Teqtivity

2026 Quarterly IT Asset Intelligence Report

The Distributed Asset Problem

How Remote Work is Exposing Weaknesses in Asset Accountability



Teqtivity

Table of Contents

Letter from the Teqtivity Team 04

Executive Summary 05

The Macro Thesis: Deployment Is No Longer the Hard Part 06

Force 1: A Permanent Distributed Workforce

Force 2: Contractor and Contingent Worker Growth

Force 3: Cross-Border Deployment Complexity

Deep Dive: The Distributed Asset Problem 10

The Offboarding Gap

The Multi-Vendor Custody Problem

The Contractor Device Problem

The Security Consequence

Evidence from the Field

Teesnap: 5,000+ Leased iPads, One System, No More Guessing

Industry Signals 16

The Teqtivity View 19

How Organizations Are Responding

Lifecycle Control Starts With Ownership

One Record Across Every Entity

Cross-Border Asset Management Requires Context

Where Teqtivity Fits

Teqtivity

Table Of Contents

Looking Ahead 23

Q3 2026 Preview: The Cost of Broken Lifecycle Control

Next Steps for Your Organization

Every location. One record. No exceptions.

Appendix 25

Methodology

Data Sources

About Teqtivity

Teqtivity Asset Intelligence Q2 2026:
The Distributed Asset Problem

How Remote Work is Exposing Weaknesses in Asset Accountability

Letter from the Teqtivity Team

After the Q1 report was published, the question we kept hearing from customers was no longer, “What do we own?”

It was, “How do we maintain control when work no longer happens in one place?”

That question says a lot about where ITAM is now. Remote and hybrid work are no longer temporary conditions IT is managing through. They are part of the operating model. Among U.S. employees with remote-capable jobs, 52% now work hybrid and 26% work fully remote. Only 22% are on-site full time.[1]

The infrastructure assumptions traditional ITAM was built around, a workforce tied to an office, a known network, and a centralized return path, no longer hold.

That shift creates a different kind of pressure. **Lifecycle control gets harder when devices move continuously across geographies, vendors, entities, and employment types.** Each handoff creates another place where ownership can blur, custody can go unverified, and asset records can stop matching what is actually deployed.

This matters because the workforce is not consolidating back into a model IT can fully see from one place. **Q2 looks at what it takes to maintain accountability when the people carrying company assets, and the places they carry them, keep changing.**

Hiren Hasmukh
Founder & CEO
Teqtivity

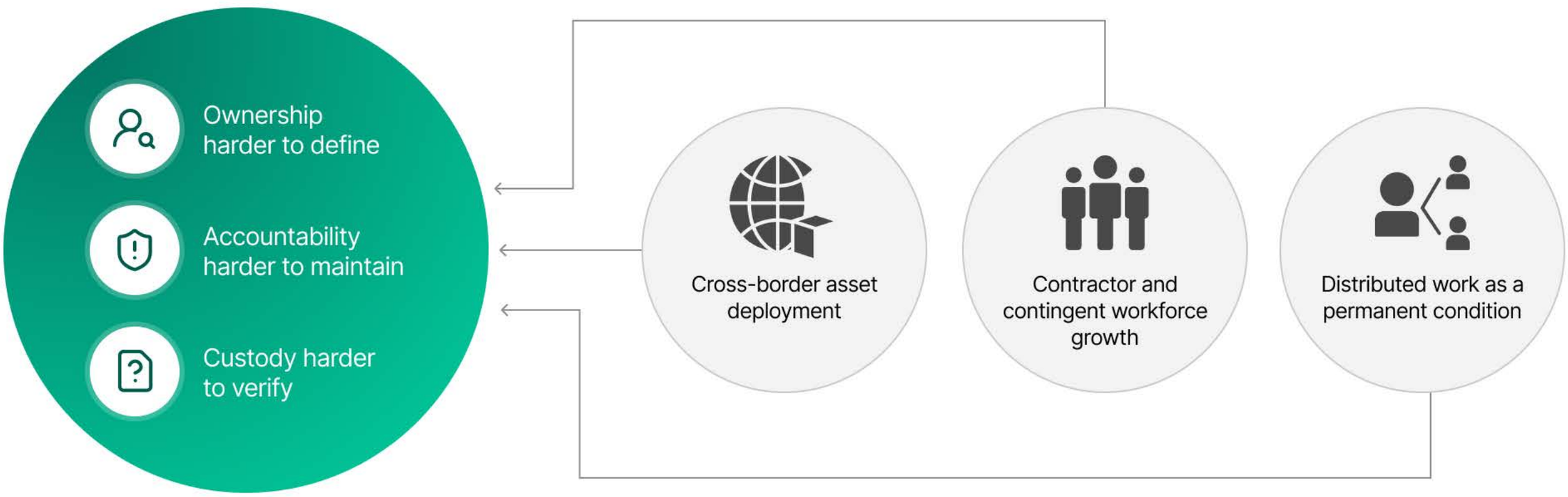
Executive Summary

Q1 showed what organizations often cannot see: hardware that exists somewhere in the business but no longer has a reliable record behind it.

Q2 looks at what happens when that hardware stays in motion.

Hybrid and remote work have settled into the operating model. Among U.S. employees with remote-capable jobs, 52% work hybrid and 26% work fully remote.[1] Asset fleets now move across home offices, contractor networks, regional teams, and international deployments that traditional ITAM programs were not built to govern.

Three forces are driving the shift: distributed work as a permanent condition, contractor and contingent workforce growth, and cross-border asset deployment. Together, they make ownership harder to define, custody harder to verify, and accountability harder to maintain across the lifecycle.



That pressure is clearest during offboarding. In a centralized environment, the office created natural checkpoints for returning devices, confirming custody, and updating records. In a distributed environment, those checkpoints disappear. Assets can remain assigned to inactive users, sit with contractors after a project ends, move between vendors, or cross entities and borders before the system of record catches up.

The result is not just a visibility problem. It is a lifecycle control problem. When organizations cannot connect each device to a current owner, location, custody history, and lifecycle state, asset records stop matching what is actually deployed.

This report examines where that mismatch begins, why it compounds, and what organizations need to regain control as work becomes more distributed, more contingent, and more global.

The Macro Thesis: Deployment Doesn't Mean Control

ITAM was built for a more centralized world.

Devices lived in offices. They sat on networks IT could see. They followed a predictable path: purchased, imaged, assigned to a desk, supported by IT, and returned when the employee left.

That no longer matches how companies operate.

