Ivan McPhee
Nov 4, 2022 -- Market Radar

GigaOm Radar for NetDevOps v2.0

Table of Contents

1. Summary

NetDevOps is the application of DevOps principles and techniques to network operations (NetOps), minimizing operator interactions and optimizing programmable network processes to configure, deploy, and manage the environment. Prioritizing alignment with business objectives over network control, NetDevOps—also known as DevNetOps, or network automation—relies on automation and intelligent infrastructure management to increase efficiency and ensure network availability, quality, and reliability.

NetDevOps alleviates challenges and increases agility by applying DevOps behaviors, culture, and principles to network operations. It minimizes manual administrative tasks (such as configuration changes, service provisioning, and security tasks), reducing human error as one of the root causes of network downtime. And by automating the planning, configuration, testing, and deployment of network infrastructure, the NetDevOps pipeline reduces the lead time between development and implementation. In addition, it enables small incremental changes to be injected into the network with minimal effort and zero end-user impact, resulting in increased agility, quality, and speed of operations.

This report provides an overview of the NetDevOps landscape based on the following table stakes, which are mature, stable solution features common across all NetDevOps solutions:

services using tools familiar to application developers—such as Bitbucket, Docker, GitLab, GitHub, and Jenkins—on an as-needed basis.

- **Automated workflows:** Automated workflows provide complete lifecycle management functionality to configure, deploy, and upgrade network elements seamlessly. A collection of carefully orchestrated building blocks, automated workflows split higher-level activities into subtasks linked to network events, triggering proactive or reactive actions encompassing inventory checks, pre-checks, post-checks, show-commands, user approvals, scheduled background tasks, and other tasks.
- **State awareness:** The state of the network is monitored in real time with full protocol and transport neutrality. Awareness of automated network infrastructure deployments and implementations is required to ensure the desired network state is achieved and maintained. State awareness enables the continuous synchronization of the network state and configuration in real time using open, state-streaming APIs. It also provides advanced artificial intelligence (AI) and machine learning (ML) analytics capabilities for visibility, troubleshooting, and compliance.
- **Infrastructure as code (IaC):** Network configurations are abstracted as code for replication, reuse, repurposing, or testing, providing optimal resource usage. In conjunction with continuous delivery, IaC manages infrastructure (connection topologies, load balancers, networks, and virtual machines) in a descriptive model to reduce environment drift by eliminating inconsistencies leading to deployment issues requiring manual resolution. Furthermore, based on the principle of idempotence, IaC ensures you always end up with the same end state irrespective of the starting state.
- **Policy creation:** Vendor-agnostic automation policies are created by transforming the intent—as described in the automation models—into device-specific configurations and commands at runtime. Policy creation eliminates the challenge of first rolling out configurations and then maintaining and enforcing them at scale. In addition, a flexible, model-driven approach enables administrators to maintain compliance based on the desired state or roll out a specific configuration for deployment across network devices.
- **On-demand elasticity:** On-demand elasticity is the ability to spin up and down test, development, and sandbox infrastructure environments on demand without jeopardizing compliance, governance, performance, security, or stability. Unlike scalability, which refers to adding resources to accommodate larger loads, elasticity enables network resources to be added or removed dynamically based on changing application traffic patterns, such as seasonal or peak traffic surges.
- **Self-service access:** Robust, role-based self-service access to network infrastructures—such as dynamic host configuration protocol (DHCP), domain name system (DNS), firewalls, load balancers, and other network services—allows development teams to consume networking services easily and quickly. Eliminating network team provisioning and configuration bottlenecks, self-service access enables application delivery teams to initiate the automated deployment and configuration of network services while ensuring compliance.

The list of vendors included in this report is by no means exhaustive. As a new sector evolving to meet the demands of agile networking, we anticipate rapid evolution in the next 18 to 36 months. New players will emerge with lean, innovative solutions, while established networking vendors will compete by acquiring solution vendors and expanding critical partnerships. With so many different NetDevOps solutions and the landscape evolving, choosing the best option for your organization depends on your use cases, existing software stack, architectural choices, and in-house capabilities.

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

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical 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.

2. Target Markets and Deployment Models

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

For the NetDevOps sector, we recognize five target markets:

- **Cloud service provider (CSP):** Providers delivering on-demand, pay-per-use cloud-based infrastructure or storage services over the internet, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).
- **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.

- **Large enterprise:** 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 (<100 employees) to medium-sized (100-1,000 employees) businesses 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 NetDevOps sector, we recognize private cloud, public cloud, hybrid cloud, and multicloud deployment models:

- **Private cloud:** Used exclusively by one enterprise or organization, cloud computing resources are physically located in an on-premises data center or hosted by a third-party colocation service provider. Tailored to meet specific requirements, private clouds offer compliance, control, and flexibility. The NetDevOps solution is typically deployed on physical or virtual servers with configuration data stored in either an embedded or external database.
- **Public cloud:** Owned and operated by a third-party cloud service provider and delivered over the internet, public cloud providers provide cost-effective, scalable, and reliable on-demand resources for enterprises and SaaS vendors. The NetDevOps solution is deployed on Amazon Web Services (AWS), Microsoft Azure, Google Cloud, or other public cloud infrastructures as virtual machines (VMs), containers, or microservices with configuration data stored in either an embedded or externally hosted database.
- **Hybrid cloud:** Enabling data and apps to move seamlessly between environments, a hybrid cloud combines private, on-premises infrastructure with a public cloud. Hybrid cloud allows compute to be brought closer to the edge where data resides—reducing latency and increasing reliability—while still meeting regulatory compliance and data sovereignty requirements. The NetDevOps solution is deployed as VMs, containers, or microservices in a distributed architecture spanning private and public clouds.
- **Multicloud:** Comprising multiple public cloud services performing different functions, multicloud allows enterprises and organizations to take advantage of various public cloud capabilities or geographies. Multicloud deployments may include private clouds, resulting in cloud deployment that is both hybrid and multicloud. The NetDevOps solution is deployed as VMs, containers, or microservices in a distributed architecture spanning multiple public clouds, including AWS, Azure, Google Cloud, or other public cloud infrastructures.

Table 1. Vendor Positioning for Target Markets

	MARKET SEGMENT					DEPLOYMENT MODEL			
	CSP	NSP	MSP	Large Enterprise	SMB	Private Cloud	Public Cloud	Hybrid Cloud	Multicloud
Anuta Networks	–	+++	+++	+++	++	++	++	++	++
Blue Planet	–	+++	++	+++	–	++	+++	–	++
Elisa Polystar	–	+++	++	++	++	+++	++	++	++
Gluware	–	–	++	+++	++	+++	++	++	++
HashiCorp	–	–	–	+++	++	++	++	++	+++
Itential	++	+++	++	+++	–	+++	++	++	++
Juniper Networks	++	+++	++	+++	–	++	++	++	++
Micro Focus	++	++	++	+++	++	++	++	++	–
NetBrain Technologies	–	–	+++	+++	–	++	–	–	–
Resolve Systems	–	++	++	+++	++	++	++	++	++

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

Following the general criteria introduced in GigaOm's "Key Criteria for Evaluating a NetDevOps Solution," **Tables 2, 3,** and **4** 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 NetDevOps solution, including network resilience, OS management, and robotic process automation (RPA).
- **Evaluation metrics** provide insight into the *impact of each product's features and capabilities on the organization*, reflecting fundamental aspects, including ecosystem support, integrated security, and openness.

