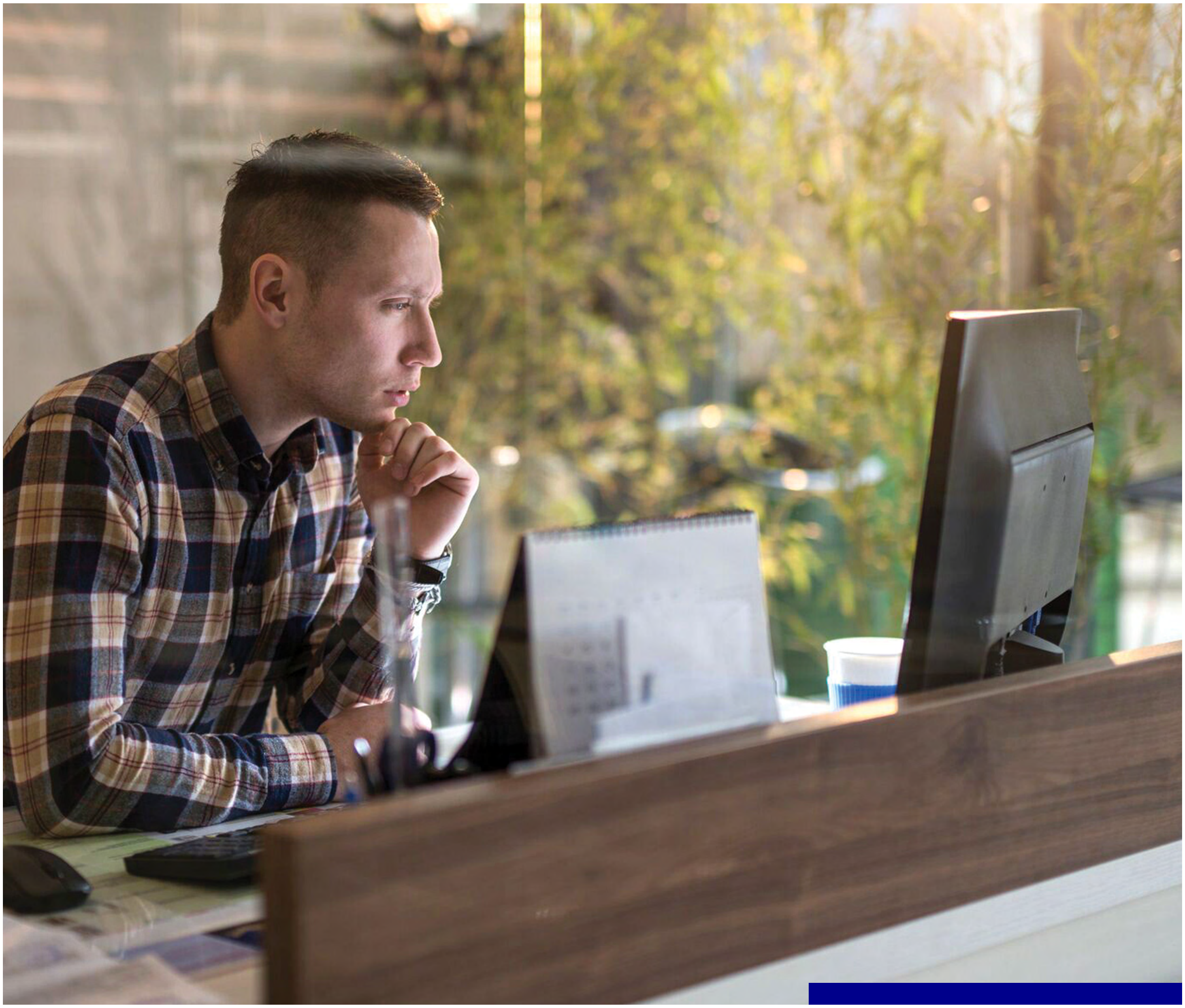


Brochure

Network Operations Management

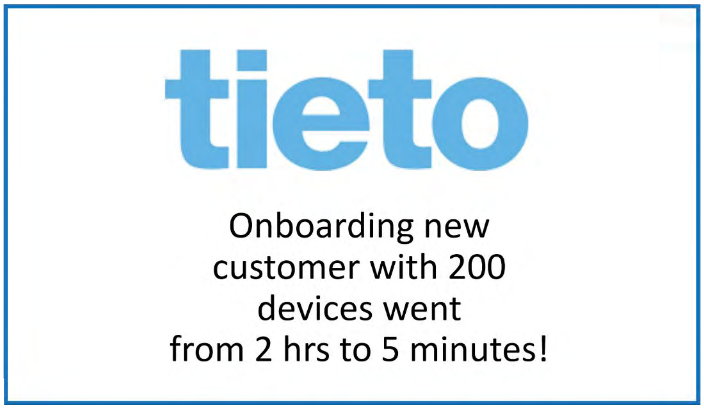
Manage, Automate, and Ensure Compliance for Physical, Virtual, and Software-Defined Networks

opentext™

Manage, Automate, and Ensure Compliance for Physical, Virtual, and Software-Defined Networks

The digital enterprise is being driven by rapid change with unprecedented levels of innovation. Enterprise networks are responsible for enabling this transformation through increased agility and adopting new technologies, while improving its security by being aware of and closing down vulnerabilities.

