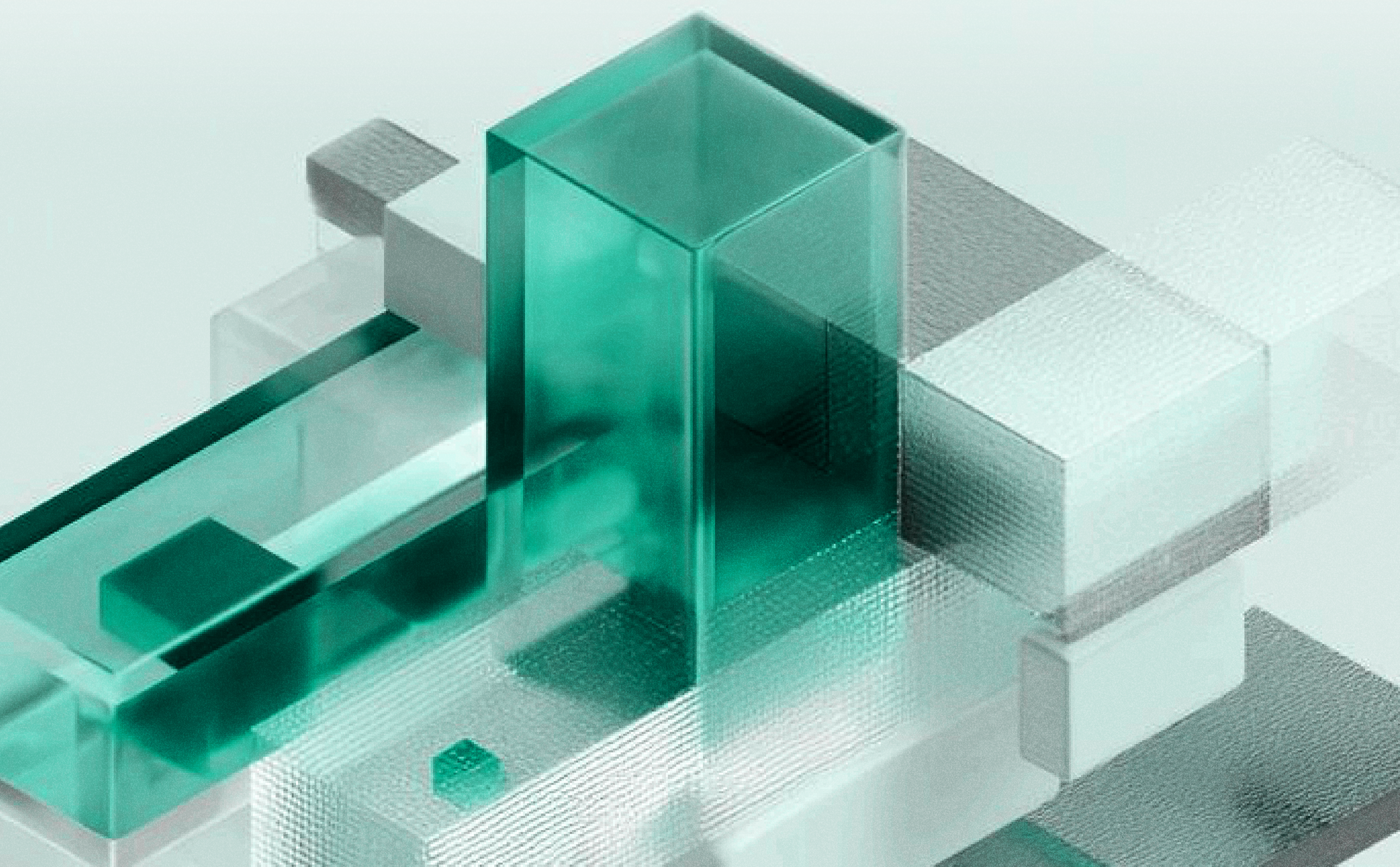
Teqtivity

2026 Quarterly IT Asset Intelligence Report

The Ghost Asset Crisis

How Inventory Drift Is Reshaping IT Governance



Teqtivity

Table Of Contents

Teqtivity

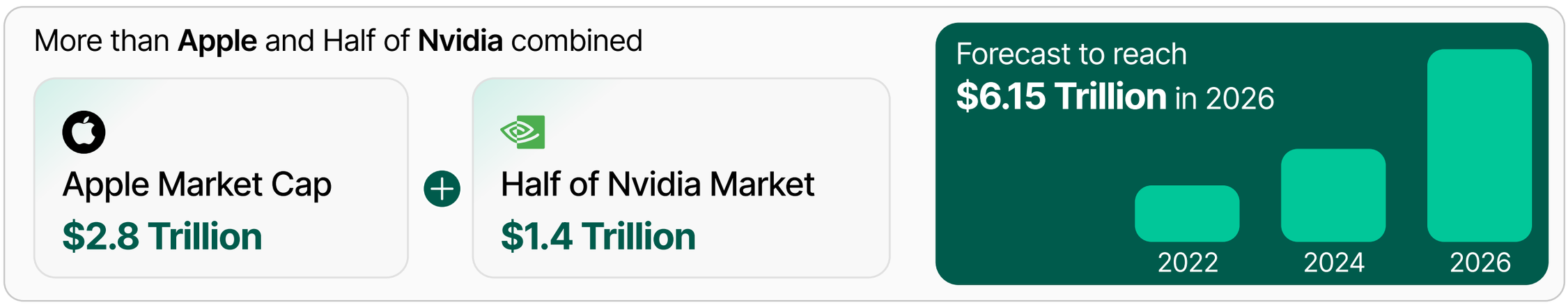
Table Of Contents

2026 Quarterly IT Asset Intelligence Report - The Ghost Asset Crisis

Letter From The Teqtivity Growth Team

IT spend keeps rising. Control is not keeping pace.

Worldwide IT spending is forecast to reach **$6.15 trillion in 2026**.[1] Yet across many organizations, a basic operational question still goes unanswered: *what devices actually exist, who has them, and where are they right now.*



This is a foundational control problem, not a clerical one. When device records drift from reality, the consequences show up everywhere: **delayed rollouts, duplicated purchases, offboarding exposure, audit friction, and slower incident response.**

This report marks the beginning of Teqtivity's 2026 IT Asset Intelligence quarterly series.

What IT Asset Intelligence Means

IT Asset Intelligence is the operational capability to maintain a trusted, decision-grade view of company-owned devices across their full lifecycle, including what exists, who is responsible for it, where it is, and whether it is fit for use and compliant with company policy.

This is not a report about acquiring more tools. It is a report about operational control.

What to Expect in the 2026 Series

Each quarter will go deep on a single theme and publish predictions that we will revisit & evaluate over time.

Q1 addresses the foundational issue: hardware visibility and ghost assets. Subsequent quarters will build on that foundation, examining consolidation pressures across IT stacks, AI-era governance, and the growing demand for audit-grade lifecycle proof.

Executive Summary

In my conversations with technology leaders, the same uncertainty still surfaces. What devices actually exist in the environment? Who has them? Where are they right now?

Those questions sound simple. In many organizations, they are surprisingly hard to answer.

That gap between asset records and operational reality is one of the problems we set out to solve with Teqtivity. It is also why we are publishing this quarterly series on IT asset intelligence.

When we first began working with organizations on asset lifecycle control, lost or untracked devices were often treated as background noise. Something to reconcile during the next inventory cycle or audit. As environments expanded across locations, contractors, and distributed teams, small gaps in asset custody began to compound.

This Q1 report focuses on a pattern we see repeatedly across organizations: ghost assets and the widening drift between asset records and reality. Rather than presenting another set of statistics, this report connects several signals that emerge as device volume, operational velocity, and organizational complexity increase.

These patterns appear across industries, company sizes, and technology stacks. They point to a broader control challenge. As technology environments scale, governance often evolves more slowly than the infrastructure it is meant to manage.

In our work with organizations ranging from high-growth SaaS companies to global enterprises, the teams that make the most progress approach the problem differently. They do not rely on periodic cleanup. They build control into the way devices move through the organization.

This report explores the signals behind ghost assets, the structural forces accelerating them, and the governance models beginning to emerge in response. I hope this report proves useful as you evaluate your own environment and consider the next steps toward stronger asset governance.

Hiren Hasmukh
Founder & CEO
Teqtivity

The Macro Thesis: Why 2026 Is The Inflection Point

The $6.15T Inflection Point

In 2026, worldwide IT spending is forecast to reach **$6.15 trillion,** a 10.8% increase year over year.[1]

That growth reflects more than budget expansion. It signals a fundamental shift in how infrastructure is created, distributed, and governed. It reflects expanding AI systems, software-defined operations, and workforce decentralization at a scale that legacy governance models were not designed to manage.

