WHITEPAPER /

The **SaaSification** of **Network Automation** – A Modern Approach to Network Management and Monitoring

More Information at www.brillio.com

Leveraging Network Automation for Network Management & Monitoring

Networks have become the backbone of enterprises today as they have started relying more on digital transformation to run their businesses. The pandemic has further accelerated this transition towards digitization due to the prevalence of online operations. As a result, networks have become increasingly complex. Modern networks are now diverse with devices from multiple vendors having different software stacks. Networks are spread across the globe and continuously grow in size and complexity. Also, the adoption of the cloud for compute workloads and data storage has made connectivity to the cloud critical to ensure business continuity.

As networks grow, the chances of something going wrong increase and any disruption in the network has significant implications for the business. There could be multiple reasons for network failures – human errors, hardware failures, software errors, link failures, and misconfigurations.

With network IT teams responsible for the smooth functioning of the networks, it has been observed a lot of time is spent in troubleshooting network issues, finding the root cause, and then fixing everything. This is where network automation helps to simplify, speed up and automate network visibility and control – cutting the operating costs in half while avoiding 70% of the time spent trying to identify and diagnose network issues (Gartner, “5 Network Cost Optimization Opportunities” June 2019).

Traditionally, enterprises have automated network operations with the help of NMS systems and scripts. To meet the scale of networks for supporting new technologies such as IoT and edge devices, advanced automation systems are needed for health and performance management. Enterprises will need plug-n-play systems having low-touch operations with auto-discovery of network devices. The automation platform should be able to prevent network failures by using predictive techniques and self-heal by making necessary changes to network settings without manual intervention. Decisions would need to be made in real-time and IT teams would rely more on data-driven insights than gut instincts to resolve network issues. Extreme automation is the need of new-age networks.

Network Automation has evolved into a significant market and in this whitepaper, we explore an important dimension of it being offered as a cloud-based, software service to Enterprises, hosted on public cloud platforms such as AWS, GCP, and Microsoft Azure. SaaSification acts as a catalyst for Network Automation. The whitepaper dives into various facets of SaaS-based Network Automation covering its technical aspects, present market landscape, business models around it, use of AI/ML, and gold standards for SaaS offering – to meet the goals of making networks more reliable, efficient, and easy to manage.

Advanced Network Automation

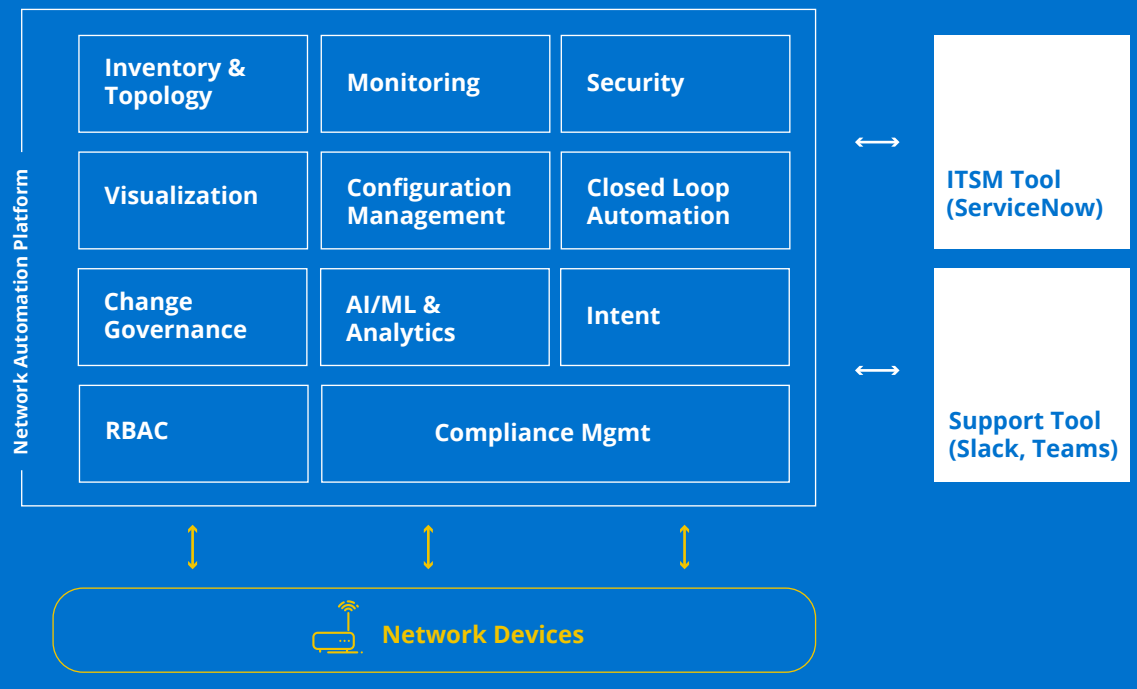
The diagram below shows the overarching functions of an advanced Network Automation platform. It presents a comprehensive scope including basic functions and advanced features. Advanced features are supported in a software solution depending upon the problem it aims to solve.

