IP FABRIC

10 Network Assurance Outcomes to Comply with NIST CSF 2.0 Recommendations

ipfabric.io ↗

10 Network Assurance Outcomes to Comply with NIST CSF 2.0 Recommendations

NIST Cybersecurity Framework (CSF) is a framework to reduce risk, not a regulation, yet it is a foundation that supports many specific regulations. NIST recently released the first major update to the framework since it was introduced in 2014. The NIST Cybersecurity Framework 2.0 has an expanded scope that goes beyond protecting critical infrastructure, such as hospitals and power plants, to all organizations in any sector. It also has a new focus on governance, which includes how organizations make and carry out informed decisions on cybersecurity strategy. The CSF's governance component emphasizes that cybersecurity is a major source of enterprise risk, and senior leaders need to account for the potential impact on company financial performance and reputation.

The purpose of this document is to illustrate **ten outcomes of using the network assurance platform** IP Fabric, and how they relate to various function, categories, subcategories, and implementation examples in NIST 2.0, which would help organizations improve their overall risk exposure. In the examples, we map the specific language of the framework to IP Fabric capabilities.

→ **NIST 2.0**
Implementation Examples

View PDF

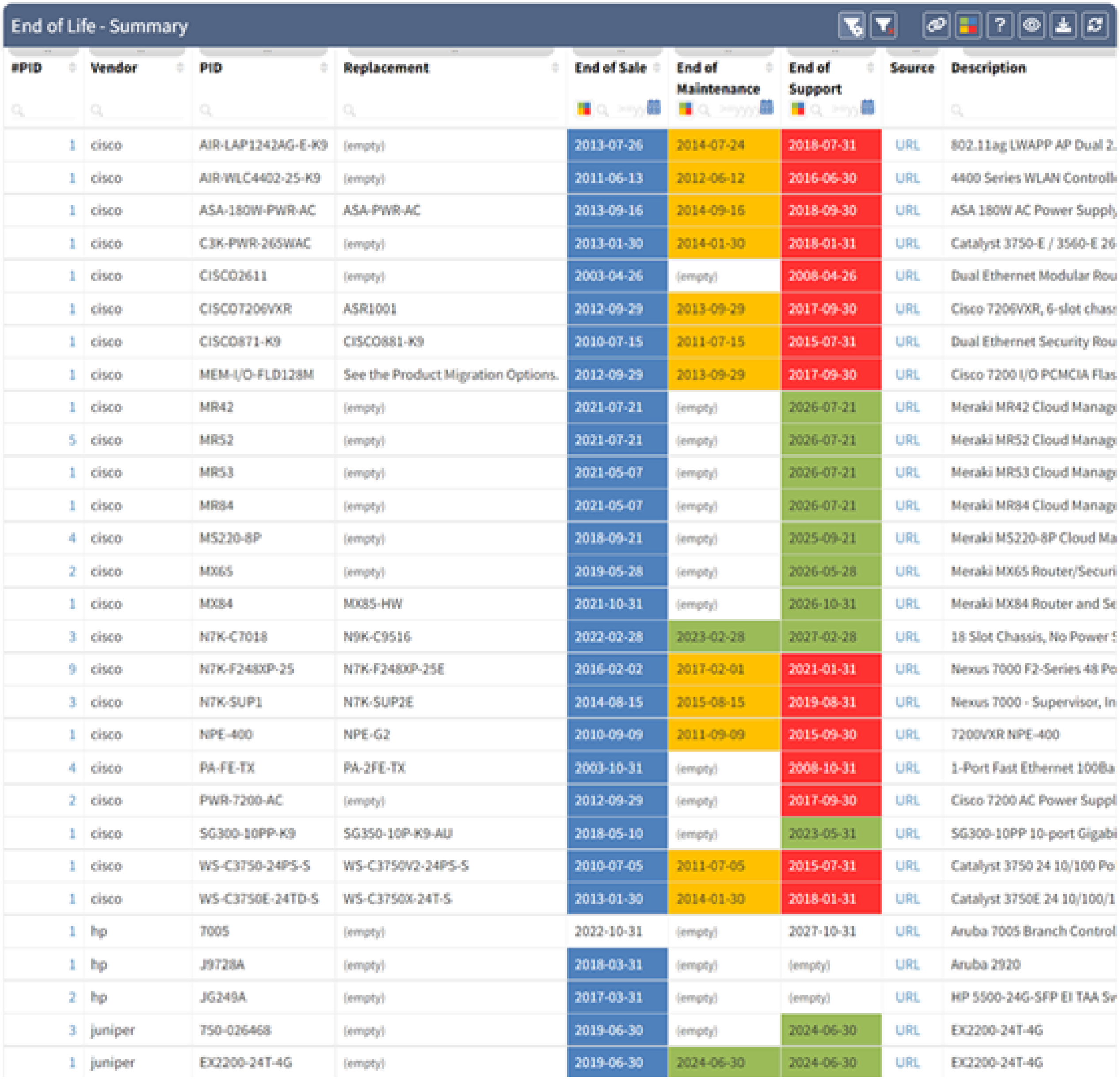
View Excel

IP Fabric's Automated Network Assurance is a foundational technology to help meet NIST 2.0 standards.

10 Outcomes of Using the IP Fabric's Network Assurance Platform

01. Cloud + Network Asset Inventory, Updated Daily

IP Fabric provides a complete and normalized cloud and network asset inventory list, including detailed device lifecycle information (e.g. End of Support and End of Life milestones, and suggested replacements). This information is normalized across vendors, domains, and technologies, making it accessible for non-experts and usable for automation projects, identifying vulnerabilities, end-of-life device management, configuration compliance, network planning, and more.



