ivanti

Expand Visibility, See Clearly, Act Decisively

Better IT Insights for Better Business Outcomes

Table of Contents

Introduction

If you take away nothing else from this white paper, consider this:

Gaining a full view of your IT assets, services, security posture, processes, and outcomes lays the foundation to properly manage, secure, and optimize your IT estate. You'll see more clearly, be able to act more decisively, and become more effective. This, in turn, will help you optimize costs and future budgets, improve the experience of your customers and employees, and position your team to be more productive and efficient.

And who wouldn't want that in today's world of highly regulated industries and compliance mandates; the need to provide clear direction for patching, cost optimization, application control, and asset location; and IT's "seat-at-the-table" objective of becoming a center of innovation, not just a cost center.

The truth is, full visibility is attained by degrees—with first steps, then more steps. For example:

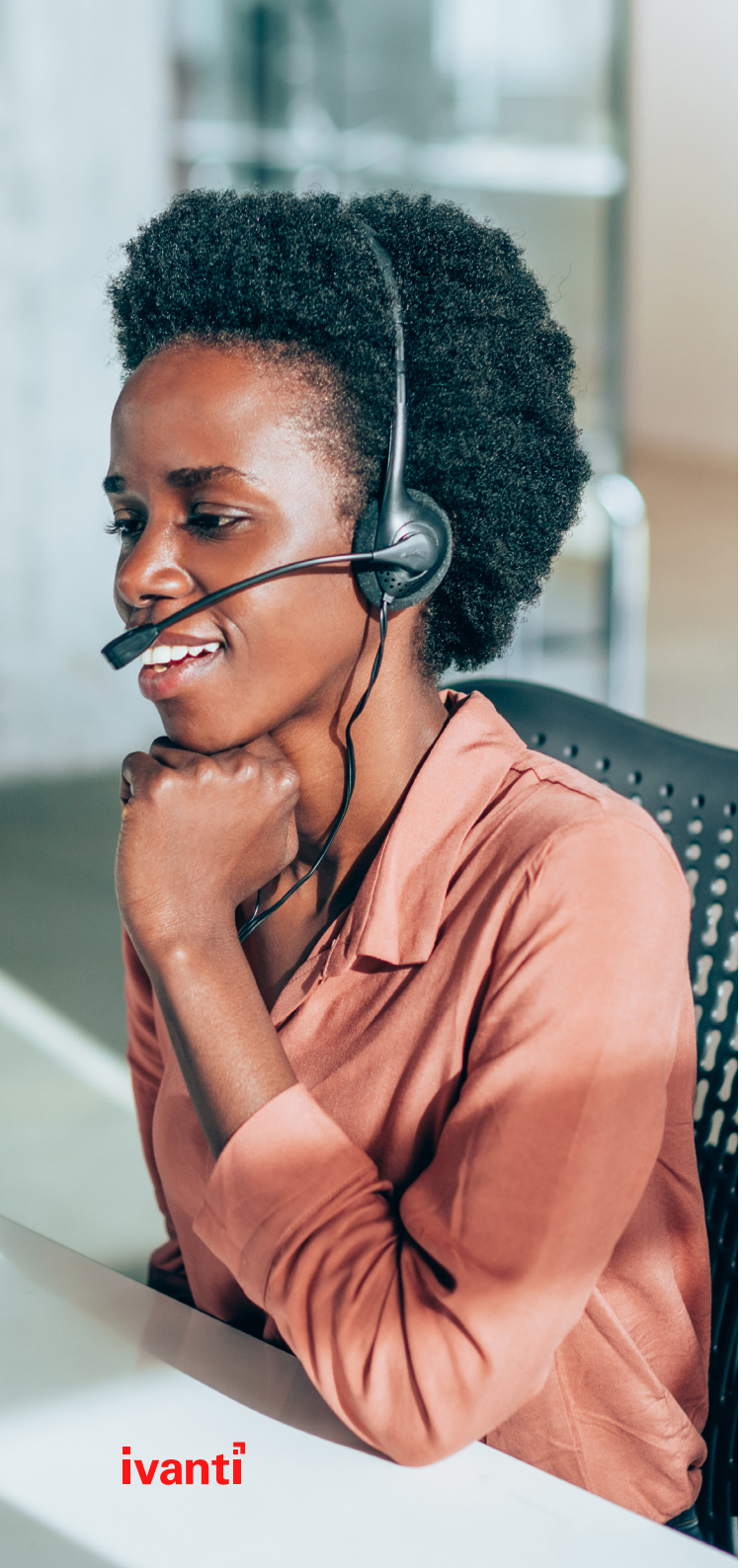
- Without establishing a baseline of where you're starting from, how can you know what you have from an asset, security, process, and maturity perspective, or the amount and type of work coming into IT?
- How can you manage what you don't know about in your IT environment?
- How can you deliver greater value to the business with the same budget and IT resources?
- How can you provide wider support for a broadening array of endpoint-device types with immature and/or manual practices that limit visibility across the board?