Modern applications are becoming increasingly distributed. To maintain high quality of service levels requires dynamic and adaptive network infrastructures. Software defined networks (SDN) seek to meet these requirements by decoupling and centralizing the control of network fabric configuration from the data-flow. When implemented and managed correctly, SDN can provide rapid change to support increased performance levels even as demand scales. This introduces a significant change from traditional device-centric network model of the past several decades. As a result, network management needs to play a supervisory role, assuring secured, compliant configurations are maintained, in addition to its traditional fault and performance monitoring role.



tieto

Onboarding new customer with 200 devices went from 2 hrs to 5 minutes!

Today, cloud services, wireless access, and mobile devices support the digital enterprise through improved and flexible access; but also require management solutions to ensure secure connectivity—for example when adding a new external link to a SD-WAN to increase capacity, each link type is likely configured to be secured by different protocol-appropriate methods (IPSec etc.) depending on company policies.

Additionally, enterprise networks remain a critical line of defense against security threats, as many vulnerabilities can reside in the network itself.

To manage modern, dynamic networks, and increase security, network engineering and operations teams must work together closer, and implement a new paradigm of collaboration which also unifies network functions including: monitoring, diagnosis, optimization and automated remediation.

Here's Why

- **Network management solutions are continually called onto to adapt to new technologies, while retaining value of existing ones**, including: SDNs, multiple connection methods to the cloud and Internet, remote sites, and WiFi networks. All of these technologies require closer collaboration between network engineering and operations because of their dynamic nature, which requires fast and deep understanding of the technologies to operate effectively.

More than 90% of network professionals believe that SDN requires Operations and Engineering to work more closely together than before to monitor and solve problems.[1]

- **SDN is accelerating the rate of change within networks.** Expectations of reduced mean time to remediate (MTTR) and new provisioning are driving the need to unify functions including network monitoring, diagnosis and automation. All of these must be in-sync to ensure accurate changes occur and issues are diagnosed holistically, including performance and traffic analysis, while maintaining continuous compliance.

Two-thirds of network professionals preferred a unified network management solution that includes SDN, virtual, traditional, as well as monitoring, configuration and compliance functions.[2]

- **Increasing security threat levels demand that all monitoring tools identify and report vulnerabilities to thwart threats.** This goes beyond relying solely on dedicated security tools and departments. Ultimately, security is a shared concern, and network management plays an increasingly important role.

Greater than 80% of enterprise network teams are now involved with security investigations—indicating a major shift in the role of those teams within enterprise.[3]

- **Ongoing initiatives to maximize productivity and efficiency necessitate a consolidated tool and team approach.** Using and maintaining fragmented toolsets is costly, inefficient and reduces staff productivity. Unified toolsets quickly isolate root causes of network issues from a single source of truth, support new service rollouts, and improve staff efficiency while reducing costs.

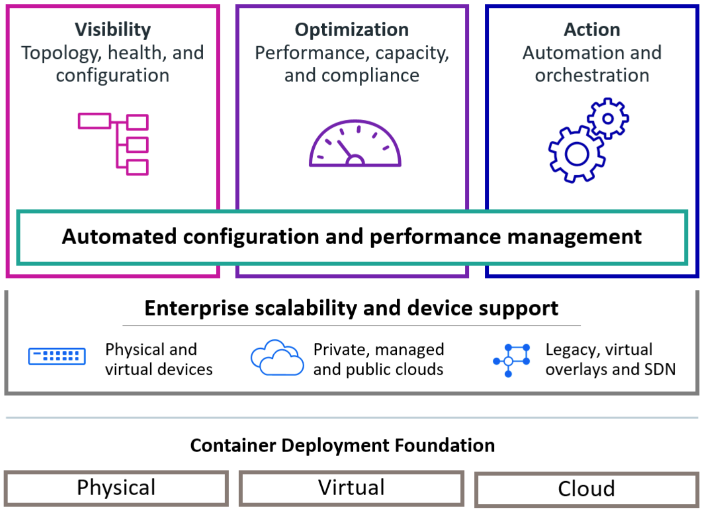

Visibility
Topology, health, and configuration
Optimization
Performance, capacity, and compliance
Action
Automation and orchestration
Automated configuration and performance management
Enterprise scalability and device support
Physical and virtual devices
Private, managed and public clouds
Legacy, virtual overlays and SDN
Container Deployment Foundation
Physical
Virtual
Cloud

Figure 1. NOM environment and functional overview

The Solution

Introducing Network Operations Management

OpenText™ Network Operations Management is the first heterogeneous network management solution to provide unified management for modern networks.

