Lansweeper

LEVEL UP YOUR IT: TRANSFORM UPGRADE CHALLENGES INTO WINS

LEVEL UP YOUR IT: TURNING INFRASTRUCTURE UPGRADE CHALLENGES INTO WINS

This whitepaper addresses the strategic importance of technology infrastructure upgrades, with a focus on overcoming challenges such as fragmented data silos, compliance risks, and visibility gaps. Using the upcoming end-of-life for Windows 10 as a practical example, the paper outlines frameworks and actionable recommendations to ensure seamless infrastructure modernization.

Background and Objectives

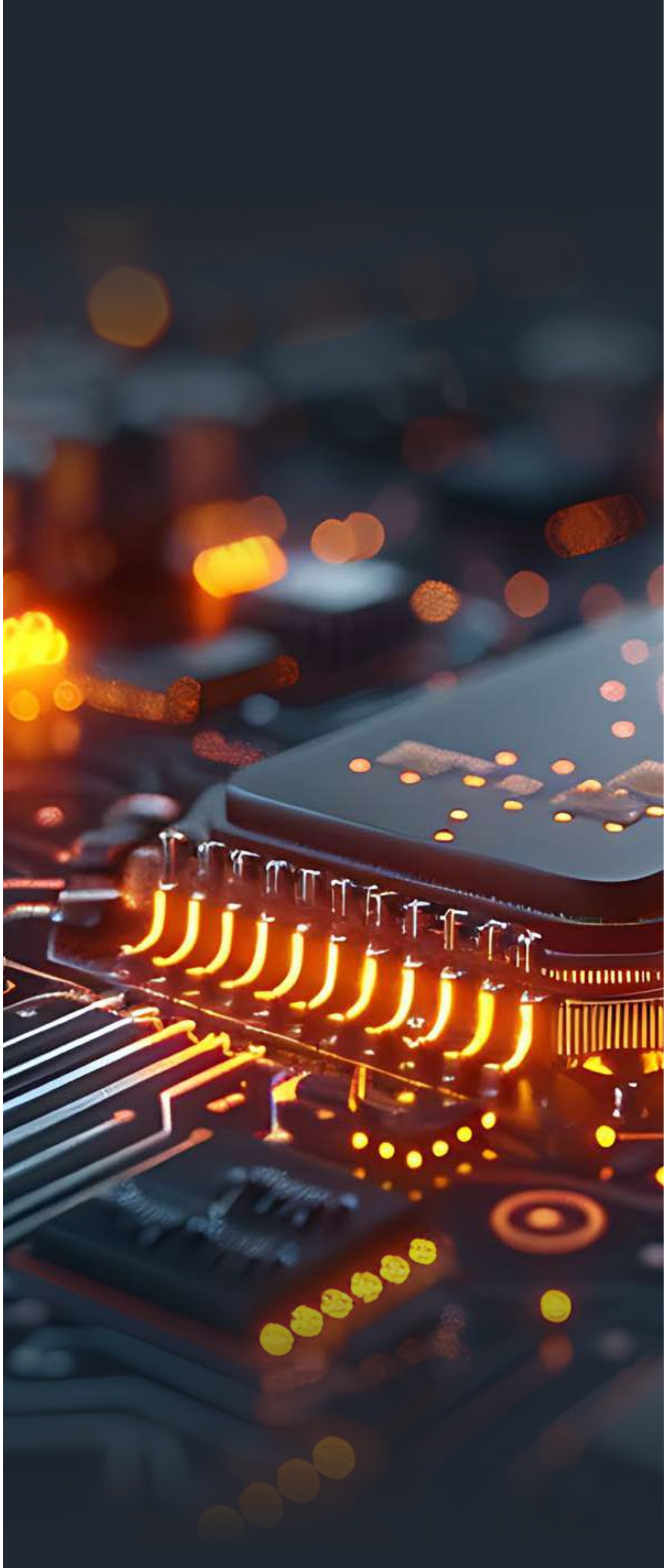
Modern technology environments face growing complexity due to rapid technological change, shadow IT, and evolving compliance requirements. In this whitepaper we aim to provide IT leaders with a structured approach to assessing their current infrastructure state, planning upgrades, and executing transitions to meet organizational goals.

Key Findings

- Visibility issues hinder effective decision-making, with shadow IT and siloed data creating blind spots.

- Outdated systems increase compliance risks and operational inefficiencies.

- Lack of financial clarity prevents optimal resource allocation and ROI assessment.



Proposed Solutions

A dual strategy of current state analysis and future state planning is recommended, supported by:

- Integrated asset management tools (e.g., CMDBs) for data centralization and collaboration.

- Automation to streamline compliance, asset tracking, and migration workflows.

- Lifecycle management to prioritize upgrades and align with business objectives.

Conclusions

By adopting proactive planning, automation, and integrated tools, organizations can reduce risks, optimize costs, and align infrastructure modernization with long-term strategic goals.

INTRODUCTION

Windows 10 will officially retire after more than 10 years of service in October 2025. According to research by Lansweeper, 60% of Windows clients are still running Windows 10, alongside 14% of Windows Servers that are operating on an end-of-life (EOL) system. This means that a lot of businesses will be taking steps in the coming months to either extend support or upgrade their client devices and servers. If it wasn't on your radar yet, it is time to get started on planning and executing the necessary Windows 10 to Windows 11 migration or upgrade.

Upgrading your organization's operating systems can be a significant undertaking, but with proper planning and execution, the transition can be smooth. Beyond ensuring compliance and performance, upgrading infrastructure can yield significant cost savings by removing inefficiencies, reducing maintenance costs, and eliminating legacy support fees. Outdated systems often require more frequent repairs, incur higher operational costs, and require special legacy support contracts making upgrades a more economical choice in the long term. This is where the entire IT team, from IT managers to system administrators and network administrators, plays a critical role to ensure business continuity while maintaining the performance and cost efficiency required by the organization. Additionally, modern systems and software often provide advanced automation capabilities that reduce manual labor, lowering operational expenses. Upgrade cycles don't only apply to operating systems, however, as they also extend to other core infrastructure components like networks, servers, and applications.