One of the essential features is the discovery of network devices such as routers, switches, Wi-Fi APs, SD-WAN, and virtual devices, listed as part of the inventory and visually showing the interconnectivity between the devices. This is typically achieved with the help of protocols such as SNMP, CDP, and LLDP. The platform creates the topology of the network, helps trace the path between 2 network endpoints, determines latency, and finds any broken links between them.

Network configuration management allows users to manage and automate the configuration of multi-vendor devices of Enterprise IT networks and track & manage configuration changes in real-time to ensure network stability. This is achieved by maintaining configuration history, comparing different configuration versions, permitting rollback to previous configurations, and setting a baseline configuration. Changes to device settings could be sensitive in nature and require an approval process that is driven through the governance function. This is done with the integration of 3rd party ITSM tools such as ServiceNow.

Network devices are monitored to understand the state and performance of the network. This includes monitoring parameters such as CPU, memory utilization, interface status, interface utilization, and packets received & dropped. The automation platform also tracks the alarms, events, and KPIs of network devices. Incident tickets can be created to manage the alarms or to report any abnormalities observed in the network.

Functions of Network Automation Platform



Intuitive dashboards that showcase the overall network status along with the ability to drill down into the specifics of a network device help IT teams derive quick network insights.

Security, a critical concern for Enterprises, is another aspect of the automation platform allowing the user to define policies to guard incoming and outgoing network traffic and provide only authorized access to the network.

To minimize human intervention in addressing network issues, thereby making the network self-healing, closed-loop automation triggers changes to the network based on user-defined policies and conditions (e.g., switching off a network interface if it continuously flaps its state over a period).

Any configuration change in a multi-vendor network usually requires a sequence of workflow steps to be executed. Network automation platforms allow users to provision such workflows to perform repetitive tasks and ensure their correct execution. Workflow automation can be made intuitive with the help of graphical tools to define workflow steps and dependencies.

The growing complexity of networks makes troubleshooting and fixing issues extremely time-consuming and it becomes a costly affair as business operations get impacted. It would be of great value if network failures can be detected and predicted by continuously assessing network performance. This is where AI/ML comes into focus to support Network automation. Machine learning models are trained with the help of device logs, alarms, configurations, and KPIs. These models are deployed to pinpoint anomalies in network behavior, predict failures and fix commonly occurring network issues with the help of closed-loop automation. AI/ML and data analytics techniques drastically cut downtime to resolve network issues for the following reasons:

- Analyzing different data formats such as Syslog, SNMP, KPIs, and text, in real-time
- Correlating this data to find anomalies and aberrations in the network
- Using trained AI/ML models that help trace the root cause.