Ivanti Illuminates Every Corner of Your Enterprise IT Estate

Gaining visibility must become a foundational practice, and proven solutions from Ivanti direct a spotlight on every aspect of your enterprise IT estate. A unified IT approach brings together the IT teams from IT Service Management, IT Asset Management, Endpoint Security Management, and User and Workspace Management—organized under the pillars of Enterprise Service Management and Unified Endpoint Management. Supplied with greater clarity and visibility, you're more in sync with your users, services, and assets across the enterprise—and with your IT landscape, security posture, and processes and data. You have the wherewithal to attain more of your strategic objectives.

About this White Paper

This white paper provides six brief, illustrative use cases and research data points to help you assess where your IT organization could gain greater clarity and visibility, and it invites you to evaluate Ivanti solutions that are proven to help organizations do so.



Lack of Visibility: 6 Use Cases

Consider the six use-case scenarios that follow, and pain points typically associated with a lack of visibility.

1 Laptops in Slow-Mo

A help desk agent notices an uptick in calls concerning issues around slow laptop performance. After many time-consuming follow-up calls, the agent learns an executive returned from a conference a week earlier with what the exec deemed was a “killer app” and encouraged downloading from his USB drive, resulting in reuse of the same license. Further investigation also reveals the app is a resource hog, but it’s unclear how many laptops now have the app installed.

Many IT organizations today have immature and/or manual practices in place that limit visibility across the board. Without visibility, it’s very difficult to detect, manage, and secure hardware and software, as well as manage software usage effectively.

The scenario above touches on several unknowns:

- The risk of non-compliance due to unlicensed software used.
- Shadow IT—employees circumventing IT and installing unauthorized software.
- The number of laptops potentially affected.
- The total number of incoming related incidents.
- Security risks created by the unauthorized software installation and usage.
- Unknown license true-up risks.

Reinforcing the message that you can’t manage, protect, and optimize what you don’t know you have nor can easily see, an Ernst & Young (EY) white paper titled “Data Validation the Best Practice for Data Quality in Fixed Asset Management” states that 56% of enterprises verify the location of their fixed assets once a year, while 10% to 15% have not verified their assets in more than five years.

With no formal IT Asset Management (ITAM) program, teams often rely solely on Active Directory or basic inventory information from endpoint management

43%

of organizations surveyed are still using spreadsheets.

50%

are using an endpoint management solution.

45%

use inventory tools as one of their resources.

solutions. On the topic of tracking assets, the ITXM Survey research study commissioned by Ivanti in December 2019 found the following. Please note that organizations may be using more than one of these options:

Multiple sources of data that must be married together—such as ITSM, ITAM, and SAM data—restrict the speed to gain needed insight and overall visibility. According to research by Enterprise Management Associates (EMA), 50% of organizations have 12 or more discovery and/or inventory tools, and 11% have more than 30 tools. On average, organizations spend 10 hours a week resolving data accuracy issues, while 32% spend more than 25 hours per week.

In short, lack of visibility means you can't manage, protect, and optimize what you don't know you have nor can easily see. Ivanti solutions use powerful data-importing capabilities that help you combine data from several sources—spreadsheets, inventory tools, barcode scans, discovery services, etc.—to compare actual data against discovered data and report on discrepancies. With these insights, decision makers can validate assumptions and make sure asset information is always up to date and accurate.

2 Routers on the Receiving Dock

The Network Ops team gets a call from the receiving dock. A pallet of new routers has just arrived. The Ops team starts configuring the new routers to replace some older ones before they realize no one had ordered the new routers in the first place.

A lack of visibility leads to plenty of unknowns. What's the procurement history? Who are the preferred vendors and fulfillment paths? What are some of the potential security risks from unauthorized hardware connecting to the network?

The Ivanti-commissioned ITXM Survey (December 2019) mentioned earlier asked about how organizations track and monitor purchase data, contracts, and warranty data for their IT assets. The survey found the following. Again, please note that organizations may be using more than one of these options:

39%

of respondents use multiple systems and repositories.

38%

annually track this as part of their inventory spreadsheets.