NOM challenges and improves upon traditional network management models in several ways:

First, NOM breaks down functional siloes of visibility, optimization and action *(see Figure 1)*, by introducing guided user workflows that cross all three areas. Both the operations and engineering teams benefit from having automated network topology, health, and configuration status and details at their disposal. Armed with these, issues are resolved faster so network services are maintained at a high level.

[1] *Dimensional Research, Network Professional SDN Survey, December 2017*
[2] *Ibid*
[3] *M-Trends 10th Annual State of the Network Report*

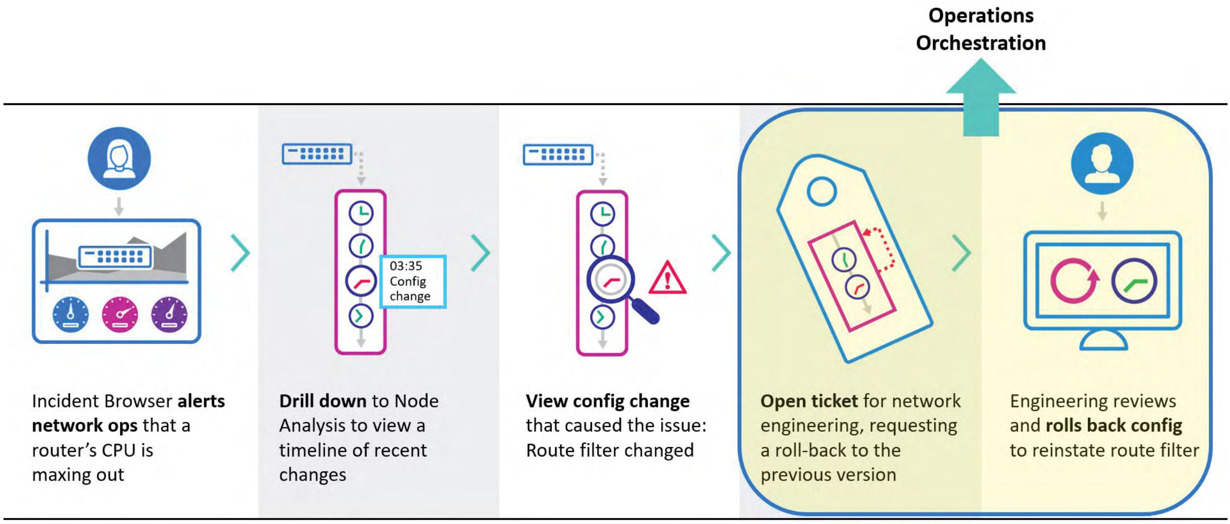

Operations Orchestration
03:35
Config
change
Incident Browser **alerts network ops** that a router's CPU is maxing out
Drill down to Node Analysis to view a timeline of recent changes
View config change that caused the issue: Route filter changed
Open ticket for network engineering, requesting a roll-back to the previous version
Engineering reviews and **rolls back config** to reinstate route filter

Figure 2. NOM Guided Workflow: SDN router misconfiguration

NOM goes beyond network diagnostic and automated configuration tasks to full-bore multi-system, change orchestration. Figure 2 depicts a typical NOM Guided Workflow which leads a user through the steps to identify and fix a router misconfiguration. NOM Guided Workflows help even inexperienced operators to follow SOPs and work more intelligently.

Second, to optimize your network's services you need to track its performance, traffic loads and capacity to specific paths through the network. In addition, knowing the configuration compliance of your network elements (through SDN, virtual, wireless and physical networks) is critical for securing your complete network, as your staff can unintentionally introduce non-approved configurations as they make changes to address network issues.

Third, achieving maximum efficiency and cost reduction will likely lead to configuration automation and even higher benefits of complete orchestration of network services. As networks will remain a mix of technologies and vendors into the future, NOM continues to optimize your total network by reducing manual intervention and nnormalizing events across both traditional and new network technologies.

The last two steps in Figure 2 can be further automated using NOM's OpenText™ Operation Orchestration (OO) subsystem. OO is able to integrate with external applications through its extensive graphically-driven library. Figure 3 shows a typical example of how NOM performs internal operations such as turning off management of the device, integrates with an external ticketing system, and records configuration details in a CMDB system. This level of multi-system orchestration provides increased efficiency, fewer errors, and reduced MTTR.