Network access failures, authentication problems, poor Wi-Fi performance, dip in network throughput are some examples where artificial intelligence and machine learning are used by the Network Automation platform to find the root cause analysis and then provide guided remediation workflow to fix the issue. Users have reported a reduction of 70% of diagnosis time as the AI/ML function can infer by looking at multiple sources and formats of data from the network.

Compliance management function assesses network's adherence to regulatory standards and corporate or IT policies.

Finally, network automation platforms are being designed to be 'Intent-based' to let users express the intended state of the network without knowing the steps that are required to achieve that state.

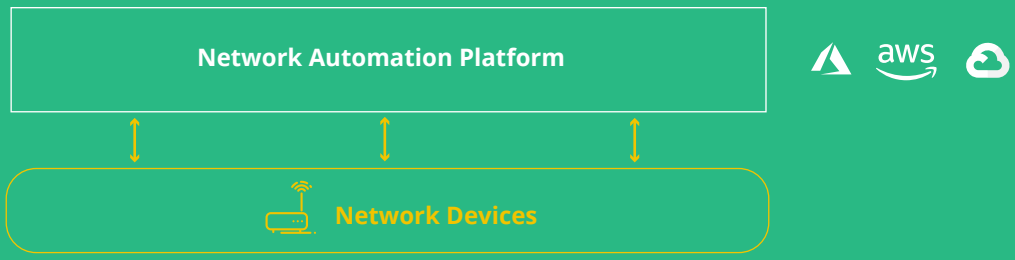
The Need for SaaSification in Network Automation

Network Automation platform needs only network connectivity to perform configuration, monitoring, and troubleshooting tasks on network devices qualifying it to be SaaS-based. But the bearings of SaaS-based Network Automation lie in continuous innovation, simplified enterprise networks, the economy of scale, and reduced entry barriers.

SaaSification provides multiple benefits. First of all, it reduces the burden on Enterprises to host yet another tool on their premise and manage its lifecycle. This reduces the internal IT effort. Hosting services on the public cloud provide continuous access to new software releases, features, and fixes, everything taken care of by the SaaS solution provider. Importantly, the SaaS solution reduces the infrastructure technical debt, i.e., it allows the enterprise to leverage the solution built on modern technologies. SaaS solutions are usually driven by an agile delivery model and hosting them on the cloud makes it possible to adapt them to new trends in technology. Enterprises upgrade on-prem solutions less frequently to prevent any disruptions in the network.

Enterprises can make a quick start with SaaS Network Automation by simply installing a software agent that communicates with on-prem network devices to send network data to the cloud. Most of the initial steps can be managed by the network IT team with minimal reliance on any professional services from the SaaS provider. As the number of network devices that depend on automation increases, the solution hosted in the public cloud scales seamlessly to support the increased workload. This happens transparently without any involvement of the network IT team. The Enterprise only pays for the services they use.

Network Automation on Public Cloud



With SaaS, Enterprises have centralized management of their network that could be spread across different geographical locations in the world. SaaS supports a try-buy option to buyers and a subscription-based model that enables them to pay as they grow without making a large upfront investment. Business workflow for SaaS can be completely digitized to cover all the stages of the customer lifecycle, including service sign-up, onboarding, agreement to licensing terms, periodic invoicing, payment processing, and end of service. Public cloud companies can help SaaS providers to meet the desired SLAs that customers demand as cloud providers have options for geo hosting and hardware & software infrastructure. The concern for business continuity can be addressed through SaaS solutions as support for data backups, data restoration, geo-redundancy, and recovery from hardware & software failures are easier to handle with public cloud hosting.

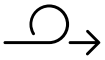
The SaaS model supports the economy of scale as the compute, storage and network infrastructure on the cloud can be shared across multiple users, allowing multi-tenancy. Profits grow manifold after an inflection point as new customers sign up for the service. The SaaS model for Network Automation also fits well with distributors and managed service providers (MSPs), who help scale the business leveraging the multi-tenancy aspect of the solution.