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 Discovery	Network Simulation	Configuration Validation	Monitoring & Telemetry	Software Management	AIOps Enablement	Network Resilience	Topology Visualization	Robotic Process Automation
Anuta Networks	+++	++	+++	+++	+++	+	+++	++	+++
Blue Planet	+++	+++	+++	++	+++	++	+++	+++	–
Elisa Polystar	++	–	+++	++	+++	+++	++	++	+++
Gluware	+++	+	+++	++	+++	+	+++	+++	+++
HashiCorp	+++	–	++	++	++	++	++	–	+++
Itential	+++	–	+++	–	+++	–	+++	–	+++
Juniper Networks	++	++	++	+++	++	+++	+++	+++	++
Micro Focus	+++	+	+++	++	+++	–	++	++	–
NetBrain Technologies	++	+++	+++	++	++	+	++	+++	++
Resolve Systems	+++	–	++	–	++	+	+++	++	++

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							
	Infrastructure Support	Ecosystem Support	Openness	Resource Consumption	Integrated Security	Vendor Support	Pricing & TCO	Vision & Roadmap
Anuta Networks	+++	+++	++	+++	++	+++	++	+++
Blue Planet	+++	++	++	+++	++	+++	++	+++
Elisa Polystar	+++	++	+++	++	++	++	+++	+++
Gluware	+++	+++	+++	++	++	+++	+++	+++
HashiCorp	++	++	+++	+++	+	++	+++	++
Itential	+++	+++	+++	+++	++	+++	++	+++
Juniper Networks	++	+++	++	++	++	+++	+	++
Micro Focus	+++	++	++	+++	+++	+++	++	+
NetBrain Technologies	++	++	+++	++	++	++	+	+++
Resolve Systems	+++	+++	++	++	++	++	++	+++

Source: GigaOm 2022

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases

Table 4. Emerging Technologies and Trends

	EMERGING TECH	
	Private 5G & Internet of Things	Edge Cloud & Multicloud
Anuta Networks	+++	+++
Blue Planet	+++	++
Elisa Polystar	+++	+++
Gluware	++	+++
HashiCorp	–	++
Itential	+++	+++
Juniper Networks	+++	++
Micro Focus	++	++
NetBrain Technologies	–	–
Resolve Systems	–	++

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.

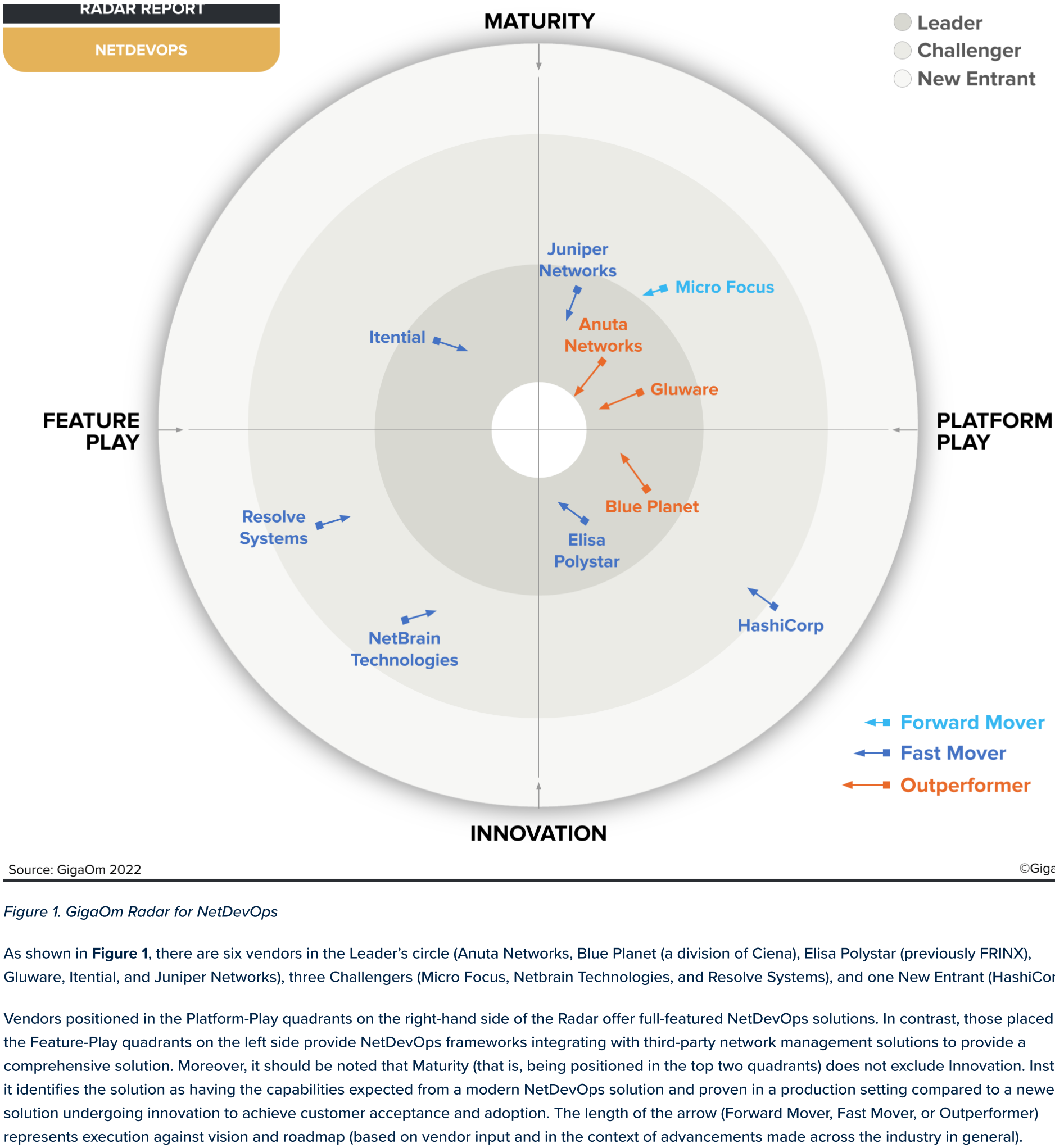

Figure 1. GigaOm Radar for NetDevOps

As shown in **Figure 1**, there are six vendors in the Leader's circle (Anuta Networks, Blue Planet (a division of Ciena), Elisa Polystar (previously FRINX), Gluware, Itential, and Juniper Networks), three Challengers (Micro Focus, Netbrain Technologies, and Resolve Systems), and one New Entrant (HashiCorp).

Vendors positioned in the Platform-Play quadrants on the right-hand side of the Radar offer full-featured NetDevOps solutions. In contrast, those placed in the Feature-Play quadrants on the left side provide NetDevOps frameworks integrating with third-party network management solutions 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 from a modern NetDevOps 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).

