

A man with short dark hair and a light beard, wearing a light blue button-down shirt, is smiling and looking down at a laptop screen. The scene is dimly lit, with soft bokeh lights in the background, suggesting an office or server room environment at night.

ivanti

Expanded IT Visibility Horizon

How to identify all assets that access your network at all times and maintain a single view of your entire IT estate

Inside:

The expansion of Everywhere Work has enabled organizations to rapidly grow. At the same time, behind the scenes, IT environments are quickly becoming more complex. Each employee uses on average 2.6 devices to do their job every day. This means that your IT team must be able to keep tabs on all assets that access your network at all times and be able to maintain any changes in their environment.

This eBook provides you with a comprehensive overview, practical steps and illustrative use cases to help you expand your visibility horizon and truly know what you have.

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit [ivanti.com](https://www.ivanti.com)



01 Challenge

02 Answer

03 How to

04 Benefits

05 Imagine this...

This eBook is part of the [ITSM+ Toolkit](#)

Challenge

Identifying all assets that access your network at all times.

You're looking for the right mix of tools and processes that will help you protect what you have now and prepare for the future. You can't protect and service what you don't know about, though.

Without full visibility into all of your technology assets and services (including endpoints and servers), you'll always be a step behind when it comes to defending the organization from ever increasing cyber threats, effectively resolving IT support requests, or staying compliant. Now that your endpoints are located far beyond the traditional perimeter, extending right to the edge, discovering and securing them is an incredibly complex task. Moreover, you may also be missing out on opportunities to optimize your technology spend.



Did you know?

Only 47% of IT professionals agree completely that their organizations have full visibility into every device that attempts to access their networks.



32%
of IT professionals think that their IT spend is wasted.

A single view of your entire IT estate that provides the full view on what you already have and keeps tabs on it as it evolves.

No more tracking spreadsheets and no more ghost assets. Once you've got that picture in place, you now **have clear visibility** into how your asset real estate is connected. Your service desk has **access to comprehensive information** on all your IT assets at all times, which allows them to quickly identify issues and fix them without flicking through a multitude of spreadsheets. What's more, they can see the potential impact of those issues on the environment and alert IT security teams if there's a larger risk to the network.

The team can easily **optimize the organization's IT spend** by identifying unused or underused assets and leveraging them to replace the ones that need replacing or re-allocate them. This way, your organization can get the most value from its IT dollar. And with the time saved, your IT team will be able to focus not just on where your technology is today but where it's headed next.



32%
of IT professionals still
use spreadsheets to track
their devices.

Look for a solution that enables not just active asset discovery, but also passive.

An **agentless approach** allows you to quickly gain a complete picture of all your IT assets without the need for installing software directly on them, saving crucial time and boosting IT productivity. This capability can be especially helpful when you're dealing with limited bandwidth, for example. By using service mapping to highlight the relationships and dependencies between your underlying data center services and your applications, you can quickly determine the root cause of an issue, evaluate its impact, and assess the risks it poses to your business.



How often should I be scanning for new assets?

Rather than periodically scanning for new assets, consider taking advantage of tools that enable **real-time detection of new assets** as they join your IT environment. That way, in addition to finding assets that you already know are present, you will also be able to quickly detect ghost assets, or devices that you didn't expect to find.

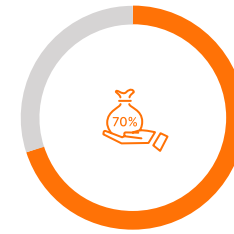


Why is active discovery alone not enough?

Active discovery only scans what you already know. You can't manage what you don't know you have, and this poses a significant security risk. Passive discovery uncovers assets you didn't even realize were part of your IT environment—often up to 20% or 30% more than you thought you had. It can also identify malicious actors who have gained unauthorized access to one or more assets in your estate. A mix of both active and passive discovery can help you **identify and secure all of your assets**—not just the ones that were already on your radar.

Benefits

- ✓ Real-time visibility across your entire IT estate
- ✓ A clear view of dependencies between services and applications
- ✓ Accurate data on all assets, all in one place
- ✓ Increased IT productivity
- ✓ Optimized IT spend



70%

Cost savings over the previous vendor achieved by an energy company thanks to modern ITSM and ITAM solutions adoption.

“Equipped with the complete picture of our infrastructure and data flow through Ivanti Neurons for Service Mapping, we now have the insights for our business continuity model to prioritize availability and quickly restore business-critical services that are most impactful to our customers.”⁴

Robert Hanson, Information Technology Director,
The First Bank

Imagine this...

You are now able to extend your visibility horizon.



While evaluating the IT environment's security, an IT analyst, discovers that only 75% of the organization's assets are known.



What's worse, machines are becoming unmanaged and many assets are either incorrectly configured or not up to date with patches.



By leveraging active and passive discovery to support enterprise service management, they can promptly create an accurate inventory and help the business more effectively manage the risks it actually faces.

Explore next steps in the full ITSM+ Toolkit.

Access your Toolkit

ivanti

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

1 800 982 2130

sales@ivanti.com