Gold Standards for a SaaS Solution

Enlisted below are gold standards for any best-in-class SaaS solution in any industry to measure the maturity of the solution. SaaS-based Network Automation solutions can be benchmarked against these standards.

Digitized Customer Lifecycle

Digitize end-2-end business workflows including customer onboarding, service sign up, purchase order processing, invoice generation, payment processing, and end of service.



Agile Delivery

Provide access to new features and fixes through an agile software delivery model. Notify customers well in advance for service unavailability, maintenance, or software upgrade procedures.

Auto-scaling

Scale cloud infrastructure up or down to meet demands of varying customer workload without requiring any intervention from the customer.

Integration Hub:

SaaS solutions should provide integration hooks with 3rd party software systems used by customers to make them integral to internal processes and systems. These systems could be incident management systems (e.g., ServiceNow), alert management systems such as Opsgenie, or collaboration platforms such as Slack & Teams.

Certifications

Certifications for some of the standards and benchmarks are critical to gain customer confidence and meet regulatory compliances. Given below are some of the standard certifications that are applicable to SaaS solutions. Some additional ones may be required based on the market verticals and geographies the solution is intended for (e.g., HIPAA for healthcare, GDPR for the European Union).

ISO 22301:
For business continuity management

ISO 27001:
For information security management

ISO 27701:
Extension to ISO27001, for privacy information management

SOC 2:
For the safety and privacy of customer's data

OWASP ASVS:
For web application security verification

CSA STAR:
For security assurance in the cloud

Customer Support:

Customer support is critical to address customer concerns and issues in a timely manner. It can be offered in multiple tiers such as 24x7, 24x5, 8x5, 8x7. Support can be provided in the form of email, chatbots, phone, or ticketing systems. As adoption for SaaS grows, it is important for the SaaS provider to create multiple levels of support teams - L1 (for frontline support), L2 (for complex issues), and L3 (for software changes).

Business Continuity:

Provide business continuity to recover from software and hardware failures with minimal service disruption time. Geo-redundancy from catastrophic failures is another aspect an Enterprise would be interested to overcome (outages in data centers, natural calamities such as earthquakes, and floods that disrupt services in a specific geography).

Data Security

Ensure customers' data is protected and encrypted. Provide support to backup customer data and restore it on a need basis.

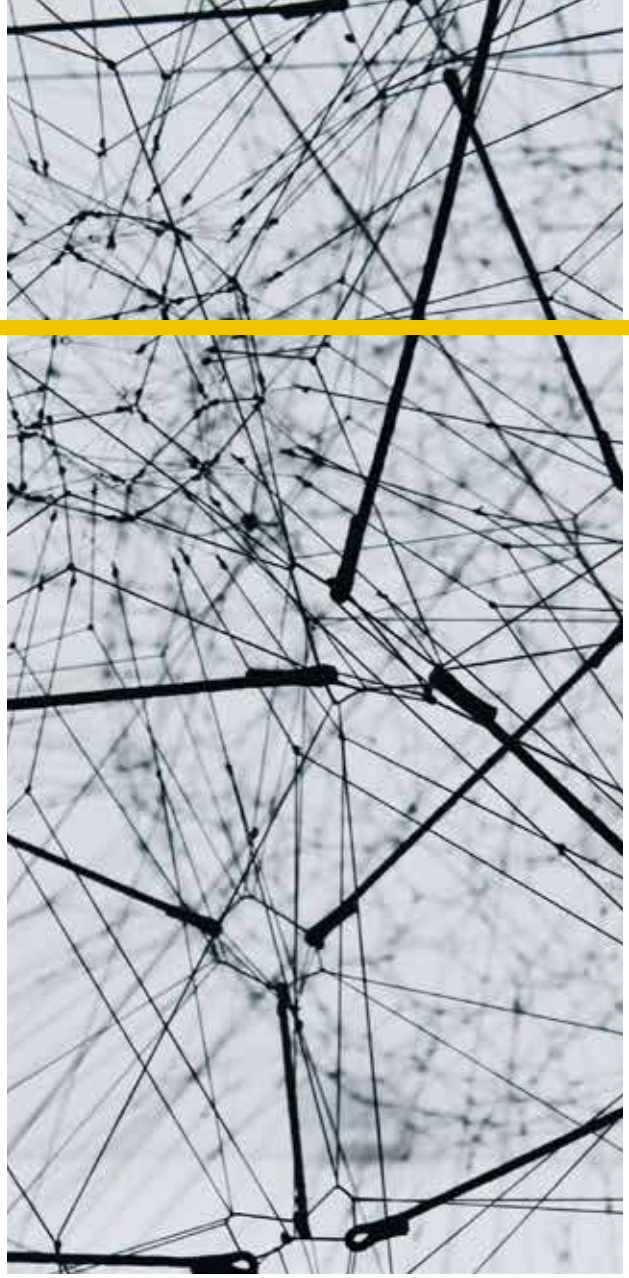
Understanding the SaaS Network Automation Market Landscape