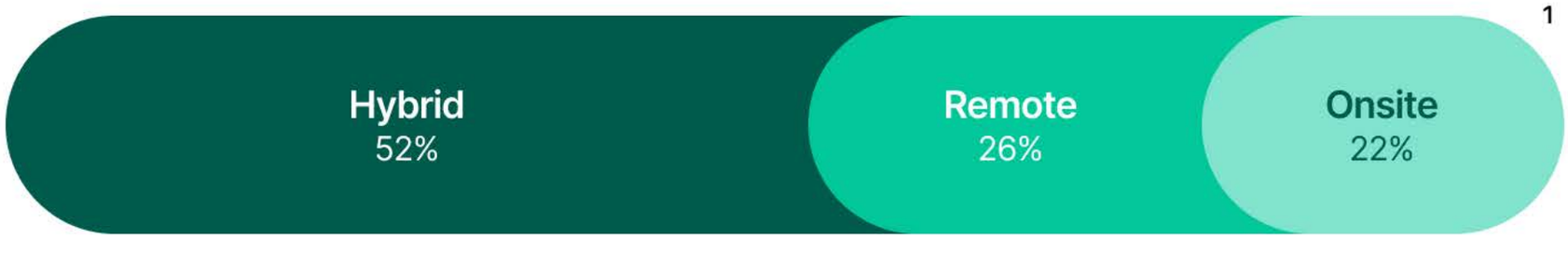
Today, devices move across homes, coworking spaces, regional offices, cost centers, legal entities, staffing partners, states, countries, regions, and borders. **The asset lifecycle did not stay in one place. It became more distributed, more fragmented, and harder to control.**

Three forces are reshaping asset accountability.

Force 1: *A Permanent Distributed Workforce*

Remote and hybrid work are part of the operating model.

Where remote-capable US employees work



[1]

The preference for flexible work has held even as labor market conditions have changed. It doesn't soften with economic pressure. Six in 10 employees who work exclusively remote say they would look for another job if that flexibility were taken away.[1]

For IT, the impact is structural.

The device fleet that once sat inside a few offices now moves with the people who use those devices, following every change of role, team, or address.

> **What used to be a fixed inventory in a fixed building is now a moving target.**

Visibility used to come from proximity: the office, the network, the storage room, and the desk.

Now visibility has to be designed into the system.

Force 2: *Contractor and Contingent Worker Growth*

Designing for visibility assumes you know who you're tracking. That assumption doesn't hold once non-employees enter the picture: **full-time employees are no longer the only people using company hardware.**

Contractors, temporary workers, consultants, vendors, and project-based teams often use devices with the same risk profile as permanent staff. They may access the same systems, handle the same data, and work from the same distributed environments.

But they are not always governed by the same onboarding, custody, and offboarding controls.

This creates an asset custody problem. When a device is issued through a staffing agency, vendor, consulting firm, or short-term project, accountability can become unclear.



1. Who approved it?
2. Who tracks custody?
3. Who retrieves it?
4. Who confirms access removal?
5. **Who is accountable if it does not come back?**

Unclear ownership allows the asset footprint to expand faster than the organization can track it. As contingent work grows, so does the number of devices IT must track, recover, secure, and account for.

Offboarding data points to the same lifecycle issue. **When access offboarding is inconsistent, hardware recovery is likely inconsistent too.**

Offboarding Risk

Indicators of lifecycle control gaps.

2

1/3

of organizations failed to offboard an ex-employee within 24 hours[5]

11%

have traced data breach to a former employee[5]

>50%

still lack lifecycle management automation[5]

Did you know?

The independent workforce has grown significantly over the past decade with freelance work rising from

2014 [3]

53 Million

Americans

2023 [4]

64 Million

or **38%** of the total U.S. workforce

2025 [5]

72.9 Million

independent workers, reflecting the broader contingent workforce

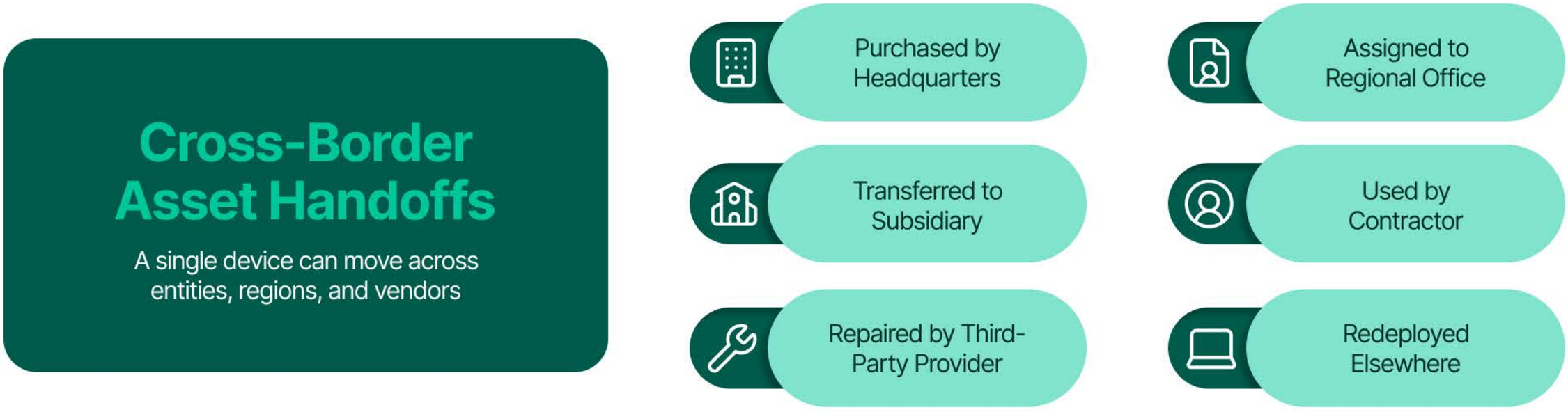
Projections show independent work continuing to expand toward a larger share of the workforce before the end of the decade.[5]

This creates operational and security exposure. Remote and contingent work models become riskier when identity, access, and asset controls are weak. In one documented threat pattern, North Korean IT workers embedded themselves in organizations as remote staff, turning weak hiring, access, and asset governance into an attack surface.[6]

Force 3: *Cross-Border Deployment Complexity*

Even when custody is clear, the rules attached to a device can change as it moves across entities, regions, and ownership structures.

Cross-border does not only mean international. A device can cross a compliance boundary by moving from one cost center or legal entity to another, each with its own tax, procurement, and reporting rules, even within a single country.



Each cross-border handoff can change the asset record. Ownership, custody, lifecycle status, entity responsibility, compliance requirements, depreciation, and recovery obligations can all shift as a device moves across teams, vendors, and locations.

Traditional asset records often break down when those changes are not captured consistently. One region may track assets one way, another team may use a different process, and an acquired company may bring an incomplete register. Some devices are purchased centrally and pushed to regional offices. Others are bought locally by separate cost centers.

Without normalized visibility, the record fragments. It becomes harder to know what the company owns, where each device is, who has custody, which entity is responsible, which rules apply, and how the asset should be recovered, redeployed, depreciated, or retired.