IT infrastructure management includes the process of managing, maintaining, and optimizing an organization's information technology (IT) systems, including hardware, software, networks, and data. Upgrading infrastructure components is a crucial part of this process, as it helps ensure that the IT systems remain up-to-date, efficient, cost-effective, and secure. Infrastructure upgrade projects are made up of 2 key components; current state analysis and future state planning.

Current state analysis is the process of assessing the organization's existing technology infrastructure, including hardware, software, networks, and systems. This involves taking inventory of all technology assets, evaluating their performance, identifying any gaps or pain points, and understanding the current capabilities and limitations of the infrastructure. The goal of the current state analysis is to gain a comprehensive understanding of the organization's technology environment as it stands today and where changes or upgrades are required. Future state planning builds upon the current state analysis to define the desired future state of the IT infrastructure. This involves identifying the organization's strategic goals, technology requirements, and business needs, and then mapping out the necessary infrastructure upgrades, replacements, and enhancements required to achieve that future state. By prioritizing scalable and cost-efficient solutions, future state planning ensures that investments made in IT upgrades deliver both immediate and long-term value. Future state planning considers factors such as scalability, flexibility, security, and alignment with the organization's overall digital transformation initiatives.

The outcome is a roadmap that outlines the specific steps, timelines, and resources needed to transition the IT infrastructure from its current state to the desired future state. This paper will focus primarily on the challenges of a current state analysis rather than future state planning.

THE CHALLENGES OF IT INFRASTRUCTURE UPGRADES AND HOW TO OVERCOME THEM

Understanding the current state of your IT infrastructure is essential for ensuring that upgrades align with your organization's needs and objectives. Without a clear baseline, IT teams may overlook critical issues such as legacy systems, overutilized resources, configuration drift, EOL equipment or unpatched vulnerabilities. An accurate assessment provides valuable insights into what devices are present in your infrastructure along with system dependencies, performance bottlenecks, and security gaps. This helps organizations prioritize upgrades effectively and avoid costly missteps. A comprehensive understanding of the current state also ensures that upgrade plans are realistic, targeted, and aligned with long-term business goals.

This section explores the key challenges IT teams face in achieving a clear view of their existing infrastructure and the solutions available to address these obstacles. Each challenge focuses on a specific problem, from maintaining compliance with evolving standards to managing shadow IT and overcoming fragmented data silos. By addressing these challenges, organizations can lay a solid foundation for informed decisions, smoother transitions, and successful IT infrastructure modernization efforts.

Lack of Visibility Across Complex Environments

Modern IT environments have become highly complex, with organizations managing a mix of cloud infrastructure, on-premise systems, IoT devices, and operational technology (OT). This diversity creates significant challenges for IT teams in maintaining a comprehensive understanding of their infrastructure. Gartner's Cybersecurity Controls Assessment benchmark of 2023 reports that only 17% of organisations can clearly identify and inventory 95% or more of their assets. Without visibility, IT teams struggle to identify EOL devices, pinpoint performance bottlenecks, critical dependencies, configuration drifts, and more. The lack of clarity often leads to inefficiencies, unplanned downtime, and increased security risks as problems are only addresses when there is an immediate business impact.

The solution lies in implementing continuous discovery and inventory tools that provide a real-time overview of the entire IT environment. These tools can automatically detect devices and their software, users, configurations and network connections within your infrastructure.

Detailed device information like warranty tracking, hardware and software EOL status, performance metrics and software & firmware versions are key in identifying where infrastructure upgrades are required and to do capacity planning. you can improve its overall efficiency by integrating this data into your tech stack,

License Compliance tools are able to accurately map license costs and suggest software or license consolidations to save cost. Security tools gain additional context about devices to improve risk analysis. IT service management (ITSM) systems can improve their use cases like change management to address EOL devices, software & firmware upgrades and more before they cause downtime.

ASSET CATEGORY	BEST PRACTICE
IT Hardware	● Audit devices regularly to detect configuration drift and ensure compliance with organizational standards and policies. ● Review hardware lifecycles consistently and plan proactively for replacements based on end-of-life (EOL) and end-of-service (EOS) dates to avoid downtime and maintain support. ● Keep track of the warranty status for all hardware, leveraging support options before warranties expire to minimize unexpected costs. ● Assess hardware resource usage frequently to address underutilized or overutilized devices, optimizing performance and resource allocation.
Network equipment	● Maintain an up-to-date network topology map to quickly identify dependencies and bottlenecks. ● Monitor key performance and capacity metrics to prevent issues and ensure timely infrastructure expansions. ● Review hardware lifecycles regularly and plan replacements proactively based on end-of-life (EOL) and end-of-service (EOS) dates to maintain system reliability. ● Schedule regular firmware updates for network devices to enhance security and ensure optimal performance.
Software	● Implement an automated change management process to ensure software remains up-to-date and secure. ● Regularly review software lifecycles and plan replacements proactively based on end-of-life (EOL) and end-of-service (EOS) dates. ● Simplify IT management by standardizing the software suite used across the organization to reduce complexity. ● Review the compatibility of business-critical services with newer operating systems to avoid disruptions during upgrades.
Operation Technology (OT)	● Regularly review hardware lifecycles and plan replacements proactively based on end-of-life (EOL) and end-of-service (EOS) dates. ● Schedule regular updates for OT devices to maintain security and ensure optimal performance.
Public Cloud Resources	● Use cloud monitoring tools to maintain an accurate inventory of instances, storage, and workloads across multiple cloud platforms. ● Regularly assess cloud resource usage to identify underutilized services or unnecessary expenses and optimize accordingly. ● Implement role-based access controls (RBAC) and continuous monitoring to ensure security and compliance with organizational policies.