While all ten vendors offer robust network discovery, diagnostic, and performance monitoring capabilities, each provides varying degrees of automation, integration, and multivendor support. For example, some offer event-driven automation to accelerate issue resolution, while others offer automated application performance optimization. Some also use advanced AI and ML capabilities for predictive remediation, while others provide automated reactive remediation. In addition, FRINX and HashiCorp are the only vendors that use open-source components, making FRINX Machine and Consul-Terraform-Sync affordable solutions for SMBs.

The leaders in this space—Anuta Networks and Gluware—offer multivendor support with microservices architectures built from the ground up. Anuta ATOM's web-scale approach allows customers to start small and scale on demand to thousands of devices, while Gluware's customer-driven roadmap enables complex enterprise use cases incorporating robotic process automation, self-operating functionality, and topology visualization. Furthermore, it's noteworthy that four vendors in the leader's ring (Anuta Networks, FRINX, Gluware, and Itential) offer no-code/low-code solutions for increased agility and automation. In addition, Anuta Networks, Blue Planet, Gluware, Itential, and Juniper have SaaS offerings, with Blue Planet Enterprise (BPE) Automation Suite available only as a SaaS offering.

New additions to the list of NetDevOps vendors for the 2023 GigaOm Radar for NetDevOps are HashiCorp and Resolve Systems, while Infovista has changed its focus from network automation to network assurance and has been removed. Moreover, since publishing the 2021 GigaOm Radar for NetDevOps, FRINX and Itential have moved from being Challengers to Leaders due to their rapid innovation, while Anuta Networks and Blue Planet have moved from being Fast Movers to Outperformers due to successful execution against their roadmaps.

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 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 built with the latest technologies, Anuta ATOM is a complete 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 compliance, configuration management, network monitoring and alerting, zero-touch provisioning, and software upgrades, ATOM supports over 150 physical and virtual platforms from more than 45 vendors.

ANUTA ATOM AT A GLANCE — GIGAOM

TARGET MARKET				
CLOUD SERVICE PROVIDERS	NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
-	X	X	X	X

DEPLOYMENT MODEL			
PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD	MULTICLOUD
X	X	X	X

PRIMARY USE CASES	
Device/service lifecycle management and FCAPS	Any method-of-procedure (MOP) automation
Custom service orchestration and automation	Assurance and closed-loop automation

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 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.

Periodically archiving and versioning device configurations, ATOM detects out-of-band changes, notifying administrators and rectifying violations upon approval. Network compliance with CIS, HIPAA, NIST, PCI, SOX or other policies is designed to defend against security threats and prevent costly data breaches. In addition, ATOM's compliance policy builder enables administrators to define and standardize configurations, with any non-compliance of

configuration lines of code impacting over 10,000 devices.

ATOM provides more than 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, the solution allows workflow execution to be carefully controlled while the entire network is monitored via SNMP, SNMP Trap, Syslog, and streaming telemetry mechanisms with comprehensive alert routing and suppression.

The solution supports multiple domains—such as cable networks, core, edge, and WAN—from all major vendors, including Arista, Cisco, F5, and Juniper, and offers seamless integration with CI/CD tools—either as an initiator or as part of the pipeline—such as Gitlab and Jenkins for releasing a constant flow of updates to speed up release cycles, lower costs, and reduce development risks. ATOM workflow automation includes pre-checks, post-checks, multilevel approvals, integration with public clouds, IP address management (IPAM) and IT service management (ITSM) tools, ticketing, billing, and other solutions. In addition, ATOM's extensible framework enables new vendors to be supported within two to six weeks.

Anuta Networks' SaaS platform, ATOM Cloud, delivers all of the capabilities of Anuta ATOM in a pay-as-you-go subscription model in three license tiers: ATOM Cloud Essentials, ATOM Cloud Professional, and ATOM Cloud Enterprise. A cloud-hosted network orchestration and service assurance solution, ATOM Cloud automates the design, development, and deployment of networks, including devices, services, and operational workflows. It offers complete network lifecycle automation for multivendor and multidomain networks, delivering stateless workflow automation, stateful service provisioning, and closed-loop automation. Built on AWS infrastructure, ATOM Cloud offers high availability, massive scalability, reliability, geographical presence, security, and OpEx savings.

Strengths: ATOM is an extensible, feature-rich, and scalable integrated platform offering customers comprehensive support for out-of-the-box, standard-based service lifecycle management and service orchestration use cases. Simplifying the design of self-service workflows with low-code automation and an interactive GUI, ATOM Workflow builder allows customers to create complex and straightforward flows with simple drag-and-drop functionality. In addition, it includes the capability to evaluate existing data and crowd-sourced analytics to automate policy generation for network performance, availability, and SLA conformance using AI/ML prioritized on the roadmap.

Challenges: 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.

Blue Planet (Ciena): BPE Automation Suite

Acquired by Ciena in 2015 and spun off as an independent division in 2019, Blue Planet provides market-leading intelligent automation software and specialized professional services to help clients—primarily telecom customers—modernize their IT and network operations. Launched in July 2021 to simplify multivendor enterprise network operations, the SaaS-based Blue Planet Enterprise (BPE) Automation Suite combines fault and performance monitoring with AI-driven capabilities to enhance network visibility and control.

TARGET MARKET				
CLOUD SERVICE PROVIDERS	NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
-	X	X	X	-
DEPLOYMENT MODEL				
PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD	MULTICLOUD	
X	X	-	X	
PRIMARY USE CASES				
Outcome-focused network automation		Proactive network operations		
BGP/IGP routing and performance analysis		Complex IP/MPLS network planning		
PRICING MODEL				
1-, 2-, or 3-year subscription pricing based on the number of devices under management				
Source: GigaOm 2022				

Figure 3. BPE Automation Suite at a Glance

Addressing the automated network configuration management and monitoring needs of large enterprises, BPE Automation Suite currently consists of three products running on AWS: Dynamic Configuration and Change Management (DCCM), Intelligent NetOps (INO), and Route Optimization and Analysis (ROA). DCCM provides automated configuration lifecycle management and compliance control for enterprise network devices; INO delivers AI-based intelligent performance monitoring and ML-based fault detection for enterprise network infrastructure; and ROA provides performance, routing, and traffic analysis and automation for IP/MPLS networks.

DCCM natively supports intent-based no-code/low-code Ansible and YAML template construction to interact with network devices via CLI commands. Hundreds of templates provide out-of-the-box functionality for various use cases. The integrity of software images is validated using cryptographic hashes. A network administrator must review configuration changes, firmware upgrade requests, and compliance policies before applying them as one-to-many and many-to-many bulk updates. In addition, all configuration changes and software upgrades are logged and can be audited. The platform includes an out-of-the-box Integration Hub supporting seamless integration with ServiceNow and other ticketing platforms for change requests and problem management. End users are notified of significant network events via integrations with Okta, OpsGenie, Slack, SNOW, Teams, and other solutions commonly used by IT operations.

