Ivan McPhee
Nov 17, 2022 -- Market Radar

GigaOm Radar for Network Validation v1.01

Ensuring Intent and Mitigating Risk

Table of Contents

1. Summary

With business-critical services on the line, managing the network holistically is essential for ensuring operational consistency. Many enterprises address network governance with manual checks of their designs and configurations. However, this approach is subject to the availability and diligence of network administrators and does not always identify configuration drift or potential network issues, especially at scale. It is error-prone, operationally tedious, and ineffective for validating and protecting the network. In addition, cloud environments are dynamic, with evolving security mandates and constantly changing network designs. As a result, network teams are often uncertain whether the network is functioning as designed before and after a change.

To verify that the network is connected, secure, and operating as intended, enterprises must deploy robust validation tools providing up-to-date visibility of the network configuration and state, including address assignment, device interface state, neighboring devices, and Layer 2 and Layer 3 protocol information. Network validation determines whether the configuration or reconfiguration of the network meets the design or intent of the network. It focuses on analytical aspects, such as validating the reasons for making changes and predicting the impact of configuration changes. Including automation to improve accuracy and reduce risk, network validation comprises pre- and post-deployment unit testing, functional testing, and verification.

- **Automated pre-deployment checks:** Validation is done proactively before deploying a network change to determine whether the proposed change violates any predefined ("golden configuration") policy before it is applied. Failed checks automatically abort the deployment process. In addition, automated validation verifies that the desired interface is selected by checking its operational state, assigned address, and connected devices before authorizing the change, which minimizes the risk of an erroneous change reaching the production network and causing an outage.
- **Automated post-deployment checks:** Validation is done automatically after deploying a change to the network to determine whether the change was completed successfully and verify it had the intended impact. Failed checks automatically trigger a rollback of the change and launch a subsequent test to ensure the network was restored to its pre-deployment state. Automation ensures that the change is quickly reversed, with relevant data collected for analysis against the desired state before making needed corrections and reapplying the change.
- **Scheduled state validation:** Network administrators must be able to schedule network state validation periodically to ensure the network is performing as intended. Since the process is read-only, the validation can be run regularly to identify potential issues that would not necessarily be flagged by the network management system (such as failure of a redundant interface), enabling teams to be more proactive. In many cases, the post-deployment validation process can be used to validate the network before any change windows open up, irrespective of the planned changes.
- **Automated trouble ticketing:** The network validation system must provide out-of-the-box integration with trouble-ticketing systems for automatically creating tickets when the network state differs from the existing or future state as defined in the NSoT inventory and metadata. While remediation may initially be manual, the system should be able to support increasing automation as the organization matures, including automated actions and network validation scans based on specific triggers.

This GigaOm Radar report provides an overview of notable vendors and their offerings. The corresponding GigaOm report "“Key Criteria for Evaluating Network Validation Solutions" outlines critical criteria and evaluation metrics for selecting a network validation solution. Together, these reports offer essential insights for ensuring network resilience, helping decision-makers evaluate solutions before deciding where to invest.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding, consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Solution Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Target Markets and Deployment Models

To better understand the market and vendor positioning (**Table 1**), we assess how well a vendor's network validation solution supports different target markets and deployment models.

For the network validation sector, we recognize four target markets:

- **Network service provider (NSP):** Service providers who own, operate, and sell network services, such as network access and bandwidth, backbone infrastructure, and/or network access points, with other Tier 1, Tier 2, and Tier 3 service providers as primary customers. NSPs include data carriers, ISPs, telcos, and wireless providers.
- **Managed service provider (MSP):** Service providers delivering managed application, communication, IT infrastructure, network, and security services and support for businesses at either the customer premises or via MSP (hosting) or third-party data centers (colocation).
- **Large enterprises:** Enterprises of 1,000 or more employees with dedicated IT teams responsible for planning, building, deploying, and managing their applications, IT infrastructure, networks, and security in either an on-premises data center or a colocation facility.
- **Small-to-medium business (SMB):** Small businesses (less than 100 employees) to medium-sized businesses (100-1,000 employees) with limited budgets and constrained in-house resources for planning, building, deploying, and managing their applications, IT infrastructure, networks, and security in either an on-premises data center or a colocation facility.

For the network validation sector, we recognize four deployment models:

- **On-premises software:** Network validation components are deployed on a physical server located on-premises.
- **On-premises virtual:** Network validation components are deployed in a virtual machine running on a server located on-premises.
- **Cloud-based (private):** Network validation components are deployed in a private cloud managed in-house.
- **Cloud-based (public):** Network validation components are deployed in a public cloud managed by a cloud vendor.

Table 1. Vendor Positioning

	NSP	MSP	Large Enterprise	SMB	On-Premises Software	On-Premises Virtual	Cloud-Based (Private)	Cloud-Based (Public)
Anuta Networks	+++	+++	++	++	–	++	++	++
BMC Software	++	++	++	++	++	++	–	–
FirstWave	+++	+++	++	++	+++	+++	++	+
Forward Networks	++	++	++	–	+++	+++	+++	+++
Gluware	–	–	++	++	–	+++	++	++
Intentionet	–	–	++	++	–	–	++	+++
IP Fabric	–	++	++	++	–	++	–	–
Itential	+++	++	++	–	++	++	+++	+++
Juniper Networks	++	++	++	–	++	–	–	–
ManageEngine	–	++	+++	++	+++	+++	++	++
Micro Focus	++	+++	++	++	++	++	++	++
NetBrain Technologies	–	++	++	++	+++	+++	+++	–
Northern.tech	–	–	++	+++	++	++	++	++
SolarWinds	–	++	+++	++	++	++	++	++

Source: GigaOm 2022

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

3. Key Criteria Comparison

Building on the findings from the GigaOm report, "Key Criteria for Evaluating Network Validation Solutions," **Tables 2** and **3** summarize how well each vendor included in this research performs in the areas we consider differentiating and critical for the sector.

- **Key criteria** differentiate solutions based on *features and capabilities*, outlining the primary criteria to be considered when evaluating a network validation solution, including compliance verification, automated remediation, and network visualization.
- **Evaluation metrics** provide insight into the *impact of each product's features and capabilities on the organization*, reflecting fundamental aspects, including ecosystem support, validation approach, and flexibility.

The objective is to give the reader a snapshot of the technical capabilities of available solutions, define the perimeter of the market landscape, and gauge the potential impact on the business.

Table 2. Key Criteria Comparison

	KEY CRITERIA								
	Network Source of Truth	Golden Image Creation	End-to-End Validation	Automated Remediation	Compliance Verification	Security Verification	Network Visualization	Hybrid Multicloud Support	Network Validation as a Service
Anuta Networks	+++	+++	+++	++	+++	++	++	++	+++
BMC Software	++	++	+	++	+++	+++	+	+	–
FirstWave	++	+	+	++	++	++	+++	–	–
Forward Networks	+++	+++	+++	++	+++	+++	+++	+++	–
Gluware	+++	+++	++	+++	+++	+++	++	+	–
Intentionet	++	+	++	–	++	++	++	++	–
IP Fabric	++	+	++	–	++	++	+++	++	–

Juniper Networks	+++	++	++	++	+	+	++	++	–
ManageEngine	++	++	–	++	++	+	+	–	–
Micro Focus	+++	++	+++	++	+++	+++	+++	+++	–
NetBrain Technologies	+++	+++	+++	++	+++	++	+++	+++	–
Northern.tech	–	+++	++	++	++	++	+	++	–
SolarWinds	++	++	+	++	++	++	++	++	–

Source: GigaOm 2022

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Table 3. Evaluation Metrics Comparison

	EVALUATION METRICS						
	Ecosystem Support	Validation Approach	Flexibility	Manageability	Vendor Support	Pricing & TCO	Vision & Roadmap
Anuta Networks	+++	+++	+++	+++	+++	+++	+++
BMC Software	+	++	++	+	++	++	++
FirstWave	++	++	+++	++	+++	++	++
Forward Networks	+++	+++	+++	+++	+++	+++	+++
Gluware	++	+++	+++	++	++	++	+++
Intentionet	++	++	++	++	++	+++	++
IP Fabric	++	++	+++	++	++	++	++
Itential	+++	++	+++	++	++	+++	++
Juniper Networks	+++	++	++	++	+++	+	++
ManageEngine	++	+	++	++	++	++	++
Micro Focus	+++	+++	++	++	+++	++	++
NetBrain Technologies	+++	++	+++	++	+++	+++	+++
Northern.tech	++	++	+++	++	++	++	++
SolarWinds	++	++	++	++	+++	++	++