COMPLIANCE REQUIREMENTS ARE HARD TO MAINTAIN AND TRACK

Organizations face growing pressure to adhere to industry standards like ISO27001, SOC2, DORA, and FEDRAMP, but ensuring compliance across a complex IT environment is a major challenge. Compliance frameworks often require detailed records of systems, configurations, and security practices, which can be difficult to maintain without centralized oversight. Non-compliance can lead to regulatory penalties, reputational damage, and vulnerabilities that may expose the organization to data breaches or operational disruptions.

Addressing this challenge requires compliance management solutions that integrate with IT asset tracking and security tools. These systems should offer features such as automated compliance checks, audit trail generation, and alerts for non-compliance risks. By centralizing compliance data and linking it to inventory and monitoring systems, organizations can streamline audits, ensure continuous adherence to regulations, and mitigate risks proactively. Tools that include templates or workflows tailored to specific frameworks make it easier for IT teams to stay compliant while reducing manual effort.

ASSET CATEGORY	BEST PRACTICE
IT Hardware	● Maintain an up-to-date inventory of hardware to track compliance-related details like, and end-of-life dates, encryption status, access management, and more. Automate compliance checks to ensure hardware aligns with required standards such as ISO27001 or FEDRAMP.
Network equipment	● Implement automated configuration audits to verify compliance with security standards, encryption protocols, and access policies. Document and regularly review network device configurations to streamline regulatory audits.
Software	● Use software management tools to monitor license compliance, version updates, and patching compliance. Ensure applications meet relevant compliance standards by incorporating automated reporting tools for audits.
Operation Technology (OT)	● Track firmware versions and device configurations to ensure compliance with industry-specific regulations like ISA/IEC 62443. Identify non-compliant OT devices that require upgrades to meet the required security and operational standards.
Public Cloud Resources	● Continuously monitor cloud resource configurations to detect non-compliance with frameworks such as FEDRAMP, GDPR, or ISO27001. ● Establish automated compliance guardrails within cloud platforms to prevent unauthorized access, ensure encryption, and maintain audit trails for resource changes.

KEEPING UP WITH RAPIDLY CHANGING CONFIGURATIONS

Configurations in IT environments evolve constantly, driven by software updates, hardware changes, and user activity. Tracking these changes manually is nearly impossible, leading to a lack of awareness about misconfigurations, lack of encryption, or devices operating outside of intended specifications. Such issues can result in degraded performance, security vulnerabilities, unexpected downtime, and compliance breaches disrupting business operations.

The solution is to use configuration management database (CMDB) tools that automatically centralize and organize information about an organization's devices, their configurations, and relationships. These tools enable IT teams to set baselines, monitor deviations, and receive alerts for unauthorized changes or errors in order to support decision-making, incident resolution, and change management.

Advanced features such as policy enforcement and automated rollback capabilities help maintain stability and security. Integrating configuration management with discovery and monitoring systems ensures a holistic approach, allowing IT teams to react quickly to changes and maintain operational efficiency.

ASSET CATEGORY	BEST PRACTICE
IT Hardware	● Use configuration management tools to track hardware settings, ensuring that updates are logged and unauthorized changes or configuration deviations are flagged.
Network equipment	● Automate network configuration tracking to detect changes in near real time and validate against predefined policies. Enable rollback features to quickly revert unintended or misconfigured network changes.
Software	● Implement tools that discover software configurations and flag unapproved changes, ensuring compliance with security baselines. Regularly audit software settings to maintain alignment with organizational and regulatory requirements.
Operation Technology (OT)	● Use OT-specific discovery systems to inventory device configuration and firmware. Develop and enforce configuration baselines tailored to the safety-critical nature of OT environments.
Public Cloud Resources	● Leverage cloud configuration monitoring tools to detect unauthorized changes and enforce organizational policies. ● Regularly assess and update security settings, access controls, and resource allocations to maintain compliance and optimize performance in dynamic environments.

SHADOW IT CREATES GAPS IN OVERSIGHT

Unauthorized devices, software, and cloud services—collectively known as shadow IT—pose significant challenges to IT teams. According to research conducted by Cisco, 46% of organizations report that shadow IT makes it impossible to protect all of their data, systems and applications all of the time, 20% of organizations report having experienced a cyber event due to unsanctioned IT resources. These unapproved assets often bypass standard security measures, increasing the organization's vulnerability to data breaches, compliance failures, and resource inefficiencies. Additionally, shadow IT complicates inventory management, leaving IT teams with blind spots that make it difficult to secure and optimize the environment.

Addressing shadow IT requires solutions that provide continuous discovery of devices and applications, aligning with a zero trust policy that enforces "never trust, always verify." Advanced discovery and inventory tools with features like automated asset detection, passive discovery, continuous tracking, and detailed device profiling enable IT teams to maintain visibility across the IT landscape.

These tools support zero trust architectures by providing accurate, up-to-date information about connected assets, enabling dynamic access controls and risk-based authentication. Combined with robust network monitoring and endpoint management, these capabilities help detect unauthorized traffic, mitigate rogue devices, and enforce consistent security policies, effectively reducing shadow IT risks.

ASSET CATEGORY	BEST PRACTICE
IT Hardware	● Implement continuous passive discovery tools to detect unauthorized or untracked devices connected to the network.
Network equipment	● Use port connection information and network diagrams to detect unauthorized devices or connections and restrict access through network segmentation. Enforce policies that require authentication for all devices connecting to the network.
Software	● Implement software discovery to identify unapproved or rogue applications in use across the organization. Implement strict application whitelisting and user training to prevent unauthorized software installations.
Operation Technology (OT)	● Conduct regular scans of OT environments to identify unauthorized devices or systems introduced without IT oversight. Integrate OT visibility tools with IT monitoring platforms to centralize control and mitigate risks.
Public Cloud Resources	● Use cloud access security broker (CASB) tools to monitor and control access to unsanctioned cloud services. ● Enforce zero trust principles by implementing strong access controls and real-time monitoring for cloud applications.