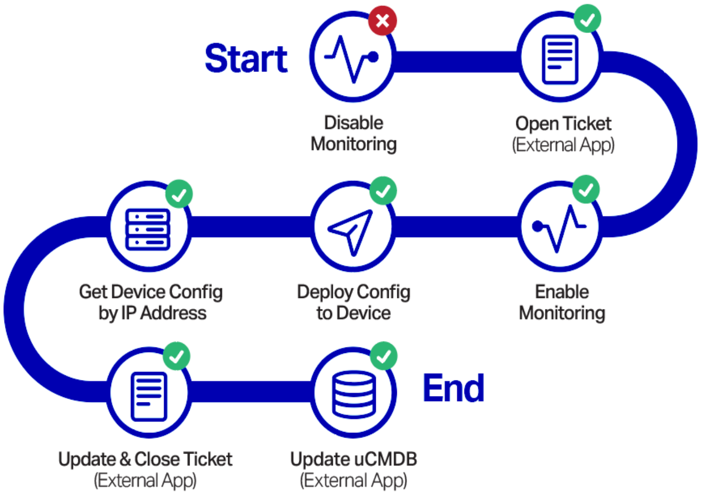

Start
Disable Monitoring
Open Ticket (External App)
Get Device Config by IP Address
Deploy Config to Device
Enable Monitoring
Update & Close Ticket (External App)
Update uCMDB (External App)
End

Figure 3. NOM's multi-system Operations Orchestration example

Enterprise Scale, Industry-Leading Heterogeneity, and Support for Modern Deployment Technologies

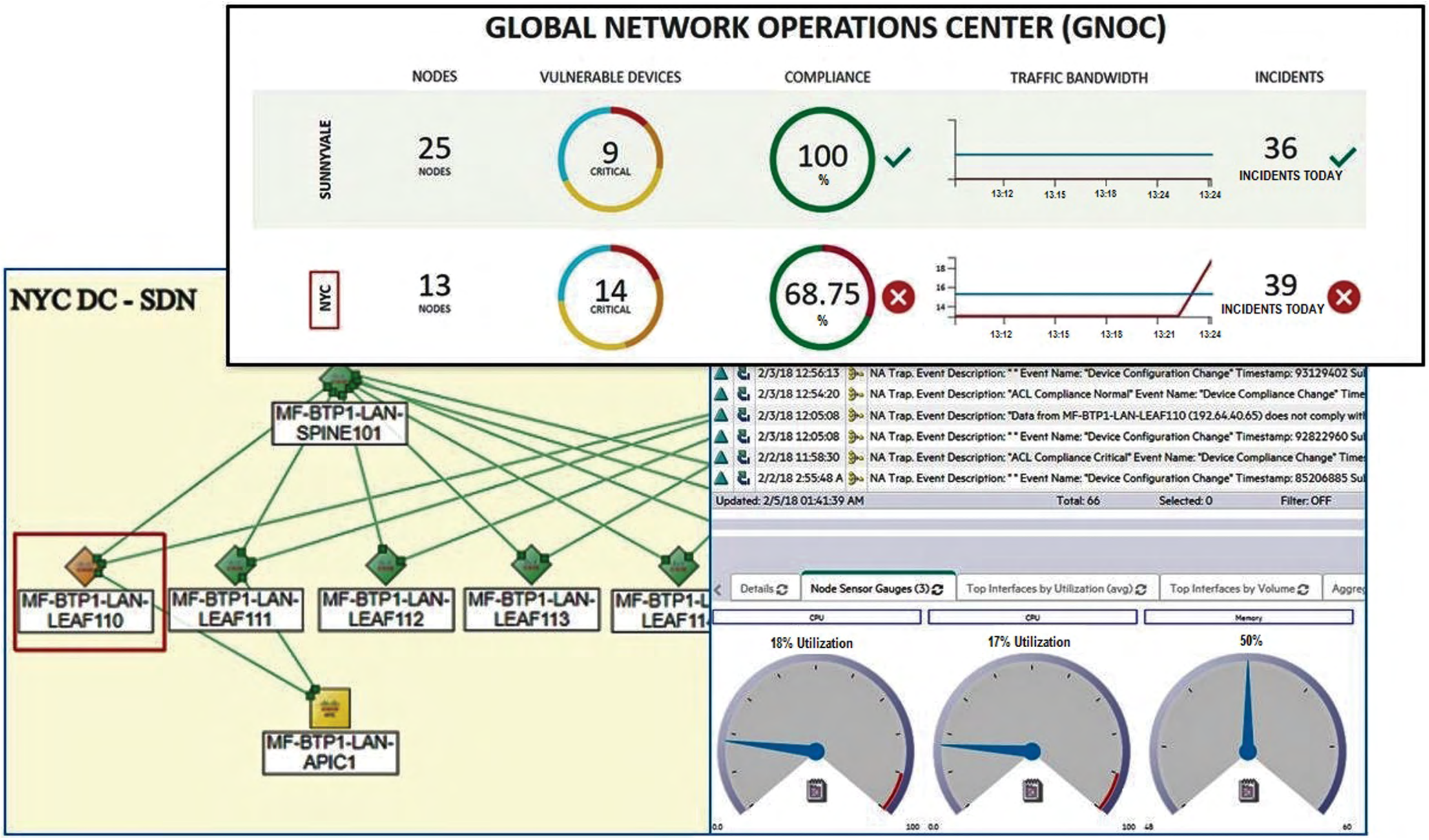
In contrast to work-group level tools, NOM can manage an enterprise network through high single system scale, as well as by combining multiple management systems consolidated into a unified solution. This provides a complete understanding of your network and improves productivity and efficiency.