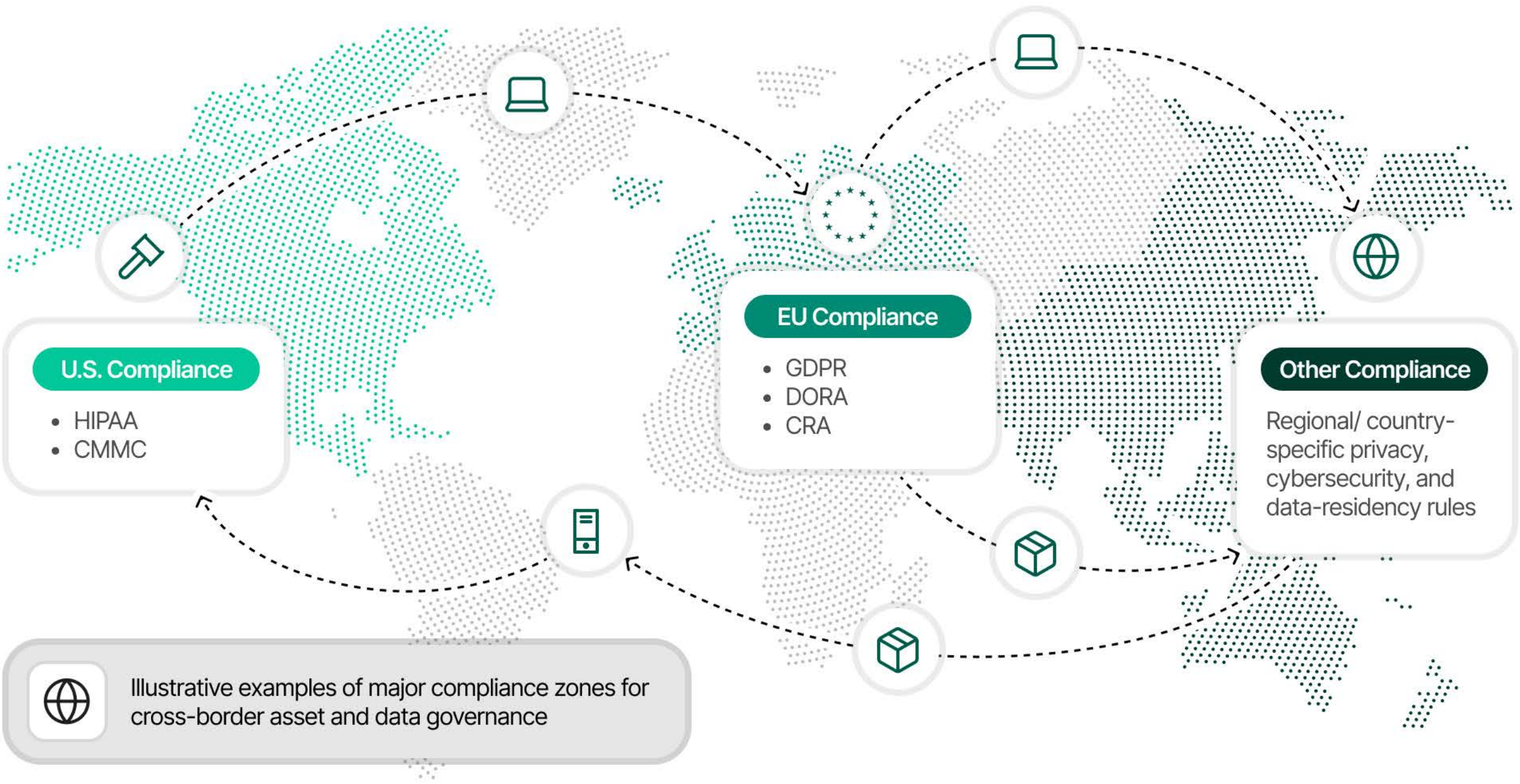
Device-as-a-Service (DaaS) providers and global logistics partners have made it easier to deploy hardware across distributed teams. **But deployment is not the same as lifecycle control.** Every additional vendor, region, entity, and handoff creates another point where asset ownership, custody, compliance context, and lifecycle accountability can fragment.

The central question is no longer whether the device reached the user. **It is whether the organization can maintain control across the device's full lifecycle, wherever it moves.**

Deep Dive: The Distributed Asset Problem

The three forces created the conditions for asset accountability to break down. Offboarding is where those conditions get tested. Every device eventually has to pass through that moment, regardless of how it entered the environment.

In Q1, the issue was ghost assets: devices that still existed somewhere in the business but no longer had a reliable record behind them. Offboarding failure is one way ghost assets are created. In Q2, that mechanism becomes harder to control. Distributed work has stretched the asset lifecycle across a wider network of people, locations, vendors, and handoffs.



That shift changes the risk.

Two failures are worth separating: access revocation and hardware recovery. Both are breaking down, but they break down in different ways. This deep dive focuses on the second failure.

A missing device is no longer just an inventory problem.

This section looks at where lifecycle control breaks down: remote offboarding, multi-vendor custody, contractor-issued hardware, and the security exposure that follows.

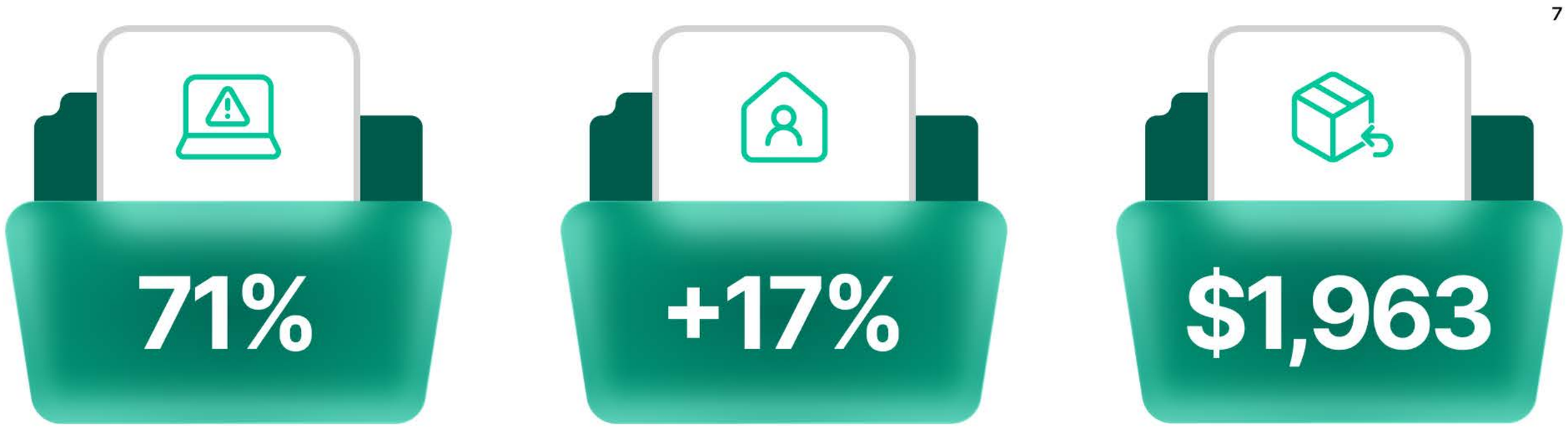
The Offboarding Gap

In a centralized office, offboarding has built-in physical checkpoints. An employee returns a badge. They clean out a desk. They hand a laptop back to IT. Even when the process is imperfect, the workplace itself creates moments where asset recovery can happen.

Remote offboarding does not have those checkpoints by default.

IT teams are expected to recover devices from employees they may never have met, across locations where they may not have direct logistics coverage, and often within a compressed timeline. That pressure increases when the departure is involuntary. The organization has to disable access, recover equipment, protect data, update records, and close the employee lifecycle without the benefit of a physical handoff.