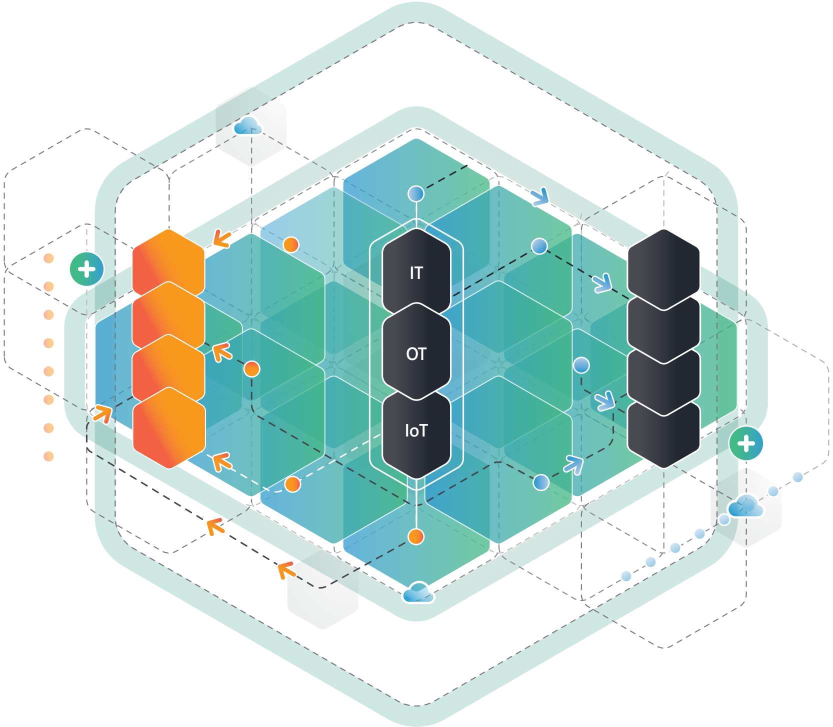
FRAGMENTED DATA SILOS OBSTRUCTING CLARITY

Data silos across IT, OT, Cloud and business systems prevent organizations from gaining a unified view of their infrastructure. These disconnected systems result in incomplete visibility, where critical information about hardware, software, and configurations remains fragmented. This leads to inefficiencies, duplicated efforts, and missed opportunities for optimization. Gartner reports that organisations lose an average of $12.9 Million a year due to poor data quality and data silos.

Siloed data often causes inaccurate capacity planning and delays in identifying dependencies between assets, increasing the risk of errors during upgrades. Without integrated data, IT teams struggle to understand the relationships between assets, making it harder to plan upgrades, troubleshoot issues, or mitigate risks effectively. Moreover, data silos can hinder proactive decision-making and contribute to security vulnerabilities by leaving certain systems unmanaged or untracked.

Breaking down data silos requires integrating asset data into centralized platforms that enable cross-team collaboration. Implementing unified asset management is essential to consolidate data from disparate systems into a single source of truth. These platforms should include robust discovery tools to ensure all assets—whether in IT, OT, or business systems—are accurately tracked. Key functionalities include API integrations, data normalization, and customizable dashboards, which allow IT teams to correlate data across domains.

Additionally, dependency mapping helps to identify relationships between assets and detect potential risks early. With a unified view, organizations can improve decision-making, streamline processes, reduce security vulnerabilities, and align IT operations with business goals. By fostering cross-departmental collaboration and integrating silos into a centralized system, businesses can proactively plan upgrades, enhance operational efficiency, and ensure infrastructure scalability.



ASSET CATEGORY	BEST PRACTICE
IT Hardware	● Centralize IT hardware data by integrating asset tracking tools with IT service management (ITSM) systems. Standardize data formats and processes to ensure compatibility across different platforms.
Network equipment	● Consolidate network device data into unified network management or discovery platforms for unified visibility and control.
Software	● Consolidate software licensing and usage data into a single platform to identify duplication or underutilization across departments. ● Create a single change management platform to track updates, patches, and upgrades across all software systems. ● Use middleware or integration platforms to combine fragmented software data into a centralized system for better oversight and reporting.
Operation Technology (OT)	● Merge OT data into a unified platform that integrates with IT tools, providing a comprehensive view of all devices. Adopt cross-functional collaboration between IT and OT teams to break down silos and share critical information effectively.
Public Cloud Resources	● Leverage cloud management platforms to centralize data about instances, configurations, and resource usage across multiple cloud environments. ● Implement discovery and inventory software that can combine cloud data with on-premises systems, enabling a unified infrastructure view.

DIFFICULTY IDENTIFYING OUTDATED AND UNSUPPORTED SYSTEMS

Data shows that 69% of physical servers are no longer covered by mainstream support.* Legacy systems and unsupported devices often go unnoticed in IT environments, creating hidden risks that can disrupt operations or expose the organization to security breaches. Fragmented data across systems and a lack of accurate, up-to-date inventory make it difficult to identify and track these assets. These systems are prone to failures, may lack vendor support, and often fail to meet modern compliance requirements.

Additionally, the absence of automated discovery tools and dependency mapping complicates efforts to pinpoint outdated systems and their relationships with other assets. Without visibility into such assets, IT teams struggle to prioritize replacements, increasing maintenance costs and vulnerability exposure. Resource constraints and organizational resistance further exacerbate the challenge, delaying upgrades and prolonging the lifecycle of unsupported devices. Automated asset discovery tools that provide detailed lifecycle tracking are key to addressing this challenge. These tools can flag devices nearing end-of-life, unsupported software versions, or systems with known vulnerabilities. By incorporating advanced discovery capabilities, they can detect hidden devices, such as IoT or shadow IT assets, which are often overlooked. Integration with ITSM platforms enables teams to link inventory data with service tickets, ensuring a proactive approach to replacements and upgrades.

