Take charge of your IT infrastructure and digital services with ServiceNow® ITOM Visibility

The IT challenge

If you can't see your IT environment, you can't manage it. Unless you have visibility of your infrastructure—and know how this delivers your mission-critical digital services—there's no easy way to diagnose and fix service outages, resolve performance issues, assess the risk of changes, optimize infrastructure costs, minimize software compliance issues, or respond quickly to security threats.

Many IT organizations still rely on traditional discovery tools and slow, error-prone manual processes to document their infrastructure and digital services. This results in long discovery delays, and there's no easy way to map discovered infrastructure to the actual services their business consumes. They spend weeks mapping services by hand using stale discovery data—by which time, the map is already out of date.

While this approach may have worked in the past, it's no match for today's dynamic virtualized and cloud environments. When change is measured in minutes, lumbering tools and manual processes just can't keep up. The result? Broken services, escalating operating costs, and an inability to respond quickly and effectively to business needs.

The ServiceNow solution

ServiceNow® ITOM Visibility discovers your end-to-end IT infrastructure and automatically maps it to your digital services, creating a complete, accurate, up-to-date, and consistent record in your ServiceNow® CMDB. And it's built to keep pace with dynamic public and private cloud environments while still providing support for legacy on-premises infrastructure.

ITOM Visibility delivers this comprehensive visibility through a set of targeted features that work seamlessly together:

- **Discovery** discovers physical and logical infrastructure CIs such as containers, Kubernetes clusters, virtual machines, servers, cloud and on-premises storage, databases and other middleware, applications, and more. It can even discover your custom applications using application fingerprinting—supervised machine learning algorithms that automatically identify new types of applications as they are deployed in your network. It also discovers relationships between CIs, mapping upstream and downstream dependencies to the TCP port and process level.
- **Service Mapping** builds on this discovered infrastructure data, automatically creating end-to-end maps of your application and technical services. It identifies all the CIs that support the service, along with their service-specific relationships. Think of this like a city bus map—Discovery shows you all the roads and junctions (infrastructure) in your city, while Service Mapping shows you the specific route that each bus (service) takes.
- **TLS Certificate Management** automatically discovers TLS/SSL certificates, creating a comprehensive inventory in your CMDB. It also provides digital workflows for expired and soon-to-be-expired certificates—for example, getting approval to renew a certificate that is about to expire and then automatically renewing it. This lets you minimize the risk associated with expired certificates, such as service outages and security breaches.
- **Firewall Inventory and Audit** lets you manage your firewall policies in the same place you manage your infrastructure. It discovers your firewalls along with their policies, versions, and other attributes, creating a centralized inventory in your CMDB. End users can submit firewall rule change requests through the ServiceNow portal, which are then automatically routed using digital workflows—for instance, to the security team for risk analysis and approval, and then to the network firewall team for fulfillment. All changes are tracked for audit purposes, and administrators can also initiate audits on demand.

Built to discover multi-cloud environments

ITOM Visibility is designed to keep pace with rapidly changing cloud infra-structure. It provides real-time visibility by integrating with event-driven cloud vendor configuration interfaces such as the AWS Config API, while still offering the option of traditional scheduled and on-demand discovery. It supports Amazon AWS, Microsoft Azure, Google GCP, and IBM Cloud—including both IaaS and PaaS infrastructure—as well as container and serverless technologies such as Kubernetes, Docker, and AWS Lambda. It also discovers virtualized VMware and Citrix infrastructure in on-premises environments.

1. Currently supports Palo Alto Networks firewalls

Accelerate your multi-cloud strategy

Get near real-time visibility of your multi-cloud and on-premises infrastructure, including out-of-the-box support for Amazon Web Services, Microsoft Azure, Google GCP, IBM Cloud, VMware, Citrix, Kubernetes, and more.

Get end-to-end service visibility

Break down infrastructure silos with up-to-date, accurate visibility of your IT infrastructure and services. Instantly see the service impact of infrastructure issues and changes, simplify root-cause analysis, and reduce MTTR.

Drive operational excellence

ITOM Visibility works seamlessly with ITOM Health, ITOM Optimization, ServiceNow® ITSM and other ServiceNow products to help you improve service quality, strengthen change processes, reduce risk, optimize infrastructure spend, and minimize software compliance issues.

Scalable and secure

ServiceNow's scalable and distributed discovery architecture uses standard protocols and encryption to securely discover your infrastructure and services.

Fast time to value

Get up and running quickly with hundreds of supported devices and services, flexible service mapping methods, and guided setup tools.