Source: GigaOm 2022

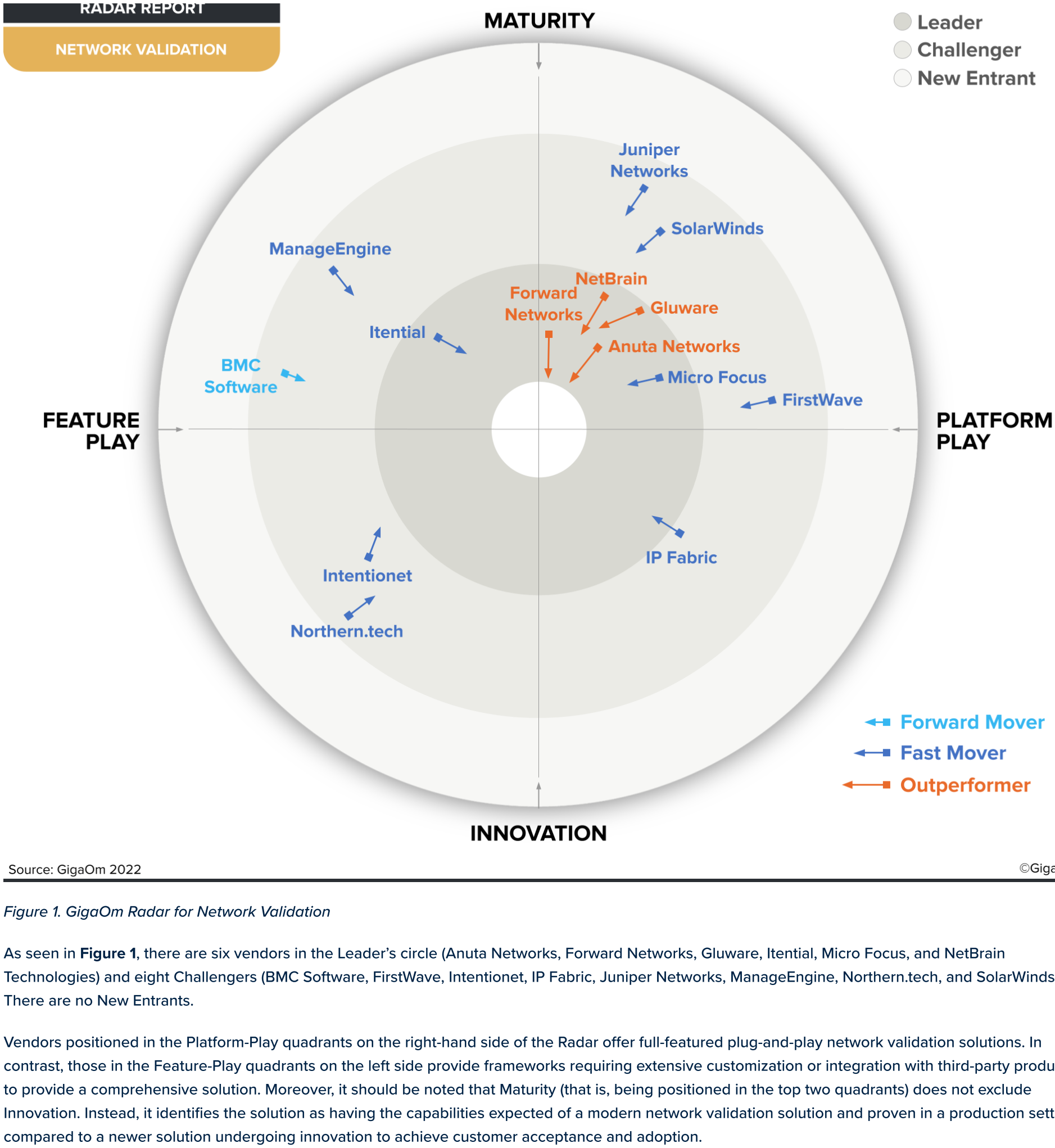
+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

By combining the information provided in the tables above, the reader can understand the technical solutions available in the market.

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to generate the GigaOm Radar in **Figure 1**. Based on their products' technical capabilities and feature sets, the chart is a forward-looking perspective on all the vendors in this report.

The GigaOm Radar plots vendor solutions across a series of concentric rings, with those set closer to the center judged to be of higher overall value. The chart characterizes each vendor on two axes—Maturity versus Innovation and Feature Play versus Platform Play—while the length of the arrow indicates the predicted evolution of the solution over the coming 12 to 18 months.



Source: GigaOm 2022 ©GigaOm

Figure 1. GigaOm Radar for Network Validation

As seen in **Figure 1**, there are six vendors in the Leader's circle (Anuta Networks, Forward Networks, Gluware, Itential, Micro Focus, and NetBrain Technologies) and eight Challengers (BMC Software, FirstWave, Intentionet, IP Fabric, Juniper Networks, ManageEngine, Northern.tech, and SolarWinds). There are no New Entrants.

Vendors positioned in the Platform-Play quadrants on the right-hand side of the Radar offer full-featured plug-and-play network validation solutions. In contrast, those in the Feature-Play quadrants on the left side provide frameworks requiring extensive customization or integration with third-party products to provide a comprehensive solution. Moreover, it should be noted that Maturity (that is, being positioned in the top two quadrants) does not exclude Innovation. Instead, it identifies the solution as having the capabilities expected of a modern network validation solution and proven in a production setting, compared to a newer solution undergoing innovation to achieve customer acceptance and adoption.

The length of the arrow (Forward Mover, Fast Mover, or Outperformer) represents execution against vision and roadmap (based on vendor input and in the context of advancements made across the industry in general). Four vendors in the Leader's circle (Anuta Networks, Forward Networks, Gluware, and NetBrain Technologies) are recognized as Outperformers.

While all fourteen vendors offer automated pre-deployment, post-deployment, and scheduled state validation, and can integrate with automated trouble-ticketing solutions, each supports different vendor devices and provides varying levels of verification. For example, some offer advanced mechanisms to verify Layer 1 to Layer 4 configuration and state constructs across the entire network to support a broad range of platforms. In contrast, others have only basic network verification logic, support a limited number of platforms, and lack coverage of security use cases, such as blast radius, device vulnerability analysis, and customizable security posture analysis. In addition, Intentionet and Northern.tech are the only vendors using open-source components and offering free licenses for limited deployments, making Batfish and CFEngine affordable solutions for SMBs. However, both solutions require advanced programming skills to implement.

The Leaders and Outperformers in this space—Forward Networks, Anuta Networks, NetBrain Technologies, and Gluware—all support a broad range of vendor devices with sophisticated validation and automated remediation capabilities. Offering complete visibility into the network topology, the leader in the space, Forward Networks, provides digital twin mapping of all possible traffic paths, while advanced search, validate, compare, and predict functions enable administrators to manage network behavior proactively in a vendor-agnostic manner. Furthermore, it's noteworthy that five vendors in the Leader's circle (Anuta Networks, Gluware, Itential, Micro Focus, and NetBrain Technologies) offer no-code/low-code capabilities for increased agility and extensibility.

INSIDE THE GIGAOM RADAR

innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.

The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

Anuta Networks: Anuta ATOM

Founded in 2010, Anuta Networks develops method of procedure (MOP)-based cloud-native, web-scale network automation solutions for branch, campus, data center, and multivendor service provider-managed enterprise networks. An extensible and scalable microservices-based, vendor-agnostic automation platform, Anuta ATOM is a complete element management system (EMS) and fault, configuration, accounting, performance, and security (FCAPS) lifecycle service orchestration and telemetry platform deployed on-premises or in the cloud for physical, virtual, and hybrid networks. Delivering a comprehensive set of out-of-the-box services and workflows for device onboarding, zero-touch provisioning (ZTP), configuration management, active assurance, compliance, network and service monitoring and alerting, and software upgrades, ATOM supports over 150 physical and virtual platforms from more than 45 vendors.

ANUTA ATOM AT A GLANCE — GIGAOM

TARGET MARKET			
NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
X	X	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	ON-PREMISES VIRTUAL	PRIVATE CLOUD	PUBLIC CLOUD
-	X	X	X
PRIMARY USE CASES			
Service monitoring and active assurance		Alert correlation and closed-loop automation	
Pre- and post-checks for MOPs and services		Multivendor EMS, FCAPS, inventory, and topology	
PRICING MODEL			
Tiered 1-, 3-, or 5-year device- or platform-based subscription licensing			

Source: GigaOm 2022

Figure 2. Anuta ATOM at a Glance

An acronym for Automation, Telemetry, Orchestration, and Monitoring, ATOM is a comprehensive closed-loop automation platform encompassing compliance, configuration maintenance, device and service lifecycle management, and network assurance. Built from the ground up by leveraging Docker containers and Kubernetes orchestration, ATOM's web-scale approach enables customers to start small and scale on demand to thousands of devices. The platform also allows NSPs to choose discrete features and functions, deploy on-premises or on private, public, or hybrid cloud platforms, and conduct selective rolling upgrades using containerization.

