The top five limitations of traditional IT discovery and how get around them

IT operators typically have a myriad of IT discovery tools, yet often lack a clean and accurate CMDB across so many different data sources.

That deficiency highlights the gap between IT discovery and actionable visibility. Segmented data isn't enough. Operators need a solution with a compete view of cloud, on-premises, and/or containerized resources.

There are five common limitations of stand-alone discovery tools:

1

Singular approach

Most IT discovery tools focus on their particular area of competence. Cloud vendors focus on cloud, agent providers focus on agents, and so on. Since traditional offerings have this singular approach, you end up with a plethora of tools for different scenarios. And none of them can seamlessly give you a complete picture.

2

Cluttered CMDB with missing and duplicate data

Most CMDBs are populated by Excel dumps, custom APIs and manual processes. That results in duplicate data, inconsistent naming formats, and incomplete information. It's easy to see how point tools can easily pollute CMDBs and why IT organizations lose trust with CMDB accuracy. It's impossible to be a modern IT organization with no single source of truth.

3

Inadequate service maps that fall out of date

The process for manually building a service map is tedious and time consuming. It requires dozens of experts trying to collaborate for a few weeks. But since applications are more dynamic, they tend to fall out of date very rapidly. It's a monumental effort to build the first map, let alone keep current going forward.

4

Certificate management and firewall policies isolated in security tools

Managing TLS certificates and firewall policies is often overlooked until a certificate expires or a security audit is needed. Then it becomes a reactive, all-hands-on deck fire drill to resolve the issues. Doing so is challenging because different teams need access to data, but it's often segmented and isolated in a single tool with limited access.

5

Siloed service ~~management~~ and operations management

Service and IT ops usually function as separate teams using disparate tools because they have different responsibilities. While this makes sense at a macro level, it often leads to inefficiencies in the teams' respective day-to-day responsibilities. To solve business problems, IT service agents must interact with IT operators, and vice versa. Siloed tools and limited data sharing will slow response times and impact user experience.

If you are experiencing one or more of these limitations, you're not alone. The good news is that you don't have to think in siloes and cobble together data from different sources across different tools. Learn more on the next page.

FINASTRA

Finastra accelerates IT issue resolution with ServiceNow ITOM

- 100% of IT assets identified and fully audited
- 115 office locations worldwide gained IT discovery visibility
- $350K a year saved with ServiceNow solutions

nbn™

NBN expands ITOM transformation

- 140 business services mapped in hybrid environment
- 1.5 million configuration items discovered every day
- 7 weeks to deploy and replace legacy tools

redhat

> **ServiceNow is the foundational platform to host data and make it available to everyone in the company.**
>
> *- Severin Launiau, Red Hat*

ServiceNow ITOM Visibility = seamless IT discovery that works

Instead of forcing IT operators to manually correlate discovery data across different sources, ServiceNow focuses on providing actionable visibility out-of-the-box with extensive views.

1. Complete approach to IT discovery

Instead of providing just one option for discovery, ITOM Visibility provides both an agent and agentless-based option to meet your unique needs. In addition, you can easily import third-party data with certified connectors. One platform can discover on-premises, virtualized, cloud, and container resources.

2. Accurate and consistent CMDB

With both a common service data model (CSDM) and tag governance, your CMDB will have common naming conventions to reduce inconsistency, minimize duplicate data, and provide more complete information. Multi-source CMDB provides a single-system of truth even when data comes from different sources.

3. Automated service maps

Automated service mapping greatly reduces the time and effort needed to understand business context. Multiple approaches including top-down, tag-based, and machine-learning to provide capabilities across different deployment models. The intuitive automation helps with both creating new maps and maintaining changes as they occur.

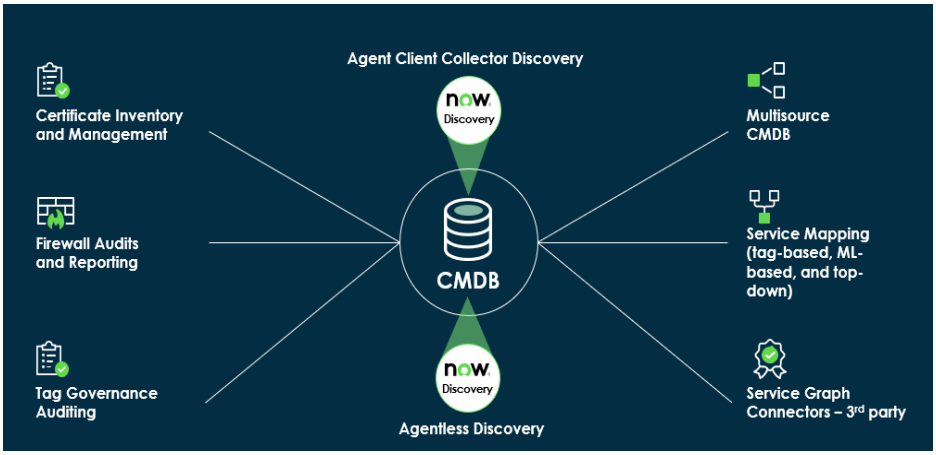
4. Unified TLS certificate and firewall policy data

ITOM Visibility helps with both security certificate management and firewall policies as part of the same platform. ITOM Visibility identifies existing certs, notifies you when they have expired or will soon expire, and allows you to renew them automatically through a simple workflow. Firewall policies are also tracked which greatly reduces the time for security audits. In addition, the IT operations team can ensure policies stay within defined standards (or guardrails). For both capabilities, all information is stored in the Now Platform so multiple teams have access to the same information.

5. One platform across IT

The unified platform provides one single place for all of IT. Service agents and IT operators can still focus separately on their responsibilities. But instead of working in siloes, they can share data, notifications, workflows, and more on the same interface. This eliminates the need for custom integrations and APIs.

> “Using ServiceNow ITSM and ITOM together is really powerful…It would be much more challenging if we were using tools from multiple vendors.
>
> – Dennis Piper, Conagra



ServiceNow ITOM Visibility features.

To learn more about ITOM Visibility, ask your ServiceNow representative or visit www.servicenow.com/ITOM