End of Life - Summary

#PID	Vendor	PID	Replacement	End of Sale	End of Maintenance	End of Support	Source	Description
1	cisco	AIR-LAP1242AG-E-K9	(empty)	2013-07-26	2014-07-24	2018-07-31	URL	802.11ag LWAPP AP Dual 2.
1	cisco	AIR-WLC4402-25-K9	(empty)	2011-06-13	2012-06-12	2016-06-30	URL	4400 Series WLAN Controll
1	cisco	ASA-180W-PWR-AC	ASA-PWR-AC	2013-09-16	2014-09-16	2018-09-30	URL	ASA 180W AC Power Supply
1	cisco	C3K-PWR-265WAC	(empty)	2013-01-30	2014-01-30	2018-01-31	URL	Catalyst 3750-E / 3560-E 26
1	cisco	CISCO2611	(empty)	2003-04-26	(empty)	2008-04-26	URL	Dual Ethernet Modular Rou
1	cisco	CISCO7206VXR	ASR1001	2012-09-29	2013-09-29	2017-09-30	URL	Cisco 7206VXR, 6-slot chas
1	cisco	CISCO871-K9	CISCO881-K9	2010-07-15	2011-07-15	2015-07-31	URL	Dual Ethernet Security Rou
1	cisco	MEM-I/O-FLD128M	See the Product Migration Options.	2012-09-29	2013-09-29	2017-09-30	URL	Cisco 7200 I/O PCMCIA Flas
1	cisco	MR42	(empty)	2021-07-21	(empty)	2026-07-21	URL	Meraki MR42 Cloud Manag
5	cisco	MR52	(empty)	2021-07-21	(empty)	2026-07-21	URL	Meraki MR52 Cloud Manag
1	cisco	MR53	(empty)	2021-05-07	(empty)	2026-07-21	URL	Meraki MR53 Cloud Manag
1	cisco	MR84	(empty)	2021-05-07	(empty)	2026-07-21	URL	Meraki MR84 Cloud Manag
4	cisco	MS220-8P	(empty)	2018-09-21	(empty)	2025-09-21	URL	Meraki MS220-8P Cloud Ma
2	cisco	MX65	(empty)	2019-05-28	(empty)	2026-05-28	URL	Meraki MX65 Router/Securi
1	cisco	MX84	MX85-HW	2021-10-31	(empty)	2026-10-31	URL	Meraki MX84 Router and Se
3	cisco	N7K-C7018	N9K-C9516	2022-02-28	2023-02-28	2027-02-28	URL	18 Slot Chassis, No Power
9	cisco	N7K-F248XP-25	N7K-F248XP-25E	2016-02-02	2017-02-01	2021-01-31	URL	Nexus 7000 F2-Series 48 Po
3	cisco	N7K-SUP1	N7K-SUP2E	2014-08-15	2015-08-15	2019-08-31	URL	Nexus 7000 - Supervisor, In
1	cisco	NPE-400	NPE-G2	2010-09-09	2011-09-09	2015-09-30	URL	7200VXR NPE-400
4	cisco	PA-FE-TX	PA-2FE-TX	2003-10-31	(empty)	2008-10-31	URL	1-Port Fast Ethernet 100Ba
2	cisco	PWR-7200-AC	(empty)	2012-09-29	(empty)	2017-09-30	URL	Cisco 7200 AC Power Suppl
1	cisco	SG300-10PP-K9	SG350-10P-K9-AU	2018-05-10	(empty)	2023-05-31	URL	SG300-10PP 10-port Gigabi
1	cisco	WS-C3750-24PS-S	WS-C3750V2-24PS-S	2010-07-05	2011-07-05	2015-07-31	URL	Catalyst 3750 24 10/100 Po
1	cisco	WS-C3750E-24TD-S	WS-C3750X-24T-S	2013-01-30	2014-01-30	2018-01-31	URL	Catalyst 3750E 24 10/100/1
1	hp	7005	(empty)	2022-10-31	(empty)	2027-10-31	URL	Aruba 7005 Branch Control
1	hp	J9728A	(empty)	2018-03-31	(empty)	(empty)	URL	Aruba 2920
2	hp	JG249A	(empty)	2017-03-31	(empty)	(empty)	URL	HP 5500-24G-SFP EI TAA Sv
3	juniper	750-026468	(empty)	2019-06-30	(empty)	2024-06-30	URL	EX2200-24T-4G
1	juniper	EX2200-24T-4G	(empty)	2019-06-30	2024-06-30	2024-06-30	URL	EX2200-24T-4G

End of Life Data as Illustrated in IP Fabric

This aligns with NIST2.0 implementation examples across the Identify, Govern, and Protect Categories, which include “replace hardware when it lacks needed security capabilities or when it cannot support software with needed security capabilities”, and “define and implement plans for hardware end-of-life maintenance support and obsolescence.”.

How else does this apply to NIST2.0?

Identify (ID)

Asset Management (ID.AM)

ID.AM-01: Physical devices and systems within the organization are inventoried.

ID.AM-02: Software platforms and applications within the organization are inventoried.

ID.AM-03: Organizational communication and data flows are mapped.

ID.AM-04: Inventories of services provided by suppliers are maintained.

ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.

ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.

ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles..

Govern (GV)

Risk Management Strategy (GV.RM)

GV.RM-01: Risk management processes are established, managed, and agreed to by organizational stakeholders.

GV.RM-02: Organizational risk tolerance is determined and clearly expressed.

GV.RM-03: Risk management processes are established, managed, and agreed to by organizational stakeholders.

Protect (PR)

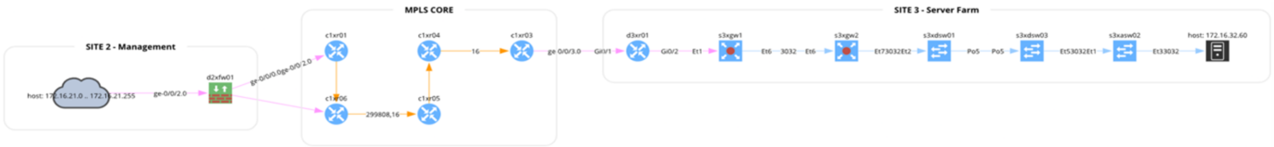
Platform Security (PR.PS)

PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.

> “
>
> **IP Fabric provides a complete and normalized cloud and network asset inventory list, including detailed device lifecycle information**

02. End-to-End Path Lookup

With simply the input of a source and destination address, IP Fabric will generate the end-to-end path of data from ingress to egress from your infrastructure. You can drill down into specific devices along the way, pinpoint single points of failure or lost redundancy, and compare paths from day to day to understand what's changed.



Access to these end-to-end path lookups, both to generate in the moment and as a historical record of the network, have utility across the Identify, Protect, and Detect Functions of NIST. For example, the following implementation examples in the Identify-Asset Management (ID-AM) subcategory in particular would be fulfilled by IP Fabric's end-to-end path functionality:

- **Ex1:** Maintain baselines of communication and data flows within the organization's wired and wireless networks
- **Ex2:** Maintain baselines of communication and data flows between the organization and third parties
- **Ex3:** Maintain baselines of communication and data flows for the organization's infrastructure-as-a-service (IaaS) usage
- **Ex4:** Maintain documentation of expected network ports, protocols, and services that are typically used among authorized systems.

How else does this apply to NIST2.0?

Identify (ID)	Protect (PR)	Detect (DE)
Asset Management (ID.AM) **ID.AM-03:** Organizational communication and data flows are mapped. **ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-10:** Response and recovery plans are tested.	**Security Continuous Monitoring (DE.CM)** **DE.CM-01:** The network is monitored to detect potential cybersecurity events. **DE.CM-07:** Monitoring for unauthorized personnel, connections, devices, and software is performed. **DE.CM-08:** Vulnerability scans are performed.

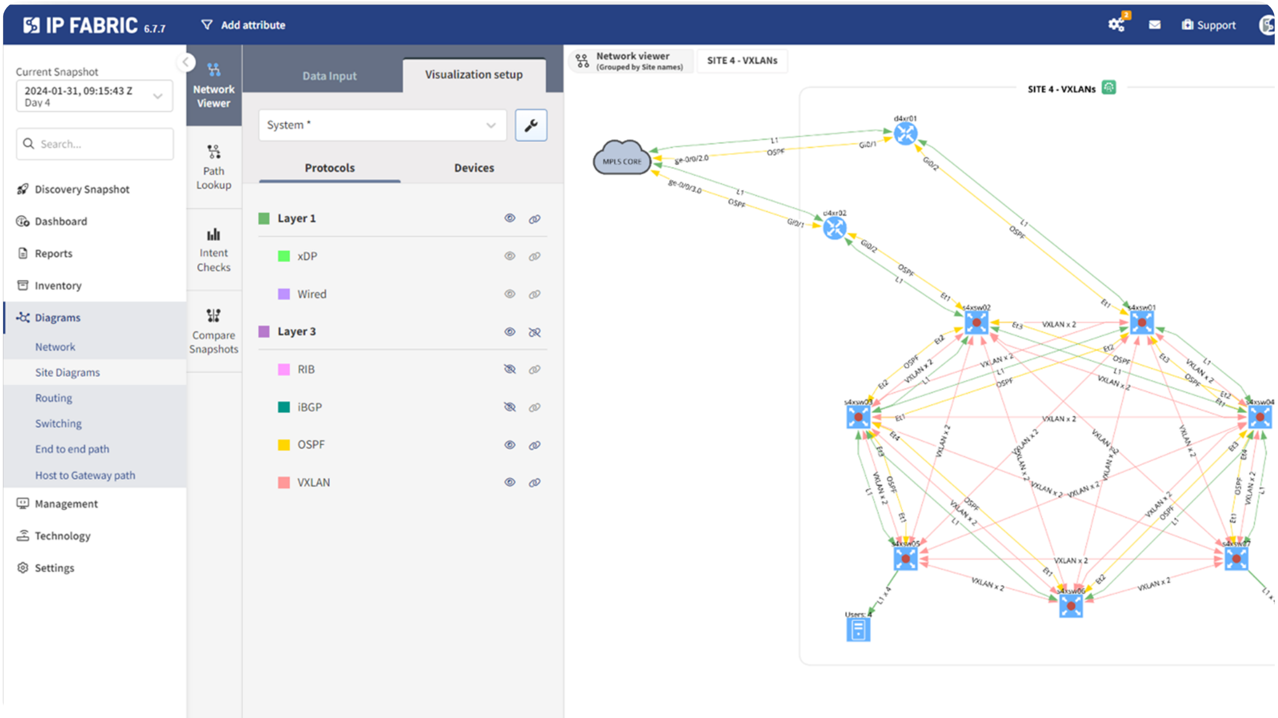
03. Complete and Holistic Cloud and Network Discovery