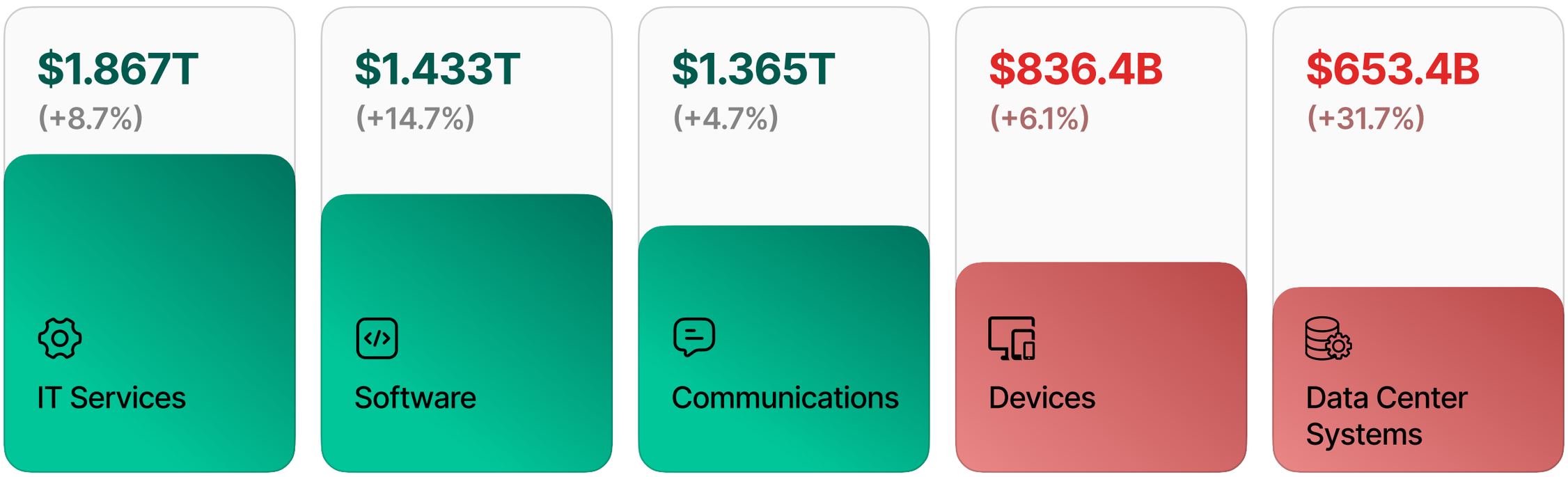
The challenge is no longer capital allocation, but maintaining governance at scale.

Infrastructure is evolving faster than most organizations can maintain a trusted understanding of what they already own, where it resides, and who is accountable for it.

2026 marks the inflection point.

Spend Is Accelerating Upstream

The 2026 budget mix[1] reveals an important imbalance:



The fastest growth is in upstream categories: compute, infrastructure, and software. These are the engines powering AI deployment, automation, analytics, and digital expansion.

Device spend, where work is actually executed, is growing far more slowly.

This asymmetry has a practical consequence.

> **Every dollar invested upstream ultimately depends on an endpoint to deliver value.**

AI tools, SaaS platforms, security controls, identity systems, collaboration software: all of it terminates at a device.

If the accuracy of device records does not keep pace with the rate of infrastructure change, organizations create a structural imbalance:

> **Organizations are funding capability faster than they can govern it.**

Three Structural Forces Converging in 2026

Three long-horizon shifts are colliding in 2026. Each is manageable alone. Together, they expose the same structural weakness: organizations are building on device data they cannot fully trust.

Technology deployment is accelerating

Infrastructure and software spending are expanding rapidly, with data center systems growing 31.7% and software 14.7%.[1] Every rollout assumes accurate device knowledge. When records drift, coverage becomes uneven, configurations diverge, and unmanaged endpoints persist beyond enforcement.

Remote work is the baseline

Devices now move continuously across geographies, teams, and environments, dissolving the perimeter that once anchored endpoint visibility. With global device spend projected to exceed $836 billion,[1] governance complexity is structural, not temporary.

Compliance failures are getting expensive

Compliance frameworks increasingly require proof that controls were applied to specific devices at specific points in time. When inventories, ownership, and custody records cannot withstand scrutiny, visibility gaps become measurable exposure.

Individually, these forces are **manageable**. **Together**, they **eliminate the margin** for assumed accuracy and make lifecycle governance foundational to execution.

Three Conditions of Effective Execution

Spending alone does not produce outcomes. Execution at 2026 scale requires three structural conditions:

1. Visibility

A real-time, trustworthy view of what exists, where it is, and what state it is in. Not what was true at the last audit. What is true now.

2. Accountability

Clear custody and ownership across the lifecycle. Who has the device, who is responsible, and what happened between assignment and return.

3. Enforceability

The ability to act on that truth: target deployments precisely, recover assets consistently, retire devices with documented evidence, and produce proof on demand.

> **If any one of these weakens, infrastructure velocity becomes liability when device visibility breaks.**

The cost is not theoretical. It appears in:

- delayed rollouts
- unmanaged endpoints
- duplicated spend
- audit failures
- regulatory non-compliance
- increased exposure during security incidents

The Strategic Constraint of 2026

Device visibility is no longer an operational hygiene metric. It is a strategic constraint.

You cannot deploy what you cannot target.

You cannot secure what you cannot account for.

You cannot demonstrate compliance for assets you cannot trace.

You cannot forecast cost or demand against inventory you do not trust.

The $6.15T moment makes one thing clear:

> **In 2026, complexity scales automatically. Control does not.**

Organizations that build on strong asset intelligence move faster and face fewer disruptions. Those that don’t simply magnify problems as spending increases.

This Q1 report focuses on the most visible manifestation of this imbalance: the Ghost Asset Crisis.

Deep Dive: The Ghost Asset Crisis

When Inventory Drift Becomes Breach Risk

The average global cost of a data breach is **$4.44 million.**[3] In the United States, the average rises to **$10.22 million**.[3] In healthcare, the average reaches **$7.42 million.**[4]

$4.44 million.[3]
Average Global Data Breach Cost

$10.22 million.[3]
Average Data Breach Cost in US

$7.42 million.[4]
Average Data Breach Cost in Healthcare

These are not extreme scenarios. They are statistical norms.

Now consider a separate but related signal:

71% of HR respondents indicate that at least **one ex-employee did not return** company equipment.[5]

These are not unrelated statistics. They describe the same exposure from two angles.

Every device that leaves organizational custody without verified retrieval and formal retirement becomes an unmanaged endpoint. Every unmanaged endpoint retains stored credentials, cached sessions, access history, and corporate data. According to the 2025 Data Breach Investigations Report, stolen credentials remain one of the most common initial access vectors in breaches.

CrowdStrike reinforces the shift:

82% of detections were malware-free, reflecting identity-driven and interactive intrusions.[1]

Valid account abuse accounted for 35% of cloud incidents globally.[15]

Modern breaches begin with access, not malware.

Ghost assets are **not an inventory management concern**. They are **evidence of weakened governance**, elevated risk, and quantifiable financial impact.

How Inventory Drift Actually Forms

Ghost assets do not appear overnight. They accumulate through normal operational activity.

1. Hiring Acceleration

Devices are provisioned at speed.
Records are created. Updates lag behind deployment reality.

2. Role Changes

Custody shifts informally. A laptop moves desks, teams, or geographies. Documentation does not consistently follow.

3. Offboarding

Logical access is revoked immediately. Physical retrieval depends on process discipline. In distributed environments, that discipline varies.

4. Refresh Cycles

New devices are issued. Old devices are not always formally retired. Both remain “active” in reporting systems.

Each event is ordinary.
At scale, drift is not an anomaly. It is the default state of unmanaged lifecycle velocity.

In an organization processing **2,000 lifecycle events per month**, this creates **24,000 annual opportunities** for records and reality to diverge.

Most organizations do not detect drift when it begins.
They discover it during an audit, a security incident, or a budget reconciliation.