Easy extensibility

Easily add support for new types of infrastructure and services with built-in no-code/low-code tools.

Ensure data integrity and consistency

ITOM Visibility is designed to help you avoid data consistency and accuracy issues. It works seamlessly with the ServiceNow® Identification and Reconciliation Engine (IRE) to accurately map discovered data to CIs and prevent duplicate CIs. It also ensures that discovered data is consistently mapped to the right CIs by enforcing compliance with the ServiceNow® Common Data Service Model (CDSM). This allows ServiceNow apps to use discovered data out of the box and increases reporting accuracy.

Confidently ingest third-party data with Service Graph Connectors

ITOM Visibility also includes Service Graph Connectors—certified integrations that allow you to ingest data from third-party systems directly into your CMDB. These connectors are developed and tested by third-party vendors under ServiceNow's rigorous engineering oversight and prescriptive guidance. This ensures data timeliness, integrity, and consistency for third-party data in the same way that Discovery does for discovered data. This includes leveraging the IRE and enforcing compliance with the CSDM.

Maximize data quality with a multisource CMDB

Often, the same discovery information is available from multiple discovery sources. Discovery collects and stores data from all these sources and lets you decide which sources should be used to populate your CMDB. For example, if you are collecting data for CI attributes X and Y from sources A and B, you can decide to populate attribute X from source A and attribute Y from source B. You can also switch sources at any time, in which case your CMDB is automatically updated.

Discovery provides detailed reports that allow you to determine the available discovery sources for specific CIs, identify data discrepancies between sources, and pinpoint data gaps. This allows you to maximize data quality and complete-ness in your CMDB by choosing the best discovery sources, to reduce costs by retiring unused discovery sources, and to bring unmanaged CIs that are not currently being discovered under management.

Create service visibility with flexible service mapping options

ServiceNow provides multiple service mapping methods, giving you the flexibility to choose the optimum one for a specific scenario. These include:

- **Top-down mapping**: This creates a very precise map of the applications and supporting infrastructure components that make up an application or technical service. It also identifies the relationships between these components. It is well suited for mapping mission-critical services. This includes cloud-native services—for instance, it can detect Lambda to Lambda calls and Lambda to RDS connections to build dynamic service maps. However, you will need to create instructions (patterns) that tell ITOM Visibility how to discover non-standard services.
- **Tag-based mapping**: If you consistently tag your cloud resources using a well-defined tagging policy, ServiceNow can discover these tags and use them to build service maps. For instance, it can create a service map containing all cloud resources tagged with a specific application service. This requires significantly less upfront effort than top-down mapping but it only identifies the set of components that support the service—it does not identify the dependency relationships between these components. Tag-based mapping is well-suited for less mission-critical applications and for use cases that do not require dependency relationship information.
- **Service mesh mapping:** This provides service mapping for cloud-native services that use an Istio-based service mesh architecture. ServiceNow can use Istio data to discover the microservices within the service and map the connectivity between microservices.
- **Traffic-based mapping:** This mechanism uses machine learning to build service maps based on discovered or imported traffic flow information. This requires very little upfront effort, but the resultant maps may contain extraneous CI information that makes the map difficult to use. This is best used to quickly create an initial service map prior to carrying out top-down mapping.
- **Dynamic CI groups:** You can also map application service using dynamic CI groups—collections of CIs based on attribute values. For example, you can create an application service that contains all servers tied to a specific location or cost center. This is particularly useful when compute power is provided as a service, such as in development and test environments.

ServiceNow also allows you to create service maps manually. However, this approach requires major effort and—unlike the methods above—doesn't automatically update the service map when changes occur. Because of this, it should only be used when a service can't be mapped using another method.

Scalable and secure

ITOM Visibility has a scalable and secure discovery and service mapping architecture. It interacts with your infrastructure via distributed Management, Instrumentation, and Discovery (MID) Servers that run behind your firewall as a Windows service or UNIX daemon on standard hardware or a virtual machine. Each MID server handles thousands of IT components, and you can deploy multiple MID servers to provide virtually unlimited scalability. All communications between the MID Server and main ServiceNow instance are encrypted, with the MID Server initiating connections to the main ServiceNow instance. Device credentials are also stored on the MID server so that they remain securely behind your firewall.

Easily extensible with no-code/low-code tools

ITOM Visibility comes with hundreds of patterns—pre-built instructions to discover and map specific types of infrastructure and services. New patterns are released regularly through the ServiceNow Store. You can also create your own patterns with ITOM Visibility's built-in pattern framework, which lets you configure new patterns for any IP-enabled device with little or no coding.

servicenow.