omnitza

Published July 2025

The Overlooked Perimeter

The Critical Role of IT Asset Management in Defending Against Lifecycle-Based Reconnaissance Threats

"Threat actors have adapted to the enhanced visibility of traditional endpoint detection and response (EDR) sensors by altering their exploitation tactics for initial access and lateral movement. They are now targeting the network periphery, where defender visibility is reduced..."

— *CrowdStrike 2024 Global Threat Report*

Executive Summary

Modern enterprise security strategies remain heavily focused on protecting active, visible, and deployed endpoints. But attackers are increasingly bypassing these controls—not by going through them, but by going around them.

Sophisticated adversaries are now exploiting what Oomnitza defines as "The Overlooked Perimeter"—the less-visible asset states across the IT asset lifecycle that fall outside traditional security controls. This includes unsupported infrastructure, orphaned devices, and the accumulated tech debt left behind by prior deployments, mergers, or incomplete offboarding. Assets in transitional or dormant phases—such as staging, storage, and decommissioning—are frequently unmonitored, unmanaged, and excluded from standard detection and response workflows.

These overlooked states provide low-friction entry points into enterprise environments. Threat groups like UNC3944, Medusa, PlayCrypt, and Black Basta have been observed compromising devices before EDR is installed, reactivating decommissioned endpoints, harvesting credentials from discarded hardware, and exploiting legacy systems still connected to the network but outside IT's line of sight. As confirmed in reports from Mandiant, CrowdStrike, and IBM, these are not edge cases—they are repeatable, active tactics driving breach volume, dwell time, and response costs.

Most traditional tools—EDR, SIEM, CAASM, and vulnerability scanners—operate on the assumption that assets are online, deployed, and known—excluding shadow systems, orphaned assets, and the tech debt that quietly accumulates outside normal governance. In today's threat landscape, that assumption is not just incomplete—it's dangerous.

This white paper explores:

How lifecycle-based reconnaissance and compromise work in the wild	Why the non-production phases of IT assets are increasingly targeted	Where traditional security stacks fall short	How platforms like **Oomnitza** provide the critical visibility and control needed to close this perimeter

If your asset isn't visible, it isn't defensible. In a world of persistent attackers and lifecycle-aware exploits, securing the full digital asset lifecycle is no longer optional—it's imperative.

The New Blindspot in Security

As threat actors evolve their tactics, organizations face widening blind spots across the IT asset lifecycle. While most cybersecurity tools focus on operationally active devices, advanced adversaries are expanding their reconnaissance and attack strategies to include assets at any stage of the lifecycle, including those that are not yet deployed, are temporarily offline, or have been retired but remain accessible. These asset states often lack monitoring, agent coverage, or governance, making them prime targets for exploitation.

These advanced groups like UNC3944, PlayCrypt, 8Base, Medusa, and Black Basta are targeting procurement ops, supply chain, IT support and help desk teams, in an effort to find ways to bypass modern security controls to acces the technology stack across the entire lifecycle. Mandiant's M-Trends report warns of a rise in "living off the land" (LOTL) techniques, specifically emphasizing a new twist:

Adversaries are using legitimate assets that have been procured but not yet deployed or that are awaiting decommissioning or disposition to evade detection.

This shift is already contributing to real-world breaches. According to the 2023 IBM Security Cost of a Data Breach Report, conducted by the Ponemon Institute, 67% of breaches were not detected by internal security tools or teams, and follow-on analysis indicates that shadow IT, unmanaged or misconfigured assets, and unmanaged data repositories were implicated in over 33% of breaches. While often associated with cloud misconfigurations, these risks are just as prevalent across physical and hybrid assets in non-canonical lifecycle states—including devices in staging, left in storage, neglected or unsupported hardware, legacy endpoints abandoned during refresh cycles, improperly decommissioned systems, and technical debt that quietly expands the attack surface.

Mitigating these risks requires extending visibility, governance, and security policy enforcement across the entire IT asset lifecycle—not just to systems that are active and in production. That means integrating asset intelligence from procurement through disposal into broader IT, security, and compliance workflows to reduce blind spots and minimize exposure across environments.

This white paper outlines a strategic response: how deploying an IT Asset Management (ITAM) platform with full lifecycle visibility, rich third-party integrations, and high data accuracy can provide your security organization with the insights needed to protect this often-overlooked perimeter.

The New Frontier of Reconnaissance and Attack

Reconnaissance is a critical initial phase in the cyber kill chain. Traditionally, adversaries focused on active endpoint and networked assets. However, leading threat actors are now expanding their reconnaissance methods to target the full digital asset lifecycle.