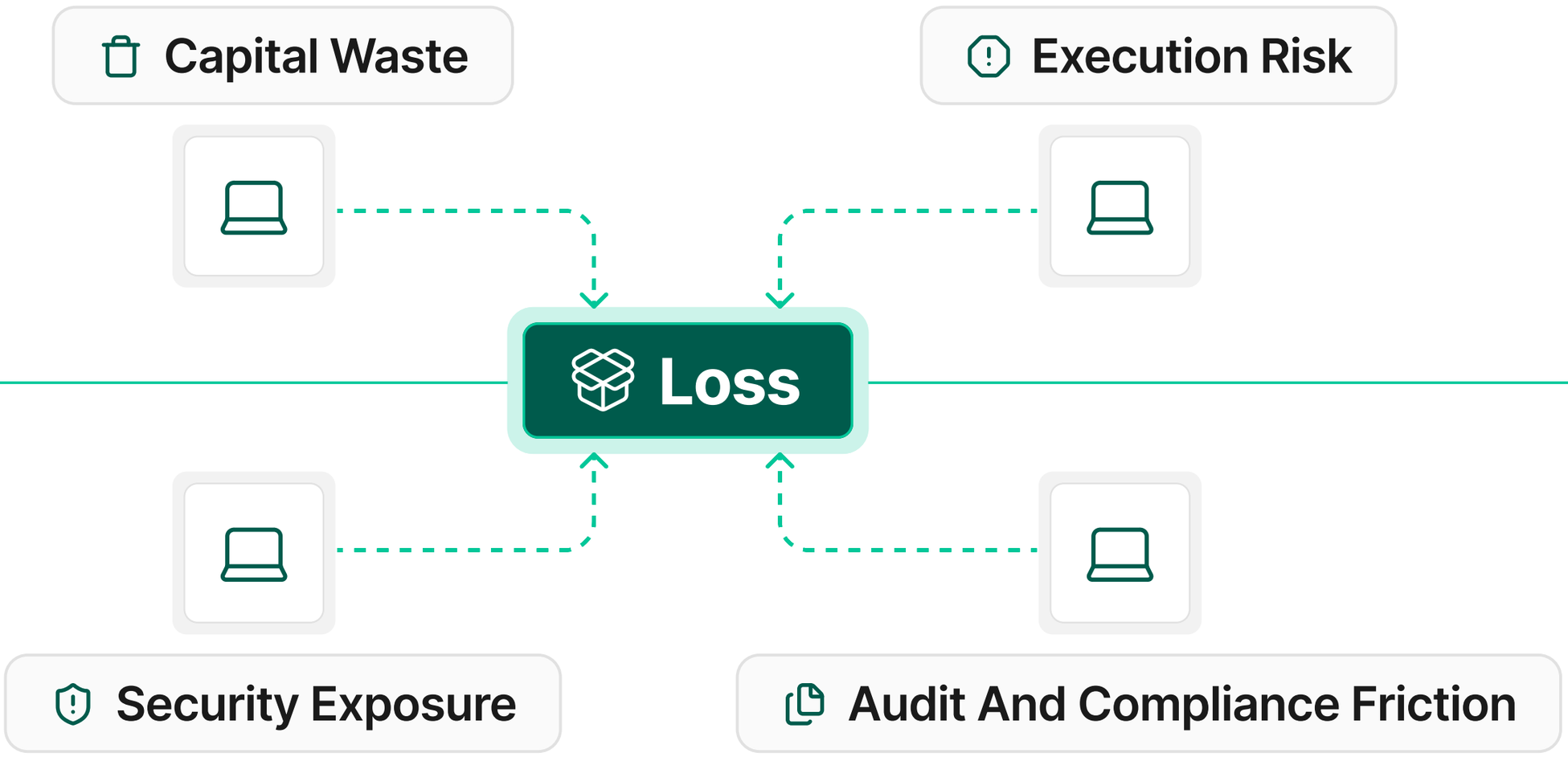
Persistence thrives where oversight is episodic.

In one documented intrusion, adversaries maintained access for 22 months before disruption.[15]

Key takeaway
What’s **routine at the event level** becomes **risk at scale**.
Drift compounds faster than organizations can detect it.

The Business Impact: Four Dimensions of Loss

Inventory drift rarely appears as a single failure. It accumulates through routine operations and ultimately surfaces as measurable risk across the business, affecting capital efficiency, execution integrity, security posture, and compliance credibility.

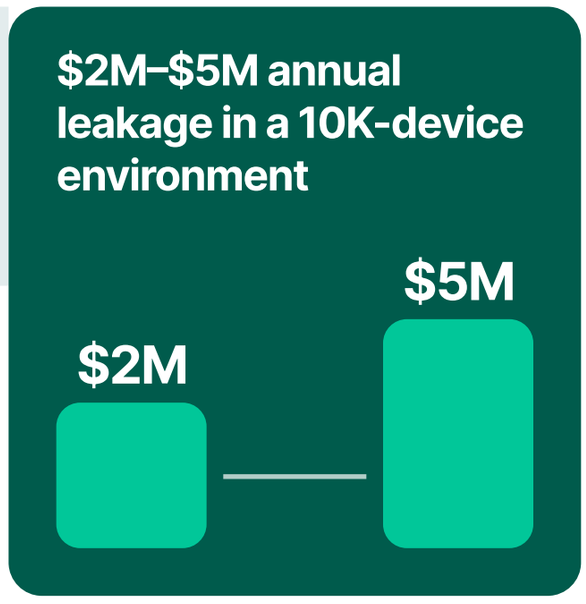


1. Capital Waste

When devices are not recovered or formally retired, financial drag accumulates quietly

- Replacement purchases increase
- License counts inflate
- Refresh budgets overshoot
- Storage costs compound

In a 10,000-device environment with a 7% accuracy gap, conservative modeling places annual financial leakage between **$2 million** and **$5 million.**



That figure reflects duplicate procurement, idle hardware, misallocated licenses, and distorted refresh planning. The loss rarely appears as a single event. It persists across budgeting cycles, quietly compounding as infrastructure scales.

2. Execution Risk

Operational dashboards often signal confidence:

100% patch deployment • 100% rollout coverage • 100% compliance confirmation

In practice, coverage may be **88%** or **92%.** The gap resides inside inaccurate records.

When asset data drifts, execution metrics become directional rather than factual. Security initiatives appear complete while unmanaged endpoints remain outside enforcement.

Leadership believes deployment succeeded. The environment tells a different story.

When inventory integrity fails, execution reporting becomes optimistic fiction.

3. Security Exposure

Every untracked device expands the attack surface.

The compression of intrusion timelines makes that exposure more consequential:

- Average breakout time has fallen to **29 minutes**
- The fastest observed breakout occurred in **27 seconds**[15]

Meanwhile, organizations take an average of **241 days to identify and contain a breach - 267 days across complex environments**[3]**.**

When stolen credentials are involved, containment averages **246 days**[3].

> **It takes minutes for attackers to gain control, and months for organizations to uncover it**

Unretrieved devices widen that asymmetry.

Credential-driven intrusion now dominates modern threat patterns. Cloud-targeted activity is rising, stolen corporate access is actively traded, and zero-day exploitation continues to accelerate. Attackers are not forcing entry. They are using valid access.

Unmanaged devices function as durable credential containers: cached sessions, persistent tokens, stored profiles, and historical access pathways. Until custody is verified and retirement confirmed, exposure remains open.

Inventory drift is not an administrative delay.
It is unverified access.

4. Audit and Compliance Friction

Governance expectations have shifted. Auditors no longer accept policy documentation alone. They expect lifecycle evidence.

When inventory cannot withstand scrutiny:

- Audit cycles extend
- Findings multiply
- Remediation costs rise
- Leadership credibility weakens

Inventory accuracy has become a governance signal — one that reflects operational discipline as much as technical control.

The financial multiplier reinforces this reality. Detection, escalation, and lost business represent the largest share of breach cost.

The financial multiplier reinforces this reality. Detection, escalation, and lost business represent the largest share of breach cost[3]. Organizations with mature automation reduced breach impact by **$1.76 million** and shortened containment timelines by **108 days**[3].

Lifecycle governance produces the same effect.