The table below enlists different companies in the Network Automation space including on-prem players and compares them against various capabilities of an automation platform.

In terms of maturity, SaaS-based Network Automation is still in its mid-early stages. Existing solutions in the market address some aspects of advanced Network Automation, but there is no single comprehensive solution presently that addresses all aspects discussed in the earlier sections. The grey spaces in the table denote areas yet to be supported by the vendor. Significant work needs to go into building AI/ML capabilities to diagnose and troubleshoot network issues. This is partly because failures can happen due to multiple reasons in a network with a diverse set of devices. AI/ML models need to be trained to address this aspect. Security, Compliance Management, and Intent-based Networking are other areas that need to be addressed for providing complete SaaSified Network Automation. Closed-loop automation capabilities are presently available in limited form to make the network truly free from manual interventions.

Market size for SaaS-based Network Automation is growing. For reference, the combined network configuration change management market (both on-prem & cloud) is estimated to reach $2.5 billion by 2027 with a CAGR of 8.8% from 2021-2027, out of which ~60% is expected to be SaaS-based (according to Market Research Future report on Global Network Configuration & Change Management, 2021). The total network AIOPs market is estimated to cross $10 billion by 2027 with a CAGR of 20% from 2019-2027. A significant portion of that market will belong to SaaS. North America is expected to hold the highest market share (~40%), followed by Europe, Asia, and the Rest-of-the-World.

	Solarwinds	Whatsup Gold	Manage Engine	Zenoss	LogicMonitor	Gluware	Itential	Anuta
SaaS/On-prem	On-prem	On-prem	On-prem	Hybrid	Hybrid	Hybrid	SaaS	Hybrid
NW Monitoring	●	●	●	●	●			●
Config Management	●	●	●		●	●	●	●
Workflow Automation						●	●	●
Change Governance								
RBAC	●	●	●	●	●	●	●	●
Security	●							
Intent Networking						●		
AI/ML				●	●			
Closed Loop Automation								●
Inventory	●	●	●	●	●	●	●	●
Topology	●	●	●					●
Visualization	●	●	●	●	●	●	●	●
Compliance Management	●		●					●



Disruptive Commercial Models

SaaS-based Network Automation can drive monetization with the help of a multi-layered economy and with the right pricing strategy. The channel partner ecosystem is vital for the success of a SaaS business to penetrate different market verticals, scale for profitability, and leverage various external sales channels rather than invest in building one's own. Revenue generation is also driven with the help of different pricing plans based on the target customer and the nature of the engagement with the customer.

01

The Channel Partner Ecosystem

DISTRIBUTORS:
Distributors are typically resellers who manage the complete customer lifecycle. For a SaaS-based system, it would not be possible for the solution provider to reach out to every market that needs network automation. This is where distributors can help by selling through their existing network of customers and established relationships.

