What should you monitor?

In particular, monitor your network for behavior that indicates a possible threat. To do this, you must gain an understanding of and work toward defining what the network is: What items are in it, how many items of each type are present, and which items are within your area of responsibility. Before you can monitor a network for threats, you must first discover and precisely identify what the network is. From what is, your focus can distill to what on your network must you maintain a vigilant watch over. This precise accounting of your "assets under management" is introduced in the topic Targets, Identity & Work Area.

In the context of network security, what had been good enough will no longer suffice. Knowing what your network is does not make it secure. And securing the network without bogging down its performance has become increasingly difficult. The level of attentiveness necessary to keep a network safe from intended and unintended harm has become a time-and-resource sinkhole. And knowing that that a gap exists between what is and what should be on your network has become a burden. Each lapse, lack, and misconfiguration represents a vulnerability that puts your livelihood and your business at risk.

With Asset Manager to keep yourself and your colleagues continually apprised of anomalous conditions, you are in a much better position to remediate problems without delay and enjoy peace of mind.

- Network Change & Complexity
- IPv6 Traffic
- BYODs & Cloud-based Applications
- Routes Traversed

Network Change & Complexity

It is mission-critical for an enterprise in a constant state of change have the ability to manage technology and ensure confidentiality, integrity, and the availability of information. Maintaining information security requires a dynamic process, proactively managed. Organizations must employ tools that give them the capability to identify and respond to new vulnerabilities and evolving cyber threats.

The continuous monitoring of security controls allows your organization to detect threats and vulnerabilities from today’s sophisticated and persistent adversaries. It’s instrumental in mitigating enterprise-wide risk through system-level network monitoring and detection. Asset Manager detects and alerts your information security professionals regarding network changes requiring attention.

IPv6 Traffic

IPv6 Discovery passively monitors ICMPv6/NDP traffic, monitors the OSPF routing infrastructure, and finds network paths and devices via active discovery techniques.

Use IPv6 Discovery to:

- Identify IPv6-enabled devices, both native and dual-stacked
- Find IPv6 routes and paths on the network
- Collect attributes of native IPv6 network equipment
- Deliver IPv6 discovery results in real-time

- Locate unwanted IPv6 devices and routes
- Identify unintentionally configured IPv6 devices
- Secure and manage policy-compliant IPv6 equipment
- Halt unwanted IPv6 activity

Encourage prospects to improve the quality of their network provisioning, fault monitoring, and service-level reporting/verification by adding IPv6 Discovery capabilities to their mix.

BYODs and Cloud-based Applications

In highly dynamic environments with constantly changing technologies and a proliferation of BYOD programs, cloud-based applications, and virtualized devices, and organization's ability to track the security state of a system on an ongoing basis is essential.

Routes Traversed

To see the path over which network traffic travels, run Routing Protocol Analysis, which is an OSPF route-monitoring service attached to a managed IP network that provides you with real-time awareness of the routes actually used throughout an OSPF domain.

Routing Protocol Analysis

- Enables your clients to monitor routing state in real-time.
- Gathers topology and network state information from an OSPF domain.
- Provides real-time awareness of the routes actually used (aka paths) throughout an OSPF domain.
- Passive OSPF listening of our route analytics methodology adds virtually no traffic and has zero impact on network performance.
- Lightweight: Updates are no more frequent than changes to the underlying network.

Be in-the-know on atypical network conditions

Large-scale examples of network characteristics of concern include traffic volume, increased bandwidth, and heavy use of a single protocol. Specifically, consider monitoring . . .

- IPv6 Traffic
- Routes Traversed