The data confirms what many IT leaders already sense.



[7]

Remote offboarding is harder to execute than office-based offboarding. Fifty-five percent of IT and security professionals describe it as more challenging than its in-office equivalent.[8]

That gap is a structural signal. The processes built for desk-based offboarding do not automatically transfer to a distributed workforce. And once vendors and logistics partners enter the picture, that gap widens further.

The Multi-Vendor Custody Problem

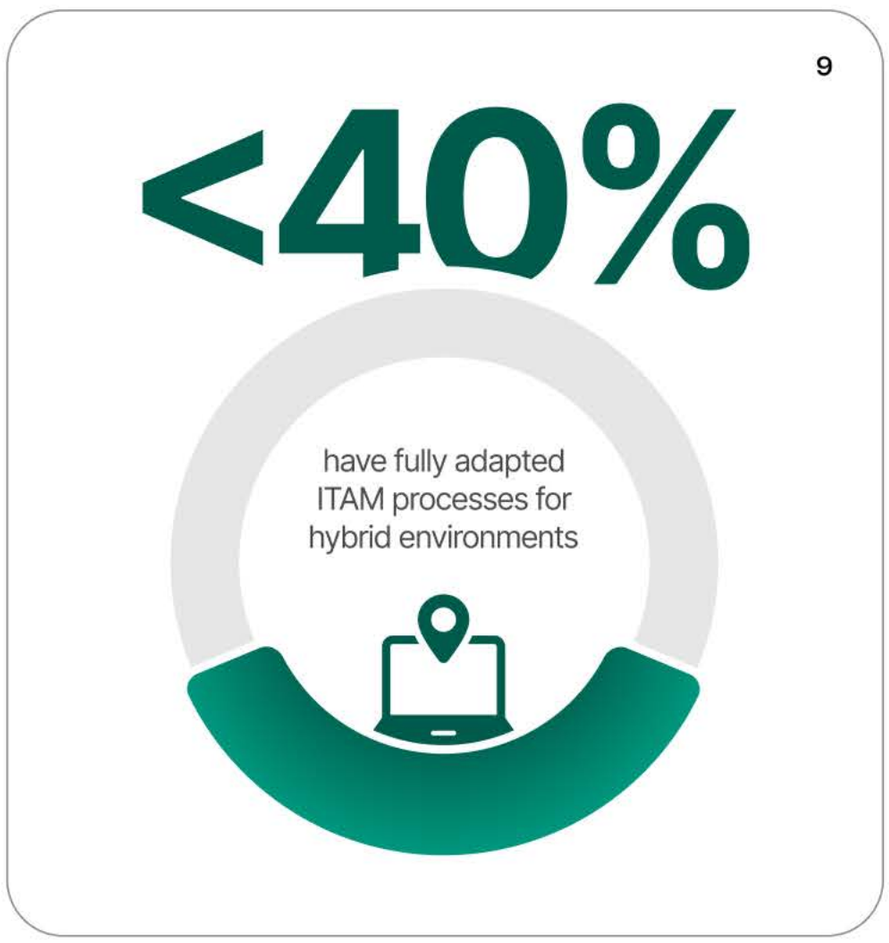
Devices now pass through more hands before and after employee use. A DaaS provider may prepare and ship the device. A logistics partner clears it through customs. A local vendor images or configures it. Later, a retrieval vendor may collect it for storage, repair, redeployment, or disposal.

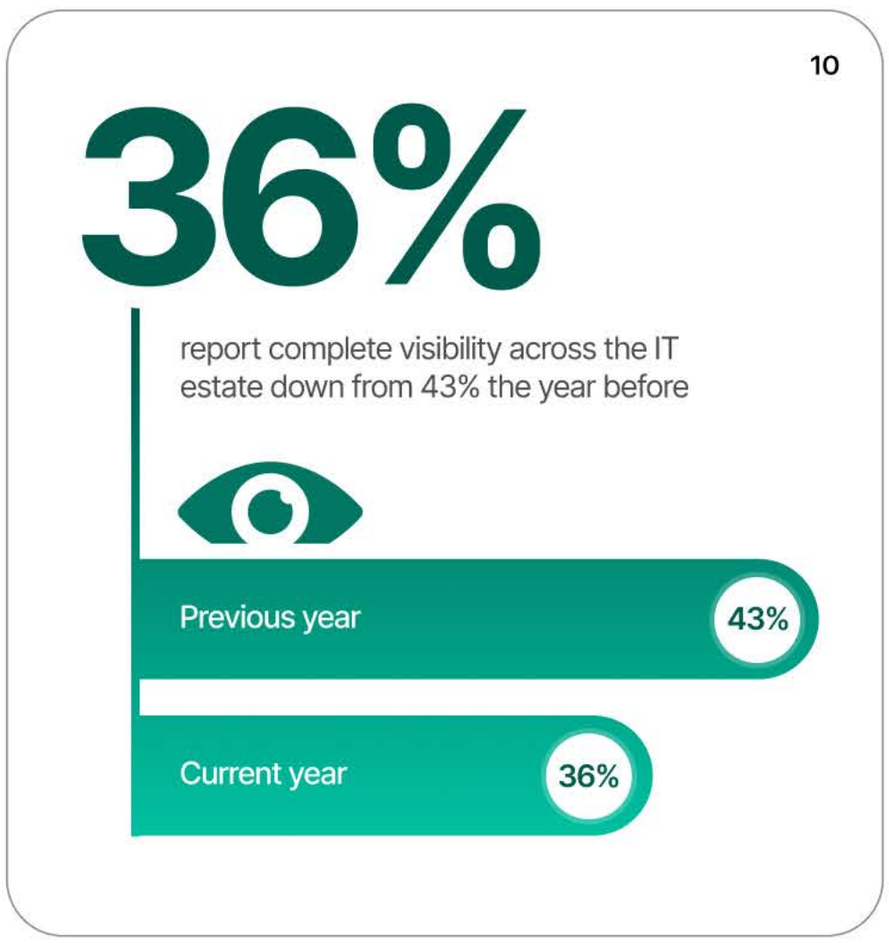
Each handoff also creates a moment where custody, ownership, lifecycle status, and compliance context need to be updated.

In practice, that record often lags behind the movement of the device.

When a retrieval vendor collects a laptop but the ITAM system does not reflect it, the device still appears to be missing. IT follows up with the employee. The employee points to the courier. The courier points to the retrieval record. The device may be physically moving through the right process, but the system of record has fallen behind.

This is where a logistics issue becomes an accountability problem. The scale of that problem shows up in the data.





Together, those numbers point to the same failure from two angles: asset movement has outpaced process design, and visibility remains inconsistent even as ITAM tooling expands.

As the lifecycle becomes more distributed, custody control becomes more important. A system that cannot track every handoff, status change, entity, region, and responsible party leaves organizations with partial records and unclear accountability.