IP Fabric uses a CLI-based and SSH discovery mechanism to perform a lightweight and secure interaction with your network based on a seed device and read-only credentials. It looks for known neighbors, collects detailed network state information from every discovered device, and computes cross-technology dependencies to create a complete model of your cloud and network infrastructure.

IP Fabric discovers all supported IP-based active network devices, such as switches, routers, firewalls, load-balancers, WAN concentrators, wireless controllers, and wireless access points.

IP Fabric also uses APIs to communicate with vendor controllers (Versa, Viptela) or cloud vendors (AWS, Azure, NSX-T).

This information Is represented in technology tables, and network topology models, and is accessible via API. This means your understanding of your infrastructure is always 1) complete and 2) up to date. No gaps thanks to shadow IT, lagging documentation, and rogue devices.



The visualization flexibility of an automatically generated network topology map

- **Ex3:**
  Identify unofficial uses of technology to meet mission objectives (i.e., shadow IT)
- **Ex4:**
  Periodically identify redundant systems, hardware, software, and services that unnecessarily increase the organization's attack surface
- **Ex5:**
  Properly configure and secure systems, hardware, software, and services prior to their deployment in production
- **Ex6:**
  Update inventories when systems, hardware, software, and services are moved or transferred within the organization

How else does this apply to NIST2.0?

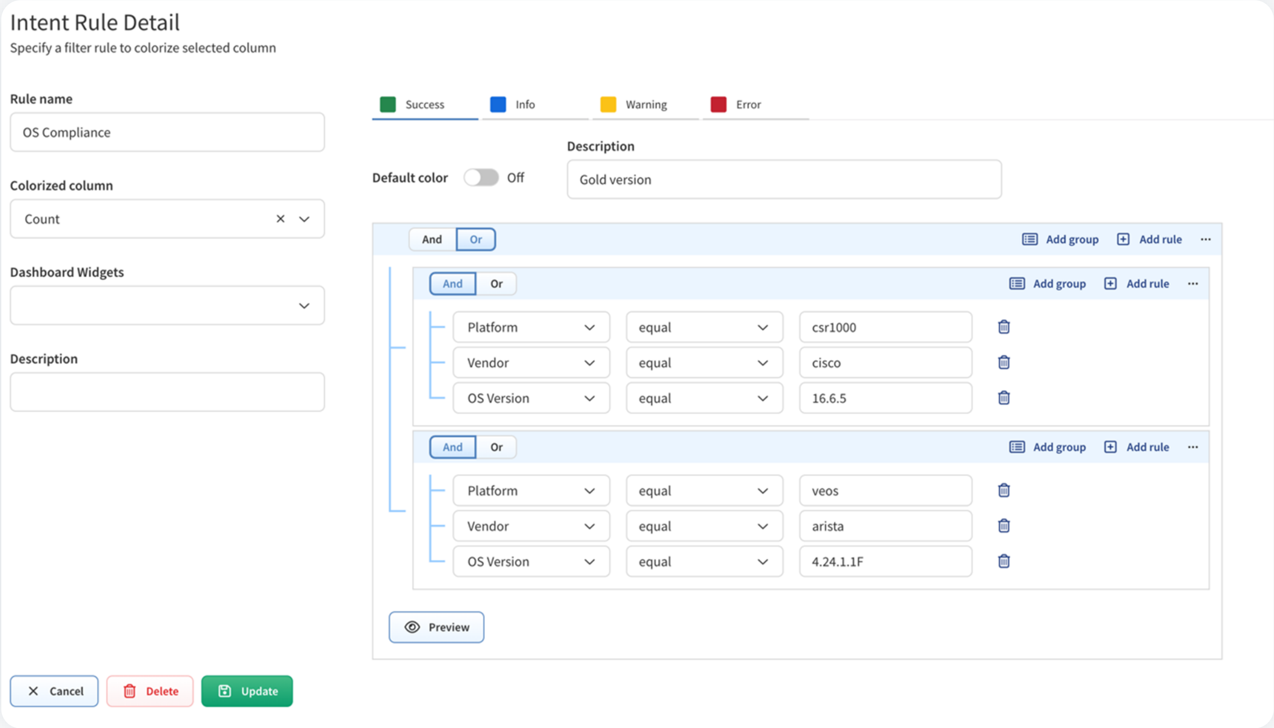
Identify (ID)	Protect (PR)	Detect (DE)
Asset Management (ID.AM) **ID.AM-01:** Physical devices and systems within the organization are inventoried. **ID.AM-02:** Software platforms and applications within the organization are inventoried. **ID.AM-03:** Organizational communication and data flows are mapped. **ID.AM-04:** Inventories of services provided by suppliers are maintained. **ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission. **ID.AM-07:** Inventories of data and corresponding metadata for designated data types are maintained. **ID.AM-08:** Systems, hardware, software, services, and data are managed throughout their life cycles.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-01:** A baseline config. of information technology / industrial control systems is created and maintained. **PR.IP-02:** A System Development Life Cycle to manage systems is implemented. **PR.IP-03:** Configuration change control processes are in place. **PR.IP-10:** Response and recovery plans are tested.	**Security Continuous Monitoring (DE.CM)** **DE.CM-01:** The network is monitored to detect potential cybersecurity events. **DE.CM-07:** Monitoring for unauthorized personnel, connections, devices, and software is performed. **DE.CM-08:** Vulnerability scans are performed.

04. Configuration Checks & Validation

IP Fabric includes 150+ out-of-the-box configuration and compliance checks (also called “intent checks”). Additional custom configuration and compliance checks are simple and fast to build. Use them to set rules about policies and configurations you need to be secure and resilient and measure your network behavior against these rules daily.

Identify drift from compliance before it becomes an issue and remediate it quickly, equipped with exact knowledge of where the misconfiguration, inconsistency, or inefficiency lies and what is causing it.

See this essential compliance information about your cloud, securing, and network devices and connections in a single pane of glass dashboard view, and easily share it across teams or with non-experts.