INO incorporates ML to identify network-related issues, which are remediated using DCCM, eliminating the need to define monitoring rules manually and providing end-to-end, closed-loop network lifecycle automation capabilities. Using a variety of protocols—including NETCONF, REST APIs, SNMP, and Syslog—critical telemetry from network devices is ingested, correlated, and analyzed using proprietary AI-based models for actionable recommendations and user-controlled remediation steps. All AI models are based on the Open Neural Network Exchange (ONNX) standard supported by most AI frameworks, including MATLAB, MXNet, and TensorFlow.

Simplifying complex IP/MPLS network planning by providing real-time visibility into IP/MPLS topology and Layer 2/Layer 3 routing, ROA correlates IGP/BGP routing, performance, and traffic data to analyze the way routing changes impact network and service delivery. ROA includes historical analyses of IP routing issues by capturing and storing routing events and path changes and what-if analyses to simulate the impact of network architecture or traffic changes.

The BPE Automation Suite supports RBAC, integrating with third-party identity and access management (IAM) platforms to simplify the management of user credentials and provide added security mechanisms, including multifactor authorization. In addition, data is encrypted at rest and in transit, with SSL certificates used to secure the connection between the agent on-premises and the software in the cloud.

Supporting network devices from leading network equipment providers, including Aruba, Ciena, Cisco, Fortinet, Juniper, Palo Alto Networks, and VeloCloud, BPE Automation Suite is deployed on AWS infrastructure on a Kubernetes cluster distributed across multiple availability zones, providing high performance, reliability, and high availability. In addition, a microservice is deployed at the customer site to provide network data capture and storage continuity in the event of connectivity loss between the managed devices and the public cloud.

Supported by an ecosystem of system integrator and service provider partners, the products within the BPE Automation Suite may be deployed together, independently, or as part of a partner-delivered managed service offering alongside other Blue Planet products. However, combining DCCM and INO provides the best results with end-to-end closed-loop network lifecycle automation capabilities via a unified UI.

these containers to create and enable SDN management and control, NFV orchestration, and multidomain service orchestration. Moreover, despite being a division of Ciena, Blue Planet supports non-Ciena access, metro, core, and cloud domains, enabling enterprises and service providers to select and deploy best-of-breed platforms while delivering end-to-end service orchestration.

Challenges: While it can be extended easily to other public clouds, BPE Automation Suite currently runs only on AWS and lacks multitenancy support and intent-based security management. Moreover, though Blue Planet's roadmap includes plans to incorporate DCCM and INO multitenancy, support for zero trust networks (ZTNs), and out-of-the-box compliance assessment policy packages, potential customers requiring these capabilities should confirm delivery dates before committing. In addition, APIs supporting a range of third-party ITSM solutions and operations management platforms may be included on the roadmap but are not yet available in BPE's built-in Integration Hub.

Elisa Polystar: FRINX Machine

Founded in 2016 and acquired by Elisa Polystar in 2022, FRINX Machine leverages open-source projects—including Docker, Kubernetes, and the Netflix Conductor workflow engine—to enable network service automation solutions for customers, creating automated and repeatable digital processes to build, grow, and operate their digital infrastructure. The company's software enables low-code workflow design and operation, analytics to support machine learning, and intent-based infrastructure control to integrate devices and services across multivendor backbone, fixed-access, and transport networks. The acquisition of FRINX products and software complements Elisa Polystar's AI/ML-enabled zero-touch analytics and automation portfolio, helping network service providers automate their network management processes in a multivendor telecom network environment.

FRINX MACHINE AT A GLANCE — GIGAOM

TARGET MARKET				
CLOUD SERVICE PROVIDERS	**NETWORK SERVICE PROVIDERS**	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
-	X	X	X	X

DEPLOYMENT MODEL			
PRIVATE CLOUD	**PUBLIC CLOUD**	**HYBRID CLOUD**	**MULTICLOUD**
X	X	X	X

PRIMARY USE CASES	
Automating services using hybrid resources	Automating capacity increases in mobile networks
Automating core network functions	Managing internet and infrastructure services

PRICING MODEL

Perpetual or 1-, 2-, or 3-year subscription licensing pricing based on the number of devices under management

Source: GigaOm 2022

Figure 4. FRINX Machine at a Glance

Capturing intent, mapping current and future states, implementing configuration changes, and obtaining operational data from the network, FRINX Machine translates the network topology into version-controlled code with complete snapshot, commit, and rollback capabilities. Simplifying the definition, execution, monitoring, and operation of complex workflows, FRINX Machine comprises FRINX UniConfig for physical and virtual network configuration management, FRINX Workflow Manager for orchestrating microservices and managing events and workflows, and FRINX Resource Manager for real-time network inventory, resource management, and topology visualization. FRINX Machine comes out of the box with a library of prepackaged service workflows and device drivers, enabling the orchestration of heterogeneous networks with multiple tasks merged into a single workflow.

Used as a standalone solution or as a part of FRINX Machine, UniConfig runs on open-source OpenDaylight, a modular open platform for customizing and automating networks of any size and scale. FRINX UniConfig uses a layered design, with each layer providing a higher level of abstraction from the underlying network elements. Two separate data stores store the actual and intended state of the network—described by YANG models—with applications able to read any information and use any layer within the system. In addition, UniConfig leverages an open-source device library supporting connectivity to hundreds of networking devices and virtual network functions (VNFs).

Configuring network devices and automating network services, FRINX Workflow Manager consists of a workflow engine, a GUI-based workflow builder for low-code or no-code workflow design and operation, a microservices layer preloaded with essential automation functions, and a service portal with RBAC for users and APIs to interact with workflows. In addition, Workflow Manager leverages a horizontally scalable, common persistence layer supporting a wide

capabilities.

FRINX Machine provides real-time network inventory and resource management, including network and service topologies. Providing a robust GUI and a GraphQL-based API with a Python client library to create, read, update, and delete assets, FRINX Resource Manager was developed as a single source of truth for network and infrastructure engineers working with communication networks to manage their physical and logical assets and resources.

A partner of the Telecom Infra Project (TIP) Open Automation Solution Project Group (OA-SPG), FRINX is participating in the initiative to create composable "building blocks" supporting service lifecycle automation for orchestrating services deployed across end-to-end, service provider multidomain networks. In addition to supporting industry leaders like Facebook Connectivity, SoftBank, Telefonica O2, and VodafoneZiggo, FRINX offers turnkey design, implementation, deployment, and operations via a growing solution practice.

Strengths: FRINX's multivendor support and unique approach to NetDevOps leveraging open-source components offer a robust solution for a broad range of customers. Leveraging ML algorithms to trigger workflow execution, FRINX Machine provides closed-loop automation for large-scale communication service provider networks. The GUI-based workflow builder and a broad selection of out-of-the-box microservices in Python allow users to create services in their chosen programming language for greater flexibility and adoption. In addition, FRINX's acquisition by Elisa Polystar and its partnerships and installed base assure users of ongoing innovation and support.