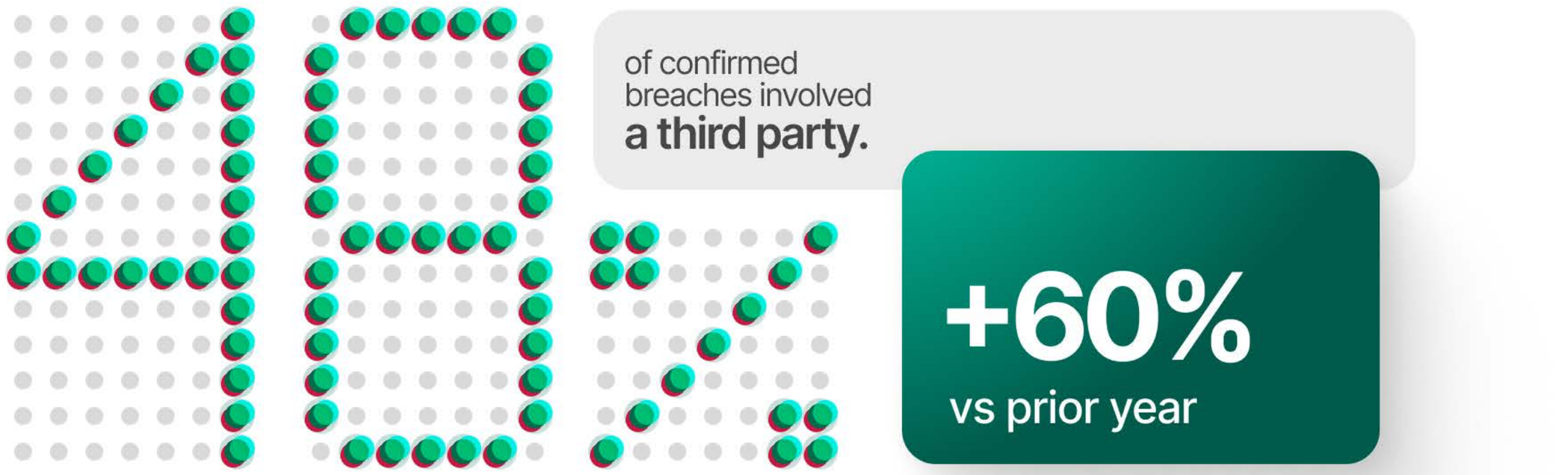
The Contractor Device Problem

The custody problem described above assumes an employee is at least visible inside the ITAM system, even if the device has moved faster than the record. Contractors often fall outside that visibility model.

Contractors, consultants, vendors, and temporary workers may receive the same laptops, monitors, and mobile devices as full-time employees. They may access the same systems, handle the same data, and work across the same distributed environments. But they are not always governed by the same lifecycle process.

When a full-time employee leaves, HR, IT, and finance typically have some coordinated process, however imperfect. When a contractor engagement ends, device retrieval often shifts to the team that owns the vendor relationship. That may be procurement, finance, a business unit leader, or a regional team rather than IT.

If the device was provisioned outside standard onboarding channels, the problem starts even earlier. It may have been purchased by a department, shipped through a third party, assigned by a vendor, or tracked in a spreadsheet outside the central asset record. At that point, IT is not behind on the record. **The device may not be in the record at all.**



This figure is not specific to contractors. It measures third-party risk generally, and contractor-issued devices are part of that category.[6] Nearly half of confirmed breaches trace back to a third party, and that third-party surface keeps growing. Unmanaged contractor hardware is not an edge case. It is one of the clearest examples of the broader accountability problem.

Contractor-issued devices turn third-party risk into an asset accountability problem.[6] Without a shared system of record, hardware, access, custody, and vendor responsibility can sit outside IT's normal controls, tracked only by the team or contract owner closest to the relationship.

The Security Consequence

Each breakdown leads to the same outcome.

Remote offboarding checkpoints that do not exist. Custody records that trail the device. Contractor hardware that was never fully tracked. Three separate failures create one shared outcome: incomplete visibility into the devices that still carry business risk.

An unretrieved or unmanaged device is more than missing equipment. It is an active endpoint that may still hold company data, credentials, and access to internal systems.



The hardware exposure alone can be significant. Based on the data, Teqtivity estimates that for organizations managing managing 10,000 devices, a 5%–15% unreturned device rate can represent approximately $1 million to $2.9 million in unrecovered hardware value each year, based on an average value of $1,963 per unreturned device. The security consequences can extend well beyond that replacement cost.

The risk is already visible. Unreturned devices often still contain sensitive information, while many organizations cannot fully lock former employees out of the equipment.[7] Together, those realities point to the same conclusion: **when a device is not recovered, the organization may lose control of the data and access attached to it.**

A related pattern appears in unmanaged and BYOD environments, where infostealer malware compromised credentials on 46% of devices carrying corporate logins.[11] The issue is not only ownership. It is visibility.

Lifecycle control is now a security requirement. Forty-two percent of IT and security professionals struggle to make informed security decisions about the devices accessing their network and corporate resources.[12]

If an organization cannot confirm offboarding, reconcile custody, or see contractor hardware, it cannot clearly account for the devices in its environment. And it cannot secure what it cannot see.

Distributed work exposed the limits of asset processes built around office-based handoffs, manual follow-up, and incomplete records. That is the breakdown at the lifecycle level. The next section shows how it appears across industries.

Evidence from the Field



Teesnap: 5,000+ Leased iPads, One System, No More Guessing

In wheel-and-spoke environments, where thousands of assets move through deployment, return, and redeployment, a logistics problem becomes an accountability problem the moment the system of record no longer reflects where the device actually is.

Teqtivity gave Teesnap a single source of truth for custody and location, replacing the guesswork.[13]

Result

Custody and location, always current, always in one place.

- Deployment-to-return visibility for every leased device.
- Automatic status updates through Shipstation and UPS.
- Device history linked to support tickets through HubSpot.

> **It's almost bulletproof now. Unless a customer loses a device, we can't lose it anymore.**
>
> Cole Christensen, Teesnap

Industry Signals

The asset accountability problem shows up differently by sector, but the pattern is consistent. Devices now move across distributed environments faster than many asset records can keep up.

The result is uncertainty around custody, access, ownership, compliance context, and recovery.