Supporting unit tests, functional tests, verification, and service-level agreement (SLA) compliance, ATOM's compliance policy builder enables the administrator to define and standardize configurations. Network devices can be onboarded manually or automatically, with brownfield devices discovered through seed and sweep mechanisms and greenfield devices added via ZTP. In addition, ATOM integrates with continuous integration/continuous deployment (CI/CD) tools such as GitLab, allowing networking teams to release a constant flow of software updates to accelerate release cycles and reduce

specific devices using “show | compare” command-line interface (CLI) commands.

ATOM provides over 225 out-of-the-box service lifecycle management and service orchestration use cases spanning various capabilities to simplify the user experience. The intuitive, drag-and-drop, low-code workflow automation framework automates complex workflows, including diagnostic and troubleshooting scenarios, network migration, software upgrades, and device return merchandise authorization (RMA). Supporting role-based access control (RBAC) and multitenancy, workflow execution can be carefully controlled with the entire network monitored via SNMP, SNMP Trap, Syslog, and streaming telemetry mechanisms with comprehensive alert routing and suppression.

Strengths: ATOM is an extensible, feature-rich, and scalable integrated platform offering customers comprehensive support for out-of-the-box service lifecycle management and service orchestration use cases. Simplifying the design of self-service workflows with low-code automation and an interactive graphical user interface (GUI), ATOM includes the capability to evaluate existing data and crowd-sourced analytics to automate policy generation for network performance, availability, and SLA conformance using artificial intelligence/machine learning (AI/ML) that’s been prioritized in the roadmap. In addition, Anuta offers network validation as a service via ATOM Cloud.

Challenges: While including significant out-of-the-box functionality, deploying Anuta ATOM generally requires relying on professional services, which increases the cost and time to implement. In June 2020, Anuta Networks announced a strategic partnership with Juniper Networks to integrate the ATOM platform with Juniper’s network automation portfolio, resulting in both complementary and overlapping capabilities—such as active service assurance and built-in AI/ML features. In addition, the ATOM platform lacks path computation capabilities and is dependent on the support of Juniper’s Paragon Automation Portfolio to deliver them. While the partnership is anticipated to cement Anuta’s position in the market, customers should be aware of the choices that need to be made (including integration with third-party AI/ML solutions) and the potential complexity resulting from introducing alternative technologies.

BMC Software: TrueSight Automation for Networks

Founded in 1980 to help companies optimize their investments in mainframe technologies, BMC Software has expanded through organic growth, R&D, and strategic acquisitions to include infrastructure, networks, and services in distributed environments spanning data centers and multicloud environments. Managing physical and virtual network devices and software-defined networking (SDN) infrastructures via a single solution, BMC’s TrueSight Automation for Networks helps administrators accelerate the provisioning, configuration, compliance, maintenance, auditing, and vulnerability management of routers, switches, wireless devices, load balancers, firewalls, and intrusion detection system (IDS) solutions. Administrators can browse real-time device configurations for troubleshooting or job status updates or complete a compliance audit by capturing configuration, compliance, and security data across the entire network in minutes.

TRUESIGHT AUTOMATION FOR NETWORKS AT A GLANCE			GIGAOM
TARGET MARKET			
NETWORK SERVICE PROVIDERS	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
X	X	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	**ON-PREMISES VIRTUAL**	**PRIVATE CLOUD**	**PUBLIC CLOUD**
X	X	-	-
PRIMARY USE CASES			
Vulnerability prioritization and management		Regulatory compliance	
Automated network remediation		Closed-loop change tracking	
PRICING MODEL			
Pricing available only on request			
Source: GigaOm 2022			

Figure 3. TrueSight Automation for Networks at a Glance

Running on the same server or different servers or virtual machines (VMs), TrueSight Automation for Networks comprises the TrueSight Network Automation application server and TrueSight Network Automation remote device agents running on Linux or Windows hosts to manage devices that are not reachable from the application server or those with overlapping IP addresses. Device agents interact with devices using telnet, SSH, HTTP(S), TFTP, FTP,

the Network Automation user interface (UI)—can be used to perform tailored device interactions.

The network is discovered via BMC Discovery, CiscoWorks, Entuity Network Analytics, HelpSystems Intermapper, Progress WhatsUp Gold, user-defined database queries, or CSV formatted files, with the information stored in the BMC Atrium Configuration Management Database (CMDB) where network configurations are proactively assessed, and the impact of changes on services and compliance reported based on business context. When non-compliant devices are detected, incident tickets are automatically opened in BMC Remedy ITSM Incident Management and network changes are tracked and approved through BMC Remedy ITSM Change Management.

TrueSight Automation leverages BMC's SmartMerge technology to auto-generate scripts for configuration updates, rollbacks, and standards enforcement without rebooting the device. In addition, integration with vendor security advisories and the NIST National Vulnerability database security notifications help ensure vulnerabilities are quickly identified, device images remediated, and upgrades installed according to the policy-based application of operational, security, and regulatory guidelines.

Strengths: TrueSight Automation for Networks is a part of BMC's IT Operations Management (ITOM) portfolio and integrates with BMC's IT service management and governance solutions. Improving compliance audit readiness, reducing errors and omissions, and freeing up resources, TrueSight Automation for Networks allows changes to be quickly rolled out across large Cisco and Juniper Networks environments. In addition, TrueSight Automation for Networks enables intent-based networking with intelligent, policy-based changes designed to avoid unintended consequences and outages.

Challenges: TrueSight Automation for Networks supports a limited selection of hardware devices compared to other solutions. While BMC's TrueSight Automation for Networks includes REST application programming interfaces (APIs) and offers advantages for customers using other BMC solutions in Cisco and Juniper Networks environments, customers find the product complex and challenging to use, with limited out-of-the-box integrations and documentation of real-world examples, which slows down the enablement of new features. In large environments with multiple application servers, the servers do not share data or content, requiring synchronization by pushing the content from one server and pulling it into all the other application servers. Pricing is available only on request.

FirstWave: Network Management Information System (NMIS)

Founded in 1999 and acquired by FirstWave Cloud Technology Limited in January 2022, Opmantek was a leading provider of open-source enterprise- and service provider-grade network management, automation, and IT audit software, with more than 150,000 customers in over 175 countries. Often deployed to replace or consolidate legacy systems, Network Management Information System (NMIS) delivers scalable network automation and visibility irrespective of the size, location, or type of the underlying hardware and software infrastructure. FirstWave offers various optional NMIS modules, including opConfig (automated configuration management), opAddress (IP address management and auditing), opEvents (centralized log and event management), opReports (advanced analysis and reporting), and opCharts (interactive, actionable dashboards). In addition, FirstWave's Open-AudIT is a network discovery, inventory, and audit application that accurately captures what is attached to the network, how it is configured, and when it changes, while its CyberCision platform enables providers to deliver security services to customers.

NETWORK MANAGEMENT INFORMATION SYSTEM AT A GLANCE GIGAOM

TARGET MARKET			
NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
X	X	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	ON-PREMISES VIRTUAL	PRIVATE CLOUD	PUBLIC CLOUD
X	X	X	X
PRIMARY USE CASES			
Automated configuration management		Automated compliance management	
Disaster recovery		Network troubleshooting	
PRICING MODEL			
Free time-unlimited 20-node license; 1-year device-based subscription licensing			

Source: GigaOm 2022

Figure 4. Network Management Information System at a Glance

organization's IT environment, assists in identifying and remediating faults, and provides valuable information for IT departments to use in planning expenditure and IT changes.

Continuously monitoring the configuration of devices discovered by FirstWave's Open-AudIT Enterprise or managed by NMIS, opConfig captures, tracks, pushes, and rolls back configuration changes for any device or cloud application on your network, storing a complete history of configuration information. Implementing RBAC, opConfig simplifies the management of configuration files in a multivendor environment, maintaining a complete record of configuration changes and audit results for comparing changes and ensuring regulatory compliance (APRA, COBIT, PCI-DSS, SOX) for device configuration, software versions, and hardware. Organizations can efficiently manage the backup and comparison of configuration information using customized or prebuilt industry-standard rule sets, such as Cisco-NSA. In addition, opConfig enables network administrators to create robust command sets for root cause analysis of faults.

Used by over 130,000 organizations worldwide, Open-AudIT's agentless device discovery intelligently scans an organization's network and stores the configurations of the discovered devices, providing immediate access to software licensing, configuration changes, non-authorized devices, capacity utilization, and hardware warranty status reports. Collecting and cataloging significant amounts of data across different network architectures, Open-AudIT provides compliance baselines for comparing software, hardware, users, and *netstat* data against required standards.

Strengths: The combination of the CyberCision (cybersecurity-as-a-service), NMIS (network management), and Open-AudIT (network discovery, inventory, and audit) products enable FirstWave to provide a comprehensive end-to-end solution for network discovery, management, and cybersecurity for enterprises and service providers globally. NMIS is used to centrally manage Microsoft's internal networks, including automated device discovery capability, detailed data center inventory, event configuration, and compliance management. In addition, NASA chose NMIS to support the Artemis moon exploration program because of its ability to handle real-time events in mission-critical settings.