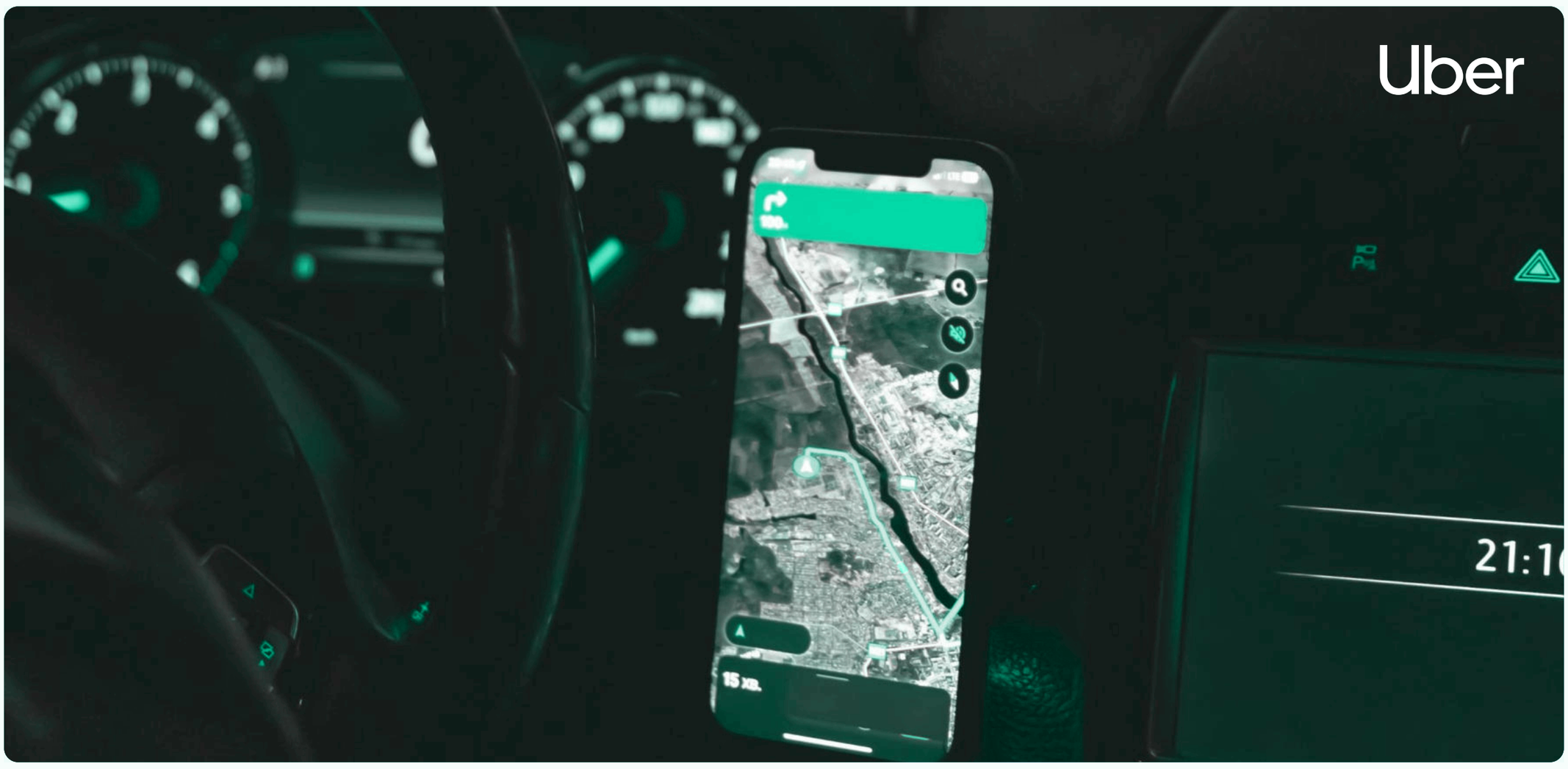
When custody is verified and reconciliation is continuous, exposure duration contracts and capital waste declines.

When governance lags, cost compounds quietly.

Key takeaway

Hidden inefficiencies across assets translate directly into **measurable loss** - t**hrough wasted spend, elevated risk, and compliance overhead**.

Evidence from the Field



Uber: $4 Million in OPEX Recovered Through Ghost Assets

In large-scale environments, small percentage improvements translate into significant cost recovery.

By strengthening lifecycle governance and eliminating inventory blind spots, Uber identified excess device allocation, improved recovery workflows, and reduced unnecessary procurement.

Result

$4 million in operational expense savings.[6]

- Not through workforce reduction.
- Not through vendor renegotiation.
- **Through visibility.**

> **The opportunity was already on the books.**
> **It required clarity to unlock.**

Savings came from:

- Accurate reassignment instead of repurchase
- Clear retirement workflows
- Reduced idle hardware
- Corrected license allocation

Bubo P., Flyr Labs: Visibility became Operational Leverage

At Flyr Labs, distributed operations created lifecycle complexity.

Hiring acceleration, role changes, and global mobility increased device movement. Without integrated governance, inventory drift was inevitable.

Under Bubo's leadership, the focus shifted from periodic cleanup to continuous control:

- HR-triggered provisioning and retrieval workflows
- Structured offboarding enforcement
- Defined custody checkpoints
- Real-time visibility across IT and Finance

As Bubo summarized:

After using Teqtivity for more than five years, I'm still waiting to hear a 'we can't do that' from their team.

It's more than a tool - it's a trusted partner that grows with me. Wherever I go in my career, Teqtivity goes.

The Convergence Point

The latest industry data points to the same conclusion:

- Spending is accelerating.
- Complexity is increasing.
- Governance maturity is lagging.
- Identity abuse is rising.
- Detection timelines remain long.

Ghost assets sit at the intersection of these forces.

They represent infrastructure without verified custody.

Credentials without continuous validation.

Capital without trusted accountability.

In 2026, asset intelligence becomes a leadership discipline rather than an operational function.

> **Organizations that institutionalize lifecycle governance will treat visibility as infrastructure. Those that do not will experience it as a recurring financial, security, and compliance surprise.**

Industry Signals

Evidence Across Sectors

The governance gap outlined earlier is not confined to one vertical. It appears across regulated industries, high-growth environments, public institutions, and distributed operational models.

The consequences vary.
The structural pattern does not.

Across sectors, devices are deployed, reassigned, and retired faster than records are updated. What begins as small inconsistencies accumulates into systemic uncertainty.

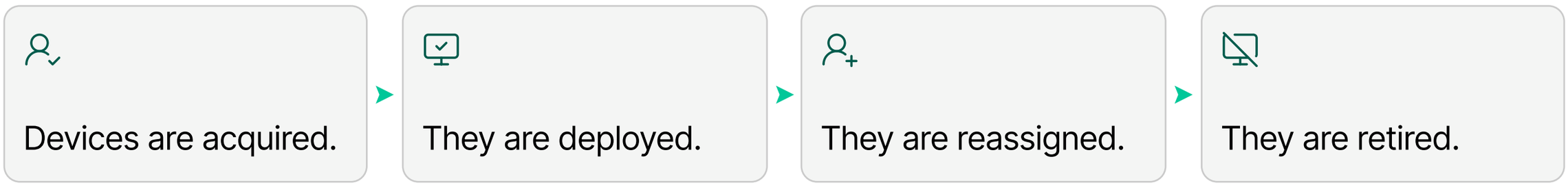
The table below highlights how this strain manifests across industries

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
Healthcare	• $7.42M average breach cost[3] • 279-day breach lifecycle[3] • Top 5 Industries Targeted by Interactive Intrusions[15]	Shared, mobile clinical devices operating under strict regulatory mandates	Delayed containment, failed audits, escalating regulatory penalties	• Make device custody part of compliance controls. • Require verified asset reconciliation during audits, offboarding, and clinical reassignment.
Financial Services	• $5.56M average breach cost • 50% increase in access broker activity	Identity-dense environments with constant regulatory scrutiny and global operations	Audit delays, control exceptions, reputational and regulatory exposure	• Integrate asset verification into risk and audit workflows. • Enforce continuous device-to-user validation, not periodic reviews

Industry	Signal	Structural Context	Business Impact	Strategic Pivot
Technology & SaaS	• 13% annual turnover • 71% non-return rate • Up to 30% retrieval improvement with structure • Top Industry Targeted by Interactive Intrusions[15]	High hiring velocity, remote onboarding, constant role changes	Onboarding slowdowns, duplicate purchases, growing ghost asset base	• Automate lifecycle enforcement. • Tie onboarding, role changes, and offboarding to mandatory device check-in and reassignment verification.
Education & Research	• Up to 25% IT budget impact from ghost assets	Shared fleets, academic turnover cycles, limited IT staffing	Wasted capital, funding inefficiencies, audit findings	• Establish inventory accuracy targets. • Require verified counts before refresh cycles, funding approvals, and annual audits.
Manufacturing / Industrial	• A measurable data point drawn from industry evidence that indicates the scale or direction of the issue.	The operational conditions in which organizations manage assets, explaining why lifecycle governance becomes more complex in that environment.	The operational, financial, or compliance pain organizations experience when lifecycle control breaks down.	• The direction organizations must take in governance and lifecycle management to regain control and reduce asset risk.
Global Enterprises	• 10–30% of devices misassigned without active management • 82% malware-free intrusions[15] • $6.15T global IT environment[1] • 276-day breach lifecycle[3]	Multi-region operations, vendor-managed logistics, contractor complexity	Slow incident response, fragmented reporting, executive uncertainty	• Create a single global source of asset truth. • Centralize lifecycle tracking and require real-time reconciliation across regions and vendors.