Centralizing asset data and automating compliance checks also simplifies meeting regulatory requirements, reducing the risk of penalties. Reporting and predictive analytics further empower IT teams to make timely decisions, streamline resource allocation, and address prioritization challenges efficiently, ultimately minimizing risks, maintenance costs, and operational disruptions.

ASSET CATEGORY	BEST PRACTICE
IT Hardware	● Use lifecycle management tools to identify hardware nearing end-of-life or lacking vendor support. Prioritize replacement of critical devices that impact operations or security.
Network equipment	● Regularly audit network devices to track firmware versions and support status, ensuring timely upgrades or replacements. Integrate these audits with monitoring tools to flag unsupported or legacy equipment.
Software	● Implement software inventory tools to detect outdated or unsupported applications and assess their risk level. Schedule updates or plan replacements for software that no longer meets security or compliance standards.
Operation Technology (OT)	● Conduct routine assessments of OT devices to check for unsupported firmware or discontinued vendor support. Develop upgrade plans for critical OT systems while ensuring minimal operational disruption.
Public Cloud Resources	● Use cloud asset management tools to identify deprecated services or instances running unsupported configurations. ● Automate lifecycle tracking and integrate cloud asset data with on-premises systems to ensure timely updates and replacements.

LIMITED VISIBILITY INTO COSTS AND ROI

A lack of clear visibility into infrastructure costs makes it challenging for IT teams to evaluate ROI or justify budget allocations for upgrades. To such a point that 27% of respondents to a Gartner survey on cost optimisation programs mentioned that implementing IT asset management practices was one of their top strategic initiatives. Without accurate data, organizations risk overspending on maintenance, underestimating upgrade needs, or missing opportunities to optimize costs.

Service interruptions during upgrades can lead to significant downtime costs, further straining budgets and delaying modernization. Additionally, failure to address compliance requirements for outdated systems may result in fines, compounding financial risks. This often results in inefficient use of resources and delayed modernization efforts. Continued reliance on legacy systems during phased upgrades increases interim maintenance costs, while unaddressed vulnerabilities can lead to breaches with associated financial losses.

The solution involves using financial tracking tools that integrate with IT asset management systems. These tools provide insights into total cost of ownership (TCO), including upfront costs, maintenance expenses, and operational risks associated with aging systems. They can also help identify and mitigate downtime costs by providing real-time tracking of system dependencies and upgrade schedules, reducing the likelihood of service interruptions. Features such as cost forecasting, scenario analysis, and ROI tracking help IT teams plan and justify investments more effectively.

Compliance tracking capabilities ensure organizations address outdated systems proactively, avoiding fines and regulatory penalties. With better financial visibility, organizations can allocate resources strategically and ensure upgrades align with budgetary constraints and long-term goals. Additionally, these tools can highlight the rising maintenance costs of legacy systems during phased upgrades and identify vulnerabilities that could lead to costly security breaches, ensuring a more comprehensive financial management approach.

ASSET CATEGORY	BEST PRACTICE
IT Hardware	● Use financial tracking tools to calculate the total cost of ownership (TCO) for hardware, including purchase price, maintenance, and energy consumption. Prioritize replacing hardware with high operational costs, risk or low efficiency to improve ROI.
Network equipment	● Optimize network investments by replacing aging or EOL network devices minimizing risk. Align upgrades with business growth and scalability requirements.
Software	● Track software licensing costs, renewal schedules, and usage metrics to identify redundant or underutilized applications. Consolidate software licenses and decommission unused software to optimize expenses.
Operation Technology (OT)	● Assess the operational costs of OT devices, including extended vendor support and energy usage, against their criticality to processes. Replace outdated OT systems when the risks or costs outweigh their utility.
Public Cloud Resources	● Use cloud cost management tools to monitor and control resource consumption, including storage, compute, and bandwidth. ● Conduct regular ROI assessments for cloud services to identify underutilized resources and opportunities for cost optimization.

Tying It All Together: Preparing for What's Next

Infrastructure upgrades are no longer isolated projects—they are part of a broader strategy that ensures organizations remain agile, secure, and cost-efficient in an increasingly complex IT landscape. As we've seen, challenges such as fragmented data silos, compliance requirements, evolving configurations, shadow IT, and limited visibility into costs and ROI can obstruct effective infrastructure management. However, the solutions outlined emphasize the need for integration, automation, and cross-team collaboration to overcome these barriers.

A PRACTICAL EXAMPLE, WINDOWS 10 END-OF-LIFE

Understanding the full impact of Windows 10 reaching its end-of-life is critical to developing a successful migration strategy. The end of support not only means no more security updates but also the potential loss of compatibility with newer software, and security tools. This leaves systems increasingly vulnerable to cyberattacks, compliance violations, and operational risks. IT teams must assess which devices, systems, and applications are dependent on Windows 10 to prioritize their upgrade or replacement. This evaluation should include identifying business-critical services, ensuring compatibility with Windows 11, and addressing potential performance bottlenecks during migration. Without this comprehensive evaluation, organizations risk disruptions, unexpected costs, and long-term inefficiencies. A proactive approach, including lifecycle tracking, dependency mapping, and real-time inventory management, is essential to minimize these risks and ensure a seamless transition.