Challenges: FRINX primarily focuses on transport network orchestration and automation with FRINX Machine designed to automate the discovery and configuration of network services and devices. As a result, it lacks advanced features such as network simulation. While FRINX is currently being integrated with other Elisa Polystar products—including Virtual NOC—to provide advanced AI/ML capabilities, a fully integrated solution will only become generally available in the next six to nine months. Moreover, since FRINX leverages open-source technologies, the company relies on the open-source community, which may affect innovation, refresh cycles, and support. Finally, enterprises should be aware that FRINX's vision and roadmap are primarily targeted at meeting the needs of NSPs.

Gluware: Gluware Intelligent Network Automation

Entering stealth in 2007 and launched in 2011, Gluware provides a suite of intent-based, idempotent network automation solutions with closed-loop verification, enabling extensible, scalable, and secure multivendor, multidomain, and multicloud networks. Supporting over 40 network operating systems and cloud platforms—including AWS, Azure, and Google Cloud—Gluware's modular, microservices-based NetDevOps solution includes intelligence for each vendor platform with continuous discovery and out-of-the-box network monitoring and management. Gluware's Network Robotic Process Automation (Network RPA) provides the ability to create, manage, and monitor no-code process automation, integrating with StackStorm to provide over 167 external installable integrations. In addition, in October 2022, Gluware introduced Gluware Service Connectors—Gluware-provided and supported management-plane integrations—beginning with EfficientIP and ServiceNow.

GLUWARE INTELLIGENT NETWORK AUTOMATION AT A GLANCE GIGAOM

TARGET MARKET				
CLOUD SERVICE PROVIDERS	NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
-	-	X	X	X

DEPLOYMENT MODEL			
PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD	MULTICLOUD
X	X	X	X

PRIMARY USE CASES	
Network inventory and assessment	Automated network lifecycle management
Network configuration and security audits	Network configuration drift monitoring

PRICING MODEL
Free or 1-, 3-, or 5-year subscription pricing based on the number of devices under management

Source: GigaOm 2022

Figure 5. Gluware Intelligent Network Automation at a Glance

Gluware's Intelligent Network Automation platform comprises Gluware Control and a suite of intent-based applications, including Config Drift and Audit, Config Modeling, Dashboard, Data Explorer, Network RPA, OS Manager, Topology, and Workflows. These integrated components provision inventory, drift, audit, and configuration management tasks via SSH to enterprise network devices and via REST to network controllers.

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.

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. Automated line-by-line comparisons detect changes, triggering device remediation or promoting the snapshot to the current default.

The new Gluware Topology module offers increased network visibility leveraging the data collected during network discovery and ongoing detailed device discovery. Gluware Topology maintains network documentation and export diagrams in standard formats, including Microsoft Visio, to meet compliance and regulatory requirements. In addition to providing off-the-shelf applications, Gluware Lab accelerates deployment by eliminating the need for network teams to build their own automation. A self-contained CI/CD ecosystem deployed on-premises, Gluware Lab enables customers to develop their own features, networking packages, and workflows on top of the Gluware platform for on-premises or cloud-based deployments.

Hosted on-premises or in the cloud, Gluware Enterprise offers flexibility and scalability to address the needs of larger enterprises or those requiring special sizing. It can scale to any size network, and customers can select which components of the Gluware Application Suite they want to deploy. Incorporating Gluware Zone Engine Servers, Gluware Enterprise enables provisioning power to be distributed to geographical regions, edge locations, or data centers with a cluster of network devices.

In addition to offering Gluware Enterprise as a privately hosted SaaS, Gluware's full SaaS offering leverages traditional network access, enabling a full-scale, cloud-based deployment similar to the on-premises privately hosted SaaS. In addition, Gluware Pro targets smaller managed deployments inside protected environments using the Gluware Secure Gateway (GSG) virtual appliance. Designed for networks of up to 2,000 devices, a single GSG provides dual provisioning engines with Gluware Pro supporting the deployment of two GSGs on each customer network for redundancy.

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 does not include analytics, SNMP monitoring, or service assurance, though it integrates programmatically with third-party platforms to provide those features. Currently lacking AI/ML predictive analytics and automation capabilities, Gluware is an event-driven platform supporting external triggers via Syslog or API integration. Gluware uses optional agents to collect information and feedback from network devices. Prospective clients should be aware that Gluware Pro lacks the scalability of the on-premises or privately hosted Gluware Enterprise versions.

HashiCorp: Consul-Terraform-Sync

Founded in 2012, HashiCorp leverages open-source projects to develop multicloud infrastructure automation products. In 2016, HashiCorp started offering both open-source and commercial versions of its tools, including Consul (service mesh), Nomad (orchestration), Terraform (infrastructure as code), and Vault (security). HashiCorp also maintains open-source projects for HashiCorp Boundary (identity-based user access), Packer (golden image creation), Vagrant (configuration workflow management), and Waypoint (application lifecycle management). Released in March 2021 as part of its Network Infrastructure Automation (NIA) initiative, HashiCorp's Consul-Terraform-Sync (CTS) combines Consul's service networking capabilities with the power of Terraform's provider ecosystem, allowing enterprises to manage their entire network infrastructure by automating workflows and implementing repeatable deployment lifecycles.

TARGET MARKET				
CLOUD SERVICE PROVIDERS	NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
-	-	-	X	X
DEPLOYMENT MODEL				
PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD	MULTICLOUD	
X	X	X	X	
PRIMARY USE CASES				
Self-service enablement		Accelerate configuration changes		
Eliminate human configuration errors		Simplified auditing		
PRICING MODEL				
Free download from GitHub with optional enterprise support available from HashiCorp				
Source: GigaOm 2022				

Figure 6. Consul-Terraform-Sync at a Glance

Running in near real time, CTS leverages the power of Terraform's provider ecosystem and Consul's service networking capabilities to implement a declarative-, workflow-, and service-driven network automation architecture spanning multiple platforms. Containing up-to-date infrastructure and services state information based on continuous monitoring, CTS relies on Consul's service catalog as the network source of truth (NSoT). Triggered by a change in a service's state or health, CTS leverages Terraform as the underlying automation tool and the Terraform provider ecosystem to drive relevant changes to the network infrastructure.

HashiCorp Consul is a service networking solution enabling teams to manage secure network connectivity between services spanning on-premises and multicloud environments and runtimes. Implemented individually or together in a single deployment, Consul includes service discovery, service mesh, traffic management, and automated updates to network infrastructure devices. Using a shared registry—updated in real time—to create a real-time directory of all services, including health status, Consul enables network middleware automation with service discovery for dynamic reconfiguration throughout the services lifecycle.

Supporting a robust ecosystem, HashiCorp Terraform provides IaC workflows for provisioning, compliance, and management across any public cloud, private data center, or third-party service. Enabling organizations to build, change, and version infrastructure safely and efficiently—including both low-level components (compute instances, storage, and networking) and high-level components (such as DNS entries and SaaS features)—Terraform offers a familiar, IaC approach to multicloud network provisioning, compliance, and management via a single workflow.

Leveraging the capabilities of Consul and Terraform, CTS executes one or more automation tasks based on updates from the Consul service catalog for managing network infrastructure in near real time. CTS runs as a daemon and integrates the network topology maintained by a Consul cluster with the network infrastructure to dynamically secure and connect services. Each task consists of a runbook automation written as a compatible Terraform module using resources and data sources for the underlying network infrastructure through ecosystem integrations.