Industry	Signal Evidence indicating scale or direction of issue	Structural Context Environment in which asset governance operates	Business Impact Consequences when lifecycle control breaks down	Strategic Pivot Direction organizations take to restore control
Financial Services	• Financial-sector oversight, including requirements under DORA, increasingly depends on device-level evidence and operational proof. • 52% of financial organizations lack full visibility across users, assets, infrastructure, and applications.[14] • Nearly 9 in 10 financial institutions report material impact events and noncompliance penalties tied to fragmented IT environments and poor data lineage.[14]	• Home offices • Branches and advisor networks • Regulated workflows • Audit-heavy environments	• Audit teams spend more time reconstructing device history from spreadsheets, tickets, HR records, and manager confirmations. • Control exceptions increase when teams cannot prove which devices accessed regulated data. • Regulatory and reputational exposure grows when device-level evidence is incomplete.	• Maintain a device-level audit trail that connects each laptop to its owner, user, location, access status, custody history, and lifecycle state. • Use dashboards and reports to surface devices that are missing required controls, assigned to inactive users, or overdue for review. • Standardize device attestation and reconciliation before audits, access reviews, employee transfers, and offboarding.
Global Enterprises	• Global enterprises face the most complex custody environment. • More than 35 million people work in large-scale multinational enterprise groups across EU and EFTA countries.[15] • The world's 500 largest MNEs are matched to more than 130,000 subsidiaries.[16] • 67% of IT leaders say they lack complete visibility into all work devices.[17]	• Remote teams • Regional offices and subsidiaries • Vendors and logistics partners • Local procurement and M&A • Jurisdiction-specific compliance rules	• Leadership cannot get a reliable view of what is owned, assigned, supported, governed, or recoverable across regions. • Reporting slows when regional, vendor, and local procurement records do not match. • Security and compliance decisions become harder when ownership, custody, and device status are fragmented.	• Create a normalized asset record across regions, entities, vendors, locations, and lifecycle stages. • Track ownership, custody, region, legal entity, cost center, compliance context, and recovery status in one system of record. • Use role-based dashboards, audit trails, and workflow automation so regional teams can act locally while leadership retains global visibility.

Industry	Signal	Structural Context	Business Impact	Strategic Pivot
Healthcare	• The same device used by multiple nurses may be tracked in the facilities system, the MDM, and the ITAM platform, or in none of them consistently. • 44% of healthcare facilities lack comprehensive shared-device policies.[18] • Over 60% of health systems cite significant limitations in protecting unmanaged medical devices.[19] • Healthcare breach cost averages $7.42M.[20] • Without asset tracking, 23% of shared-use mobile devices are lost annually.[18]	• Shift-based clinical work • Devices moving between departments, facilities, carts, clinicians, and care teams • Asset records split across facilities systems, MDM tools, ITAM platforms, and informal handoffs	• Clinicians lose time finding usable devices during shifts. • IT teams spend more time reconciling conflicting records across systems. • Security teams have less confidence that shared endpoints are patched, monitored, and recoverable.	• Create a shared-device record that tracks location, custodian, assignment state, lifecycle status, and last verified activity. • Use lifecycle workflows to document device handoffs, department transfers, repairs, redeployments, and retirement. • Connect ITAM records with MDM, support, and facilities data so shared clinical devices do not disappear across systems.
Technology & SaaS	• Tech companies scale faster than their asset processes. • Remote-capable tech employees are 47% fully remote and 45% hybrid.[21] • The freelance and contingent workforce referenced earlier, 64 million Americans, 38% of the U.S. workforce, as of 2023,[3] grows fastest inside tech.	• Fast hiring • Remote onboarding • Contractor-heavy teams • Global shipping • Project-based work	• IT buys replacements while recoverable devices sit with former workers, inactive contractors, or teams that no longer need them. • Unrecovered devices and licenses create budget leakage. • Live access risk increases when device recovery and access removal are not tied to worker status changes.	• Tie asset assignment, shipment, reassignment, and recovery to onboarding, role changes, contract end dates, and offboarding workflows. • Trigger device recovery, reassignment, lock, wipe, or deactivation when employment or contractor status changes. • Give IT, HR, finance, and security a shared view of assigned devices, open recovery tasks, overdue returns, and available inventory.

Industry	Signal	Structural Context	Business Impact	Strategic Pivot
Education & Research	• Distributed learning expands the number of locations where devices must be tracked, recovered, and reused. • 53.8% of postsecondary students were enrolled in distance education courses in fall 2024.[22] • One large district reported up to 77,000 lost or stolen devices in a single year.[23]	• Students and faculty • Departments, campuses, homes, labs, and libraries • Limited IT teams • Academic-year turnover cycles	• Schools overbuy during refresh cycles because device status is unclear. • Funding decisions become harder to defend when inventory counts are unreliable. • Devices that could be recovered, repaired, or reused remain lost in department-level processes.	• Use check-in and check-out workflows for laptops, tablets, loaners, and lab equipment, with each assignment tied to a person, department, location, and due date. • Build recovery workflows around semester starts, semester ends, graduations, staff transitions, and refresh cycles. • Use reporting to verify counts, identify overdue assets, confirm available inventory, and support funding or audit reviews.

The signal across sectors is clear: **distributed work has outgrown traditional asset tracking.**

Asset accountability now requires a current, trusted record of control that connects every device to its owner, user, location, access status, recovery path, and business context.

ITAM needs to move beyond static inventory and support lifecycle intelligence. The strategic pivots above point toward the same underlying capability, no matter the industry. The next section looks at what that capability requires in practice.

The Teqtivity View

How Organizations Are Responding

Lifecycle Control Starts With Ownership

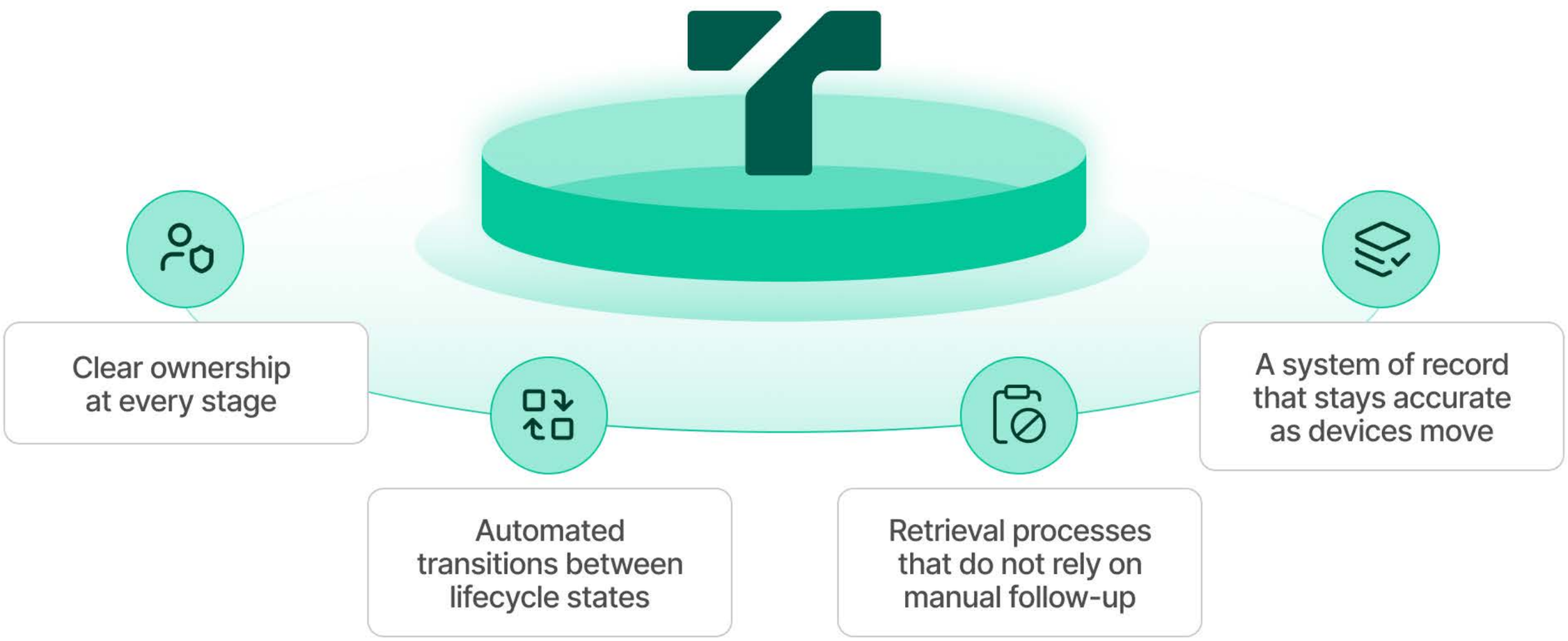
Deployment got easier. Ownership didn't get clearer along with it, and that gap is where the record starts to drift from what's actually deployed.