Windows 10 End-of-Life Migration Guide/Checklist

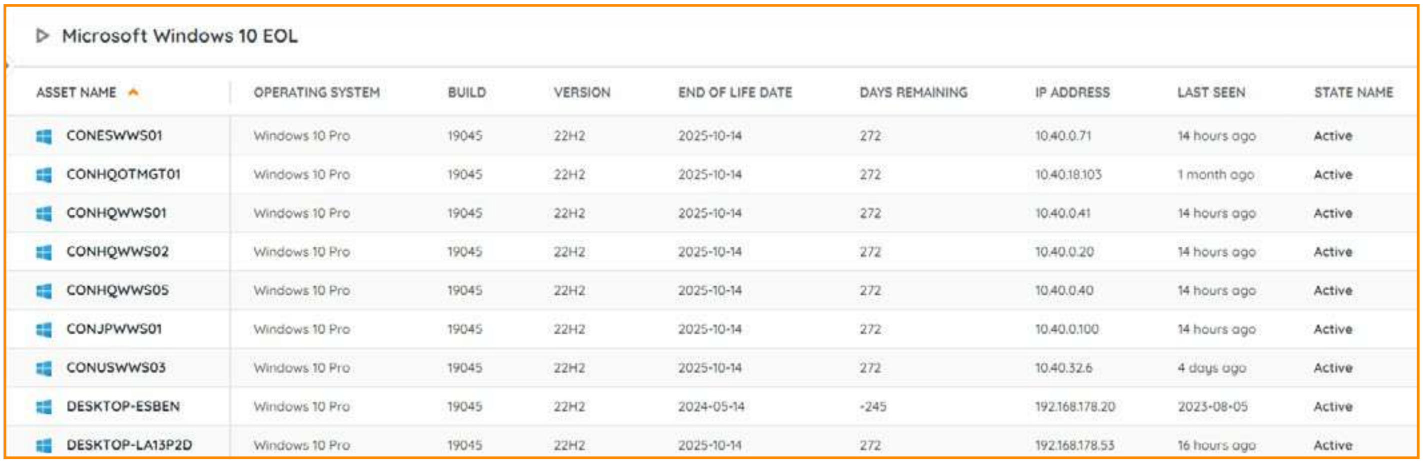
1. Implement Comprehensive Device Discovery

The first step in your Windows 10 migration process is to start with the basics. Implementing a discovery tool in your environment. Use a combination of passive, active and agent-based discovery to ensure full coverage and provide flexibility in how you want (or need) to discover every single device in your environment.

2. Get a Complete View of Windows 10 Devices in Your Environment

With discovery covered, you should now have the ability to get a full overview of all devices running a Windows 10 operating system, including their edition, end-of-life status and date, and also additional details like who is using that device, the hardware within that device and more.

Within Lansweeper, this can be achieved in multiple ways. The easiest is to utilize one of the over 400 built-in reports. The Windows 10 EOL Audit provides an accurate overview of exactly what you need.



▷ Microsoft Windows 10 EOL

ASSET NAME ^	OPERATING SYSTEM	BUILD	VERSION	END OF LIFE DATE	DAYS REMAINING	IP ADDRESS	LAST SEEN	STATE NAME
CONESWWS01	Windows 10 Pro	19045	22H2	2025-10-14	272	10.40.0.71	14 hours ago	Active
CONHQOTMGT01	Windows 10 Pro	19045	22H2	2025-10-14	272	10.40.18.103	1 month ago	Active
CONHQWWS01	Windows 10 Pro	19045	22H2	2025-10-14	272	10.40.0.41	14 hours ago	Active
CONHQWWS02	Windows 10 Pro	19045	22H2	2025-10-14	272	10.40.0.20	14 hours ago	Active
CONHQWWS05	Windows 10 Pro	19045	22H2	2025-10-14	272	10.40.0.40	14 hours ago	Active
CONJPWWS01	Windows 10 Pro	19045	22H2	2025-10-14	272	10.40.0.100	14 hours ago	Active
CONUSWWS03	Windows 10 Pro	19045	22H2	2025-10-14	272	10.40.32.6	4 days ago	Active
DESKTOP-ESBEN	Windows 10 Pro	19045	22H2	2024-05-14	-245	192.168.178.20	2023-08-05	Active
DESKTOP-LA13P2D	Windows 10 Pro	19045	22H2	2025-10-14	272	192.168.178.53	16 hours ago	Active

3. Ensure Budget Allocation

Assuming that you'll at least have a few old devices that won't be able to upgrade to Windows 11, you'll need to take this into account when creating your yearly budget, allocating funds to specific budgets or creating additional budget requests.

Using the data gathered, you should be able to create an accurate budget for the Windows 10 EOL including all the devices that cannot be upgraded and the cost of replacement.

If your budget request requires a financial risk analysis or ROI proof, the following items can all be used to put hard numbers on a sheet of costs associated with delaying migration to a supported Windows version:

- **Mitigate Security Risks:** Avoid vulnerabilities and cyberattacks due to lack of updates.
- **Ensure Compliance:** Meet regulatory standards and avoid fines for non-compliance.
- **Reduce Maintenance Costs:** Lower repair costs and eliminate expensive legacy support fees.
- **Future-Proof Systems:** Support new technologies and ensure compatibility with modern applications.
- **Reduce Downtime:** Prevent unplanned outages caused by aging hardware.

4. Develop Migration Priorities

Now that you have an overview of all devices that require an upgrade it is time to prioritize and plan out the migration. In most cases, this would include evaluating business-critical dependencies, but since Windows 10 is a client OS, we presume you don't have business critical applications hosted on them.

Other items you can use to prioritize migration on include:

- Devices used by key personnel or teams driving core business functions (e.g., finance, sales, operations).
- Devices used by key personnel or teams handling sensitive data or connected to critical networks that could pose a higher risk if breached.
- Devices that can be upgraded to Windows 11 and meet the Windows 11 Requirements

5. Link Your Discovery System to Your CMDB and ITSM Tool

With priorities and potential deployment rings figured out, its time to incorporate your plans into your tech stack. This means ensuring your discovery/data systems are connected to the rest of your tech stack like your CMDB, ITSM and ERP tooling.