The Common Pattern

Across industries, the progression is consistent:



Records lag behind each step.

Small inconsistencies accumulate into structural uncertainty. Over time, organizations lose confidence in their asset data. **Once confidence erodes, teams cannot reliably deploy technology, enforce security controls, or demonstrate compliance.**

> **When asset collapses, governance collapses with it**

The issue is not limited to high-growth companies or heavily regulated sectors. It is systemic. The operating environment has accelerated. Governance maturity has not scaled proportionally.

Complexity Is Rising Faster Than Governance

The broader environment reinforces the same pattern.

- IT spending is projected to reach **$6.15 trillion in 2026**.
- Credential-driven intrusion now defines modern threat activity.
- Workforce turnover remains elevated.
- Breach lifecycles remain prolonged.

These forces do not operate independently. They compound.

The modern IT environment expands simultaneously across multiple dimensions:

- Device volume
- Deployment velocity
- Workforce distribution
- Compliance expectations
- System interdependencies

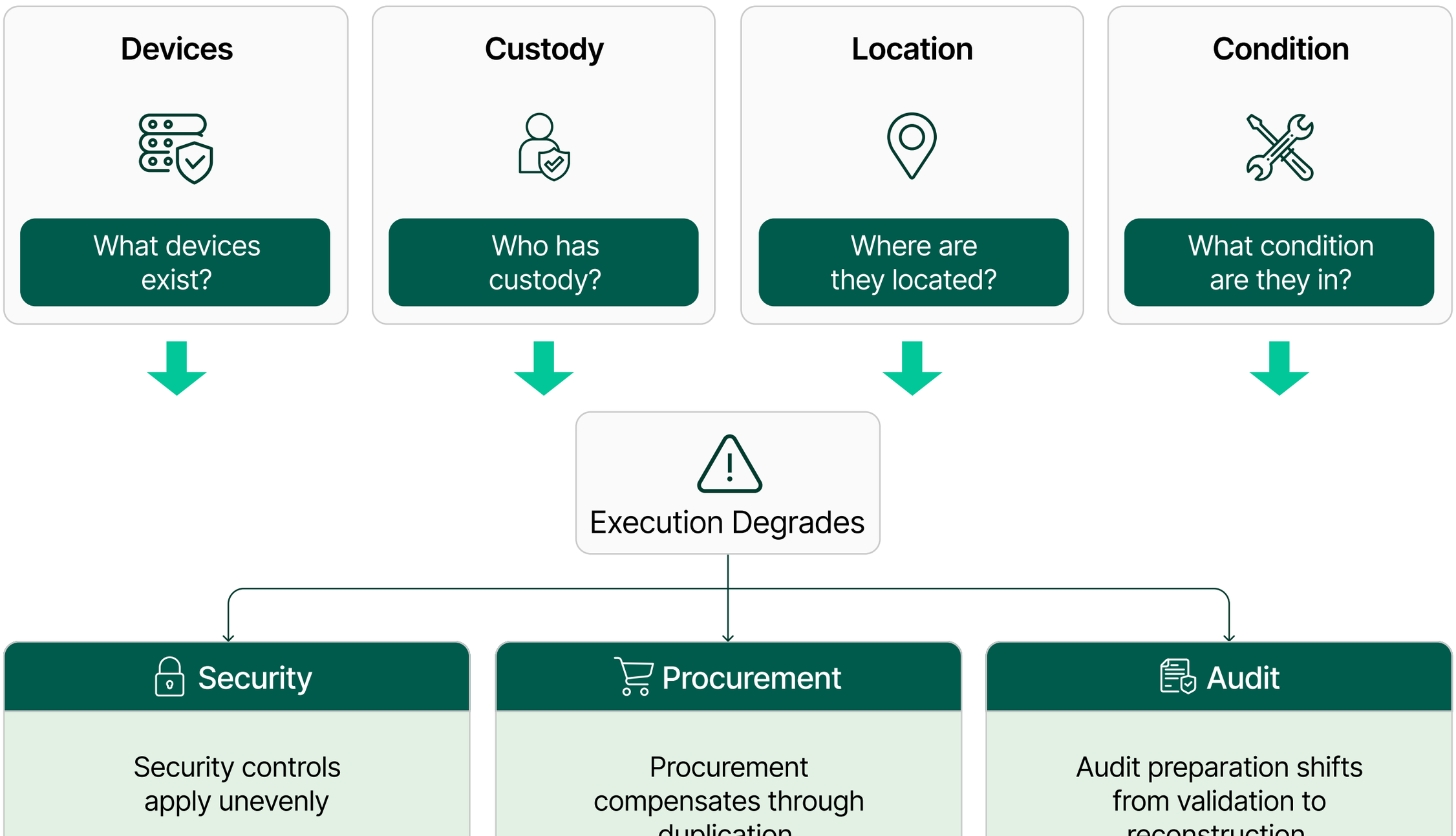
Each layer increases coordination burden.

Each expansion raises the cost of inaccuracy.

In slower operating environments, asset drift could be contained through periodic audits or manual correction. In 2026, drift accumulates faster than traditional controls can reconcile.

Only **23%** of organizations report having formal AI governance frameworks in place, even as deployment accelerates.[17] Governance maturity continues to trail operational scale.

When organizations cannot confidently answer four foundational questions:



This is not about the industry.
It is not about the tools.
It is about control under scale.

Organizations are responding, but not all responses address the root condition

The next section analyzes emerging response patterns, maps the current solution landscape, and clarifies Teqtivity's position within the evolving lifecycle governance category.

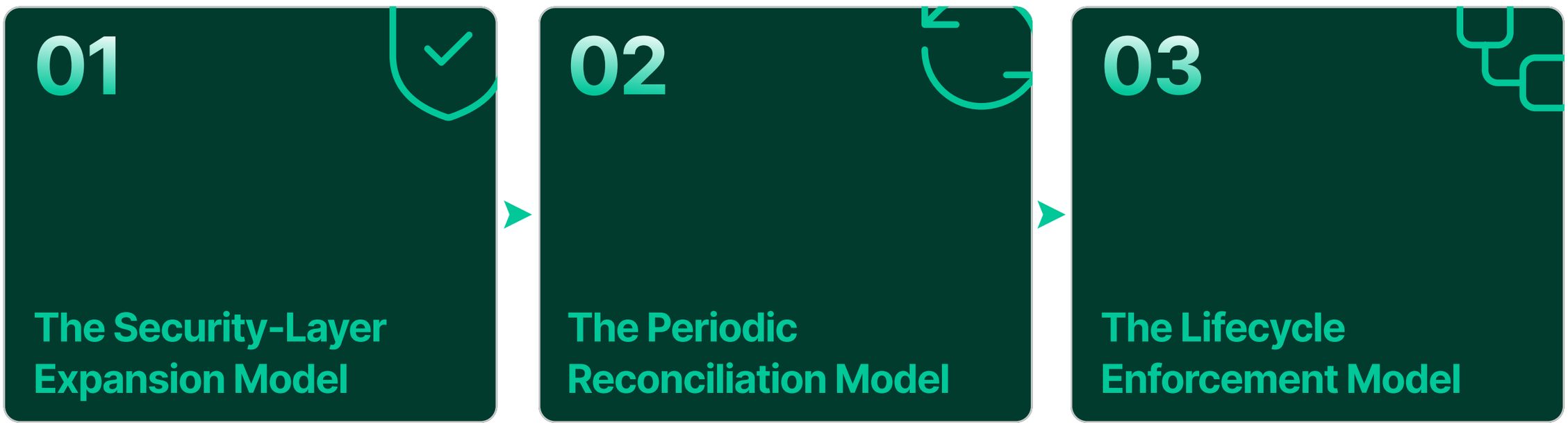
3 Ways Organizations Respond

Current Response Patterns

In 2026, organizations are not ignoring asset drift. They are responding.

Across the market, responses consistently cluster into three distinct operating models. Each model reflects a different assumption about where risk originates and how control should be restored.

These patterns appear repeatedly across the organizations we work with and across broader industry practices.