Incorporating high availability and redundancy capabilities, CTS runs on a serverless Consul cloud deployment on AWS Amazon Elastic Compute Cloud (EC2), AWS Elastic Kubernetes Service (EKS), or Hashicorp Cloud Platform (HCP), or as a self-managed Consul Kubernetes deployment on either AWS EC2 or EKS. In addition, HashiCorp's NIA Integration Program allows partners to build integrations to automate dynamic application workflows using third-party network and security infrastructure at runtime. Current partners include A10 Networks, AWS, Check Point, Cisco, Citrix, F5, NS1, Palo Alto Networks, and VMware.

Strengths: CTS combines the functionality of HashiCorp Consul and HashiCorp Terraform to bring infrastructure as code to core networking, streamlining application deployments where physical devices are involved. Used for Day 0, 1, and 2 operations, administrators can use Terraform to deploy network devices and infrastructure quickly and consistently in a controlled manner and then integrate Consul's catalog to register services into the system via CTS. Whenever a change is recorded in the service catalog, CTS triggers a Terraform task using partner ecosystem integrations to automate Day 2 updates and deployments for load balancers, firewall policies, and other service-defined networking components.

Challenges: As a lightweight agent-based, event-driven solution, CTS lacks the proactive capabilities of advanced NetDevOps tools with predictive AI/ML analytics capabilities. In addition, CTS currently lacks built-in drag-and-drop, observability, and topology visualization capabilities, relying on third-party vendors to fill functional gaps. However, as CTS is the primary tool supporting HashiCorp's NIA initiative, we expect HashiCorp to regularly roll out new functions and features (version 0.7 was released in September 2022).

Founded in 2014, Itential is a multidomain network automation and orchestration 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 NetDevOps engineers to extend the reach of their pipelines across disparate network technologies and domains.

ITENTIAL AUTOMATION PLATFORM AT A GLANCE				GIGAOM
TARGET MARKET				
CLOUD SERVICE PROVIDERS	**NETWORK SERVICE PROVIDERS**	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
-	X	X	X	X
DEPLOYMENT MODEL				
PRIVATE CLOUD	**PUBLIC CLOUD**	**HYBRID CLOUD**	**MULTICLOUD**	
X	X	X	-	
PRIMARY USE CASES				
4G/5G and IP core automation and orchestration		SD-WAN and backhaul orchestration		
Private/public hybrid cloud automation		Branch office activation and lifecycle automation		
PRICING MODEL				
1- or 3-year on-premises or SaaS subscription licensing based on devices under management				
Source: GigaOm 2022				

Figure 7. 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 integrate instantly 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. Network provisioning requests are sent to Itential to determine which components are affected, triggering automated actions to process the request using the relevant tools.

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, IAP 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.

Providing robust CLI and script-based technology support, IAG is a standalone application enabling users to onboard existing NetDevOps assets and incorporate them into more complex workflows and orchestration activities. IAG provides an API layer for integration with Ansible, NetMiko, Nornir, Python, and Terraform, and IT systems such as Jira, Remedy, and ServiceNow, supporting many use cases spanning network and IT operations. In addition, IAG supports OpenAPI and uses popular modeling languages such as TOSCA, YAML, and YANG.

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 with tasks requiring manual intervention, including controlling when, how, and with what data a workflow should run.

The platform includes IAS for defining workflows—including branching logic, pre-and post-configuration validation, and exception handling—using a GUI-driven, drag-and-drop no-code canvas. Moreover, with over 200 adapters and more than 26,000 API calls for common workflows available out of the box, IAP automatically generates objects related to third-party systems when integrated, presenting those objects for end-to-end network configuration, compliance, and automation. In addition, the Itential Adapter Builder allows customers to auto-generate their own adapters supporting specific use cases, simplifying integration, and mitigating vendor lock-in.

system models upon which it acts, IAP federates data and logic and models workflows independently of underlying network products, providing an open, modular architecture incorporating existing management platforms and tools. In addition, Itential's SaaS platform allows organizations to evaluate IAP in a complete, feature-rich cloud environment, with training courses designed to accelerate onboarding and time to value.

Challenges: Designed for enterprises and wireless network service providers who have already embarked on their automation journey, Itential's solution lacks its own domain-specific network modeling system and monitoring, simulation, telemetry, and visualization capabilities, relying on integration with best-of-breed 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.

Juniper Networks: Juniper Automation

Founded in 1996, Juniper is an industry leader in networking and has aggressively acquired several companies to fill out its AI-driven automation portfolio. Recent acquisitions include 128 Technology (session-smart networking), Apstra (intent-based networking and automated closed-loop assurance), and Mist (AI-enabled campus and branch solutions). Intending to leverage AI to change the way networks are built, operated, and secured in the cloud era, Juniper currently segments its automation offerings into three categories: client-to-cloud (Juniper Mist), data center (Juniper Apstra System and Juniper Contrail Networking), and WAN (Juniper Paragon Automation). In addition, Juniper Networks resells Anuta ATOM to extend visibility into applications and services running on multivendor infrastructure, ensuring service assurance and SLA compliance for the end-to-end network.

JUNIPER AUTOMATION AT A GLANCE — GIGAOM

TARGET MARKET				
CLOUD SERVICE PROVIDERS	NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
X	X	X	X	-

DEPLOYMENT MODEL			
PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD	MULTICLOUD
X	X	X	X

PRIMARY USE CASES	
Deploy private, public, or hybrid clouds	Automate NFV through service chaining
Zero-touch provisioning	Automate Day 0, 1, 2+ network lifecycle operations

PRICING MODEL
1-, 2-, or 3-year subscription pricing based on the number of devices under management

Source: GigaOm 2022

Figure 8. Juniper Automation at a Glance

Delivered as a cloud service, Juniper Mist Cloud combines network intelligence, artificial intelligence, deep-learning insights, and microservices agility to deliver wired and wireless access seamlessly at the edge for enterprise-grade network and security infrastructure. Comprising analytics, assurance, location, and troubleshooting services, Juniper Mist Cloud automates several critical elements of the IT stack to deliver predictable, reliable, and measurable network access across the wired LAN to the WAN with complete visibility into the user experience.

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

Apstra supports many mainstream network vendors, including Juniper, Arista, and Cisco Systems, and includes deep integration with Enterprise SONiC (Dell's distribution of SONiC) and VMware NSX-T. Based on Juniper's current multivendor strategy, Apstra customers can enjoy the benefits of IBN without the fear of being locked into a single vendor.

Combining Apstra's IBN capabilities with 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, Juniper Contrail Networking provides virtual networking and security for virtualized and containerized cloud-native workloads. Leveraging Juniper or third-party virtualized and physical

Built for 5G and multicloud scenarios, Juniper Paragon Automation is a modular portfolio of cloud-native software applications delivering closed-loop automation. Built from the ground up for modern network operations, Paragon Automation includes Paragon Active Assurance (test and service assurance), Paragon Insights (monitoring and analytics), Paragon Pathfinder (provisioning, management, and monitoring), Paragon Planner (planning and simulation), and third-party Anuta ATOM (multivendor configuration and compliance management, service orchestration, and workflow and closed-loop automation).