Attack Mapping Across Asset Lifecycle

Lifecycle Stage	Attack Focus	Techniques / TTPs	Notable Actors
Forecasting	Target planning data	Shadow IT expansion, budget system compromise, social engineering	APT29, UNC1878
Procurement	Vendor targeting, procurement fraud	Business email compromise (BEC), supply chain impersonation	UNC3944, FIN7
Supply Chain & In Transit	Intercepted or manipulated deliveries	Tampered shipments, fake hardware, firmware backdoors	Volt Typhoon, APT41
Receive, Storage, & Staging	Pre-deployment compromise	Default credentials, remote console access, LOLBins, mislabeling	Play, UNC3944
Provision, Ownership Assignment, & Deploy	Exploiting setup misconfigurations	Imaging flaws, identity misprovisioning, unsecured API access	Scattered Spider, LAPSUS$
Use & Monitor	Exploiting production systems	Credential theft, token hijacking, device sprawl	Cozy Bear, UNC3944
Security (active)	Evasion and persistence	EDR bypass, registry tampering, DLL sideloading, scheduled tasks	FIN12, Lazarus Group
Maintain, Patch, & Refresh	Exploiting patch lag or stale assets	N-day exploitation, unpatched firmware, unmanaged devices	Conti, TA505
Decommission/ Retirement	Reactivation or data leakage or silent persistence	Orphaned AD residue objects, ghost servers, improper wipes	8Base, Black Basta
Disposition or Reuse	Data leakage or hardware backdoors	Improper wipes, resale recovery, supply chain attack	Medusa, Black Basta
Final Depreciation & Closure	Exploiting gaps in records or misreporting	Ghost asset reactivation, asset fraud, data retention lapses	Insider threats, APT32

These groups are known to exploit weak security during transitional asset phases, especially where visibility or policy enforcement is inconsistent.

Lifecycle Attack Surface: Emerging Threat Vectors by Asset Stage

Forecasting & Procurement Reconnaissance

- **Targeting IT asset data or access before they are received**

  Adversaries are now focused on identifying hardware/software assets moving through the procurement process, targeting suppliers, resellers, ticketing systems, and corporate procurement systems. Objectives are to gain valuable knowledge to gain access, improve effectiveness of phishing attacks, and develop exfiltration strategies. Evidence supports attacker groups are successfully building network topology mappings, supply chain understanding, and forecasting/deployment strategies on targeted corporations. This phase is particularly vulnerable in organizations with decentralized procurement, email-based purchase workflows, insufficient supplier vetting, and weak segmentation between procurement and operational systems. Procurement platforms integrated with corporate SSO or ticketing tools may inadvertently expose asset and network planning details through phishing or credential compromise.

Storage or Staging (Not Yet Active)

- **Determining devices in storage, or exploiting powered-on devices in staging process**

  Threat intelligence evidence suggests adversaries have massive collections of valid device data for future use. By gaining early access to devices before endpoint protection is installed, new techniques are proving to bypass modern security tools. They are using staged devices to pivot internally (e.g., shared switches or test networks) and traverse networks. Incident response data proves attackers gain access to a stored device to install a persistence and later launch via a scheduled task or bootkit before or as the device enters production.

  This phase is particularly vulnerable in high-volume refresh cycles, remote depot setups, contractor-led deployments, or environments with loosely monitored storage rooms or staging areas. Devices with preloaded OS images, open ports, or partial domain joins are especially attractive targets due to the lack of active monitoring during this phase.

Provision & Deploy

- **Configuration exploits, device compromise, and identity hijacking**

  Adversaries are actively targeting assets during initial provisioning and deployment, exploiting gaps in configuration, identity assignment, and access control. Misconfigured imaging processes, unprotected cloud-init scripts, and default administrative credentials are common entry points. Compromised assets at this stage can serve as launch pads for lateral movement or privilege escalation; often before endpoint protection is fully operational. Threat actors have leveraged impersonated service accounts, OAuth tokens, and misaligned directory joins to silently insert persistence during the first boot process. This phase is particularly vulnerable in fast-scaling environments, remote onboarding setups, and DevOps pipelines.