NOM supports more than 180 vendors and 3,400 models of physical, virtual, and SDN network devices. This level of completeness is critical as your network transitions to newer technologies over time. And, NOM continually adds to its list of supported technologies, vendors and devices. NOM's decoupled architecture allows for off-release-cycle additions to new devices, historically on a bi-monthly schedule.

Underpinning all these capabilities NOM includes advanced technologies to improve user understanding and productivity. It's what's behind NOM's modern interfaces, that matters most—a fast, scalable, and intelligent architectural foundation. NOM's incremental, continuous, run-time discovery keeps up with rapid network changes needed to drive comprehensive and accurate root-cause analysis network issues *(see Figure 4)*.

Comprehensive Compliance

Networks are becoming increasingly complex which impacts costs. NOM helps reduce expenses by providing a three dimensional network compliance model that maps device information, including configuration, OS version, and run-time diagnostics, into rules and policies to identify violations in real time for fast remediation. NOM also offers a



```
2/3/18 12:56:13  NA Trap. Event Description: " " Event Name: "Device Configuration Change" Timestamp: 93129402 Su
2/3/18 12:54:20  NA Trap. Event Description: "ACL Compliance Normal" Event Name: "Device Compliance Change" Time
2/3/18 12:05:08  NA Trap. Event Description: "Data from MF-BTP1-LAN-LEAF110 (192.64.40.65) does not comply with
2/3/18 12:05:08  NA Trap. Event Description: " " Event Name: "Device Configuration Change" Timestamp: 92822960 Su
2/2/18 11:58:30  NA Trap. Event Description: "ACL Compliance Critical" Event Name: "Device Compliance Change" Time
2/2/18 2:55:48 A NA Trap. Event Description: " " Event Name: "Device Configuration Change" Timestamp: 85206885 Su
Updated: 2/5/18 01:41:39 AM          Total: 66          Selected: 0          Filter: OFF
```

Figure 4. NOM's rich UX with dashboards and navigation to operational views

security update service and repository which provides patches for multiple vendors' equipment. It also monitors your network for equipment that is behind in these updates.

NOM Benefits

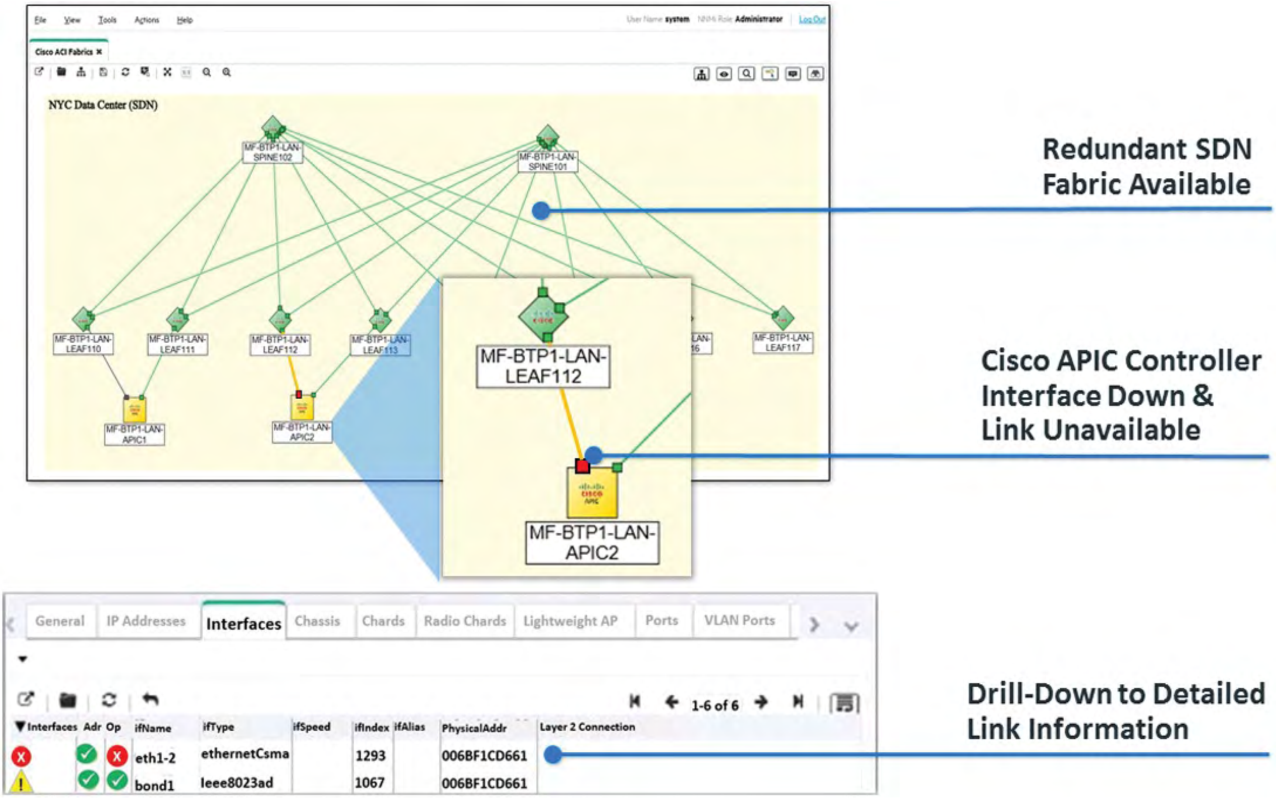
Accelerate Network Transformation with Unified Management of SDN, Virtual, Wireless and Physical Networks