Intent Rule Detail

Specify a filter rule to colorize selected column

Rule name: OS Compliance

Colorized column: Count

Dashboard Widgets:

Description:

Description: Gold version

Default color: Off

And / Or

- And / Or
  - Platform equal csr1000
  - Vendor equal cisco
  - OS Version equal 16.6.5
- And / Or
  - Platform equal veos
  - Vendor equal arista
  - OS Version equal 4.24.1.1F

Easily build custom network intent checks in IP Fabric

Utilizing IP Fabric’s compliance checks for everything from automated risk assessments and incident response, covering NIST2.0 functions Identify, Protect, Detect, and Respond and covering implementation examples like the following in ID.RA-01:

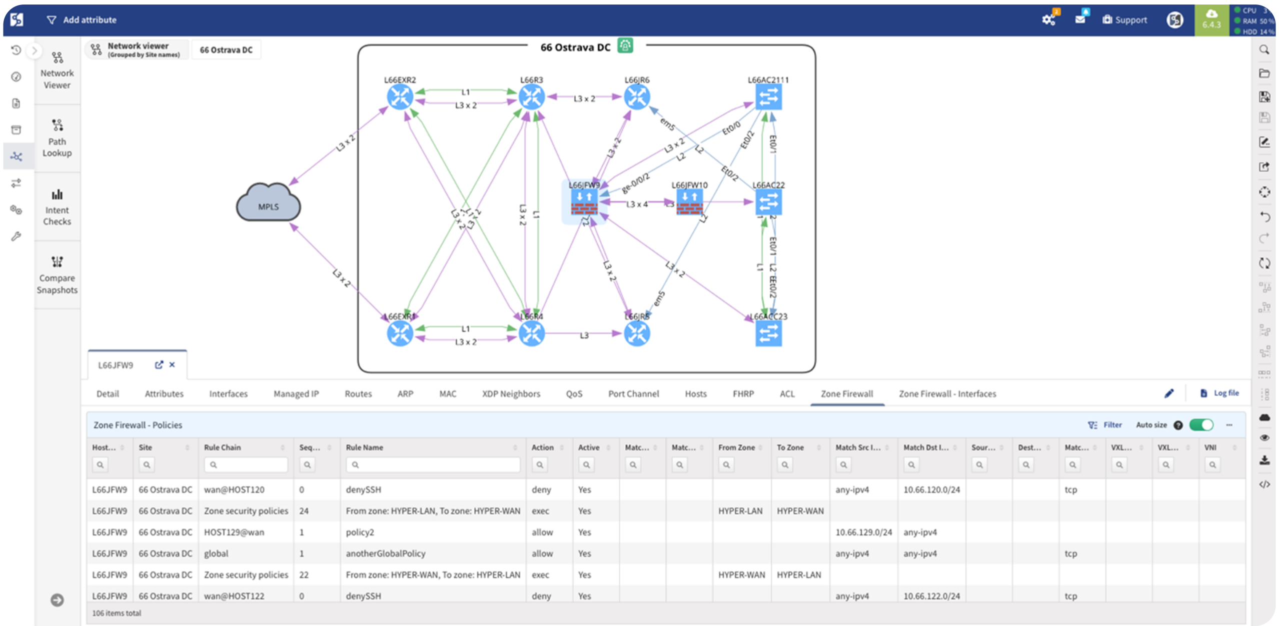
- **Ex3:**
  Use vulnerability management technologies to identify unpatched and misconfigured software
- **Ex4:**
  Assess network and system architectures for design and implementation weaknesses that affect cybersecurity
- **Ex5:**
  Review, analyze, or test organization - developed software to identify design, coding, and default configuration vulnerabilities
- **Ex6:**
  Monitor sources of cyber threat intelligence for information on new vulnerabilities in products and services

How else does this apply to NIST2.0?

Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)
Asset Management (ID.AM) **ID.AM-01:** Asset vulnerabilities are identified and documented. **ID.AM-02:** Cyber threat intelligence is received from information sharing forums and sources. **ID.AM-03:** Threats, both internal and external, are identified and documented. **ID.AM-04:** Potential business impacts and likelihoods are identified. **ID.AM-05:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. **ID.AM-06:** Risk responses are identified and prioritized.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-01:** A baseline configuration of information technology/industrial control systems is created and maintained. **PR.IP-02:** A System Development Life Cycle to manage systems is implemented. **PR.IP-03:** Configuration change control processes are in place. **PR.IP-10:** Response and recovery plans are tested.	**Security Continuous Monitoring (DE.CM)** **DE.CM-01:** The network is monitored to detect potential cybersecurity events. **DE.CM-07:** Monitoring for unauthorized personnel, connections, devices, and software is performed. **ID.AM-08:** Vulnerability scans are performed.	**Mitigation (RS.MI)** **RS.MI-01:** Incidents are contained. **RS.MI-02:** Incidents are mitigated. **RS.MI-03:** Newly identified vulnerabilities are mitigated or documented as accepted risks.

05. Validate Security Posture is Effective as Expected

Whether you've implemented network segmentation or micro-segmentation or have specific firewall policies to ensure zero trust, with IP Fabric, you can validate that this implementation is operating as expected with every network snapshot, giving you daily peace of mind regarding your security posture. Identify potential threats by understanding devices connected and configured at your network edge and highlight issues with third-party connectivity or remote access.



Zone Firewall - Policies

Host...	Site	Rule Chain	Seq...	Rule Name	Action	Active	Matc...	Matc...	From Zone	To Zone	Match Src I...	Match Dst I...	Sour...	Dest...	Matc...	VXL...	VXL...	VNI
L66JFW9	66 Ostrava DC	wan@HOST120	0	denySSH	deny	Yes					any-ipv4	10.66.120.0/24			tcp			
L66JFW9	66 Ostrava DC	Zone security policies	24	From zone: HYPER-LAN, To zone: HYPER-WAN	exec	Yes			HYPER-LAN	HYPER-WAN								
L66JFW9	66 Ostrava DC	HOST129@wan	1	policy2	allow	Yes					10.66.129.0/24	any-ipv4						
L66JFW9	66 Ostrava DC	global	1	anotherGlobalPolicy	allow	Yes					any-ipv4	any-ipv4			tcp			
L66JFW9	66 Ostrava DC	Zone security policies	22	From zone: HYPER-WAN, To zone: HYPER-LAN	exec	Yes			HYPER-WAN	HYPER-LAN								
L66JFW9	66 Ostrava DC	wan@HOST122	0	denySSH	deny	Yes					any-ipv4	10.66.122.0/24			tcp			

106 items total

Firewall Policy Implementation as Visualized in IP Fabric

How else does this apply to NIST2.0?

Identify (ID)

Asset Management (ID.AM)

ID.AM-01: Physical devices and systems within the organization are inventoried.

ID.AM-02: Software platforms and applications within the organization are inventoried.

ID.AM-05: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.

Risk Assessment (ID.RA)

ID.RA-01: Asset vulnerabilities are identified and documented.

ID.RA-02: Cyber threat intelligence is received from information-sharing forums and sources.

ID.RA-03: Threats, both internal and external, are identified and documented.

ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

Protect (PR)

Access Control (PR.AC)

PR.AC-01: Identities and credentials are managed for authorized devices and users.

PR.AC-03: Remote access is managed.

PR.AC-04: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

Access Control (PR.AC)

PR.IP-01: A baseline configuration of information technology/industrial control systems is created and maintained.

PR.IP-03: Configuration change control processes are in place.

Detect (DE)

Security Continuous Monitoring (DE.CM)

DE.CM-01: The network is monitored to detect potential cybersecurity events.

DE.CM-07: Monitoring for unauthorized personnel, connections, devices, and software is performed.

ID.AM-08: Vulnerability scans are performed.

Respond (RS)

Mitigation (RS.MI)

RS.MI-01: Incidents are contained.