Leveraging machine learning, network analytics, and automation to optimize path computation and network resource usage, Paragon Automation is designed to translate business intent into real-world performance, bringing cloud flexibility, elasticity, and resiliency to the WAN. Hosted on-premises or in a public cloud environment, Paragon can be deployed in redundant node clusters within a single data center or across multiple clouds in a high-availability scale-out architecture. In July 2022, Juniper launched pay-as-you-go Paragon Automation as a Service, enabling service providers to accelerate the adoption of new automation use cases while reducing costs.

Strengths: While the campus network, data center network, and WAN have historically been managed in silos, more and more enterprises are looking for ways to break down barriers and optimize application performance and automate operations across the entire network. Based on its acquisition spree and Anuta partnership, Juniper can now offer one of the industry's most complete end-to-end AI-driven network automation portfolios.

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.

Micro Focus: Network Operations Manager

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 MANAGER AT A GLANCE				GIGAOM
TARGET MARKET				
CLOUD SERVICE PROVIDERS	**NETWORK SERVICE PROVIDERS**	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
X	X	X	X	X
DEPLOYMENT MODEL				
PRIVATE CLOUD	**PUBLIC CLOUD**	**HYBRID CLOUD**	**MULTICLOUD**	
X	X	X	-	
PRIMARY USE CASES				
Improved operational efficiencies		Accelerated deployment		
Reduced operational and regulatory risk		Accelerated SDN, branch, and wireless remediation		
PRICING MODEL				
3-year subscription-based and edition-based perpetual licensing				
Source: GigaOm 2022				

Figure 9. Network Operations Manager 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. In addition, ongoing Syslog monitoring ensures that any change in configuration, running state, or operating system drift is identified quickly and compared against predefined policies, triggering automated remediation if required.

NOM's automation and orchestration capabilities enable complete lifecycle automation for adding, updating, and retiring devices on the network, including provisioning and monitoring. IT process orchestration authoring enables central IT to define the combination of multiple discrete automated tasks into an overall repeatable process workflow relevant to its needs and environment. These defined workflows are then executed by the IT process orchestration

access additional content used in intent-based workflows.

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. In addition, various device, component, interface, and custom KPIs are collected automatically. Leveraging Micro Focus' on-premises or SaaS-based OPTIC Data Lake (Operations Platform for Transformation, Intelligence, and Cloud), NOM's Incident Troubleshooting and Performance Troubleshooter workflows allow administrators to quickly explore, compare, and contrast any KPI data relevant to an incident, device, component, or interface.

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 stemming from policy violations. In addition, using a combination of performance monitoring and change automation, NOM can reroute traffic to eliminate bottlenecks, thereby optimizing network behavior.

NOM 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 requirements and rollback capabilities. In addition, Ultimate includes network services monitoring of MultiProtocol Label Switching (MPLS), IP telephony, and IP multicast.

NOM Ultimate also 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 8,000+ operations workflows, 300+ application components, and 80+ integrations. In addition, Ultimate audits the network for compliance based on industry best practices and vendor vulnerability notices, with exceptions triggering automatic remediation across three dimensions of device data, including configurations, running state, OS version, and other device attributes.

Strengths: NOM offers a single toolset delivering complete network visibility and comprehensive compliance, configuration, fault, and performance management, with industry-leading support for physical, virtual, and SDN-enabled devices across 200+ network infrastructure vendors. Real-time 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 service level agreements 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 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. However, Micro Focus has been slow to provide a comprehensive CI/CD approach or innovate in critical areas such as robotic process automation and advanced visualization. Potential customers should verify the progress made in these areas during the discovery phase.

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 quality of service (QoS) requirements of specific applications. 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's platform comprises Dynamic Maps, No-Code Runbooks, and Intent-Based Automation.

TARGET MARKET				
CLOUD SERVICE PROVIDERS	NETWORK SERVICE PROVIDERS	MANAGED SERVICE PROVIDERS	LARGE ENTERPRISES	SMBs
-	-	X	X	-
DEPLOYMENT MODEL				
PRIVATE CLOUD	PUBLIC CLOUD	HYBRID CLOUD	MULTICLOUD	
X	-	-	-	
PRIMARY USE CASES				
Optimized network operations		Incident response automation		
Change management automation		Intelligent network documentation		
PRICING MODEL				
1-, 3-, or 5-year subscription pricing based on the number of devices under management				
Source: GigaOm 2022				

Figure 10. NetBrain at a Glance

The core technology behind the platform, NetBrain's intent-based automation works with its dynamic digital twin to ingest available data from IT configuration and monitoring tools, unifying data silos into a single contextual view. NetBrain's "just in time" automation capability automatically maps around the problematic service 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 issues via thousands of network intents, including all of the underlying Layer 2 and Layer 3 contextual data from physical and logical topologies and geographically distributed sites.

Mapping the relationship between the network and the virtual endpoints involved, Dynamic Map enables users to visualize and manage their Cisco ACI and VMWare NSX infrastructure from all the most relevant perspectives, including overlay, underlay, and application-centric views. NetBrain also claims to be "the industry's only true borderless end-to-end visual management console for the entire hybrid network," providing insight into public cloud infrastructures —including hop-by-hop application paths from the public cloud to the network edge—to identify the root cause of performance issues with native cloud applications.

NetBrain alerts administrators to specific, predefined problems that could cause network degradation or downtime. Users can run automated diagnostics to gather relevant data and drill into what could be causing the problem. 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 map.

No-Code Runbooks provide a dynamic, interactive workspace for capturing and sharing consistent, best-practice diagnostic actions, operational procedures, and workflows, transforming them into executable no-code automation. Data, knowledge, and prebuilt automation are "extracted" from PDAS and third-party ecosystem tools—including BMC Remedy and ServiceNow—and enhanced by subject matter experts to create repeatable, best-practice network operation processes for network administrators to execute. In addition, the dynamic nature of NetBrain's No-Code Runbooks supports collaborative remediation, providing teams with the visibility, context, and tools they need to quickly identify root causes and speed up time to resolution.

NetBrain's Intent-Based Automation 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 enables subject matter experts 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.

Providing a 360-degree view of automation maturity from requirements to deployment and execution, NetBrain claims to have an installed base of over 2,500 enterprise and service provider customers, including one-third of the Fortune 500. In addition, the company offers an "Automation Maturity Index" for customers to measure and compare their success in reducing downtime and costs.

Strengths: NetBrain's intent-based 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

automated or manual resolution.

Challenges: While NetBrain offers in-depth analysis, diagnostic, and visualization tools, it is primarily a scalable automation platform for network problem prevention and remediation. NetBrain provides in-depth support for Cisco (especially IOS and IOS-XE) and VMware environments but lacks out-of-the-box integrations with standard tools. In addition, NetBrain relies on third-party tools for deep network fault and performance monitoring. The solution has 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.