Challenges: While reducing deployment costs, prospective customers should be aware that NMIS is an open-source network management system relying on community involvement for development and support. However, FirstWave provides enterprise-grade support and develops additional modules running on NMIS under low-cost commercial licenses for configuration management, database integration, event management, high availability, advanced reporting, and other capabilities.

Forward Networks: Forward Enterprise

Founded in 2013, Forward Networks is a leader in intent-based verification and network assurance, focusing on helping network administrators proactively manage network complexity and ensure network health by making networks more agile, reliable, and secure. Creating an accurate digital twin of the network, Forward Enterprise enables network operators to verify intent, predict network behavior, and simplify network management. The solution supports all major networking vendors and cloud, hybrid cloud, and multicloud environments, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

FORWARD ENTERPRISE AT A GLANCE — GIGAOM

TARGET MARKET			
NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
X	X	X	-
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	ON-PREMISES VIRTUAL	PRIVATE CLOUD	PUBLIC CLOUD
X	X	X	X
PRIMARY USE CASES			
Workflow automation/integration		End-to-end multicloud visibility	
Security posture verification/vulnerability management		Path verification and analysis	
PRICING MODEL			
1-year or multiple-year per device or per cloud compute instance subscription-based licensing			

Source: GigaOm 2022

Figure 5. Forward Enterprise at a Glance

the network topology, the digital twin maps all possible traffic paths, while advanced search, validate, compare, and predict functions enable administrators to manage network behavior proactively in a vendor-agnostic manner. Moreover, the digital twin allows network engineers to search the on-premises and multicloud network infrastructure like a database, perform forensic analysis, accelerate troubleshooting, predict network behavior before pushing changes live, visualize on-premises and cloud topology, and trace all possible traffic flows.

The Forward Verify function continuously audits the network, sends non-compliance alerts, and automates pre- and post-deployment checks using a complete suite of network verification features, including network query engine (NQE) verification to detect violations, predefined verification to verify common Layer 1 to Layer 4 configuration and state constructs across the entire network, and user-defined intent verification to ensure compliance, fault tolerance, reachability, and security. Network and security violations trigger tickets, proactively informing network operators of problems requiring remediation. In addition, Forward Enterprise's "behavioral diffs" function surfaces changes across different layers in the network stack and determines what effect those changes have on the network intent policies defined by the network administrator, reducing the time it takes to verify network behavior after a change in configuration and state and mitigating the risk of change-induced outages or rollbacks.

Forward Enterprise provides a modern, intuitive, and robust user experience with out-of-the-box wizards to simplify configuration. By integrating seamlessly with existing IT workflows for automation, chat, IP management, and ticketing—including Ansible, BlueCat, ServiceNow, and Slack—via REST APIs, Forward Enterprise's single source of truth can be extended across ecosystem vendors to accelerate network and security operation workflows. In addition, customers can enhance the network's security posture with cloud security verification, automated security posture connectivity analysis, identification of the blast radius of compromised hosts, and enhanced automated vulnerability analysis.

Strengths: Scaling to over 50,000 network infrastructure devices and complex public cloud deployments, Forward Enterprise supports virtual client devices hosted in public cloud services, over 456 device types, and more than 1479 OS versions across 19 major networking vendors. The solution helps IT teams proactively manage network complexity and prevent incidents by ensuring network health, predicting how changes will impact network behavior, and ensuring network compliance with industry best practices for real-world networks. In addition, the digital twin allows network and security engineers to search the network like a database, trace all possible traffic flows, visualize on-prem and cloud topology, predict network behavior before pushing changes live, perform forensic analysis, and accelerate troubleshooting.

Challenges: Forward Enterprise's network source of truth contains an enormous amount of valuable data that needs to be unlocked to enable new cloud, network, and security change and posture management applications, making it available to a broader set of users. Leveraging the known data includes providing out-of-the-box integrations with third-party platforms for gathering new data and generating compounding value in the market. In addition, Forward Enterprise currently lacks automated remediation, change prediction for Layers 2 and 3, and Layer 2 overlays in the network topology map. However, we expect the company to make significant progress in these areas over the next 12 to 18 months.

Gluware: Gluware Intelligent Network Automation

Entering stealth in 2007, launched in 2011, and relaunched in 2017, Gluware provides a suite of applications to discover, inventory, manage, monitor, and audit the network, including generating network topologies, monitoring configuration drift, automating operating system upgrades, and automating processes. Supporting over 40 network operating systems and cloud platforms—including AWS, Azure, and Google Cloud—Gluware's modular, microservices-based network validation solution includes intelligence for each vendor platform with continuous discovery and out-of-the-box network monitoring and management. In addition, the low-code Gluware Lab integrated development environment (IDE) enables customers to customize abstractions and business logic and integrate with additional third-party solutions.

TARGET MARKET			
NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
-	-	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	ON-PREMISES VIRTUAL	PRIVATE CLOUD	PUBLIC CLOUD
-	X	X	X
PRIMARY USE CASES			
Multivendor application validation and support		Network process automation	
Configuration drift, backup, compliance, and audit		Security vulnerability management and verification	
PRICING MODEL			
1-, 3-, or 5-year hosted or on-premises subscription-based licensing			
Source: GigaOm 2022			

Figure 6. Gluware Intelligent Network Automation at a Glance

Gluware's Intelligent Network Automation platform comprises Gluware Control and a suite of intent-based applications, including Device Manager App (a single source of truth with deep discovery and inventory of the entire multivendor enterprise network), Config Drift and Audit (high-resolution snapshots of the network to detect drift and accelerate network audits), Config Modeling (converts imported CLI-based features and running configs into automated network policy at scale), Network RPA (no-code process automation enabling drag-and-drop builds of user-defined process workflows), OS Manager (for network upgrades, downgrades, and patching), and Topology (a visual representation of the network). These integrated components provision inventory, drift, audit, and config management tasks via secure shell (SSH) protocol to enterprise network devices.

Deployed on-premises or in the cloud, Gluware Control is a centralized control panel and orchestration engine for Gluware's platform, enabling administrators to manage users with role-based access, create organizations for multitenant network management, import devices, perform inventory, and load and manage software packages and applications. Communicating with multivendor, multiplatform physical and virtual systems via an API or CLI, Gluware's intelligent orchestration engine provides data-model driven, intent-based intelligence to discover, analyze, and validate network actions at scale, including accelerating the replacement of less extensible and less secure legacy network configuration and change management (NCCM) solutions.

Gluware performs built-in closed-loop pre- and post-checks of the configured state to determine what changes are needed to implement and verify the intended state. Gluware is also extensible, enabling customers to define additional operational state checks related to the interface state, a protocol state, or a connectivity check to define network-wide data models for end-to-end verification. Actions are automated via Gluware's intent-based applications incorporating modular, purpose-built functions for device management and inventory, configuration drift and audit, OS upgrades, configuration modeling, and workflow automation. For example, the Gluware Config Drift application takes periodic high-resolution "snapshots" of either the entire network or specific nodes to establish a baseline configuration. Then, automated line-by-line comparisons detect changes, triggering device remediation or promoting the snapshot to the current default.

Strengths: Incorporating intent-based intelligence for zero-touch network provisioning and lifecycle management, Gluware Intelligent Network Automation is a no-code/low-code automation suite enabling customers to create a digital twin of their network, detect drift, conduct audits, and orchestrate configuration remediation based on their desired state. Gluware enables network engineers to abstract the complexities of network management, remotely deploy new devices, and centrally manage features and services. Furthermore, Gluware's customer-driven roadmap is focused on enabling complex enterprise use cases incorporating robotic process automation, self-operating functionality, and visualization.

Challenges: Gluware currently lags behind some competitors in ease of use and integration among the various Gluware applications, though its 2023 roadmap simplifies its flexible no-code/low-code drag-and-drop capabilities and extends them throughout the entire product suite. Moreover, Gluware does not provide native hybrid, multicloud, or overlay support. The Config Modeling application uses Terraform as a vendor adapter to configure virtual private clouds in AWS, Azure, and GCP. Prospective clients should be aware that Gluware also uses optional agents to collect information and feedback from network devices and that the SaaS version, Gluware Pro, lacks the scalability of the on-premises Gluware Enterprise version.

Intentionet: Batfish

Founded in 2015, Intentionet is the startup behind the Batfish open-source network analysis engine developed in collaboration with industry and academic partners. Batfish handles the operational state of the network such as BGP announcements and interface status. Intentionet's enterprise version, Batfish Enterprise, simulates the impact of a network change, flagging outages and security vulnerabilities before changes are deployed in production. On

source Batfish while Batfish Enterprise will be discontinued.

