure: practical guidance

- Maintain a current and complete inventory of all external identities, vendors, and integrations
- Classify external parties based on data sensitivity and operational privilege
- Require MFA and unified identity enforcement for all external access
- Monitor external access behavior relative to historical baseline patterns
- Detect credential exposure by monitoring breach and dark web sources
- Remove external access promptly at contract or project conclusion
- Review OAuth, API, and service integration trust relationships regularly
- Include external access in incident response exercises

The goal is not to reduce collaboration or limit vendor efficiency. It is to ensure **visibility is consistent across internal and external access paths**.

How FrontierZero supports this

FrontierZero provides continuous visibility into external identities and the systems they access. The platform:

- Identifies all external accounts across SaaS platforms and integrations
- Establishes and updates behavioral baselines for each external identity
- Detects access behavior that deviates from baseline patterns
- Identifies missing MFA enforcement and privilege drift
- Monitors for credential exposures connected to external identities
- Enables rapid restriction or removal of external access when needed

This turns vendor and third-party access from an implicit trust relationship into one that is observable and manageable.

Communicating the importance to leadership

When presenting this risk to leadership teams, it is most effective to frame it in operational terms:

- The organization depends on external parties to operate efficiently
- These external parties hold access to systems and data that are essential
- We currently lack continuous visibility into how that access is used
- Strengthening visibility reduces both breach likelihood and regulatory exposure
- This is not additional security complexity. It is the completion of access governance.

Supply chain security is no longer a matter of rare edge cases. **It is a standard component of day-to-day enterprise risk management.**

About FrontierZero

FrontierZero is the only SaaS Security Posture Management (SSPM) platform built in the UAE, created to solve a problem every modern organization faces: SaaS sprawl without visibility or control.

Founded to help compliance-driven sectors protect their most valuable assets, FrontierZero was awarded Rising Star in Cyber Defence 2025 for its innovation in securing SaaS environments in real time. Our mission is simple: give organizations the visibility and control they need to stop threats before they escalate.

With FrontierZero, you can:

- See everything — Full SaaS inventory visibility, including shadow and unapproved apps.
- Spot risks early — Detect abnormal activity, risky permissions, and MFA bypasses before they become breaches.
- Enforce security — Lock down external integrations with stronger identity and context-based controls.
- Respond instantly — Map exactly which vendor connections to cut in a breach scenario.
- Stay compliant — Continuously meet audit requirements without adding complexity or overhead.

From hidden AI tools to forgotten accounts, we reveal the blind spots others miss—helping you stay compliant, resilient, and ready for what's next.

Want to see what your Supply chain and external connections look like?

Get Your External Access Map