Lifecycle Attack Surface: Emerging Threat Vectors by Asset Stage *(continued)*

omnitza

Decommissioning

- **Reactivating or hijacking assets marked as decommissioned but still connected or accessible**

An adversary reuse of device IDs, MAC addresses, IP leases, or lingering Active Directory entries exposes credentials, topology, and data to exploitation techniques. These Tactics, Techniques, and Procedures (TTPs) have proven to be effective in exploiting assets that are no longer receiving patches or monitoring. There is also risk of attackers' use of stolen credentials tied to former endpoints or reactivation of "disabled" assets. Evidence now suggest key groups like APT40 and Black Basta are combining ransomware delivery with lateral movement initiated from an exposed decommissioned device. This phase is particularly vulnerable when organizations delay final disposition, rely on manual offboarding workflows, or lack automated reconciliation between ITAM, directory services, and endpoint agents. Assets sent to storage, retained for backup, or missed during refresh campaigns often remain reachable via VPN, Wi-Fi, or internal VLANs, providing an unexpected backdoor into the enterprise.

Disposition (Awaiting Destruction/Reuse/Resale)

- **Physically or logically abandoned assets containing residual data**

Adversaries are becoming more successful at targeting and recovering data, credentials, SSH keys, or config files from improperly disposed and wiped devices. Harvesting firmware images or old software builds to look for vulnerabilities that may still exist in the current active environment. There is evidence now of attacker groups purchasing assets of targeted companies to build an understanding of devices, software, firmware, and other possible exploitable artifacts. These TTPs are enabling attackers to reintroduce asset profiles into another network (supply chain implant scenario) or simply extract credential vaults from improperly sanitized drives.

This phase is particularly vulnerable when sanitization processes are manual or inconsistently verified, or when decommissioned devices are handed off to third parties, resellers, or recycling centers without strict controls. Devices stored in satellite offices, retained for backup, or repurposed without a secure wipe often escape formal tracking and can be exploited well after assumed disposal.

These attacks are not hypothetical—they're active and ongoing, often revealed only through post-breach forensics.

Vectra AI 2023 Threat Detection Report: 70% of security incidents originated from unmonitored devices, including retired, unmanaged, or unknown systems.

Mandiant and CISA: Warn, attackers used legacy, decommissioned infrastructure or orphaned devices as initial access points, bypassing security controls focused only on actively managed assets.

Gaps in Visibility and Detection of Lifecycle-Based Threats

Advanced attackers bypass modern endpoint security tools, exploit misconfigured or unmonitored assets, and launch ransomware or credential theft campaigns from within the network perimeter on devices typically not covered by security policies. According to Mandiant's Threat Intelligence Report, many cybersecurity products deliver sophisticated detection and prevention when the device is known, visible, and actively monitored. However, these tools fail to address assets outside active deployment—leaving significant gaps in coverage.

Modern Security Technologies

Tool Category	Asset Lifecycle	Why Modern Security Tools Miss This
Endpoint Security & EDR/XDR	✖	Focuses on assets after deployment; no visibility into procurement, staging, or retirement
SIEM & Security Analytics	● (Partial)	Can ingest signals if available, but needs clean lifecycle data from external sources
Ransomware Prevention & Resilience	✖	Some combine behavioral AI, isolation, and rollback. Most only protect during active use if deployed, not across entire lifecycle
UEBA	✖	Limited to user behavior; does not map asset movements or history outside user context
SOAR	✖	Automates response after detection; requires complete, clean data to be useful
Network Detection & Response (NDR)	✖	Sees real-time traffic; blind to procurement, staging, imaging, disposal, depreciation
Next-Gen Firewalls (NGFW)	✖	Preventive network control; cannot correlate lifecycle phases or track individual assets
Cloud Security (CSPM / CNAPP)	✖	Tracks cloud configuration/drift; no visibility into physical asset lifecycle or procurement
IAM / PAM / MFA	✖	Secures identity access—not the asset lifecycle; no procurement-to-disposal oversight
Vulnerability Management	● (Partial)	Limited visibility to assets actively scanned; no insight into offline, staged, or decommissioned assets
Object-Centric Data Model ITAM Platforms (omnitza)	●	Designed for full lifecycle visibility
CAASM Data Model ITAM Platforms	● (Partial)	Aggregates active inventory, but not lifecycle stages like procurement disposal/depreciation.
Threat Intel / Deception	✖	Detects attacker TTPs; not tied to asset lifecycle data