Your adoption of new technologies to gain business benefits should not be slowed down by your network management software. Leading the market adoption of new technologies, NOM provides a unified view of your heterogeneous network including SDN fabric, virtual (host-based) networks, and physical devices. NOM includes discovery, visualization, monitoring, diagnostics, configuration, and compliance management of all these network infrastructures, allowing network operators and engineers to have a consistent view across their modern infrastructure. This is critical as you begin to deploy SDN in specific regions of your network, and benefit from management of all networks from a single tool. Unlike network vendors' device management tools, NOM consolidates connections across multi-vendor heterogeneous networks, and its event subsystem translates complex technical messages into normalized content that works for a broader audience. This reduces the learning curve for both operators and engineers compared to those who use multiple management tools, and it identifies issues in one place, with a single source of truth.

Increase Network Availability and Performance

In Figure 5, NOM has discovered a Cisco ACI SDN network consisting of controllers, spine, leaf nodes, interfaces and links. We can readily see two issues: a configured down interface on APIC1 controller, and an interface error on APIC2 controller. NOM will track if the configuration of APIC1 was done by NOM within compliance. NOM also has more information on the errors coming from APIC2 as seen in its event browser in Figure 5 bottom. NOM's rich and accurate topology clearly shows these two controllers share the same SDN fabric and likely provide redundancy

Figure 5.
NOM's monitorinç
of Cisco SDN
includes fabric
health in addition
to performance
and configuration



Interfaces	Adr	Op	ifName	ifType	ifSpeed	ifIndex	ifAlias	PhysicalAddr	Layer 2 Connection
☒	✓	☒	eth1-2	ethernetCsma		1293		006BF1CD661	
⚠	✓	✓	bond1	Ieee8023ad		1067		006BF1CD661	

Redundant SDN Fabric Available

Cisco APIC Controller Interface Down & Link Unavailable

Drill-Down to Detailed Link Information

for each other. The network controllers are at risk of losing connection with its SDN fabric if additional failures occur, causing widespread connectivity and performance issues. NOM also informs if any SDN fabric is running non-compliant configurations and will show traffic and performance changes that may be related to configuration changes.

Ensuring Network Security While Delivering Network Services

Helping you to deliver high-level services to your customers, NOM assures your network's availability, performance across all deployed technologies, while maintaining compliance of network configurations.

NOM establishes and guards SDN, virtual, wireless and physical configurations so they adhere to your organization's compliance policies. NOM detects any deviation from these configurations, updates dashboards, and sends intelligent alerts to your NOC operators. And NOM goes even deeper by diagnosing the specific changes (for example a rogue device password change), and can be configured to automatically roll back those changes to return to a compliant configuration.

Costs of operating under compliance vs. non-compliance averaged four times lower cost per employee, in a recent study by the Ponemon Institute.[4]

CATO NETWORKS
November 2016

Performance Issues Due to Configuration Changes

Another unique visualization NOM provides are Diagnostic Analytics Views *(see Figure 6)*. When problems are the result of configuration changes to devices including SDN controllers, these views not only alert staff of critical performance changes, but overlays potentially related configuration changes that are possible causes. This will focus Operations to check out the configuration first, which is much more efficient than an events-only triage model.

Configuration indicators are shown at inflection points in the performance curve. This saves time looking for such relationships. From this view, its easy to drill down into a comparison of before/after configuration differences. This provides you the final piece of information to know if configuration is the cause.