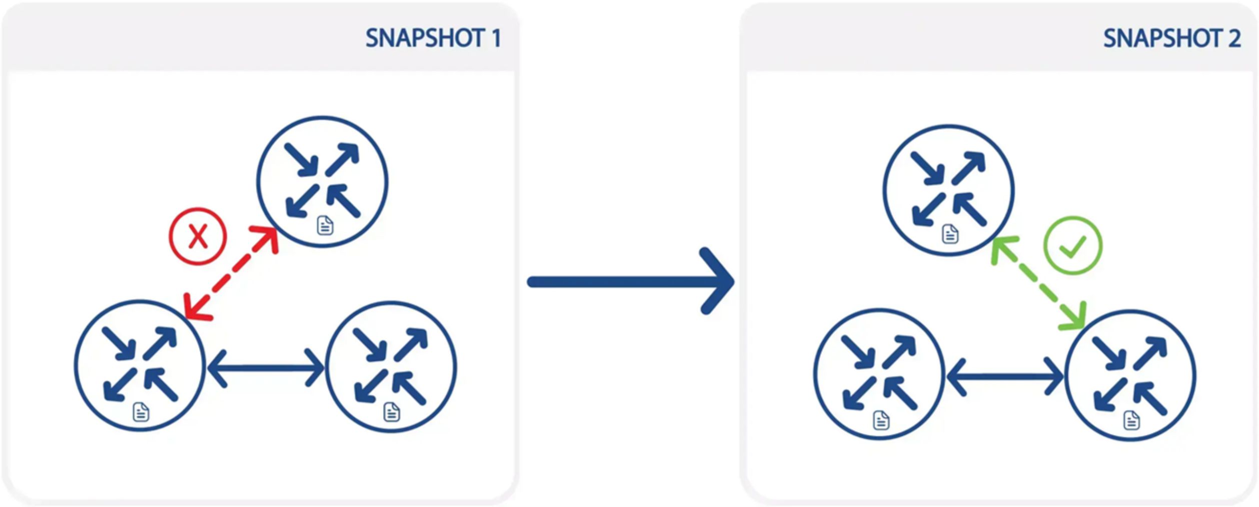
RS.MI-02: Incidents are mitigated.

RS.MI-03: Newly identified vulnerabilities are mitigated or documented as accepted risks.

06. Historical View of the Network

IP Fabric saves every snapshot of your network so you can use it for historical troubleshooting, comparative analysis, post-mortem incident analysis, and pattern analysis for future planning.

Understanding exactly what your cloud and network infrastructure looked like at a particular time is central to root cause analysis and understanding the scope of an incident and is critical to safely managing large-scale migrations or deployments.



This is useful for NIST implementation examples across the Identify, Detect, Respond, and Recover functions, for example:

Incident Analysis (RS.AN):

- **Ex1:**
  Collect, preserve, and safeguard the integrity of all pertinent incident data and metadata (e.g., data source, date/time of collection) based on evidence preservation and chain-of-custody procedures.

Technology Infrastructure Resilience (PR.IR):

- **Ex1:**
  Monitor usage of storage, power, compute, network bandwidth, and other resources.

- **Ex2:**
  Forecast future needs, and scale resources accordingly.

How else does this apply to NIST2.0?

Identify (ID)

Asset Management (ID.AM)

ID.AM-01: Physical devices and systems within the organization are inventoried.

ID.AM-02: Software platforms and applications within the organization are inventoried.

ID.AM-05: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.

Risk Assessment (ID.RA)

ID.RA-01: Asset vulnerabilities are identified and documented.

ID.RA-02: Cyber threat intelligence is received from information-sharing forums and sources.

ID.RA-03: Threats, both internal and external, are identified and documented.

ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

Detect (DE)

Security Continuous Monitoring (DE.CM)

PR.AC-01: Identities and credentials are managed for authorized devices and users.

PR.AC-03: Remote access is managed.

PR.AC-04: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

Access Control (PR.AC)

PR.IP-01: A baseline configuration of information technology/industrial control systems is created and maintained.

PR.IP-03: Configuration change control processes are in place.

Respond (RS)

Incident Analysis (RS.AN)

DE.CM-01: The network is monitored to detect potential cybersecurity events.

DE.CM-07: Monitoring for unauthorized personnel, connections, devices, and software is performed.

ID.AM-08: Vulnerability scans are performed.

Recover (RC)

Incident Recovery Plan Execution (RC.RP)

RS.MI-01: Incidents are contained.

RS.MI-02: Incidents are mitigated.

RS.MI-03: Newly identified vulnerabilities are mitigated or documented as accepted risks.

07. Automatically Enrich Infrastructure Monitoring with Key Network Intelligence

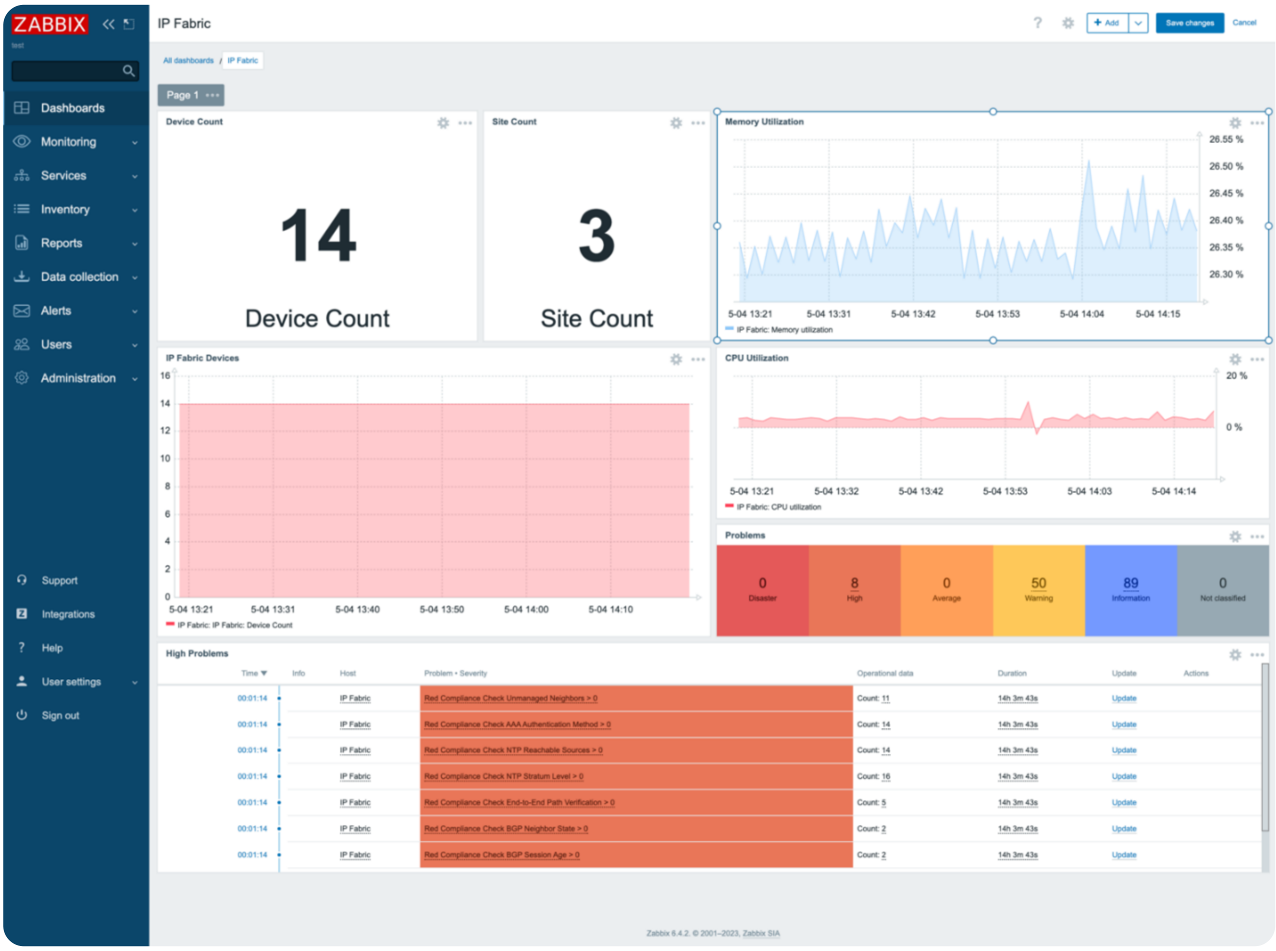
Real-time monitoring is essential for enterprise cloud and network infrastructure to respond quickly to incidents at scale. However, there are downsides to traditional monitoring tools including:

→ **Population (am I monitoring everything I need to?)**

→ **Alert fatigue (am I monitoring what is important?)**

→ **Lack of context (something is happening, but why? What else does this affect?)**

Network assurance fills these gaps and enriches monitoring systems with deep contextual data for data-backed decision-making resolution of issues before they become a problem.



Problems

0	8	0	50	89	0
Disaster	High	Average	Warning	Information	Not classified

High Problems

Time ▼	Info	Host	Problem • Severity	Operational data	Duration	Update	Actions
00:01:14		IP Fabric	Red Compliance Check Unmanaged Neighbors > 0	Count: 11	14h 3m 43s	Update	
00:01:14		IP Fabric	Red Compliance Check AAA Authentication Method > 0	Count: 14	14h 3m 43s	Update	
00:01:14		IP Fabric	Red Compliance Check NTP Reachable Sources > 0	Count: 14	14h 3m 43s	Update	
00:01:14		IP Fabric	Red Compliance Check NTP Stratum Level > 0	Count: 16	14h 3m 43s	Update	
00:01:14		IP Fabric	Red Compliance Check End-to-End Path Verification > 0	Count: 5	14h 3m 43s	Update	
00:01:14		IP Fabric	Red Compliance Check BGP Neighbor State > 0	Count: 2	14h 3m 43s	Update	
00:01:14		IP Fabric	Red Compliance Check BGP Session Age > 0	Count: 2	14h 3m 43s	Update	

This fulfils implementation examples across the Identify, Detect, and Respond functions:

This fulfils implementation examples across the Identify, Detect, and Respond functions:

- **Ex1:**
  Monitor DNS, BGP, and other network services and protocols for adverse events
- **Ex2:**
  Monitor wired and wireless networks for connections from unauthorized endpoints
- **Ex3:**
  Monitor facilities for unauthorized or rogue wireless networks
- **Ex4:**
  Compare actual network flows against baselines to detect deviations
- **Ex5:**
  Monitor network communications to identify changes in security postures for zero trust purposes

Continuous Monitoring (DE.CM-06):

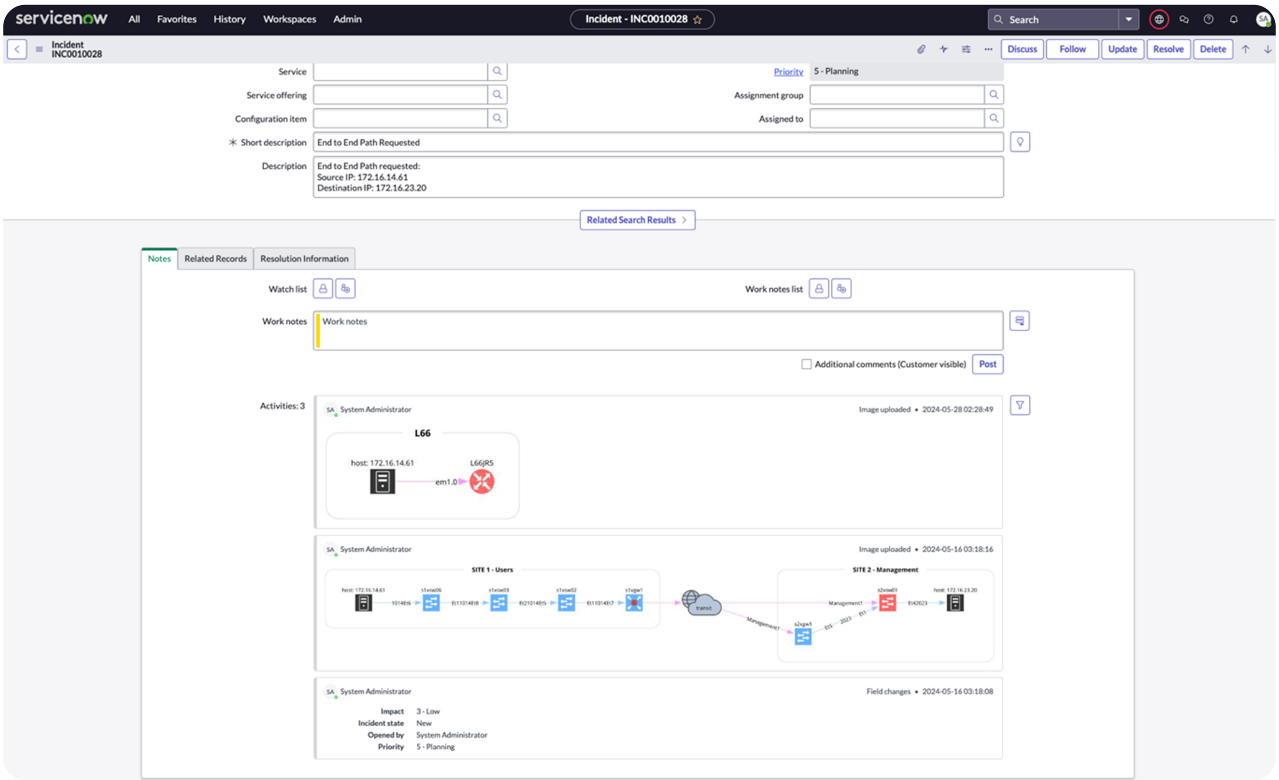
- **Ex2:**
  Monitor activity from cloud-based services, internet service providers, and other service providers for deviations from expected behavior.

Identify (ID)	Detect (DE)	Respond (RS)
Asset Management (ID.AM) **ID.AM-03:** Representations of the organization's authorized network communication and internal and external network data flows are maintained.	**Security Continuous Monitoring (DE.CM)** **DE.CM-01:** The network is monitored to detect potential cybersecurity events. **DE.CM-07:** Monitoring for unauthorized personnel, connections, devices, and software is performed. **DE.CM-08:** Vulnerability scans are performed.	**Incident Analysis (RS.AN)** **RS.AN-03:** Analysis is performed to establish what has taken place during an incident and the root cause of the incident. **RS.AN-06:** Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved. **RS.AN-07:** Incident data and metadata are collected, and their integrity and provenance are preserved. **RS.AN-08:** An incident's magnitude is estimated and validated. Incident Response Reporting and Communication (RS.CO) **RS.CO-02:** Internal and external stakeholders are notified of incidents. **RS.CO-03:** Information is shared with designated internal and external stakeholders.