BATFISH ENTERPRISE AT A GLANCE			GIGAOM
TARGET MARKET			
NETWORK SERVICE PROVIDERS	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
-	-	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	**ON-PREMISES VIRTUAL**	**PRIVATE CLOUD**	**PUBLIC CLOUD**
X	X	X	X
PRIMARY USE CASES			
Change impact analysis and ACL testing		Network configuration auditing	
Pre-deployment validation		Post-deployment validation	
PRICING MODEL			
Free download from GitHub or 1-, 3-, or 5-year device-based subscription licensing			
Source: GigaOm 2022			

Figure 7. Batfish at a Glance

An open-source, multivendor network analysis tool, Batfish allows customers to manage the operational state of the network, validating configuration data, querying control plane state, verifying access control list (ACL) rule sets, analyzing routing and flow paths, and simulating network failure. Mitigating the risk of network outages or security breaches, Batfish builds complete models of network behavior from device configurations, detects violations of built-in, user-defined, and best-practices network policies, and guarantees the security, reliability, and compliance of planned or current network configurations. Running as a containerized Docker service, Batfish supports configurations for a growing set of physical and virtual devices, including Arista, Cisco, Check Point, Cumulus, Juniper Networks, and Palo Alto Networks. In addition, Batfish provides visibility into the state of AWS cloud infrastructure but does not provide pre- or post-deployment validation.

Discovering the network via snapshots, Batfish runs offline with no direct access to network devices required. Once the snapshot (including device configuration and server details) has been uploaded to the Batfish service, a series of internal vendor-agnostic models are built. Holding both network configuration and the network control plane data, these models can be queried via questions using Ansible or Python software development kits (SDKs) to verify configurations. Moreover, the analysis can be enhanced with additional information from BGP routes received from external peers or topology information advertised by link layer protocols (LLDP or CDP).

Building on the open-source Batfish, Intentionet's fully supported, cloud-based Batfish Enterprise provides a dynamic, real-time network map and flexible, out-of-the-box change validation and review workflows for proposing and evaluating changes to network device configurations. A web-based policy dashboard provides continuous validation of network security and availability, while a visual traceroute determines network paths across on-premises and cloud networks. In addition to delivering multilingual APIs, a Python SDK, and integrations with third-party tools such as GitHub, RANCID, ServiceNow, and Slack to enable custom workflows, Batfish Enterprise will soon support pre- and post-deployment validation for AWS, Azure, and GCP using HashiCorp Terraform.

Strengths: Batfish is a free, open-source validation solution offering a range of network modeling and simulation features. Simulating a Layer 3 impact analysis of the network, Batfish allows users to disable a link or node and then compare the state of the network in terms of compliance, reachability, and security before pushing changes to the production environment. Performing virtual traceroutes and reachability tests across the network topology, Batfish also allows users to validate the outcome of sending specific traffic flows through an ACL or sets of multiple ingress/egress filters. In addition, Batfish provides an extensive range of configuration attributes that can be queried, including BGP, OSPF, and interface properties.

Challenges: While eliminating complex, time-consuming, and resource-intensive traditional methods of validating the network changes, Batfish lacks the advanced capabilities of many other network validation solutions. Moreover, the network model is inaccurate because it is based only on the device configuration and ignores the device state. In addition, Batfish only uses basic 5-tuple path analysis, has limited Layer 2 support, and lacks coverage of security use cases, such as blast radius, device vulnerability analysis, and customizable security posture analysis. Furthermore, the open-source Batfish requires Python skills to extract the data for verifying configurations. Finally, Batfish Enterprise will be sunset as the Intentionet team focuses on supporting open-source Batfish along with the open-source community.

Founded in 2015, IP Fabric strives to empower network professionals globally and cross-functionally by automating network documentation, accelerating the troubleshooting process, and visualizing the network infrastructure. IP Fabric's Automated Network Assurance Platform helps network engineers discover, verify, and document large-scale enterprise networks within minutes by automating network infrastructure data collection and providing predefined verifications highlighting inconsistencies, misconfigurations, and issues within enterprise networks.

AUTOMATED NETWORK ASSURANCE PLATFORM AT A GLANCE			GIGAOM
TARGET MARKET			
NETWORK SERVICE PROVIDERS	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
-	X	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	**ON-PREMISES VIRTUAL**	**PRIVATE CLOUD**	**PUBLIC CLOUD**
-	X	-	-
PRIMARY USE CASES			
Network visibility and assurance		Network security policy management	
Multicloud networking		Network visualization and documentation	
PRICING MODEL			
1-, 3-, or 5-year device-based subscription licensing			
Source: GigaOm 2022			

Figure 8. Automated Network Assurance Platform at a Glance

IP Fabric's multivendor network analytics platform automates network discovery, modeling, verification, and visualization by enabling an intent-based approach to network management and instant application path simulation of large-scale networks. Shipping with over 120 built-in customizable intent verification rules recommended as best practices, IP Fabric can discover over 3,000 devices per hour and supports up to 20,000 managed devices in a single virtual appliance, offering scalability for the most extensive networks. In addition, the solution collects data from the network regularly, creating a digital point-in-time snapshot of the entire network.

Using a unique network model and algorithms, IP Fabric then reconstructs the network's forwarding and policy behavior, simulating actual packet flows to detect critical violations, identify inefficiencies, and verify policy compliance. Vendor-specific output is parsed to enable understanding of each device's configuration, state, and relationships. The platform also models control plane relationships—such as routing protocol peering and spanning tree neighbors—to provide a comprehensive picture of network behavior. Built-in checks highlight single points of failure and reduced redundancy across the network topology, while custom intent verification rules allow administrators to create end-to-end path simulations representing application flows to validate behavior and compliance against organizational standards. In addition, IP Fabric uses webhooks to trigger automated systems to alert administrators and remediate configuration drift.

IP Fabric's interactive visualization capability allows administrators to view the network in terms of how they want to gain in-depth insights into its topology and behavior, including forwarding and policy decisions made at every device from the source device to the destination. In addition, protocols can be switched on or off, automatically generating layouts and creating network views that can be exported and shared across teams. IP Fabric currently operates as a standalone VMware 5.0 virtual server supporting a broad range of public clouds and networking and security vendors, including F5, Arista, Aruba, AWS, Azure, Check Point, Cisco, Dell, Fortinet, HPE, Huawei, Juniper Networks, Ruckus, and Versa Networks.

Strengths: IP Fabric Automated Network Assurance Platform helps network and security teams discover, model, verify, and visualize large-scale networks within minutes. IP Fabric's flexible, state-of-the-art topology data overlay visualization capabilities allow administrators to compare the network's past states, verify changes, perform root cause analysis, and improve troubleshooting processes through an automated toolset. In addition, IP Fabric helps ensure that network access control technologies (such as 802.1X with authentication services) are correctly configured and standardized.

Challenges: IP Fabric does not monitor the network in real time but offers point-in-time comparison of Layers 1, 2, and 3, providing end-to-end path representation allowing administrators to see what has changed. IP Fabric can only be deployed on Hyper-V, KVM, Nutanix, and VMware OVA if required. In addition, IP Fabric only uses basic 5-tuple path analysis and lacks coverage of advanced security use cases, such as blast radius, device vulnerability analysis, and customizable security posture analysis.

Founded in 2014, Itential is a multidomain network automation software company with a mature workflow engine for operationalizing network automation, service orchestration, and policy management across network and cloud infrastructures. Available as an on-premises solution or as a cloud service, Itential Automation Platform (IAP) is a low-code, API-first, cloud-native automation, integration, and orchestration framework. Leveraging a patented method for performing data model translation and integration across platforms, IAP uses out-of-the-box adapters to integrate with any IT system or network technology within a customer's ecosystem, enabling network engineers to extend the reach of their pipelines across disparate network technologies and domains.

ITENTIAL AUTOMATION PLATFORM AT A GLANCE			GIGAOM
TARGET MARKET			
NETWORK SERVICE PROVIDERS	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
X	X	X	-
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	**ON-PREMISES VIRTUAL**	**PRIVATE CLOUD**	**PUBLIC CLOUD**
X	X	X	X
PRIMARY USE CASES			
Data center and WAN/SD-WAN		Public and private cloud	
Wireless (4G/5G Wi-Fi and satellite)		Network services (DNS, load balancers, firewalls, and so on)	
PRICING MODEL			
1- or 3-year SaaS subscription-based licensing or on-premises, term-based licensing			
Source: GigaOm 2022			

Figure 9. Itential Automation Platform at a Glance

Itential provides a feature-driven, flexible platform for automation and orchestration across all technology (physical-, virtual-, and container-based network functions and overlays) domains through patented integration and federation capabilities, enabling users to instantly integrate with and manage any controller, device, or system. While providing a federated view of the network, Itential leverages the intelligence and capabilities of third-party tools—SDN, orchestration platforms, helpdesk systems, and other IT system management software—to model and execute automation workflows.

Itential's Automation Platform (IAP) comprises four components: Itential Automation Gateway (IAG), Itential Configuration Manager (ICM), Itential Operations Manager (IOM), and Itential Automation Studio (IAS). Available as an on-premises system or as a SaaS, the Itential Automation Platform automates the configuration of on-premises networking hardware and software components and cloud services. An API-first, vendor-agnostic solution acting as an aggregated network API, IAP federates the data and functionality from existing northbound and southbound systems.