37%

track it as part of their asset management repository/ database.

22%

use a separate contract management system.

Visibility into data and data sources—knowing what data there is and having it all in one place—will do much to ease the pains listed above. That should lead to data that's consistent, accurate, and trustworthy.

As mentioned in the introduction, when Enterprise Service Management and Unified Endpoint Management are closely aligned, integrated, and automated:

- You can use asset-discovery insights to make predictions and take prescriptive action on problem asset types, models, and vendor information.
- You'll benefit from deeper insight to help improve vendor management, compliance, and warranty optimization.
- IT staff are freed from reactive or unnecessary activities to focus on more strategic projects
- Security risks are reduced by knowing what hardware is authorized for use.
- You can accomplish more while minimizing costs and administrative efforts, providing more value directly to the business.

3 Pinching Pennies

The CIO directs staff to seek budget savings for the current year. The VP of Operations wants to see if they can defer the laptop refresh cycle, but it's uncertain how many laptops would be involved, which employees may be impacted, what potential issues would be created, and how much budget it would actually save.

The visibility pain points that surface in this use case include an unknown laptop-type incident and vendor history, no consistent tracking of the entire asset lifecycle to determine health and performance of laptop types, and an unknown patching history. It's also unknown which employees could be impacted.

With proper insights, an Ivanti customer was able to extend the hardware refresh cycles by six to twelve months, saving the IT organization an initial $1.5 million without increasing incident rates or impacting service quality to end users.

What's more, the ITXM Survey research study in December 2019 found that:

Understanding asset lifecycles, performance, compliance, and cost implications is particularly important for business enterprises operating in highly regulated industries. The medical device industry and the governmental Mobile Device Regulation (MDR) and associated European Database on Medical Devices (EUDAMED) regulations in the European Union are examples.

28%

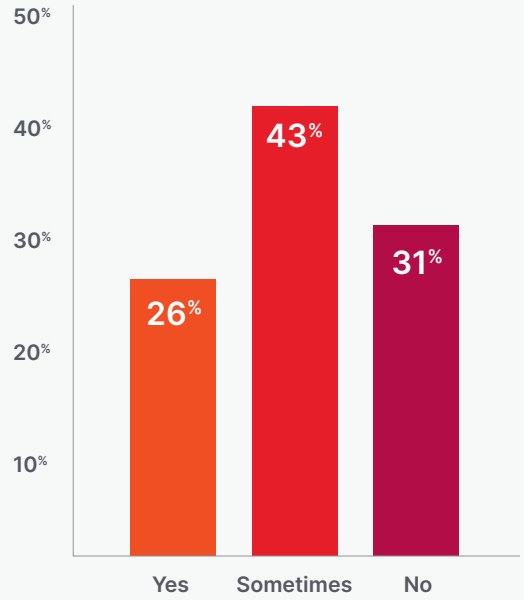
of IT professionals surveyed devote hours each week supporting out-of-warranty/ out-of-support policy assets.

20%

of them indicate they don't have insights into which assets are out of date.

Survey:
The Impact of Aligning IT Service & Asset Management Processes

Do your service management processes and request workflows automatically have visibility into asset information and relationships?



4 Snail Email

A flood of employee calls greets the help desk staff first thing in the morning. Email "isn't working" or is "extremely slow." After several calls to other IT teams, the IT Operations team concludes someone had updated the email application overnight and the current server couldn't handle the resulting configuration changes, leading to performance issues. It's not immediately clear if they have the needed hardware to alleviate the issues.

The lack-of-visibility pains here include an unclear change-and-configuration history, no view of future changes, no analysis of change impact and risks, and an unknown hardware inventory.

Organizations develop IT goals to heighten their maturity level and employ automation to realize efficiency gains. Yet many forget the critical first step—establishing a baseline to start from. This means: 1) gaining full visibility into processes and actions that affect key services and underlying assets such as change management; and 2) obtaining a full understanding of patterns in incidents, what's causing outages, and more in order to provide that baseline from which to improve.

The fact is, despite the best efforts of IT teams, poor systems and a lack of resources can make for tactical and reactive service and support activities. A systematic approach to move beyond short-term outcomes is constrained, and issues are resolved ad-hoc. What's more:

- Many processes are manual, lacking consistent IT workflows or standards.
- Visibility of status or impact is less than desired, with minimal to no reporting capabilities.
- Ongoing costs and risks are high, resolution timelines often lengthen, and service quality is low.