08. Automatically Enrich IT Service Management Systems and Speed Troubleshooting

When a trouble ticket rolls in - a site reports connectivity issues or a user can't access the network - the clock starts and the hunt for the root cause begins. Enriching trouble tickets with relevant end-to-end network paths or network diagrams means you eliminate manual troubleshooting efforts. Team members with less historical knowledge of the business can easily troubleshoot network issues without the blocker of access to knowledge of the infrastructure.

IP Fabric enhances your IT Service Management systems using the open REST API or our pre-built integrations. You can use intent check violations to trigger ticket creation and enhancement to speed troubleshooting and ensure effective information sharing.



Incident - INC0010028

Incident
INC0010028

Service
Service offering
Configuration item
Priority 5 - Planning
Assignment group
Assigned to

✳ Short description: End to End Path Requested

Description:
End to End Path requested:
Source IP: 172.16.14.61
Destination IP: 172.16.23.20

☐ Additional comments (Customer visible)

Activities: 3

SA System Administrator — Image uploaded • 2024-05-28 02:28:49

SA System Administrator — Image uploaded • 2024-05-16 03:18:16

SA System Administrator — Field changes • 2024-05-16 03:18:08

Impact	3 - Low
Incident state	New
Opened by	System Administrator
Priority	5 - Planning

An automatically generated Service Now ticket, automatically enhanced with an E2E path from IP Fabric

This will be especially helpful in fulfilling requirements like those set out in the Detect function:

DE.AE-06
Ex3: Automatically create and assign tickets in the organization's ticketing system when certain types of alerts occur.

How else does this apply to NIST2.0?

Identify (ID)

Asset Management (ID.AM)

ID.AM-03: Representations of the organization’s authorized network communication and internal and external network data flows are maintained.

Protect (PR)

Security Continuous Monitoring (DE.CM)

DE.CM-01: The network is monitored to detect potential cybersecurity events.

DE.CM-07: Monitoring for unauthorized personnel, connections, devices, and software is performed.

DE.CM-08: Vulnerability scans are performed.

Respond (RS)

Security Continuous Monitoring (DE.CM)

RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident.

RS.AN-06: Actions performed during an investigation are recorded, and the records’ integrity and provenance are preserved.

RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved.

RS.AN-08: An incident’s magnitude is estimated and validated.

Incident Response Reporting and Communication (RS.CO)

RS.CO-02: Internal and external stakeholders are notified of incidents.

RS.CO-03: Information is shared with designated internal and external stakeholders.

09. Populate and Validate Network Intent Systems for a reliable Network Source of Truth

Use IP Fabric as your observed truth of network state and compare it to your baseline intent set in tools like **NetBox** and Nautobot to ensure accuracy and quick remediation when the actual network state drifts from intent.

Use network assurance to populate these tools from the very beginning, and every time a change is made, avoiding the inevitable human error associated with manual processes.

You can use this to fulfill requirements in the Detect function, such as DE.CM-01, Implementation Example 4: “Compare actual network flows against baselines to detect deviations.”

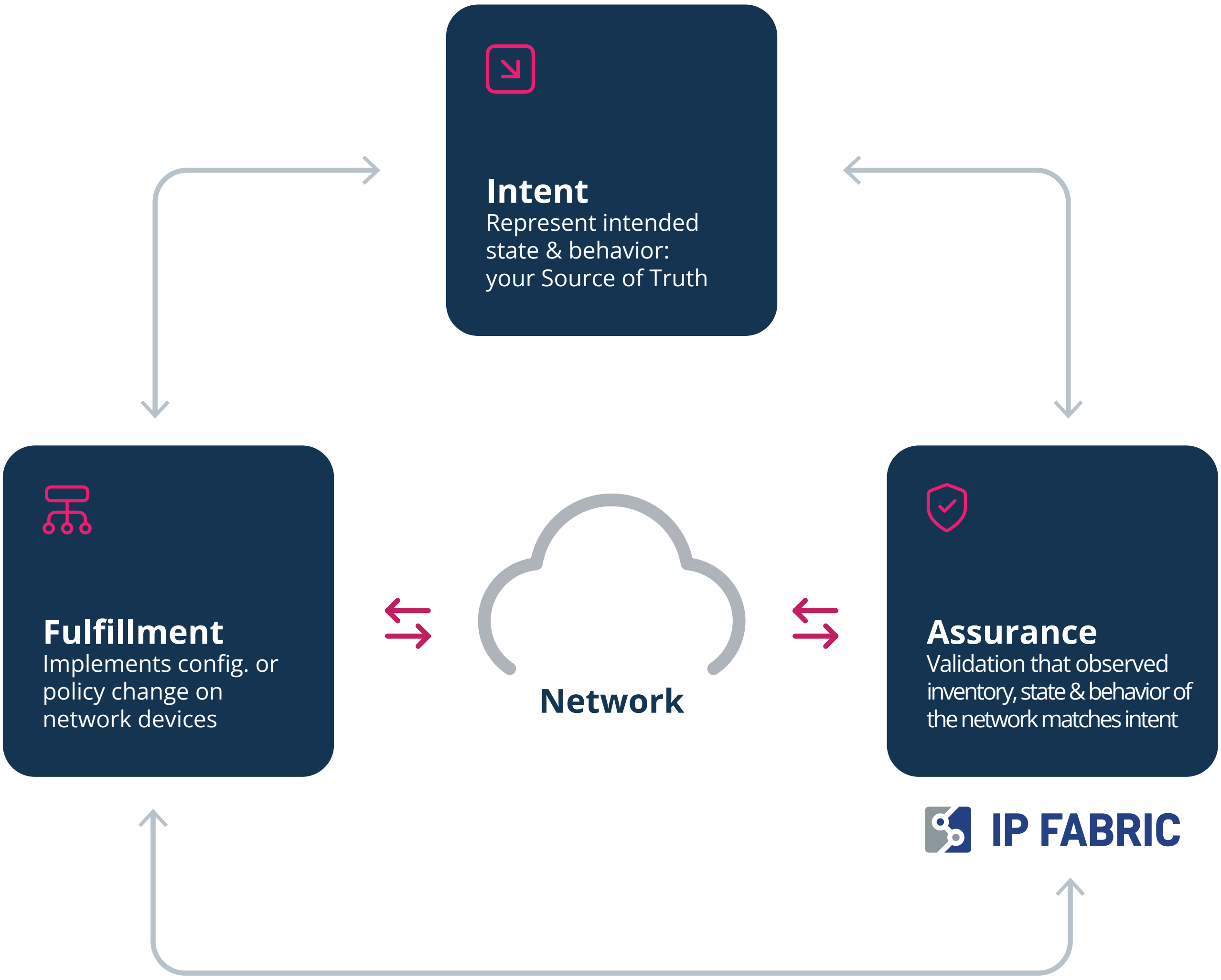
How else does this apply to NIST2.0?

Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)	Recover (RC)
Asset Mgmt. (ID.AM) **ID.AM-03:** Representations of the organization’s authorized network communication and internal and external network data flows are maintained. **Risk Assessment (ID.RA)** **ID.RA-01:** Asset vulnerabilities are identified and documented. **ID.RA-02:** Cyber threat intelligence is received from information sharing forums and sources.	**Information Protection Processes and Procedures (PR.IP)** **PR.IP-01:** A baseline config of information technology/industrial control systems is created and maintained. **PR.IP-10:** Response and recovery plans are tested.	**Security Continuous Monitoring (DE.CM)** **DE.CM-01:** The network is monitored to detect potential cybersecurity events. **DE.CM-07:** Monitoring for unauthorized personnel, connections, devices, and software is performed. **DE.CM-08:** Vulnerability scans are performed.	**Analysis (RS.AN)** **RS.AN-01:** Notifications from detection systems are investigated. **RS.AN-04:** Incidents are categorized consistent with response plans. **Mitigation (RS.MI)** **RS.MI-01:** Incidents are contained. **RS.MI-02:** Incidents are mitigated.	**Improvements (RC.IM)** **RC.IM-01:** Recovery planning and processes are improved by incorporating lessons learned into future activities.