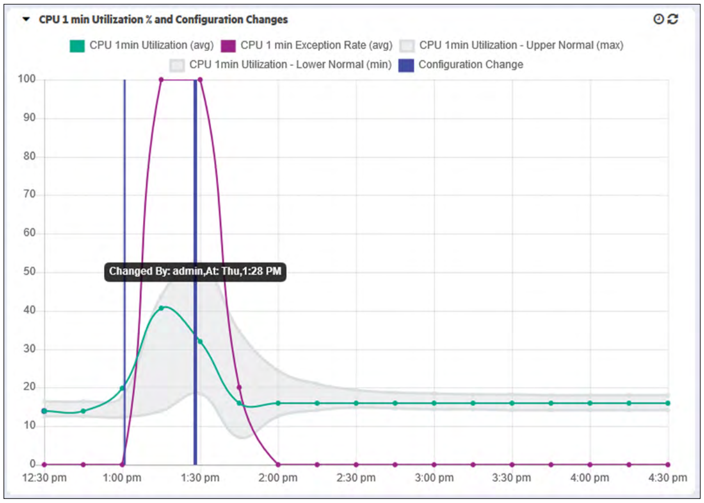


Figure 6. An example NOM Diagnostic Analytics view shows a configuration change caused CPU utilization spike

VIVACOM

50% faster problem resolution and 50,000 elements in a single management instance.

[4] **www.ponemon.org/blog/the-true-cost-of-compliance-a-benchmark-study-of-multinational-organizations**

Support Capacity Planning for Rollout of New Services

NOM collects numerous performance metrics and can present them as separate graphs *(see Figure 7)* or together along a network path. This provides greater insight than individual device metrics alone, as it helps "connect the dots" for performance, which is a collective analysis. Using a highly scalable columnar database, performance data is collected and can be analyzed in multiple ways. This valuable historic data drives capacity planning and supports investments in replacement or new network infrastructure. This data is critical for your decision-making for provisioning and associated configuration changes.

NOM's executive dashboards include a top-view of your entire network's security status. It's configurable to meet your specific network locations, and groups that are most important to you. In Figure 5, a globally distributed network's security status is summarized in a single dashboard suitable for everyone from upper management on down. From there, it's easy to navigate to a detailed view, and further on to a time-based view to correlate measurements of traffic volume and bandwidth, along with security items. In this example, the NYC network is at risk with 15 vulnerable devices out of compliance. There is a correlation with increased traffic affecting NYC and possibly San Francisco's networks. All this information helps Network Ops to focus its attention on things that matter, and notify Security Ops to quickly resolve security issues.

Rely on Comprehensive Reporting

NOM provides a rich and powerful set of executive and operational dashboards, drill-downs, and other reports for overall and specific areas of investigation. They are designed for operational, planning, and managerial oversight, and can be scheduled or user launched to investigate current issues including: asset planning, capacity planning, trend analysis, traffic engineering, and configuration and policy compliance.

NOM enables you to flexibly tune out-of-the-box reports that comply with Information Technology Infrastructure Library (ITIL) and Payment Card Industry (PCI) standards. NOM can be an important element to monitor and even prevent DDoS (Device Denial of Service) vulnerabilities.