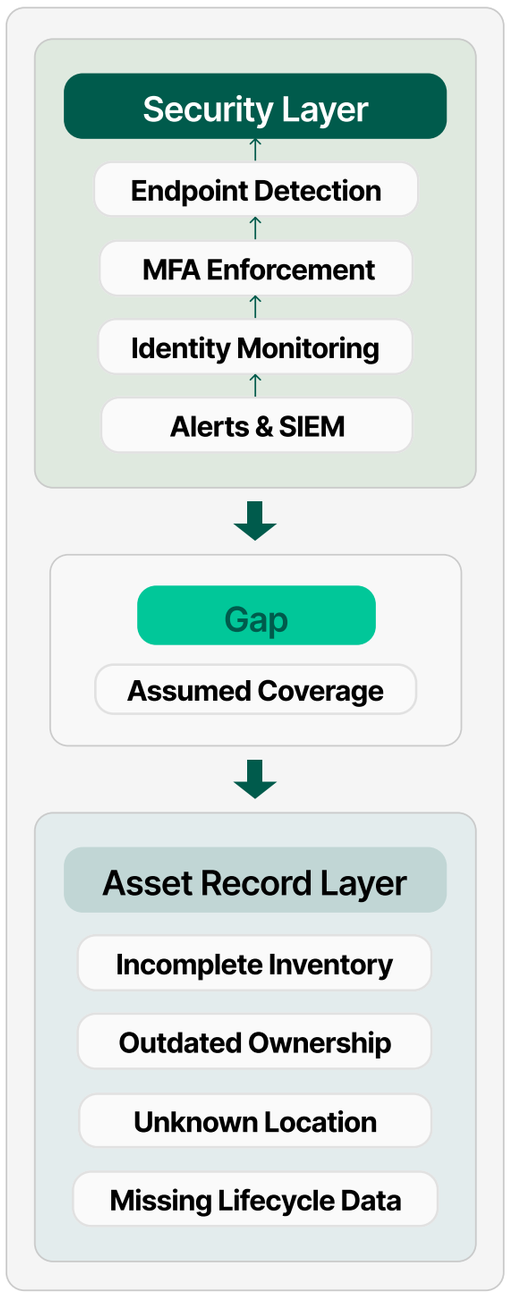
1. The Security-Layer Expansion Model

The most common response is additive.

Organizations expand endpoint detection coverage, strengthen MFA requirements, increase identity monitoring, and tighten conditional access enforcement.

- Monitoring depth increases.
- Alerting fidelity improves.

The operating assumption is that exposure results primarily from insufficient surveillance.



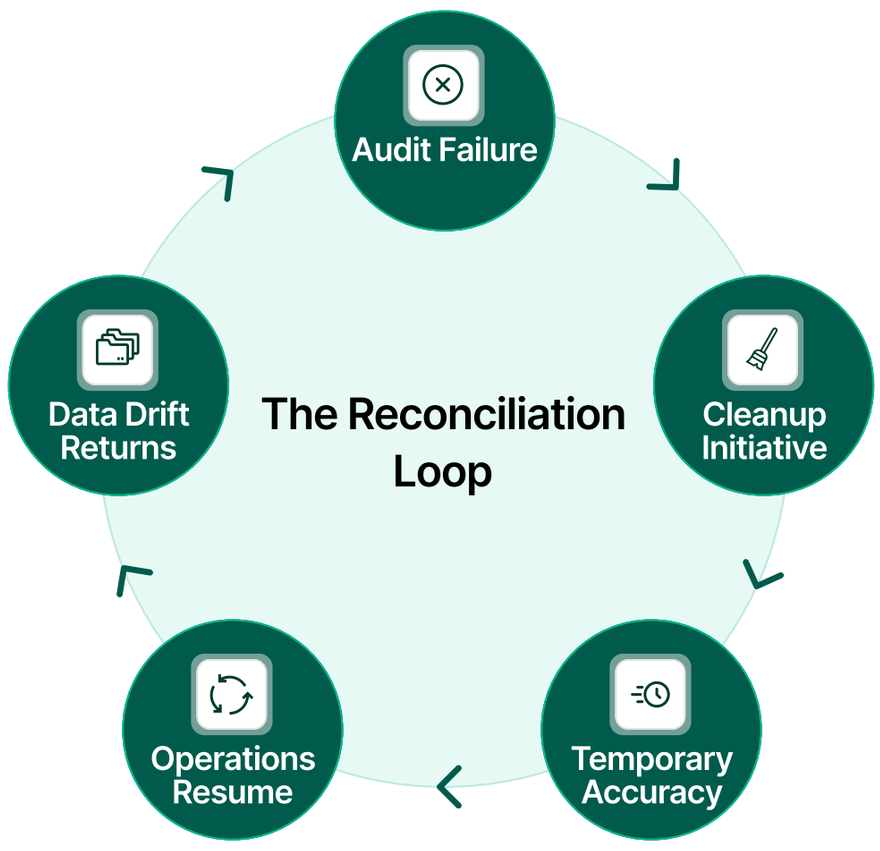
However, security controls depend on an accurate system of record. When inventory data is incomplete or outdated, coverage metrics may appear comprehensive while physical custody remains uncertain.

In this model, detection improves faster than record integrity.

Many organizations initially respond this way because security tooling is already funded, operational teams are familiar with it, and the deployment path is clear.

The result is stronger monitoring layered on top of unstable asset records.

2. The Periodic Reconciliation Mode



A second response pattern emerges when operational friction becomes visible.

Typical triggers include failed audits, reconciliation discrepancies, procurement overruns, or asset recovery gaps during employee offboarding.

Organizations respond with structured cleanup initiatives:

- Physical inventory counts
- Procurement-to-asset reconciliation
- License realignment
- Temporary reporting controls

However, without enforcement embedded in daily operations, records gradually diverge again as devices are reassigned, relocated, or retired outside the system of record.

Among the organizations we observe, this **model often becomes a recurring cycle: reconciliation restores accuracy, operational activity erodes it, and the next cleanup initiative follows**.

Drift becomes a periodic maintenance task rather than a continuous governance variable.

3. The Lifecycle Enforcement Model

A smaller but growing segment of organizations approaches the problem differently.

Instead of expanding surveillance or conducting periodic resets, they govern asset transitions directly.

- Provisioning
- Custody transfer
- Location changes
- Offboarding
- Refresh cycles
- Retirement

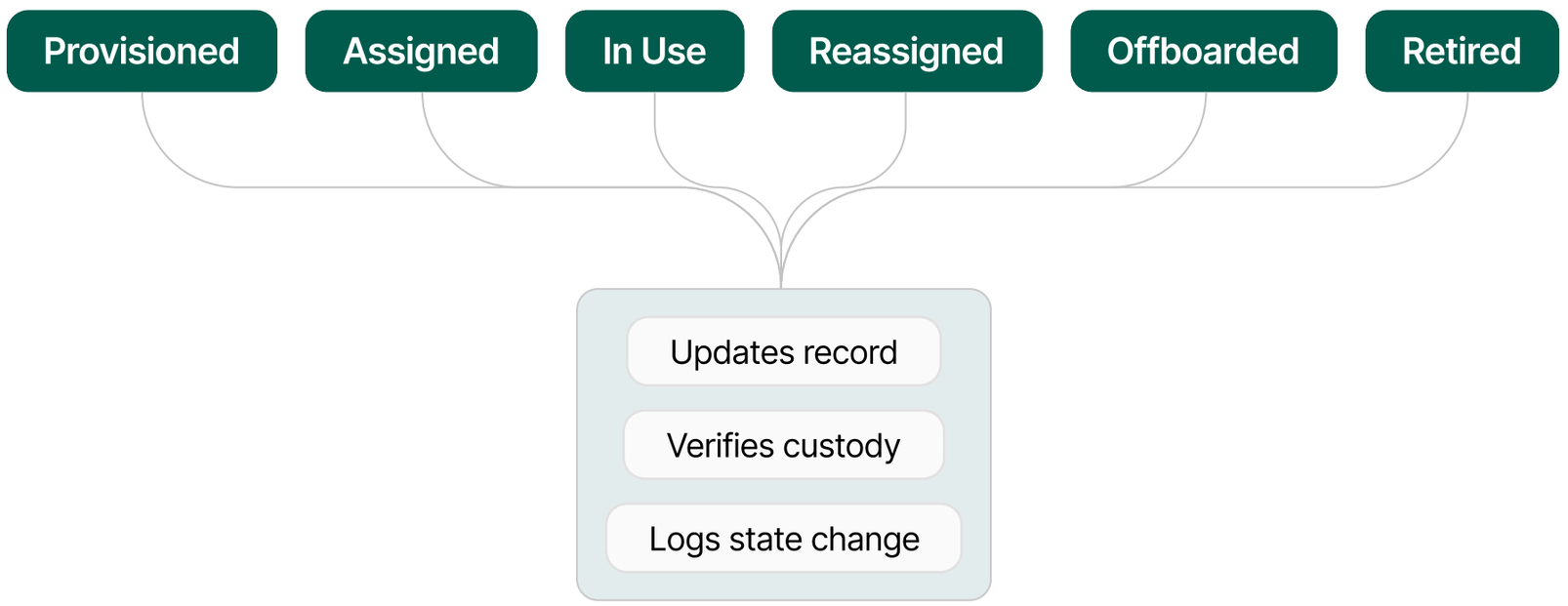
Each transition is treated as a control point.