It's also worth displaying the finding below, taken from the December 2019 ITXM Survey, revealing whether organizations' service management processes and request workflows have visibility automatically into asset information and relationships:

As you can see, fewer than one third of respondents indicated they had visibility into asset information, while the remaining two thirds did sometimes or not at all.

According to the same survey, IT professionals expect to see the following improvements with help from integrated IT service management and IT asset management processes and data:

- 63% Better visibility of the IT estate
- 59% Increased IT staff productivity
- 54% Optimized costs
- 53% Improved service delivery

5 Laptop Lockout

> Calling the help desk, a sales rep reports he's locked out of his laptop and says there's a screen message to call another number to unlock. He also mentions he had clicked on a link from an email he thought was from a partner he's worked with before, and that's when the laptop locked. It's not clear, but other employees possibly received the same email.

In this use case, the potential pains that arise from a lack of visibility include no insight into other employees who received the same email, no updated view of current patch coverage, no knowledge of who has administration privileges for machines, and no insight into the number of infected devices and their status.

An Ivanti-sponsored Windows 10 survey in 2019 found that one top security concern of respondents is the risk of data breaches (41%), followed by fear of ransomware / malware (20%). In addition, another Ivanti-sponsored survey from April 2019 found that 70% of organizations would most want to know about security status if they could obtain real-time insights, and nearly 60% would want visibility into application data.

From a Unified Endpoint Management perspective, lack of visibility increases the time involved in tackling security incidents. It also increases the risk of an incident turning into a breach that compromises an organization's data, adds pressure to overworked teams, and reduces the trust in the organization. This can be the result of limited visibility or a lack of integrated data, leading to conflicting asset data and security information that create visibility gaps and make quick action difficult.

In contrast, with visibility into accurate patch data and user access information, it's possible to respond to attacks faster, protecting the network; kill threats like ransomware and stop them from spreading; and prepare for future attacks.

Also, a lack of visibility makes it difficult to manage re-imaging needs efficiently to support remediation in situations described above.

From the perspective of a service desk analyst, full visibility into what assets are in the environment, where they are, who is using them, and how they are used—all without cumbersome spreadsheets—is essential for efficient job performance, including faster resolution times on incidents and problems. In this use case, increasing the scope of visibility of the potential threat resulting from the suspect email fosters faster remediation.

6 Into the Unknown

An IT analyst is evaluating the environment's security, and she realizes it is unknown what machines are in the environment or whether they're managed properly. Only 75% of the environment is known. Through refreshes, etc., machines are becoming unmanaged. On the server-side, virtual machines have been created without the proper configuration information, nor kept up to date with the latest patches.

In this use case instance, there's no view of endpoints and servers in the environment and therefore no insight into what's patched to production level. Knowing where all organizational assets are at all times—physical or virtual—is not only vital from a service and support perspective, but from a security standpoint. Unmanaged and unpatched assets become a risk to data integrity and compliance. And with IT vulnerabilities on the rise, keeping track of every device becomes critical.

The EY white paper mentioned earlier titled "Data Validation the Best Practice for Data Quality in Fixed Asset Management," states that 30% of IT fixed assets are "ghost" assets and can't be found. Asset visibility is a critical first step as many organizations underestimate what they have. When organizations first start out with IT Asset Management, it's not uncommon to find 20% to 30% more devices than they thought they had. You can't manage what you don't know you have, and this poses a significant security risk.

With Unified Endpoint Management solutions, you gain complete visibility and control over your endpoints, helping you secure everything and avoid threats resulting from unprotected and unmanaged devices. IT teams benefit from an automated provisioning strategy that performs real-time scans and reconciles user and location information. To avoid virtual server sprawl, it's critical to see who has administrative privileges so that other IT groups can only spin up virtual machines with security that's at production level. Even then, the ability to find these new servers and add them to groups will avoid missing the next maintenance window.

What's more, it's critical to manage assets throughout their entire lifecycle. By tracking performance asset data, issues, fixes, patch information, contracts, and licensing, you can ensure software and hardware investments are running at optimal performance and not impacting employee productivity.

Ivanti: The Eyes in the Back of Your Head

CIOs, CISOs, and VPs of IT don't attain such levels of leadership and responsibility by being Cycloptic, myopic, or shortsighted. To that end, the expanded visibility you can experience with our Unified Endpoint Management and Enterprise Service Management solutions can complement and support your team objectives, industry insight, and business mission and vision.

See for yourself how Ivanti improves your IT visibility—empowering you to act decisively toward an improved IT experience for users and realize gains in organizational efficiency and productivity. Please contact us to learn more.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com