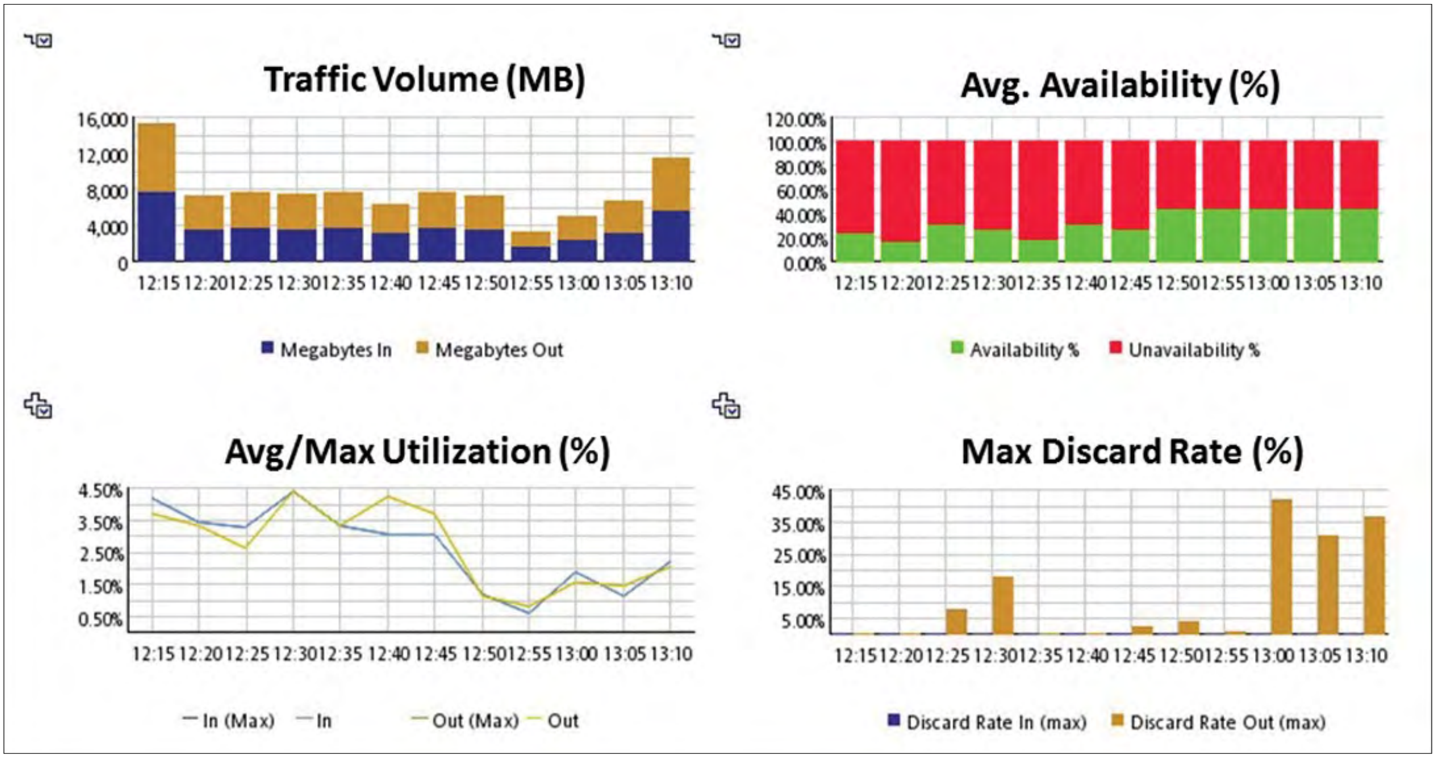


Figure 7. Example's of NOM's reporting

The Network Operations Management Difference

Network Operations Management is the industry's first network management solution that brings technologies, tools, people, and processes together in a new and collaborative model. Companies that deploy NOM can expect to see the following benefits:

- **By unifying the discovery, monitoring, diagnosis, and configuration management of the leading network technologies, vendors and protocols**, NOM breaks down siloes and becomes the definitive resource, delivering the single source of truth about your network. Knowledge and efficiency are increased, and MTTR is reduced.
- **Tool consolidation** reduces complexity, total cost of ownership, and brings teams together to solve problems, and plan for new provisioning. Comprehensive root-cause analysis and automated data gathering provide rich understanding of issues, elevates operators' knowledge, and encourages sharing with the engineering staff and collaboration between teams.
- **Highest single and multi-server scale** not only reduces TCO (Total Cost of Ownership), but consolidates management to provide you with understanding of the whole network vs. manual consolidation of work group and vendor-specific tools.
- **Advanced event management** consolidates raw events and presents higher-level root-cause events, but more importantly normalizes messages into terms that transcends specific technologies of vendors and protocols in your network. NOM elevates team knowledge of your network status and enables collaboration.
- **Comprehensive security defense capabilities.** NOM informs you when your network configurations are out of compliance with your company's policies. This has become a critical new role in network management, as security is no longer limited to your security operations team.
- **Automation accelerates productivity.** NOM provides the ability to automatically react to issues. The built-in orchestration workflow engine and included run-books, deliver the tools to mine for additional diagnostic information (before the evidence is gone), and even automatically remediate configuration changes that you deem appropriate. It's a powerful capability and can even be extended to provision extensions to your network, i.e., as new remote sites are added.

NOM is available in three editions with the following features:

Express	Premium	Ultimate
Network monitoring, device backup, and troubleshooting	**Express, plus:** Network traffic and quality reporting/ analysis and provisioning	**Premium, plus:** Monitoring advanced network fabric and compliance

Figure 8. NOM Editions

Easily Upgrade from Network Management Products to NOM

Our customer appreciation program makes it easy to upgrade licenses from OpenText™ NNMi and Network Automation products. Contact your OpenText™ sales representative and begin a guided journey to NOM at the Express, Premium, or Ultimate license level.

In addition to native support for Microsoft Windows and Linux operating systems, NOM is the first network management product to introduce a modern containerized foundation. The OpenText™ Container Deployment Foundation (CDF), is consumed in a form that delivers great value while removing the time and costs associated with administration of your network management solution. CDF includes powerful modern elements including Docker Containers and Kubernetes Services. The CDF will provide easy administration of critical services including automatic scaling and high-reliability deployment, using modern, industry-standard components and methods. NOM's CDF administration console provides more than initial software installation, adding easy patching and evening replacement of whole NOM sub-systems when required.

Learn more at
microfocus.com/nom

www.opentext.com

Connect with Us

opentext™