IAP includes analytics and command templates that can be customized to perform automated pre- and post-deployment checks across multivendor and multidomain network technologies. Checks can be performed as a part of a workflow or as a part of a scheduled activity, with tools available for engineers to develop and test customized simple or complex validation logic. IAP includes a robust compliance and validation engine, as well as multiple tools for defining the desired state and remediating out-of-compliance configurations. In addition, scans can be performed on demand, via API, as a scheduled activity, or as part of a larger automation orchestration workflow.

Furthermore, ICM simplifies the building of golden configurations for any CLI-based network device or API-based cloud service, enabling network teams to quickly build rules and verify compliance for any network device—including routers, switches, and firewalls. If a network device is reported as out of compliance, ICM can automatically remediate any part of the network to ensure it always remains in compliance. In addition, IOM tracks, analyzes, and manages automations and metrics, allowing administrators to directly view and work on tasks requiring manual intervention, including controlling when, how, and with what data a workflow should run.

Strengths: Purpose-built for workflow automation, Itential's "no-code integration with anything" allows customers to build their own integrations for free. At the same time, Itential's API-first approach extends validation beyond CLI environments to include any environment that can be addressed via an API. In addition, Itential's modular framework integrates seamlessly with orchestration and automation capabilities, enabling users to incorporate validation functionality into other orchestration flows. Finally, Itential's SaaS platform allows organizations to evaluate IAP in a full, feature-rich cloud environment with training courses designed to accelerate onboarding and time to value.

southbound systems to provide these features. Moreover, Itential's focus on federating network automation means a continuous integration cycle with third-party products, requiring regular upgrades that may be difficult to maintain for smaller IT departments. However, Itential enables customers to auto-generate integrations via new API calls, eliminating much of the time and cost associated with new integrations or updates.

Juniper Networks: Juniper Apstra

Founded in 2014 and acquired by Juniper Networks in 2021, Apstra delivers intent-based networking and analytics to help eliminate network complexities and inefficiencies. A multivendor, intent-based networking solution providing closed-loop automation, Juniper Apstra translates business intent and technical objectives into essential policy and device-specific configurations, continuously self-validating and resolving issues to ensure compliance. Customers specify the "what" (network topology, VLANs, desired capacity, redundancy requirements, access rules, and more) and Apstra delivers the "how."

JUNIPER APSTRA AT A GLANCE — GIGAOM

TARGET MARKET			
NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
X	X	X	-
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	ON-PREMISES VIRTUAL	PRIVATE CLOUD	PUBLIC CLOUD
X	X	X	X
PRIMARY USE CASES			
Automation of Day 0, 1, 2+ network lifecycle operations		Deployment of private, public, or hybrid clouds	
Zero-touch provisioning		Automation of NFV through service chaining	
PRICING MODEL			
1-, 2-, or 3-year subscription pricing based on the number of devices under management			

Source: GigaOm 2022

Figure 10. Juniper Apstra at a Glance

Boasting several Fortune 100 customers and service providers, Juniper Apstra is a software-only, multivendor, intent-based networking solution leveraging closed-loop automation and assurance for complete data center fabric management spanning Day 0, 1, and 2+ operations. Built with a highly scalable datastore tracking changes in real-time, Apstra enables customers to build networks quickly by automating network design, deployment, and management, continuously validating the network against expressed intent. Juniper claims Apstra is the industry's first and only vendor-agnostic intent-based networking platform, with customers reporting deployment accelerated by 90%, mean time to resolution (MTTR) improved by 70%, and operational expenditure (OpEx) reduced by 83%.

The Apstra software is installed as one or a set of virtual machines to connect and manage devices via agents installed on or off the devices. Customers design the rack types and fabric network using Apstra templates, which are then instantiated into blueprints representing the physical network. As the blueprint is built, Apstra automatically produces the necessary device configurations, providing an abstraction layer across vendors. Apstra provides continuous validation against intent and policy assurance, identifying configuration drift in real time and confirming that security policies are enforced as intended. Once the user commits the changes, the incremental configuration is pushed to the Arista, Cisco, Dell-EMC, or Juniper devices. Apstra is integrated with VMware NSX-T and VMware vCenter to provide network operators visibility into virtual workloads and networks.

Combining Apstra's intent-based networking (IBN) capabilities with Juniper's Contrail Networking allows customers to automate the lifecycle operations of a network overlay fabric. Offering seamless integration with Kubernetes, Mesos, OpenShift, OpenStack, VMware, and popular DevOps tools like Ansible, Contrail Networking provides virtual networking and security for virtualized and containerized cloud-native workloads. Leveraging Juniper or third-party virtualized network functions (VNFs) and physical network functions (PNFs), it dynamically creates highly scalable virtual networks, forming differentiated service chains on demand. In addition, Contrail provides deep insights into application and infrastructure performance for better visualization, diagnostics, reporting, and automation.

issues quickly. In addition, Apstra leverages predictive insights to prevent outages. Apstra accelerates time to resolution with advanced telemetry and mitigates human error with its Intent Time Voyager feature, enabling the operator to move the entire state of the network (intent, configuration, and continuous validations) backward or forward with a few simple clicks, returning it to a specific point in time.

Challenges: Juniper has the products but has yet to clarify its long-term strategy or integrate its offerings into a cohesive automation portfolio that is easy to articulate, deploy, and manage. Moreover, while Juniper has announced plans to support Apstra's multivendor functionality, customers and prospects should be aware that it may leverage the Apstra installed base to expand its footprint by offering a rip-and-replace strategy in favor of Juniper hardware when the network needs to be refreshed.

ManageEngine: Network Configuration Manager

Founded in 2002, ManageEngine develops a broad range of IT management software, with over 120 enterprise products and free tools to help manage all aspects of IT operations, including networks, servers, applications, desktops, mobile devices, service desks, Active Directory, and security. ManageEngine Network Configuration Manager (NCM) is a multivendor network configuration and change management (NCCM) solution for switches, routers, firewalls, and other network devices, enabling network operators to take control and automate the entire life cycle of device configuration management.

NETWORK CONFIGURATION MANAGER AT A GLANCE			GIGAOM
TARGET MARKET			
NETWORK SERVICE PROVIDERS	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
-	X	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	**ON-PREMISES VIRTUAL**	**PRIVATE CLOUD**	**PUBLIC CLOUD**
X	X	X	X
PRIMARY USE CASES			
Identification of faulty configurations		Automated remediation	
Better configuration management		Improved network security	
PRICING MODEL			
1-, 3-, or 5-year device-based perpetual or subscription licensing			
Source: GigaOm 2022			

Figure 11. Network Configuration Manager at a Glance

NCM auto-discovers SNMP-enabled network devices from a wide range of vendors, builds an inventory database, and allows IT administrators to control multivendor device configurations from a central, web-based administrator console. The inventory gives a detailed view into device specifics such as serial numbers, interface details, and port configurations, with trusted configurations labeled as baseline configurations or golden images. In addition, NCM keeps track of all the operations performed in the network and provides detailed operation audit trails reporting on authorized and unauthorized changes.

Device configurations are compared to those of the same devices attached to the network as well as to configurations backed up and stored in the inventory database using text- and model-based configuration validation. NCM compares the configuration file with the recent configuration backup whenever a device backup is triggered. If changes are detected, the configuration is versioned and stored, creating a configuration history that can be used to compare configurations and spot differences. The configuration backup is discarded if there are no changes between the two configuration files. When a violation is detected, NCM's diff view displays color-coded, side-by-side comparisons of the valid and invalid configuration files.

Ensuring Cisco IOS, HIPAA, PCI-DSS, and SOX compliance, NCM audits, monitors, and reports on existing IT infrastructure configurations for compliance based on a defined set of criteria, rules, and standards. Every time a configuration is backed up, NCM automatically runs a compliance check, alerting operators and generating reports whenever a rule or policy is violated. The compliance policies can be associated with devices, automating the compliance check for each configuration change. In addition, users can define their own compliance policies catering to the internal standards of their organizations. Each compliance rule can be associated with a configlet—an executable configuration template—for automated remediation when a compliance violation is detected.

Strengths: ManageEngine Network Configuration Manager offers a simple, comprehensive, and elegant solution for network change and configuration management. It offers multivendor network device configuration, continuous monitoring of configuration changes, notifications of respective changes, detailed operation audits and trails, easy and safe recovery to trusted configurations, automation of configuration tasks, and detailed reporting.

via custom commands and templates. Pre-deployment checks are on the roadmap for delivery within the next three to six months, while end-to-end validation is scheduled for 2025. Implementing automation workflows between different business processes is an ongoing initiative.

