

# Expand Visibility, See Clearly, Act Decisively

## Better IT Insights for Better Educational Outcomes

### 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 digital infrastructure. 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 students, administrators, and educators and position your team to be more productive and efficient.

And who wouldn't want that given the rapid digitization of the educational experience? Educational institutions face an urgent need to provide clear direction for asset location and distribution, patching, cost optimization and application control. This is the moment for IT to fulfill its 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 with the same budget and IT resources?
- How can you provide wider support for a broadening array of student and staff devices with immature and/or manual practices that limit visibility across the board?



### Ivanti illuminates every corner of your digital infrastructure

Gaining visibility must become a foundational practice, and proven solutions from Ivanti direct a spotlight on every aspect of your digital infrastructure. Whatever your mix of dedicated IT administrators and educators, a unified IT approach empowers your team to carry

out the critical functions of service management, IT asset management, endpoint security management and user and workspace management. Supplied with greater clarity and visibility, you're more in sync with your users, services and assets — and with your IT landscape, security posture, 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 team 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 the pain points typically associated with a lack of visibility.

### 1 Laptops in slow-mo

An IT administrator notices an uptick in calls concerning issues around slow laptop performance. After many time-consuming follow-up calls, the admin learns an educator returned from a conference a week earlier with what he deemed 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 teams 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.
- Shadow IT – administrators, educators or students 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.

It’s hard to manage, protect and optimize what you don’t know you have. With no formal IT asset management (ITAM) program, teams often rely solely on Active Directory or basic inventory information from endpoint management solutions. On the topic of tracking assets, the ITXM Survey research study commissioned by Ivanti<sup>1</sup> found that 43% of organizations surveyed are still using spreadsheets, 50% are using an endpoint management solution and 45% use inventory tools as one of their resources (note that organizations may be using more than one option). 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.

# 43%

of organizations surveyed are still using spreadsheets.

# 50%

are using an endpoint management system.

# 45%

use inventory tools as one of their resources.

# 38%

track purchase data as part of their inventory spreadsheets.

# 37%

track purchase data as part of their asset management repository/database.

# 22%

use a separate contract management system.

# 39%

use multiple systems and repositories.

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 Chromebooks in the mailroom

Your network administrator gets a call from facilities. A box of new Chromebooks has just arrived. The team starts configuring the new Chromebooks to replace some older ones before they realize that no one had ordered the new Chromebooks 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<sup>2</sup> asked how organizations track and monitor purchase data, contracts and warranty data for their IT assets. The survey found that 38% track it as part of their inventory spreadsheets, 37% track it as part of the asset management repository/database and 22% use a separate contract management system – and 39% use more than one system or repository.

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.

With an integrated solution that brings the different facets of managing your digital infrastructure together:

- 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.
- Teachers and IT administrators are freed from reactive or unnecessary activities to focus on more important projects.
- Security risks are reduced by knowing what hardware is authorized for use.
- You can accomplish more while minimizing costs and administrative efforts.



### 3 Pinching pennies

Administration wants to get serious about managing spend on devices. The question is whether it is possible to defer the refresh cycle on laptops, tablets and other issued devices. Unfortunately, there is no clear information on how many laptops would be involved, which users will 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 device incident and vendor history, no consistent tracking of the entire asset

lifecycle to determine health and performance of various devices and an unknown patching history. It's also unknown which students, educators and administrators would be impacted.

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

What's more, understanding asset lifecycles, performance, compliance and cost implications is more important than ever in the age of hybrid learning environments, when a growing number of devices issued to students are listed as unknown, missing or lost. One school district recently reported that 22% of devices issued had gone missing.<sup>3</sup>

# 28%

of IT professionals report devoting hours each week supporting out-of-warranty/out-of-support-policy assets.

# 20%

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

## 4 Snail Mail

A flood of calls greets the head of IT first thing in the morning. Email “isn’t working” or is “extremely slow.” After several calls to confer among team members, the team concludes that 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.

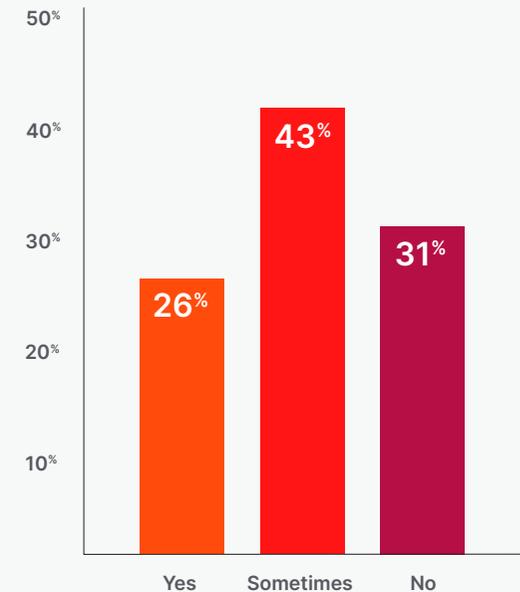
It’s also worth considering whether service management processes and request workflows have automatic visibility into asset information and relationships. Fewer than one-third of respondents to the ITXM Survey<sup>4</sup> indicated that they had visibility into asset information, while the remaining two-thirds did sometimes or not at all.

According to the same survey, IT professionals expect the integration of ITSM and ITAM processes and data to deliver significant improvements:

- 56% expect better visibility of their digital infrastructure.
- 59% expect increased IT staff productivity.
- 54% expect optimized costs.
- 53% expect improved service delivery.

### 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?





## 5 Laptop Lockout

Calling on the IT team, a teacher 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 colleague he's worked with before, and that's when the laptop locked. It's not clear, but other faculty and staff members possibly received the same email.

In this use case, the potential pains that arise from a lack of visibility include no insight into other faculty and staff members 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 survey found that one top security concern of respondents is the risk of data breaches (41%), followed by fear of ransomware / malware (20%).<sup>5</sup> A separate Ivanti survey 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.<sup>6</sup>

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.

An effective IT team needs 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. Such visibility 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 administrator is evaluating the environment's security when she realizes it is unknown what devices are in the environment or whether they're managed properly. Only 75% of the environment is known. Through refreshes, etc., devices are becoming unmanaged. Plus many devices are either lost or not tracked, raising questions about system vulnerability.

In this use case, 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 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.

When first implementing an IT asset management solution, it's not unusual for customers to tell us that they have found 20% more devices than they thought they had. Sometimes the number is as high as 30%. You can't manage what you don't know you have, which 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.

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 classroom or administrative productivity.

## Ivanti: the eyes in the back of your head

Leaders of successful IT programs for educational institutions don't get the results they want by being 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 and educational 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.

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.com](https://www.ivanti.com)

1 800 982 2130

[sales@ivanti.com](mailto:sales@ivanti.com)

1. <https://www.ivanti.com/lp/itsm/assets/s1/pr-itxm-tracking-it-assets-in-spreadsheets>
2. <https://www.ivanti.com/lp/itsm/assets/s1/pr-itxm-tracking-it-assets-in-spreadsheets>
3. <https://www.khou.com/article/news/investigations/10-million-computers-hot-spots-missing-school-districts/285-d42b6f4d-edfa-486a-a007-842c1f97c087>
4. <https://www.ivanti.com/lp/itsm/assets/s1/pr-itxm-tracking-it-assets-in-spreadsheets>
5. <https://www.ivanti.com/blog/study-professionals-users-windows-10>
6. <https://www.ivanti.com/blog/survey-it-professionals-data-sources>