Your CMDB will be the link between your discovery systems and other tools like your ITSM tool, ensuring that your ITSM tool utilizes up-to-date and accurate data to trigger workflows and automations so the right people get assigned the right tasks and have the correct data. Your ITSM tool will do the bulk of the work. Lansweeper integrates with plenty of CMDB and ITSM tools like Jira Service Management, HaloITSM ServiceNow and more.

6. Create Automations/ Workflows

With your systems connected, its time to use everything we have so far and create your change management automations in your ITSM tool using the data from your CMDB which is fed by your discovery tool.

The following is a generic, simplified automation example which you'll need to adjust to the specific conditions in your organization, but its a good example to follow.

Automation Design Process Steps:

- Identify devices running Windows 10
- Is the hardware compatible with Windows 11?
- Assign a priority to the device upgrade/replacement based on your chosen metrics
- Notify stakeholders and users of the planned upgrade/replacement
- Schedule upgrade/replacement windows to minimize disruption
- Execute the upgrade via automated deployment tools / Trigger your lifecycle management workflow to replace the device
- Validate the upgrade/replacement and resolve any issues.

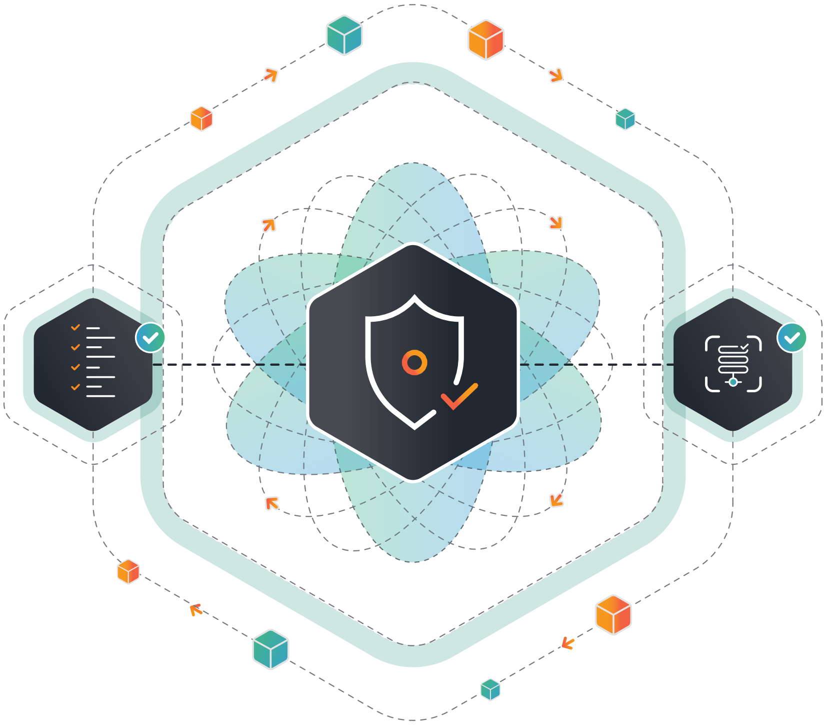
CONCLUSION

Infrastructure upgrades are a fundamental component of modern IT strategy, ensuring that organizations remain competitive, secure, and efficient in a rapidly evolving technological landscape. The challenges explored, such as fragmented data silos, outdated systems, compliance requirements, and shadow IT, highlight the complexity of managing diverse IT environments. However, by leveraging integrated tools, automation, and strategic planning, these obstacles can be effectively mitigated. As businesses prepare for major transitions like the Windows 10 end-of-life, adopting a proactive, data-driven approach to upgrades is critical for minimizing risks, optimizing costs, and enabling scalability.

Key Takeaways

1. **Proactive Planning is Essential:** Understanding current infrastructure and defining future goals ensures alignment with business needs.
2. **Visibility is Key:** Integrated tools like CMDBs and discovery platforms provide a unified view of assets, dependencies, and configurations.
3. **Compliance is Non-Negotiable:** Maintaining adherence to regulatory standards avoids penalties and strengthens security posture.
4. **Cost Optimization Drives ROI:** Accurate lifecycle tracking, cost forecasting, and license management reduce TCO and justify upgrade investments.
5. **Automation Enhances Efficiency:** Automating discovery, compliance checks, and upgrade workflows reduces manual workload and operational disruptions.
6. **Collaboration Overcomes Complexity:** Cross-functional alignment between IT, OT, and business systems is critical for breaking down data silos and enabling seamless transitions.