Resolve Systems: Resolve

Founded in 2014, Resolve helps operations teams quickly validate, diagnose, and resolve cloud, IT, and network incidents with a single, consolidated view and toolkit. Providing a reusable automation framework and visual drag-and-drop coding tools, Resolve enables organizations to incrementally automate millions of events and complex workflows with powerful operator-guided or end-to-end automation spanning both simple and complex use cases. Resolve provides thousands of plug-and-play automation actions, hundreds of automation workflows, and prebuilt third-party integrations for connecting with existing IT systems and enterprise applications for end-to-end automation. In addition, Resolve easily integrates with custom solutions or other tools via REST APIs, SNMP, SMTP, SOAP, SSH, TCP, or other common protocols.

RESOLVE AT A GLANCE — GIGAOM

TARGET MARKET				
CLOUD SERVICE PROVIDERS	**NETWORK SERVICE PROVIDERS**	**MANAGED SERVICE PROVIDERS**	**LARGE ENTERPRISES**	**SMBs**
-	X	X	X	X

DEPLOYMENT MODEL			
PRIVATE CLOUD	**PUBLIC CLOUD**	**HYBRID CLOUD**	**MULTICLOUD**
X	X	X	X

PRIMARY USE CASES	
Proactive network testing	Virtual network provisioning
Standardized network configuration	Performance monitoring/preventative maintenance

PRICING MODEL
Flexible consumption, perpetual, or subscription pricing based on automation workflows or devices

Source: GigaOm 2022

Figure 11. Resolve at a Glance

Offering built-in scalability for responding to and remediating issues faster—from simple service requests to complex, self-healing processes—Resolve was designed to overcome IT silos and eliminate human error by leveraging automation to enforce security and compliance. Resolve comprises four components: Resolve Insights, Resolve Actions, and Automation Exchange.

Resolve Insights employs agentless discovery to deliver real-time visibility and manage dynamic multivendor, multidomain environments scaling to hundreds of thousands of devices. Lightweight data collectors intelligently scan subnets or user-input boundaries to quickly identify compute, network, and storage configuration items, determining a variety of details about each entity, including vendor make, model, platform, configuration, IP address, and more. The resulting real-time configurations stored in the continuously updated management database (CMDB) can be easily viewed by device type or IP address range in custom filtered groups or a tabular list view.

In addition, Resolve Insights automatically discovers complex, distributed applications and maps dependencies to the underlying infrastructure components, including application flows and application services running on each host. For more complex applications comprising many elements, Resolves uses a proprietary clustering algorithm that dynamically discovers collections of related application services and maps the flows to the underlying infrastructure, including hybrid topologies. Finally, a drag-and-drop interface groups these flows together to create a single pane of glass to visualize the relationships among components—including fault and alert overlays—to understand how infrastructure issues impact business-critical applications.

Resolve Actions provides interactive automation capabilities (also known as human-guided or attended/unattended automation), allowing operators to choose which process steps are automated and which require human interaction. Resolve also presents embedded best practices captured by subject matter experts using the drag-and-drop interface to quickly design no-code process workflows, build decision trees, and add over 5,000 prebuilt automations from the Automation Exchange content library.

Operations Management Accelerator Pack helps automate important but tedious network-related tasks, including automated health checks, Linux and Windows patching and configuration updates, and scheduled rolling server restarts. In addition, the CMDB provides detailed visibility into all network configurations, ensuring new devices or configuration changes are automatically discovered and dependencies mapped.

Strengths: Resolve orchestrates enterprise-wide automation processes across IT functions, including IT operations, service management, network operations, cloud operations, and centers of excellence. Configurable plug-and-play automation workflow templates provide building blocks to create customized workflows without starting from scratch, while drag-and-drop automation actions include thousands of prebuilt tasks and actions for building one-click, no-code workflows. In addition, hundreds of third-party integrations seamlessly connect existing IT systems and enterprise applications for end-to-end automation.

Challenges: While Resolve offers advanced discovery, alerting, and visualization tools, it is primarily an event-driven platform for large organizations and service providers to automate proactive health checks and remediate thousands of IT issues daily without increasing headcount. In addition to having a steep learning curve, Resolve relies on third-party tools for deep network fault and performance monitoring.

6. Analyst's Take

NetDevOps prioritizes business alignment over network control, relying on intelligent infrastructure management and automation to increase efficiency and ensure network availability, quality, and reliability. In addition, NetDevOps aims to bridge the gap between DevOps and NetOps teams, minimizing manual intervention by deploying programmable network processes spanning data center, WAN, public cloud, and edge infrastructures to configure, deploy, manage, and optimize the environment.

Unfortunately, that's easier said than done, and buyers should recognize NetDevOps as a new and rapidly evolving field. Even the most advanced NetDevOps solutions have a way to go before being classified as fully integrated, end-to-end solutions for automating network operations. Furthermore, most NetDevOps tools currently are limited in their ability to discern business intent and convert it into multivendor network designs. Instead, they primarily target reducing network downtime and optimizing performance improvements through intelligent automation and orchestration.

Moreover, while newer vendors are developing their solutions from the ground up, the traditional hardware and software vendors in this space are evolving existing 24×7 network monitoring tools to enable network automation. This is especially true of Juniper Networks and Micro Focus, whose legacy solutions have large installed bases. Micro Focus is leveraging its deep in-house network monitoring and performance knowledge to grow its network automation capabilities. In contrast, Juniper Networks embarked on an acquisition and partnership spree to expand its portfolio while simultaneously expanding its footprint within the Apstra installed base. While we expect Juniper's approach to pay off in the long term, potential customers must, in the interim, navigate the broad—and somewhat confusing—portfolio to understand precisely what they need to automate their network environment.

One area to keep an eye on is NetDevOps as a service (NDOaaS). Only Anuta Networks, Blue Planet, Gluware, Itential, and Juniper have SaaS offerings. Moreover, while Blue Planet Enterprise (BPE) Automation Suite is available only as a SaaS offering, Anuta's ATOM Cloud and Itential's Automation Platform on-premises and SaaS offerings provide comparable functionality. In addition, Juniper's Paragon Automation as a Service is designed for service providers to accelerate the adoption of new automation use cases while reducing costs.

When evaluating NetDevOps tools, consider both your existing and planned network environment, including cloud platforms and hardware and software infrastructure vendors. Then, ask yourself:

- Am I comfortable with fully automated network deployment, configuration, and management, or only with administrator-approved actions?
- Am I looking for predictive remediation to support business-critical services, or is reactive remediation acceptable?
- Am I looking for end-to-end network automation, including the data center, WAN, public cloud, and edge, or only for coverage in certain areas?

Do your homework. Understand the problem you're trying to solve, explore potential trade-offs, evaluate your resources and skills, and then choose a solution—and partner—that fits in with your current and future network environment. In addition, remember that the learning curve for NetDevOps tools is generally quite steep, requiring specialized skill sets and organizational readiness to embrace new, evolving technologies. Therefore, carefully evaluate a solution with a view to deploying a proof of concept in one area of your environment to build up knowledge, understanding, and skills before scaling it across your entire network.

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.

cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

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

Edge & Networking

Knowingly Corporation
3905 State Street #7-448
Santa Barbara, CA 93105-5107