But solving the logistics problem does not solve the control problem.

Every vendor, entity, region, and handoff creates another point where ownership can blur, custody can go unverified, and the asset record can fall behind.

The organizations responding well begin by defining responsibility across the lifecycle. Who is accountable while a device is assigned to a contractor? Who owns the next action when it moves to another entity or region? Who assumes custody when a logistics partner collects it?

Once ownership is clear, the system can enforce it. Custody can be updated, recovery triggered, responsibility assigned, handoffs documented, and overdue actions escalated.



Effective lifecycle control depends on four things: clear ownership at every stage, automated transitions between lifecycle states, retrieval processes that do not rely on manual follow-up, and a system of record that stays accurate as devices move.

One Record Across Every Entity

Distributed asset environments rarely follow one procurement model.

In a hub-and-spoke model, headquarters purchases centrally and sends hardware to regional offices. Decentralized procurement creates a second path, with devices entering through local cost centers. Acquisitions introduce separate asset registers, naming conventions, and control gaps. Contractors may receive hardware through staffing partners or business units outside all three.

The result is fragmented visibility. A device may exist in a regional system, spreadsheet, or vendor record without being connected to the broader asset estate.

Lifecycle control requires normalized visibility across entities, locations, vendors, cost centers, and procurement models. Without it, regional teams make calls leadership can't see, and leadership sets policy it can't verify on the ground.



Cross-Border Asset Management Requires Context

Global compliance is often treated as a checklist: GDPR in Europe, CCPA in California, and WEEE for disposal. That model assumes the asset stays put.

Cross-border asset management is not limited to international movement. A device can cross a meaningful boundary when it moves between countries, states, subsidiaries, legal entities, cost centers, or operating units.

That movement may change the responsible entity, depreciation treatment, taxation requirements, reporting obligations, disposal rules, and compliance context.



This movement may change:

- Responsible Entity
- Depreciation Treatment
- Taxation Requirements
- Reporting Obligations
- Disposal Rules
- Compliance Context

A device moving from a U.S. entity to a UK subsidiary should be tracked according to where it is now, not only where it originated.

This requires jurisdiction-level visibility into entity ownership, custody history, lifecycle status, depreciation, taxation, and disposal. It also supports the device-level evidence needed for frameworks such as GDPR, CCPA, DORA, NIST, and WEEE.

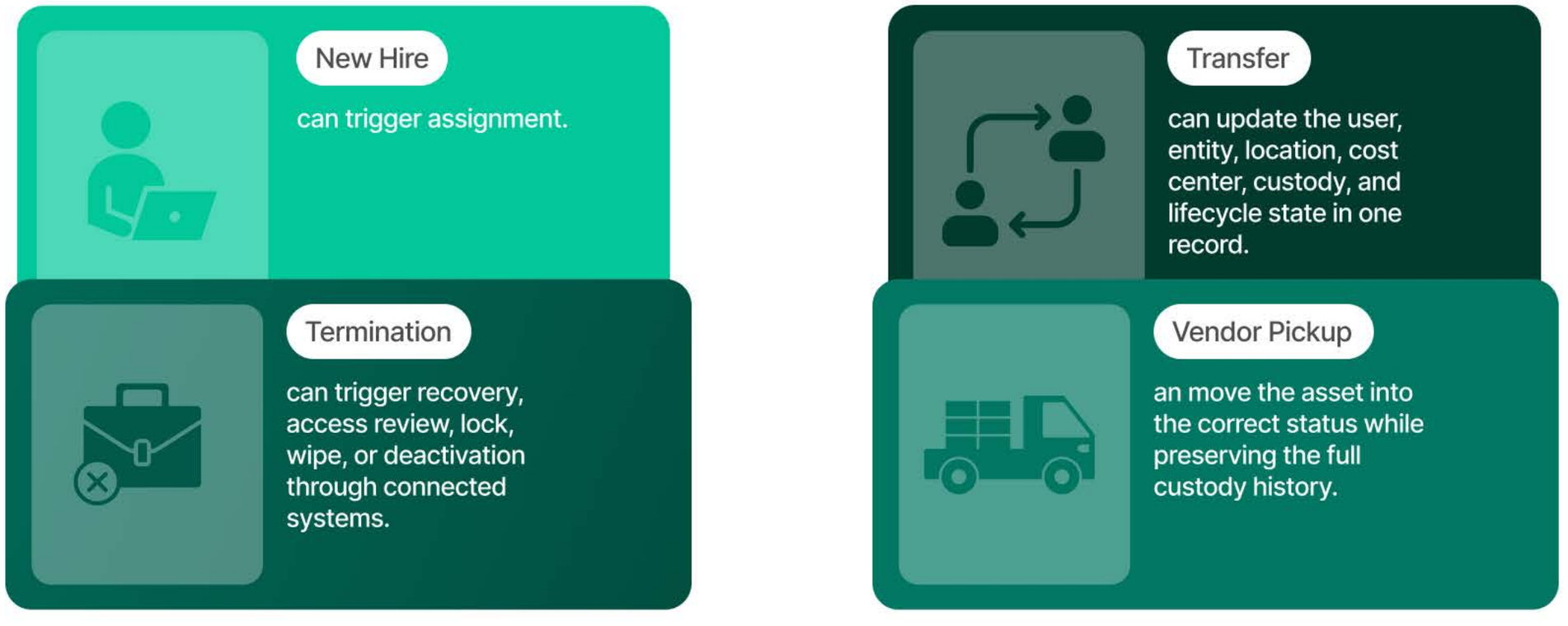
The record gives compliance and finance teams what they need to apply the right rules: where the device is, which entity is responsible, how it moved, and which lifecycle actions were applied.

Where Teqtivity Fits

Control is won or lost at the transition points.

Teqtivity operates where asset accountability is most likely to break: onboarding, offboarding, employee and contractor transfers, cross-border deployment, vendor collection, repair, redeployment, storage, and retirement.

The platform does more than record those events after they happen. **It connects lifecycle changes to automated workflows.**



Teqtivity normalizes asset data across HR, MDM, identity, service desk, procurement, logistics, and regional records. Entity management provides one structure for headquarters, subsidiaries, acquired companies, cost centers, and locally purchased assets. Cross-border movements retain the jurisdiction, depreciation, taxation, disposal, and compliance context attached to the device.

Connected workflows keep the asset record accurate as devices move.