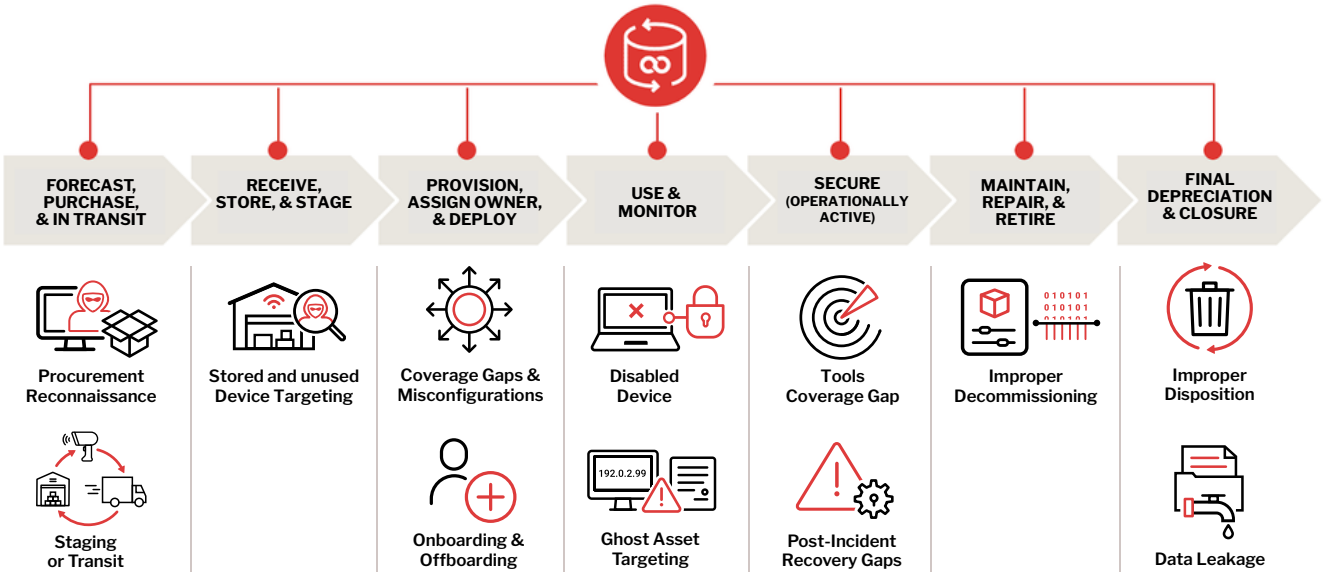
Closing the Asset Lifecycle Visibility Gap: The Critical Role of Oomnitza

Both Gartner and CISA have warned that attackers increasingly exploit refreshed, offboarded, or staged assets—devices that fall outside the visibility of traditional security stacks. These blind spots are especially common in non-production lifecycle phases, such as procurement, staging, and decommissioning.

Despite advances in EDR, SIEM, SOAR, and CAASM platforms, many tools still assume assets are fully deployed, monitored, and accounted for. In practice, this assumption leaves a growing perimeter undefended.

Supporting this, the Enterprise Strategy Group 2023 Technology Spending Intentions Survey found that 69% of organizations lack full visibility into their IT assets, especially those in inactive or transitional states. A 2024 Gartner report similarly noted that over 30% of security incidents now involve unknown, unmanaged, or retired assets—emphasizing the need for ITAM platforms to deliver continuous, full-lifecycle visibility to close these security gaps.

Compromise of the IT Asset Lifecycle



The Overlooked Perimeter isn't just a blind spot—it's a symptom of fragmentation in how enterprises manage the asset lifecycle. As devices move across functions—procurement, deployment, support, reclamation—responsibility becomes diffuse and control breaks down. Assets fall between systems, lose ownership, or accumulate configuration drift. These transitions aren't captured by traditional tools, creating long-lived exposure windows. Adversaries are now exploiting this fragmentation, targeting unmanaged infrastructure, dormant assets, and credentials that survive beyond decommissioning.

This is where Oomnitza's object-centric IT Asset Management (ITAM) platform delivers uniquely critical value.

Oomnitza Lifecycle Visibility as a Compliance and Audit Enabler

Beyond risk reduction, full lifecycle visibility and inventory is increasingly a compliance requirement. Frameworks like ISO/IEC 27001, NIST CSF, SOC 2, NYDFS, and CISA's Zero Trust Maturity Model emphasize the need for asset governance, decommissioning controls, and secure disposal. Auditors and regulators now expect organizations to demonstrate:

- Accurate inventories across all asset states—not just those in production
- Proof of ownership with procurement verification
- Controlled decommissioning, including removal from Active Directory
- Maintenance, patching systems and refresh audits
- Evidence of secure disposal and data sanitization
- Immutable records that map asset custody, access, and disposition across time

Oomnitza provides audit-grade, timestamped records for each asset across its full lifecycle, enabling organizations to meet regulatory expectations and pass audits with confidence. This level of control not only mitigates operational risk, it strengthens defensibility during compliance, investigations, and certifications.