Micro Focus: Network Operations Management

Founded in 1976, Micro Focus merged with HPE Software in 2017 to become one of the world's largest enterprise software providers. Network Operations Management (NOM) incorporates functionality from Micro Focus' Network Node Manager i (NNMi) and Network Automation (NA) with additional performance enhancements. Supporting more than 200 vendors and 3,400 devices, NOM integrates a broad set of capabilities with shared context to manage up to 80,000 discovered nodes spanning physical (wired and wireless), virtual, and software-defined networks.

NETWORK OPERATIONS MANAGEMENT AT A GLANCE GIGAOM

TARGET MARKET			
NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
X	X	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	ON-PREMISES VIRTUAL	PRIVATE CLOUD	PUBLIC CLOUD
X	X	X	X
PRIMARY USE CASES			
Improved operational efficiencies		Accelerated deployment	
Reduced operational and regulatory risk		Accelerated SDN, branch, and wireless remediation	
PRICING MODEL			
Tiered 1-, 3-, or 5-year device-based subscription or perpetual licensing			

Source: GigaOm 2022

Figure 12. Network Operations Management at a Glance

Using a patented spiral discovery process, NOM discovers devices, builds the network topology, and uncovers network changes in real time, dynamically adapting the topology model so root cause analysis is always performed against the current network state. To maintain an organization's network compliance policy, NOM monitors physical, virtual, software-defined, and wireless device configurations. It detects any deviation from base configurations and sends intelligent alerts to network operators. NOM identifies the specific change that triggered a violation—for example, a rogue device password change—and can manually or automatically roll back to a compliant configuration. Ongoing Syslog monitoring ensures that any changes to configuration, running state, or operating system are identified in real-time and validated against predefined policies, triggering automated remediation if required. In addition, NOM dashboards provide quick views for executives and department managers to understand the status of their networks.

NOM includes change indicators as part of its network performance monitoring to help identify places where drift creates performance issues, automatically detecting and remediating configuration drift and risk from policy violations. In addition, using a combination of performance monitoring and change automation, NOM can reroute traffic to eliminate bottlenecks, optimizing network behavior. Continuous audits check the network for compliance violations and vulnerabilities, providing real-time visibility to ensure the network state is always transparent across operating teams. NIST common vulnerabilities and exposure (CVE) ranked vulnerability detection and remediation policy content is updated monthly for low or medium severity CVEs and within five days of public notification for high or critical severity CVEs. NOM's security risk dashboards offer a real-time view of the status of an organization's security policies, while NOM's root-cause analysis uses related events, connectivity relationships of the network, and the critical protocol fabric overlays on the network to automatically launch targeted investigations.

Network Operations Management is available in three editions: Express, Premium, and Ultimate. Both Premium and Ultimate include configuration and software automation comprising mass configuration deployments with automated validation of pre-and post-change configuration, running state, or operating system requirements and automated rollback capabilities. In addition, Ultimate provides out-of-the-box orchestration with predefined workflows of automated tasks triggered by network monitoring incidents, compliance violations, or scheduled automation tasks. IT process orchestration authoring allows multiple discrete automated tasks to be defined as part of a repeatable process workflow based on a maintained library of more than 8,000 operations workflows, 300 application components, and 80 integrations.

mapping and change detection provide automated contextual-based troubleshooting, enabling insights-driven automated configuration changes and remediation to ensure ongoing security and compliance. SaaS-based reporting provides flexible metric reporting and interactive troubleshooting, allowing network managers to correlate network performance with broader IT SLAs and overall business goals. In addition, Micro Focus is moving toward a fully containerized architecture to accelerate innovation.

Challenges: While it is possible to use Micro Focus's SOAP API to extract topology data for use in simulation models, NOM does not currently offer simulation capabilities. In addition, the current version of NOM uses legacy technologies and does not monitor overlay networks or provide streaming telemetry (expected in the NOM 2011.11 release) or advanced AI and ML capabilities. Current complexity and usability concerns are being addressed by improving NOM's UI to organize the user experience around common workflows that are intuitive, easy to remember, and efficient.

NetBrain Technologies: NetBrain

Founded in 2004, NetBrain Technologies Inc. offers an adaptive automation platform integrating existing network management system (NMS) tools and IT workflows with patented network intent technologies to align the network with the needs of the business based on its design intents, including the connectivity, performance, and security requirements of specific applications and the network architecture itself. Providing visibility, analytics, and automation across on-premises, software-defined, and public cloud components, NetBrain Problem Diagnosis Automation System (PDAS) creates and maintains a fully functional digital twin in real-time, enabling administrators to visualize and manage their end-to-end digital infrastructure using no-code automation at scale.

NETBRAIN AT A GLANCE — GIGAOM

TARGET MARKET			
NETWORK SERVICE PROVIDERS	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
-	X	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	**ON-PREMISES VIRTUAL**	**PRIVATE CLOUD**	**PUBLIC CLOUD**
X	X	X	-
PRIMARY USE CASES			
Enforcement of security policies and zones		Monitoring critical link failovers	
Maintaining a network-wide QoS policy		Audit network designs, best practices, and rules	
PRICING MODEL			
1-, 3-, or 5-year device-based subscription licensing			

Source: GigaOm 2022

Figure 13. NetBrain at a Glance

NetBrain PDAS no-code technology uses triggered automation, interactive automation, and preventive automation to facilitate Day 2 operational tasks and find all types of network errors, including policy, non-compliance, interface, routing, and path errors, defining the intended baseline and then comparing all subsequent checks against it to identify problems. The core technology behind the platform, NetBrain's Dynamic Map, ingests available data from IT configuration and monitoring tools, unifying data silos into a single contextual view. Once an alert is received, NetBrain's "just in time" automation capability automatically maps around the problematic device and collects diagnostic data. Saving critical time that would otherwise be spent collecting and analyzing data, NetBrain provides network teams with real-time information to resolve the issue via a single map view, including Layer 2 and Layer 3 contextual data from physical and logical topologies and geographically distributed sites.

NetBrain PDAS proactively monitors network behavior and performance based on workload requirements, identifies potential problems, and triggers immediate root cause analysis for faster incident resolution. NetBrain's no-code automation framework enables teams to quickly detect configuration drift, compliance issues, and other conflicts, identifying service delivery problems before they cause outages or service degradation. The no-code technology also allows administrators to automate complex diagnostics designed to ensure that the network operates as intended. In addition, the intent-based automation dashboard provides complete control and visualization of end-to-end network performance, with users able to create, edit, and review automated operational flows for every monitored device without ever leaving the dashboard.

administrators to leverage existing ITSM approval processes as an integrated workflow. NetBrain allows rollbacks of any erroneous change—all at once, device by device, or line by line—to quickly restore a previous configuration. NetBrain also alerts administrators to specific, predefined problems that could cause network degradation or downtime. Any repetitive data collection and analysis task can be automated using a No-Code Runbook or Guidebook (various Runbooks positioned logically in a scenario-driven decision tree based on intents) displayed on the network map.

Strengths: NetBrain's intent-based, automated diagnosis can proactively monitor a complex network and prevent outages caused by human misconfiguration or performance degradation. NetBrain provides a single comprehensive, hierarchical view—with drill-down capabilities to the port level—of digital infrastructure in real time with dynamic network mapping, while runbook automation helps ensure the network meets its design intentions. Positioned as an alternative to AIOps, PDAS automatically captures best practices and updates documentation. When a new network issue is encountered, PDAS attempts to automatically diagnose it based on the PDAS' knowledge base and populate its findings directly into the IT service management ticket, triggering either automated or manual resolution.

Challenges: While NetBrain offers in-depth analysis, diagnostic, and visualization capabilities, it is primarily a scalable automation platform for network problem prevention and remediation. NetBrain provides out-of-the-box support for Cisco (especially IOS and IOS-XE) and VMware environments but lacks broad multivendor support and out-of-the-box integrations with standard tools. In addition, NetBrain relies on third-party tools for deep network fault and performance monitoring and lacks historical data caching and packet-level reporting. The platform imposes a steep learning curve and is resource intensive. Previous user reports indicated that product upgrades sometimes introduced mapping issues, but this has been resolved with the addition of self-updating capabilities.

Northern.tech: CFEngine

Founded in 2017, Northern.tech develops products to help make the connected world a more secure and safer place to live. Northern.tech's portfolio includes Mender, an open-source over-the-air update manager for IoT devices, and CFEngine, a configuration management solution for securely managing IT infrastructure. CFEngine runs on on-premises servers, embedded devices, and in the cloud, ensuring every device on the network is compliant with the organization's desired state and configuration. CFEngine is open-source software with an enterprise edition offering increased platform support and visibility, including change, compliance, and inventory reporting.