Role-based dashboards, audit trails, and reporting allow regional teams to act locally while leadership maintains visibility across the full estate. Automated workflows surface inactive-user assignments, overdue returns, missing controls, open recovery tasks, and assets ready for reassignment.

Unlimited asset pricing also means contractor devices, regional fleets, acquired inventories, shared equipment, and lower-value hardware do not have to remain outside the system of record.

This is the difference between recording inventory and controlling the lifecycle. Teqtivity keeps ownership, custody, status, and accountability current as devices move.

Looking Ahead

Q3 2026 Preview: The Cost of Broken Lifecycle Control

Q2 established where lifecycle control breaks down: remote offboarding without physical checkpoints, custody records that lag behind multi-vendor handoffs, contractor-issued hardware tracked outside standard channels, and assets moving across regions and legal entities without a single accountable record.

Q3 shifts from where control fails to what that failure costs.

As distributed work becomes permanent, asset visibility is no longer only an IT concern. It now shapes how organizations understand technology spend, recover value, prepare for audits, and manage security exposure. A device can appear as purchased in finance, assigned in IT, shipped through logistics, and still unresolved during offboarding weeks or months after an employee or contractor is gone. Each record may be accurate within its own system, but none provides the full lifecycle picture on its own. Those unreconciled records are where cost hides.

For CFOs and IT leaders, the issue is technology spend without lifecycle context. Organizations may be buying new devices while usable assets sit idle, renewing software tied to former employees or contractors, or paying for support, warranties, storage, logistics, and DaaS services without a clear view of whether the underlying asset is still assigned, in use, recoverable, or already outside their control.

The Q3 report will examine what broken lifecycle control costs organizations across unrecovered devices, labor hours, software waste, audit exposure, and security risk, and what it takes to restore lifecycle visibility before those costs are priced by finance, auditors, insurers, or regulators.

Next Steps for Your Organization

Organizations are approaching this challenge from different starting points. Some are still assessing their exposure. Others are already seeing the effects through delayed offboarding, contractor devices outside standard processes, and unresolved assets moving across regions or legal entities.

The next step is to understand where lifecycle control is weakening inside your own environment.

For organizations still defining the problem, review offboarding workflows, custody records, and asset ownership across distributed and contingent teams. Control gaps often become visible only when a real device handoff is traced from assignment through recovery.

For teams evaluating solutions, the focus should be on how well lifecycle control holds up across remote offboarding, vendor handoffs, and cross-border asset management. The objective is to assess operational fit, not compare features in isolation.

For organizations ready to move forward, a focused working session can help define rollout priorities, pilot structure, and the metrics needed to demonstrate stronger lifecycle control to leadership, auditors, and other stakeholders.

Every location. One record. No exceptions.

Remote offboarding, multi-vendor custody, and cross-border movement all create the same vulnerability: the loss of a clear, accountable asset record.

Start the next step

Request a lifecycle audit conversation: **https://www.teqtivity.com/get-started**

Email: **hello@teqtivity.com**

Appendix

Methodology

This report draws on publicly available industry research, Teqtivity customer observations, and third-party workforce, compliance, and asset lifecycle data to identify structural patterns shaping IT asset management in 2026. Sources include distributed workforce studies, contingent labor trend reports, cybersecurity reports, asset recovery data, cross-border asset management and compliance frameworks, and enterprise IT asset lifecycle research.

Rather than presenting isolated statistics, the analysis focuses on how these signals interact at enterprise scale. Permanent distributed work, contingent workforce growth, multi-vendor custody chains, contractor-issued hardware, delayed offboarding, and cross-border asset management complexity were examined together to understand where governance pressure is increasing and where operational control tends to weaken.

Particular attention was given to the conditions that cause asset records to drift from what's actually deployed. These include devices moving across regions, employees, vendors, legal entities, storage locations, and recovery partners without a single accountable record that follows the asset from deployment through return, redeployment, or disposal.

Signals were evaluated for consistency across multiple third-party sources and cross-referenced against patterns observed across Teqtivity's customer base. These observations are used to inform the operational lens of the report and are presented as qualitative context, not statistical findings.

This report is not a product brief or a workforce trend digest. It is a structural assessment of lifecycle control maturity under distribution pressure. Data points drawn from publicly available research are cited accordingly. The analysis reflects Teqtivity's interpretation of these signals and is intended to highlight the operational patterns that shape lifecycle intelligence across modern IT environments.

Data Sources

[1] Gallup. Indicator: Hybrid Work. Accessed June 2026.

[2] Cloud Security Alliance. State of SaaS Security Report 2025. April 21, 2025.

[3] Upwork. Upwork Study Finds 64 Million Americans Freelanced in 2023, Adding $1.27 Trillion to the U.S. Economy. December 12, 2023.

[4] MBO Partners. State of Independence 2025. 2025.

[5] Upwork (projection data from Statista). Freelancing Stats: Market Size, Earnings, and Future Trends. 2026.

[6] Verizon. 2026 Data Breach Investigations Report. 2026.

[7] Capterra. HR Says Ex-Workers Ghost Exit Interviews, Steal Equipment. January 31, 2023.

[8] Secureframe (citing Gartner Peer Insights data). A Guide to Onboarding and Offboarding Employees for Risk Prevention. 2024.

[9] Deloitte. IT Asset Management Global Survey 2025. November 20, 2025.

[10] Flexera. 2026 State of ITAM Report. June 2026.

[11] Verizon. 2025 Data Breach Investigations Report. April 2025.

[12] Ivanti. 2024 State of Cybersecurity Report. May 2024.

[13] Teqtivity. Solution Spotlight: Teqtivity for Teesnap.

[14] Forrester, commissioned by Akamai. Opportunity Snapshot: Financial Services. 2024.

[15] Eurostat. Employment in Large-Scale Multinational Enterprise Groups. 2024 data.

[16] OECD / United Nations Statistics Division. Monitoring Multinational Enterprises: How the OECD and UNSD Are Harnessing Open Data. February 21, 2025.

[17] ITPro. IT Leaders Are Facing Major Work Device Blind Spots — and It's Putting Security at Risk. 2025.

[18] Imprivata. The 2025 State of Shared Mobile Devices in Healthcare Report. 2025.

[19] Elisity / HIMSS Market Insights. HIMSS Survey: 60% of Health Systems Can't Protect Unmanaged Medical Devices (The Implementation Paradox, 2026).

[20] IBM. Cost of a Data Breach Report 2025.

[21] Gallup. Hybrid Work in Retreat? Barely. September 3, 2025.

[22] National Center for Education Statistics, U.S. Department of Education. IPEDS Trend Generator: Distance Education Status of Students. 2024.

[23] WBEZ Chicago. CPS Reports Up to 77,000 Computers Lost or Stolen in a Year. January 9, 2024.

About Teqtivity

Teqtivity provides an IT asset management platform built to support operational control across growing technology environments. By centralizing asset records and structuring lifecycle processes, the platform enables organizations to maintain visibility, accountability, and reliable data across distributed teams and complex device estates.

Teqtivity is designed to remain consistent as organizations scale, with unlimited asset tracking and full platform capabilities available from the start.