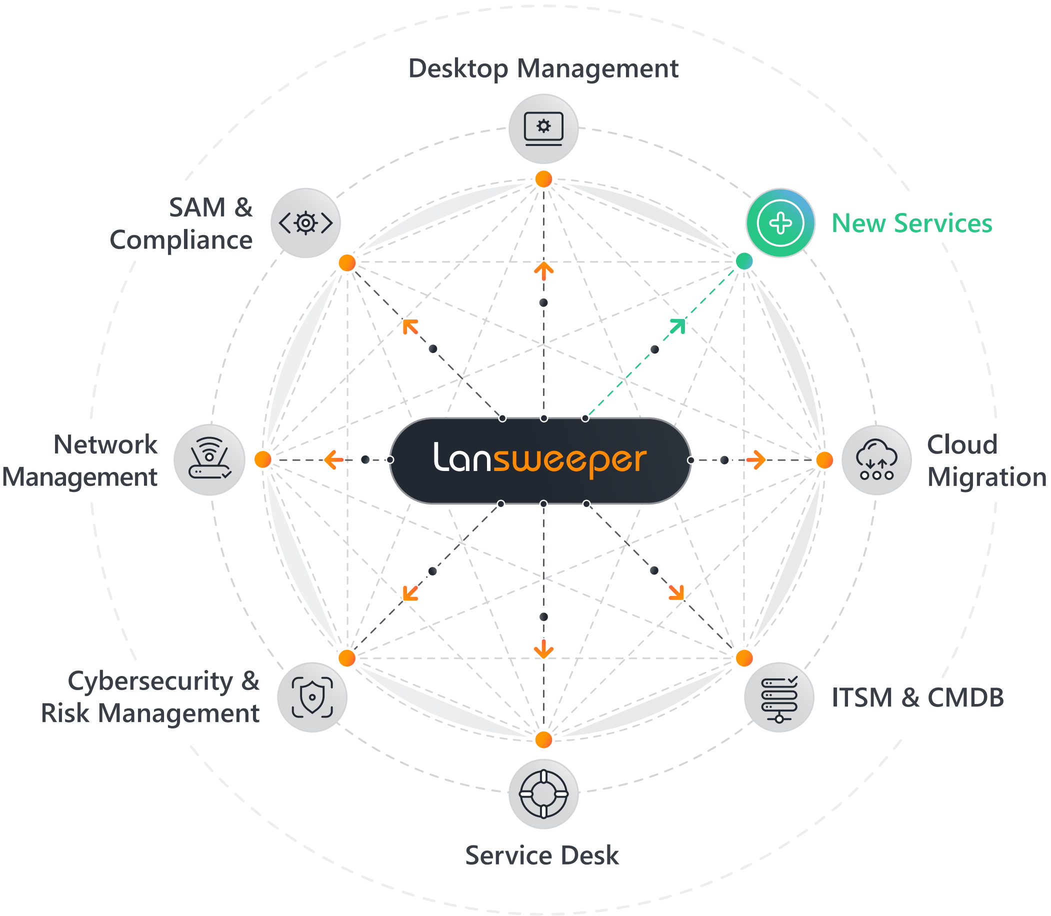
By addressing these areas with a structured and integrated approach, organizations can not only navigate the challenges of IT infrastructure upgrades but also position themselves for long-term success.



WHAT LANSWEEPER CAN DO FOR YOU

Lansweeper is a comprehensive Technology Asset Intelligence solution designed to provide organizations with unparalleled visibility into their technology environments. By automatically discovering and inventorying all hardware, software, and connected devices across networks, Lansweeper creates a centralized repository of actionable data.

Trusted by more than 20,000 customers worldwide—whether directly, through managed service providers (MSPs), or under the hood of one of our technology partners—Lansweeper helps organizations efficiently manage assets, address vulnerabilities, and align IT operations with broader business objectives. With features tailored to support operational efficiencies, security and compliance, and strategic planning, Lansweeper serves as a foundational tool for modern IT infrastructure management.



Create Operational Efficiencies for your IT Operations

One of Lansweeper's key benefits is its ability to enhance operational efficiency by automating asset discovery and inventory management. IT teams can eliminate manual tracking processes, reducing administrative overhead and the risk of errors. The platform's reporting and alerting capabilities empower teams to quickly identify outdated devices, misconfigurations, and streamline processes such as software deployments and patch management. By integrating Lansweeper with IT service management (ITSM) systems, organizations can further enhance workflows, improve ticket resolution times, and ensure that accurate asset data informs every decision.

Enhance Security and Compliance

In today's rapidly evolving threat landscape, maintaining robust security and compliance is essential. Lansweeper helps organizations proactively address vulnerabilities by identifying end-of-life hardware, unpatched software, and shadow IT devices that could expose the network to risks. Its detailed asset data supports compliance with regulatory frameworks by providing a clear audit trail of system configurations, software licenses, and security patches. Integration with cybersecurity tools enables deeper insights into asset vulnerabilities, supporting more effective threat mitigation strategies and ensuring adherence to industry standards.

Drive Strategic and Financial Planning

Beyond day-to-day IT operations, Lansweeper plays a pivotal role in strategic planning and financial management. With its detailed insights into asset lifecycles, cost structures, and usage patterns, organizations can make informed decisions about technology investments and future upgrades. The platform provides the critical data needed for accurate total cost of ownership (TCO) calculations, empowering finance teams to optimize budgets and align spending with long-term goals. Furthermore, Lansweeper's rich data provides the foundation for planning infrastructure upgrades, and aligning IT strategies with broader business objectives, ensuring maximum ROI.

Next Steps

If you're ready to bring Technology Asset Intelligence and its benefits to your organization, reach out to our team to learn how Lansweeper can enhance visibility, streamline operations, and support strategic decision-making. Our experts can guide you in leveraging Lansweeper's capabilities to address your unique challenges and maximize ROI.

Or, if you prefer to explore independently, visit lansweeper.com/try to start your free trial and experience firsthand how our platform empowers organizations to take control of their IT infrastructure.

Lansweeper

About Lansweeper

Lansweeper is the leading Technology Asset Intelligence platform empowering businesses with complete visibility and actionable insights into their technology environments. By automatically discovering and inventorying IT, OT, IoT, and cloud assets, Lansweeper provides a single source of truth that eliminates blind spots, enhances security, optimizes costs, and drives smarter decision-making.

With unmatched discovery and data accuracy, organizations can reduce risk, ensure compliance, and improve operational efficiency. Lansweeper□s powerful insights enable IT teams, MSPs, and security professionals to proactively manage vulnerabilities, streamline asset lifecycle management, and integrate with leading ITSM, security, and compliance solutions.

Founded in 2004, Lansweeper serves over 18,000 organizations worldwide, scanning and managing more than 80 million connected assets. From global enterprises like Maersk, Pepsico, and Nestlé to governments, banks, and universities, Lansweeper is the foundation of efficient IT operations, security resilience, and strategic IT management.

🔥

Want to try Lansweeper now?

Start Your Free 14-day Trial

👁️

Not ready yet?

Watch the demo video