CFENGINE AT A GLANCE — GIGAOM

TARGET MARKET			
NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
-	-	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	ON-PREMISES VIRTUAL	PRIVATE CLOUD	PUBLIC CLOUD
X	X	X	X
PRIMARY USE CASES			
Maintaining infrastructure security and compliance		Automating day-to-day network operations	
Enabling scalable configuration management		Self-repairing compliance	
PRICING MODEL			
Free open source for up to 25 hosts or 1-, 3-, or 5-year device-based subscription licensing			

Source: GigaOm 2022

Figure 14. CFEngine at a Glance

CFEngine is a fully distributed system enabling network administrators to define desired states for everything from large-scale infrastructure to small devices. Written in C, CFEngine runs on multiple platforms and architectures—from the smallest embedded devices to cloud infrastructures—scaling to hundreds of thousands of hosts. CFEngine is based on Promise Theory, a concept bridging the worlds of semantics and dynamics to describe interactions between autonomous agencies within a system. Promise Theory provides a semi-formal language for modeling intent and its outcome, enabling cooperative behavior.

Users write CFEngine policies using the CFEngine domain-specific language to define desired states that are stored in one or more central distribution points, referred to as CFEngine policy hubs. Various states can be defined, from process management to software deployment and file integrity. In addition, the state of network devices can be validated pre-change, post-change, or on a regular schedule. Lightweight CFEngine agents continuously run on each

agent downloads the latest policy to its local directory, runs a syntax check, and executes a new configuration check.

All desired-state changes are managed locally by each host and continuously repaired to ensure ongoing compliance with predefined policies. The agent persistently tries to converge towards the defined desired state, creating a log of local inventory, system states, and execution results. CFEngine maintains three states:

- Promise Kept: The actual state was equal to the desired state.
- Promise Repaired: The actual state was not equal to the desired state, but the agent was able to repair the state to ensure compliance.
- Promise not Kept: The actual state was not equal to the desired state, and the agent was not able to restore the state to ensure compliance.

The logs are stored locally—or in a central database for enterprise customers—for integrating with third-party systems to alert operators and trigger manual or automated remediation, if required. Due to the autonomous nature of CFEngine, systems are continuously maintained even if the central CFEngine server is down. Deployed CFEngine agents will opportunistically try to connect to the server. If the connection fails, the last successful policy will apply. Since all evaluations are executed locally, it doesn't matter if the characteristics of the host change or need to be reconfigured. Once the connection is restored, CFEngine will match current policies to ensure compliance during the next run.

Strengths: CFEngine is a flexible configuration management solution for securely managing IT infrastructure using a self-repairing process should anything deviate from policy. CFEngine is based on the concept of a promise or intention to act or behave in a particular manner to generate trust and ensure compliance. Ensuring consistency across different staging environments and automated application deployment, CFEngine is used in heavily regulated industries, including financial services, government agencies, health care, and telecom.

Challenges: While CFEngine is highly customizable, it requires C programming skills, which may not be available in-house. In addition, unlike many other solutions, CFEngine does not make absolute choices. Almost everything about its behavior is a matter of policy that can be changed. As a result, the flexibility and lack of out-of-the-box templates require indepth knowledge of the system and skilled resources for ongoing maintenance to ensure compliance.

SolarWinds: Network Configuration Manager

Founded in 1999, SolarWinds develops solutions for end-to-end hybrid IT management, including network and IT service management, application performance, and managed services. SolarWinds Network Configuration Manager (NCM) helps save time and improve network reliability and security by managing configurations, changes, and compliance for routers, switches, and other network devices. Running on the SolarWinds Platform (providing common alerting, reporting, and management features), NCM offers out-of-the-box support for major network device vendors, including Avaya, Cisco, F5 Networks, HP, Huawei, Juniper Networks, Palo Alto Networks, and Ruckus.

NETWORK CONFIGURATION MANAGER AT A GLANCE			GIGAOM
TARGET MARKET			
NETWORK SERVICE PROVIDERS	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
-	X	X	X
DEPLOYMENT MODEL			
ON-PREMISES SOFTWARE	**ON-PREMISES VIRTUAL**	**PRIVATE CLOUD**	**PUBLIC CLOUD**
X	X	X	X
PRIMARY USE CASES			
Device configuration change management		Real-time change detection	
Configuration change history		Scheduled configuration backups	
PRICING MODEL			
1-, 3-, or 5-year device-based perpetual and subscription licensing			
Source: GigaOm 2022			

Figure 15. Network Configuration Manager at a Glance

to fully integrate with additional network monitoring modules (network performance monitoring, NetFlow traffic analysis, wide-area network (WAN) management, VoIP, device tracking, and IP address management) and systems, storage, and virtualization management, all via a single web console.

Simplifying and standardizing frequent or complex configuration changes, NCM creates a single vendor-neutral script that can be scheduled and executed on routers, switches, and other network devices from supported vendors. NCM enables automated bulk deployment of standardized device configurations, with out-of-compliance configurations detected using config-to-config and baseline-to-config diff views, and visualized using the NCM diff viewer to help quickly identify changes within each configuration. When non-compliance is detected, network operators are alerted to trace the change down to the device level and view what changes were made and by whom. In addition, enabling real-time change detection (RTCD) lets administrators quickly determine, before deployment, whether a configuration change could potentially cause a problem.

Designed to provide real-time and historical insight into whether user activity has led to unauthorized changes or vulnerable configuration gaps, NCM's network audit tools identify unauthorized or inconsistent configuration changes, non-compliant devices, and failed backups. In addition, NCM provides out-of-the-box compliance assessments and reports for critical security standards—including DISA STIG, HIPAA, NIST FISMA, and PCI DSS—with automated remediation scripts to correct violations. NCM also automatically identifies devices with potential vulnerabilities using the NIST CVE repository service and provides the tools to manage the investigation, remediation, or waiver of each vulnerability.

Strengths: SolarWinds Network Configuration Manager helps save time and improve network reliability and security by managing configurations, changes, and compliance for routers, switches, and other network devices from supported vendors. Programmable configuration templates are used to push configurations and validate changes. In addition, NCM audits device configurations to ensure compliance with DISA STIG, HIPAA, NIST FISMA, and PCI DSS. Furthermore, integration with NPM's NetPath feature lets administrators see when a configuration in the network service path has changed.

Challenges: While SolarWinds Network Insight offers deeper visibility into complex devices such as Cisco ASA firewalls, Cisco Nexus switches, and Palo Alto Networks firewalls, NCM uses multiple-device baselines to identify configuration drift, which may not always detect device-specific vulnerabilities. While offering various deployment options, NCM does not offer a distributed edition for remote configuration management and validation.

6. Analyst's Take

As networks increase in complexity, a relatively minor change can significantly impact users' quality of experience (QoE). Network validation helps mitigate the risk by assessing whether the network functions as desired before and after the change. If pre-deployment validation checks don't catch the problem, post-deployment checks should detect an incorrect state, identify the problem, and either remediate the issue or revert to the prior configuration.

However, choosing the right validation solution for the network can be challenging. The solution landscape encompasses both open-source projects and proprietary products. While open-source projects—such as Intentionet's Batfish and Northern.tech's CFEngine—can be customized to support a variety of networks and devices and provide a low-cost entry point, they generally require a specific set of programming skills that may not be available in-house. In addition, the open-source community provides support unless enterprise support is purchased from a third-party vendor.

Furthermore, most network validation tools are currently limited in their ability to discern business intent and convert it into multivendor network designs. Instead, they primarily target the accuracy of golden configurations to eliminate human errors and reduce network downtime. In addition, the learning curve for many network validation tools is steep, requiring specialized skill sets and organizational readiness to embrace new, evolving technologies.

Before choosing a network validation solution, organizations should carefully consider both their short-term validation requirements and their long-term automation strategy. For example, while some solutions support cloud and software-defined, wide area network or software-defined wide-area network (SD-WAN) infrastructures, others support only physical on-premises deployments. In addition, some discover and support overlay networks, while others support only the underlay network.

Shortlist network validation solutions based on the scope of the end-to-end network (on-premises and private, public, hybrid, and multicloud), network equipment vendor support, and existing management ecosystem. Moreover, since implementing an end-to-end network automation strategy takes time, organizations embarking on the journey should consider network validation as low-hanging fruit, using it as an opportunity to identify in-house capabilities and skills gaps within the context of a broader network development operations (NetDevOps) approach.

7. About Ivan McPhee

Ivan McPhee

Formerly an enterprise architect and management consultant focused on accelerating time-to-value by implementing emerging technologies and cost optimization strategies, Ivan has over 20 years' experience working with some of the world's leading Fortune 500 high-tech companies crafting strategy, positioning, messaging, and premium content. His client list includes 3D Systems, Accenture, Aruba, AWS, Bespin Global, Capgemini, CSC, Citrix, DXC Technology, Fujitsu, HP, HPE, Infosys, Innso, Intel, Intelligent Waves, Kalray, Microsoft, Oracle, Palette Software, Red Hat, Region Authority Corp, SafetyCulture, SAP, SentinelOne, SUSE, TE Connectivity, and VMware.

An avid researcher with a wide breadth of international expertise and experience, Ivan works closely with technology startups and enterprises across the world to help transform and position great ideas to drive engagement and increase revenue.

8. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

9. Copyright