



Netformx Discovery – Inventory networks to automatically baseline networks and mitigate cybersecurity risks

Most enterprise technology infrastructures that are existing are considered a “brownfield” environment. Customer records typically don’t reflect the latest network configuration. This makes it difficult to plan network migrations, identify security vulnerability or opportunities to up-sell or cross-sell as equipment is nearing end-of-support or needs to be upgraded. To get access to the information you need will require performing a network discovery to gain visibility into a customers’ network topology. The network discovery can provide details such as:

- What infrastructure devices are in the network and how they are connected to the network
- What access those devices have
- Devices that are underpowered or underutilized, or even end-of-life or out of service
- Where there is potential security vulnerability

How Netformx Discovery Works

[Netformx Discovery](#) is a multi-platform engine that can be run on Windows and Unix environments (including Docker container, and can be run via a script), and is not using agents to collect data. Netformx Discovery can collect multi-vendor network infrastructure device data, utilizing SNMP (V1, V2 and V3) and Telnet/SSH.

The information collected includes the H/W configuration (utilizing for example the entity MIB, and more) and Logical Configuration (for example Show Running-Config output) along with layer 2 link information to build the topology map.

The Discovery consists of 2 main stages:

- Collection of Data
- Analysis

The data that is collected, spans from the H/W configuration tree, through various data sets related to the device such as SysLocation, SN#, Interface Tables, Routing Tables, OS versions, Running Configuration, etc.

Netformx Discovery is set by default to collect a specific set of data. However, it can be customized to collect more required data with CLI commands.

Analysis provides an output that is delivered in a JSON format, making it easy to consume either by [Netformx DesignXpert](#), [Netformx AssetXpert](#) and downstream to other systems.

By creating a physical topology map, you can potentially identify bottlenecks, points of failure, required replacements, etc., reducing network downtime.

Netformx Discovery for Cybersecurity

Network and Application Discovery are both essential for performing any type of cybersecurity analysis. Collecting the physical and logical characteristics of the network are a required baseline.

For example, to conduct an analysis of potential malicious activity or access, and take appropriate action you would need to analyze the Firewall rules to see “Any” to “Any” rules, which IP’s are allowed to pass. Netformx Discovery collects this information from the Running-Config data.

Collecting Logs and events are also at the heart of security investigation. Logs can be collected from network devices, applications & systems.

There are various methods to collect the logs such as:

- Network administrators can set up a Syslog server for Netformx Discovery to collect the log.
- Protocols like SNMP, Netflow and IPFIX allow network devices to provide standard information about their operations, which can be logged by the Discovery engine.
- Direct Access to the device / Server - using an API or network protocol can directly receive logs.

Network devices like routers, switches, access points and load balancers, which construct the network infrastructure, can provide critical data about traffic flows; such as destinations accessed by internal users, the sources of the traffic, which protocols are being used, etc.

Netformx Discovery can be customized to collect information utilizing Netflow or Jflow to collect this critical information and provide it as raw data to be analyzed by other systems.

Collecting Logs from endpoints (e.g. laptop) and Application Event Logs (e.g. from Servers) can allow creating a logical topology map of the network. This map will present what endpoints are connecting to what applications (servers) over what port & protocols, and the architecture of the application (e.g. what application accesses what database). Though not currently supported, Netformx Discovery can be enhanced to support log aggregation and analysis.

More details can be found in the [Netformx Discovery Datasheet](#).

Why Netformx Discovery?

Netformx Discovery's powerful engine can in minutes provides a comprehensive audit and analysis of a customer's multi-vendor network. With easy access to topology details down to the node level you will have the full visibility needed to support your cybersecurity practice to mitigate risks and determine vulnerabilities. Contact your account manager or sales@netformx.com for more details.

About Netformx

Netformx helps Cisco Partners design and deliver multi-vendor IT solutions quickly and effectively, increase revenues, and create an improved buying experience for their customers. The Netformx application suite streamlines the entire sales lifecycle from pre-sale to renewal while optimizing use of Cisco incentives, promotions, discounts and rebates to grow profit margins. Powerful tools comprising business intelligence, actionable insights, collaboration and automation, coupled with close integration with Cisco, enable Partners to eliminate manual work, improve efficiency and achieve better business outcomes and customer success.

Netformx has 2,000+ customers globally including ALE, AT&T, Bell Canada, BT, Cisco, NTT, Insight, Logicalis, Optus, and Telstra. Our multi-vendor KnowledgeBase™ contains client and vendor products, services, and program compliance data from vendors such as Cisco, ALE, Check Point, Juniper, Riverbed and TrippLite.