Each movement updates the system of record at the moment the asset changes state.

> **Control improves when asset transitions are governed in real time**

This model is increasingly visible among organizations scaling their IT environments. Many of the teams we work with move toward lifecycle enforcement after encountering the limitations of expanded monitoring and recurring reconciliation efforts.

In this operating model, drift rarely accumulates because lifecycle transitions are structured events rather than informal processes.



The Structural Difference

The difference between these models is not tooling depth.
It is a difference in operating philosophy.

The first model expands monitoring coverage.	The second restores accuracy through periodical resets.	The third reduces the conditions under which drift forms.

Some approaches react to exposure.
The lifecycle model prevents exposure accumulation.

In high-velocity environments, the distinction becomes operationally significant.

This Is Not a Detection Problem

Ghost assets are a governance failure, not a detection failure.

When unmanaged endpoints appear, many organizations respond by layering more security controls. That improves monitoring and identity enforcement, but it does not address the lifecycle breakdown that allowed the device to leave verified custody.

The root issue is inventory drift.

Teqtivity's position is simple:

- If lifecycle transitions are structured and enforced, unmanaged endpoints do not accumulate. Prevention happens upstream, before security exposure compounds.
- Detection tools surface symptoms.
- Lifecycle governance addresses the cause.

Where Teqtivity Fits

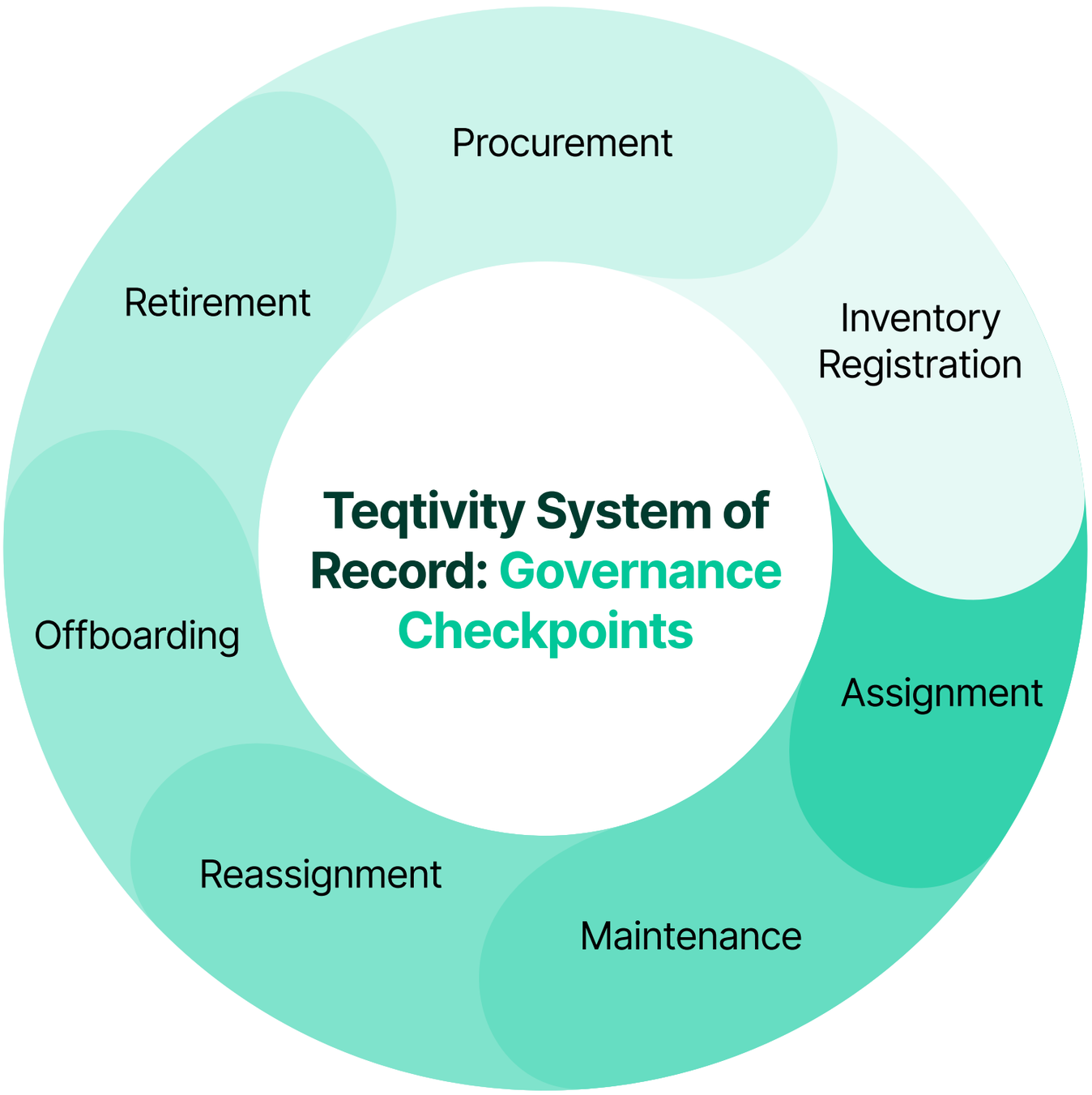
If the problem is governance drift, the solution is not another monitoring layer.

It is operational structure.

Teqtivity focuses on these lifecycle events as the foundation of effective IT governance.

Asset control is established at the moments where custody changes.

Procurement, deployment, reassignment, repair, offboarding, and disposal are governance checkpoints

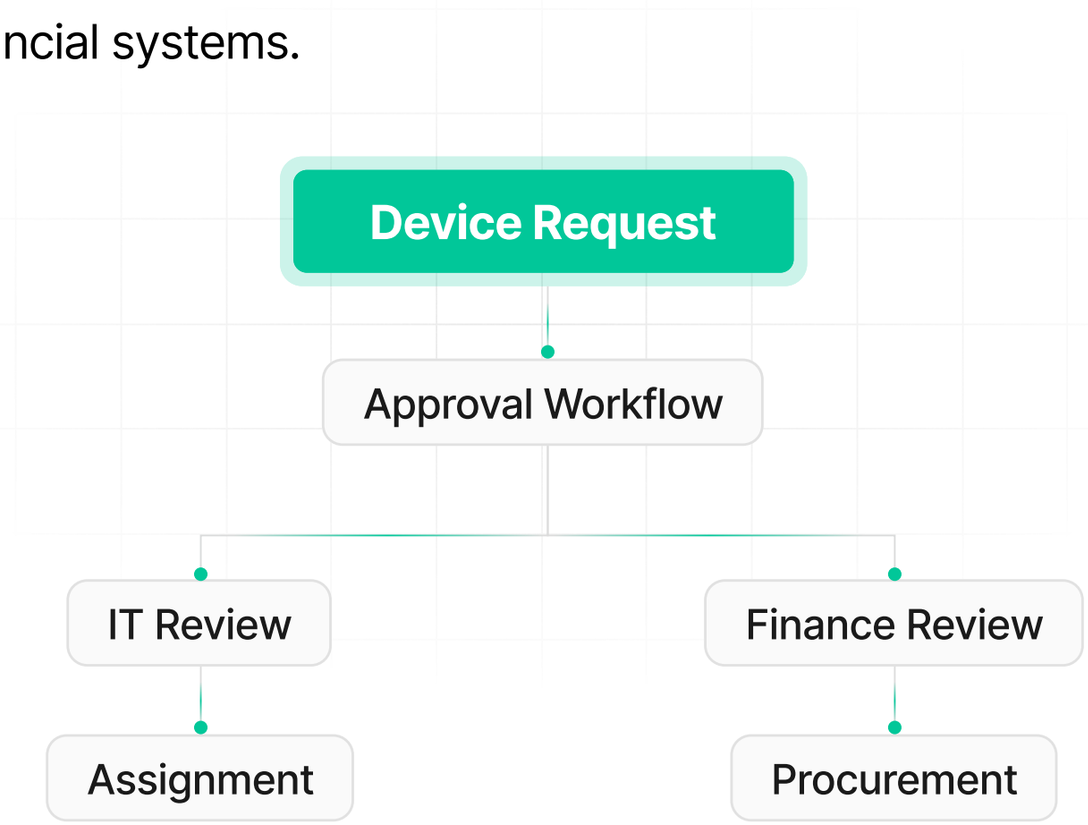


When those transitions are inconsistently recorded, inventory gradually diverges from operational reality

Teqtivity addresses this through two structural pillars: Lifecycle Control and Governance Flexibility.