10. Closed-Loop Automation – trigger remediation, validation, and documentation activity

Network assurance, in providing the structured, clean data needed for cloud and network automation, as well as the means to automatically validate network state post-change and update documentation, can pave the way for strategic business transformation.

Build closed-loop automation flows that remediate issues before they're noticed by users, using intent rules to trigger remediation action in automation tools.



Intent
Represent intended state & behavior: your Source of Truth

Fulfillment
Implements config. or policy change on network devices

Network

Assurance
Validation that observed inventory, state & behavior of the network matches intent

This lets you perform the required **Respond function RS.MI-02 Implementation Example 1:** "Cybersecurity technologies and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform eradication actions."

How else does this apply to NIST2.0?

Identify (ID)

Asset Mgmt. (ID.AM)

ID.AM-03: Representations of the organization’s authorized network communication and internal and external network data flows are maintained.

Protect (PR)

Maintenance (PR.MA)

PR.MA-02: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

Detect (DE)

Security Continuous Monitoring (DE.CM)

DE.CM-01: The network is monitored to detect potential cybersecurity events.

DE.CM-07: Monitoring for unauthorized personnel, connections, devices, and software is performed.

DE.CM-08: Vulnerability scans are performed.

Respond (RS)

Incident Analysis (RS.AN)

RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident.

RS.AN-06: Actions performed during an investigation are recorded, and the records’ integrity and provenance are preserved.

RS.AN-07: Incident data & metadata are collected, and their integrity and provenance are preserved.

RS.AN-08: An incident’s magnitude is estimated and validated.

Incident Response Reporting and Communication (RS.CO)

RS.MI-01: Internal & external stakeholders are notified of incidents.

RS.CO-03: Information is shared with designated internal and external stakeholders.

Recover (RC)

Improvements (RC.IM)

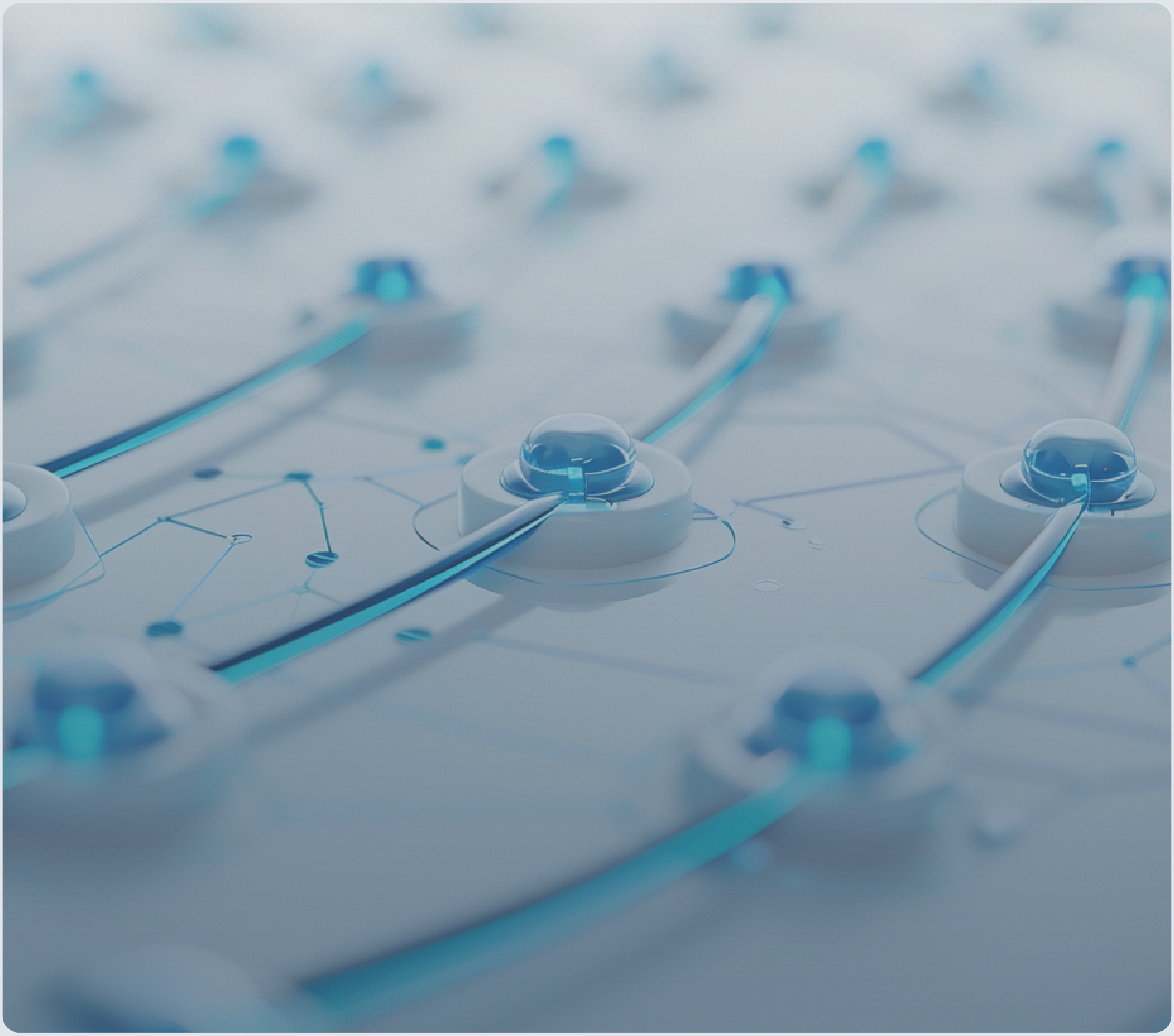
RC.IM-01: Recovery planning and processes are improved by incorporating lessons learned into future activities.

Conclusion

IP Fabric's Automated Network Assurance is a foundational technology to help meet NIST2 standards.

Another key capability of the platform is the ability to easily produce reports, diagrams, historical information, etc., which is used for planning changes, due diligence for strategic IT initiatives, and de-risking the implementation of those projects. These reports and diagrams are also the basis for evidence needed for internal audits.

Companies are spending weeks to months to produce the documentation that IP Fabric produces in a single, automated snapshot.



About IP Fabric

IP Fabric is a vendor-neutral network assurance platform that automates the holistic discovery, verification, visualization, and documentation of large-scale enterprise networks, reducing the associated costs and required resources whilst improving security and efficiency.

It supports your engineering and operations teams, underpinning migration and transformation projects. IP Fabric will revolutionize how you approach network visibility and assurance, security assurance, automation, multi-cloud networking, and trouble resolution.

Don't take our word for it

See how assurance can transform your approach to network management.

Access the demo

IP FABRIC

Support & Documentation
https://docs.ipfabric.io

HQ Office Boston
98 North Washington St.
Suite 407
Boston, MA 02114
United States

+1 617-821-3639

IP Fabric UK Ltd.
Gateley Legal,
1 Paternoster Square,
London,
England EC4M 7DX

+420 720 022 997

IP Fabric s.r.o.
Kateřinská 466/40
Praha 2 - Nové Město,
12000
Czech Republic

+420 720 022 997

ipfabric.io