MANAGED SERVICE PROVIDERS (MSPS):
MSPs manage networks for enterprises, who do not possess the skills and resources to manage their networks. MSPs leverage software solutions from multiple vendors and can effectively work out the combined value of different solutions. This makes it easier for them to adopt new technologies in the Network Automation space.

SYSTEM INTEGRATORS (SIs):
SIs are consulting companies (e.g., Wipro, Accenture, Infosys, Tech Mahindra) that deal with large strategic accounts in retail, banking, automotive, government, healthcare, hospitality, and many more. Network operations are one of the critical pieces they handle for their customers. SIs provide a solid platform for SaaS providers to present their solutions to large organizations as Sis have deep relationships with key stakeholders in large organizations. SIs can be instrumental in closing large business deals, though the nature of the deal could be different from a conventional subscription-based model.

02
Pricing Models

PAY-AS-YOU-GO PRICING:
SaaS services are based on a subscription-based model where customers are billed periodically (e.g., monthly, quarterly, annually). It means customers pay less or more depending on what they need, for true consumption advantages. This enables billing to be more consistent with real business cash-flow.

DEVICE-WISE PRICING:
Customers can be charged based on pricing tiers depending upon the number of network devices that connect to the SaaS platform. Examples of device-based pricing tiers could be: a minimum of 250 devices, up to 1000 devices, 3000+ devices. Customers can be offered discounts as they move towards higher tiers.

FEATURE-WISE PRICING:
SaaS solution providers can price their offering based on the features supported. Customers can sign up for different features and pay for only the ones they use. E.g., for a Network Automation platform, customers can be charged separately for configuration management and monitoring features.

BUNDLED PLANS:
Features can be bundled together to create attractive pricing for different markets. E.g., feature bundles for MSPs, SIs, network admin teams, etc.

PREMIUM PRICING:
While the standard features can be priced sensitively taking into consideration the cost and competitive landscape, SaaS providers can gain higher profits from niche features in the solution. For example, data backup and restoration services are important aspects for an enterprise, for which they would be willing to pay a good price to ensure business continuity.

Brillio's Capabilities in SaaS Network Automation

Brillio is a product engineering organization with roots in digital transformation. The company has significant stakes in telecom and network automation and strategically engages with tier-1 operators and large network OEMs on complete product and business lifecycle including product architecture, design & development, tech consulting, business and GTM strategy.

Brillio has made significant investments in SaaS-based Enterprise Network Automation solutions reinforced with machine learning and artificial intelligence technologies to support multi-vendor networks addressing diverse network verticals such as Wi-Fi, Routing, Switching, SD-WAN, LAN, and Cloud. In addition to product engineering, Brillio drills heavily into the business aspect of SaaS solutions with expertise in GTM strategy, sales avenues, distribution mechanism, channel partner ecosystem, pricing model, and quote-to-cash. With a seasoned team of software and business professionals providing thought leadership and execution, the company has successfully envisioned a complete digitized model of a SaaS-based solution offering.

If you are excited to build a SaaS solution and business, please reach out to Brillio at info@brillio.com.

About Us

At Brillio, our customers are at the heart of everything we do. We were founded on the philosophy that to be great at something, you need to be unreasonably focused. That's why we are relentless about delivering the technology-enabled solutions our customers need to thrive in today's digital economy. Simply put, we help our customers accelerate what matters to their business by leveraging our expertise in agile engineering to bring human-centric products to market at warp speed. Born in the digital age, we embrace the four superpowers of technology, enabling our customers to not only improve their current performance but to rethink their business in entirely new ways. Headquartered in Silicon Valley, Brillio has exceptional employees worldwide and is trusted by hundreds of Fortune 2000 organizations across the globe.

For a high level maturity assessment and road mapping for your personalization strategy, please write to us at **info@brillio.com**