Lifecycle Control ensures that asset transitions remain visible and verifiable. Teqtivity acts as a system of record for lifecycle activity, linking procurement, inventory, assignment, and retirement into a continuous operational history. Each transition updates the asset's state and chain of custody, preserving a trusted understanding of the environment as infrastructure evolves.

Governance Flexibility allows organizations to adapt lifecycle governance to their operational environment. Fields, workflows, and reporting structures can be fully customized, and a broad integration ecosystem connects Teqtivity with identity platforms, service desks, device management systems, procurement tools, and financial systems.



Core capabilities such as integrations and SSO are included as standard features, and pricing is not tied to asset counts. Organizations can track their full environment without creating incentives for selective visibility.

Implementation is supported by Teqtivity's customer success team, which works with organizations to align the platform with operational workflows and governance objectives.

The future of IT risk management will not be determined by how quickly threats are detected.

It will be determined by how effectively organizations control the lifecycle of the devices they deploy.

Organizations that govern lifecycle transitions reduce unmanaged assets, stabilize financial reporting, and strengthen audit defensibility.

Teqtivity operates where those controls become operational.

- Not at the perimeter.
- At the point of control.
- Before ghost assets become breach statistics.

Looking Ahead

Predictions for Q2 2026

The signals identified in Q1 point to a widening gap between the growth of device fleets and the governance models used to manage them.

The following developments are likely to emerge in Q2.

Prediction 1: Ghost asset exposure will increase in distributed organizations

Organizations with remote and hybrid workforces will see rising rates of unrecovered devices as employee turnover & contractor usage continue to expand. As device fleets grow across locations and ownership boundaries, equipment recovery & custody verification will become more difficult to enforce

For many organizations, **ghost assets will shift from an occasional operational issue to a persistent governance concern** tied to security exposure and capital loss.

Prediction 2: Inventory drift will surface more frequently during audits

Audit processes will increasingly reveal gaps between recorded inventory and operational reality. Organizations will encounter requests for device-level custody history, assignment records, and retirement documentation that existing systems cannot easily provide.

Rather than isolated findings, **companies will experience recurring remediation cycles** as auditors push for clearer asset accountability.

Prediction 3: More organizations will operationalize lifecycle governance

A growing number of organizations will begin enforcing structured controls around asset provisioning, reassignment, offboarding, and retirement. These lifecycle events will become the primary mechanism for maintaining inventory accuracy as environments scale.

Organizations that implement structured transitions will see **reduced inventory drift and higher equipment recovery rates** compared to those relying solely on discovery or monitoring tools.

Prediction 4: Asset certainty will improve incident response speed

Security investigations will increasingly depend on the ability to quickly identify the ownership and status of devices involved in an incident. Organizations with verified asset records will contain investigations more efficiently because response teams can immediately determine device custody and access history.

Where **inventory certainty is missing, investigations will slow** as teams attempt to reconstruct basic asset information.

What This Signals for the Rest of 2026

The second quarter will begin to separate organizations that monitor devices from those that maintain operational control over them.

As distributed environments continue to expand, asset intelligence will become less about discovery and more about ensuring custody remains verifiable as devices move through the organization.

Next Steps for Your Organization

Organizations arrive at this stage with different levels of urgency. Some are still confirming the scope of the problem. Others already see the operational impact in audits, security exposure, and procurement inefficiencies.

Wherever you are in that process, the next step is to examine how these dynamics are appearing inside your own environment.

If you are still sizing the problem, pressure-test the assumptions behind your current inventory. Many teams find it useful to walk through how asset drift typically develops and what signals indicate that ghost assets are already accumulating.

If you are actively evaluating solutions, we can help you examine how lifecycle governance performs under real conditions. That includes distributed teams, contractors, regional logistics, and audit requirements. The goal is to evaluate operational fit rather than review features in isolation.

If you are ready to move forward, you can request a focused working session to discuss ITAM rollout considerations, pilot structure, and the metrics that will demonstrate control improvements to leadership and auditors.

Start the next step

Request a consultation: **https://www.teqtivity.com/get-started**

Email: **hello@teqtivity.com**

Q2 2026 Preview: Lifecycle Control in the Remote Work Era

Remote and hybrid work have permanently changed how organizations deploy and manage devices. Asset fleets that were once concentrated in a few offices are now distributed across homes, coworking spaces, and international locations.

This shift introduces new operational complexity. Maintaining lifecycle control becomes significantly harder when devices move beyond centralized offices and into distributed environments. Remote employees already show higher equipment non-return rates, deployments increasingly span dozens of countries, and contractor-heavy teams create additional handoff points where asset custody can become unclear.

At the same time, hybrid work has stabilized as the dominant operating model. Recent research shows 32% of employees working fully remote and 41% in hybrid arrangements, reinforcing that distributed infrastructure is no longer temporary

As organizations adapt, new operational models are emerging. Device-as-a-Service providers, global logistics partners, and regional deployment hubs are helping companies provision and recover equipment across borders. These models solve logistical challenges, but they also introduce new governance questions around ownership, accountability, and how lifecycle control is maintained when asset custody spans multiple vendors and geographies.

> **The Q2 report will examine how distributed workforces are reshaping asset management practices and what organizations must do to preserve lifecycle control when devices move beyond traditional office boundaries.**

Appendix

Methodology

This report draws on publicly available industry research, including global IT spending forecasts, cybersecurity threat reports, breach cost analyses, and workforce data, to identify structural patterns shaping IT operations in 2026. Rather than presenting isolated statistics, the analysis focuses on how these signals interact at enterprise scale. Rising infrastructure investment, distributed workforces, credential-driven intrusion, and prolonged breach lifecycles were examined together through cross-source analysis to understand where governance pressure is increasing and where operational control tends to weaken.

Particular attention was given to the conditions that allow asset records to drift from reality, creating environments where ghost assets accumulate and decision-making begins to rely on incomplete infrastructure data. Signals were evaluated for consistency across multiple reports and interpreted in the context of operational governance, lifecycle accountability, and enterprise infrastructure management.

This report is not a product brief or a threat digest. It is a structural assessment of control maturity under acceleration. All data points are drawn from publicly available industry research and cited accordingly. The analysis reflects Teqtivity's interpretation of these signals and is intended to highlight operational patterns rather than provide exhaustive industry measurement.

Data Sources

1. Gartner. Gartner Forecasts Worldwide IT Spending to Grow 10.8% in 2026, Totaling $6.15 Trillion. February 2026.

2. Gartner. Gartner Forecasts Worldwide IT Spending to Grow 7.9% in 2025. July 2025

3. IBM and Ponemon Institute. Cost of a Data Breach Report 2025. February 23, 2026.

4. HIPAA Journal. Average Cost of a Healthcare Data Breach Falls to $7.42 Million. July 29, 2025

5. Capterra. HR Says Ex-Workers Ghost Exit Interviews, Steal Equipment. January 30, 2023.

6. Teqtivity. 71% of Employees Don't Return Company Equipment: How IT Asset Management Can Help. January 1, 2025

7. Verizon. 2025 Data Breach Investigations Report. July 27, 2025.

8. Venn. How Unmanaged Devices Are Worsening the Ransomware Crisis for Companies. September 3, 2025

9. LinkedIn. Ghost assets drain 25% of IT budgets as ITAM confidence gap widens. August 25, 2025

10. CPCON Group. Ghost Asset Detection: How to Find Millions in Missing Assets. February 21, 2026

11. Synetic Technologies. How to Recover 30% More IT Devices During Employee Offboarding. June 22, 2025.

12. Mercer. Results of the 2025 US Turnover Surveys. September 11, 2025

13. Teqtivity. Uber Saves $4M in OPEX with Teqtivity

14. Teqtivity. Hero Spotlight: Bubo P. at Flyr Labs

15. CrowdStrike. 2026 Global Threat Report. February 24, 2026

16. CrowdStrike. 2025 European Threat Landscape Report. November 3, 2025.

17. Info-Tech Research Group, AI Trends 2026

18. Owl Labs,, 2025 State of Hybrid Work Report: United States.

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.