Lifecycle Stage Requirements by Framework

	ISO 27001	NIST CSF	SOC 2	CISA Zero Trust	SOX	NYDFS	PCI	HIPAA	GDPR
Forecasting	✓	✓	✓	✓	✓	✓			✓
Procurement	✓	✓	✓	✓					✓
Supply Chain & Transit	✓	✓	✓	✓			✓	✓	✓
Receive, Storage, Staging	✓	✓	✓	✓		✓			
Provision & Deploy	✓	✓	✓	✓		✓			
Use & Monitor	✓	✓	✓	✓		✓			
Security (active)	✓	✓	✓	✓					
Maintain, Patch & Refresh	✓	✓	✓	✓	✓	✓			✓
Decommission	✓	✓	✓	✓	✓	✓			
Disposition or Reuse	✓	✓	✓	✓	✓				✓
Final Depreciation & Closure	✓	✓	✓	✓	✓				✓

The Lifecycle Control for Enterprise Security

Unlike tools that rely on snapshot-based data from known devices, Oomnitza establishes a persistent, object-based record for every IT asset from initial forecasting through final financial write-off. It enables a high-fidelity view of each asset's journey—whether in procurement, in transit from a manufacturer, provisioned but not activated, or awaiting secure disposal.

By capturing structured lifecycle metadata and orchestrating integrations with procurement, security, and IT operations systems, Oomnitza provides:

- Full visibility into assets, regardless of lifecycle phase—including pre-deployment, ghost, and decommissioned assets
- Proactive identification of security gaps before they become attack vectors
- Automated workflows for remediation, ensuring assets are compliant and secure
- Immutable records that support audit, regulatory compliance, and security investigations

Enhancing the Entire Security Stack

Oomnitza is not a replacement for existing security platforms—it is the foundational context layer that ensures those tools operate on a complete and accurate asset inventory. By integrating with CAASM tools like Axonius, SIEM platforms like Splunk, and EDR/XDR systems like CrowdStrike or SentinelOne, Oomnitza enables:

- Complete asset context for accurate threat correlation in SIEM/UEBA tools
- Fewer false negatives in CAASM-based risk reporting due to enriched lifecycle intelligence
- Lifecycle-triggered automation in SOAR platforms for compliance, isolation, or disposal workflows
- Reduced attacker dwell time by enabling visibility into the assets most commonly ignored

Full Lifecycle Visibility is Now a Security Imperative

Attackers are no longer focusing solely on live endpoints—they are exploiting the gaps between lifecycle phases. These gaps are real, operational, and already being used by advanced groups to bypass traditional defenses.

Today's cybersecurity tools assume assets are deployed, active, and monitored. That assumption is now a risk. Attackers aren't waiting for your endpoints to go live—they're breaching your organization before protection is even installed.

If your asset isn't visible, it isn't defensible.

The Fix: Lifecycle-Aware Security

By delivering persistent visibility across the entire IT asset lifecycle, Oomnitza closes the gap that modern attackers rely on. Our platform helps organizations:

- Eliminate lifecycle blind spots before adversaries exploit them
- Strengthen control hygiene across all asset phases
- Improve compliance posture with audit-grade records
- Reduce breach exposure before, during, and after endpoint deployment

Don't wait for a breach to discover what you failed to track.
Make asset lifecycle visibility foundational to your security strategy.

With Oomnitza, what was once overlooked becomes visible—and defensible.

Turn Technology Investments into a Competitive Edge

Oomnitza transforms IT asset management into a strategic advantage. With comprehensive visibility across the entire asset lifecycle, we empower organizations to mitigate security risks, ensure data integrity, and maintain compliance. Our asset-centric approach and workflow automation provide the control needed to safeguard against lifecycle-based threats and improve security posture. Oomnitza helps organizations secure their technology investments, reduce vulnerabilities, and optimize asset performance in an increasingly complex and risk-driven environment.

Strengthen Your Security Posture

Scan to see how Oomnitza helps protect your business from IT asset lifecycle security risks.

Unlock the Power of Oomnitza

Scan to book a demo and discover how Oomnitza can streamline and secure your asset management.

Connect with us team_oomnitza@oomnitza.com

Learn more at oomnitza.com