NetSecOps: Everything Network Managers Must Know About Collaborating with Security

Shamus McGillicuddy

Research Director
Enterprise Management Associates

Jon Kies

Manager of Network Management Product Marketing
Micro Focus

*IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING*

Featured Speakers

Shamus McGillicuddy, Research Director, EMA

Shamus has more than 12 years of experience in the IT industry, primarily as a journalist covering the network infrastructure market. At Enterprise Management Associates (EMA), he is the senior analyst for the network management practice. Prior to joining EMA, Shamus was the news director for TechTarget's networking publications. He led the news team's coverage of all networking topics, from the infrastructure layer to the management layer.

Jon Kies, Manager of Network Management Product Marketing, Micro Focus

Jon is responsible for Network Operations Management from Micro Focus and brings more than 20 years of product management and marketing experience with hardware and software products. Prior to Micro Focus, he started in Application Performance Management with Optimal Networks (later acquired by Compuware) and launched their first synthetic monitoring solution and followed that up with marketing management roles at both Check Point and Symantec.

Logistics

QUESTIONS

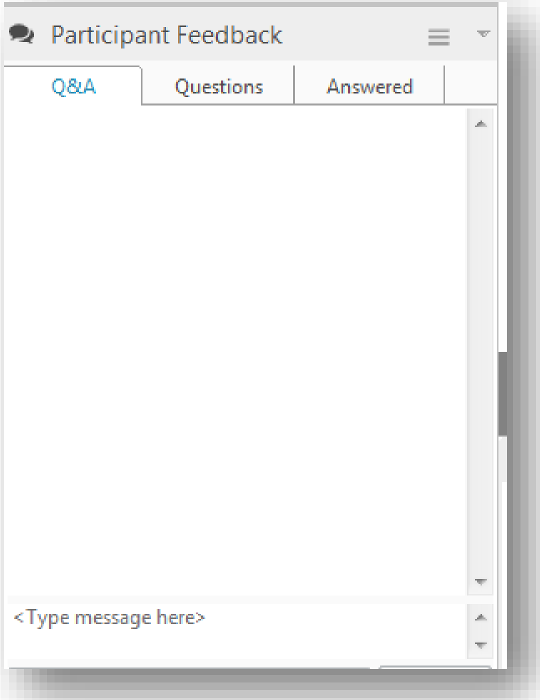
- Log questions in the chat panel located on the lower left-hand corner of your screen
- Questions will be addressed during the QandA session of the event

EVENT RECORDING

An archived version of the event recording will be available at www.enterprisemanagement.com

PDF SLIDES

A PDF of the speaker slides will be distributed to all attendees



IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

EMA Perspective on “NetSecOps”

Shamus McGillicuddy

Research Director
Enterprise Management Associates

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

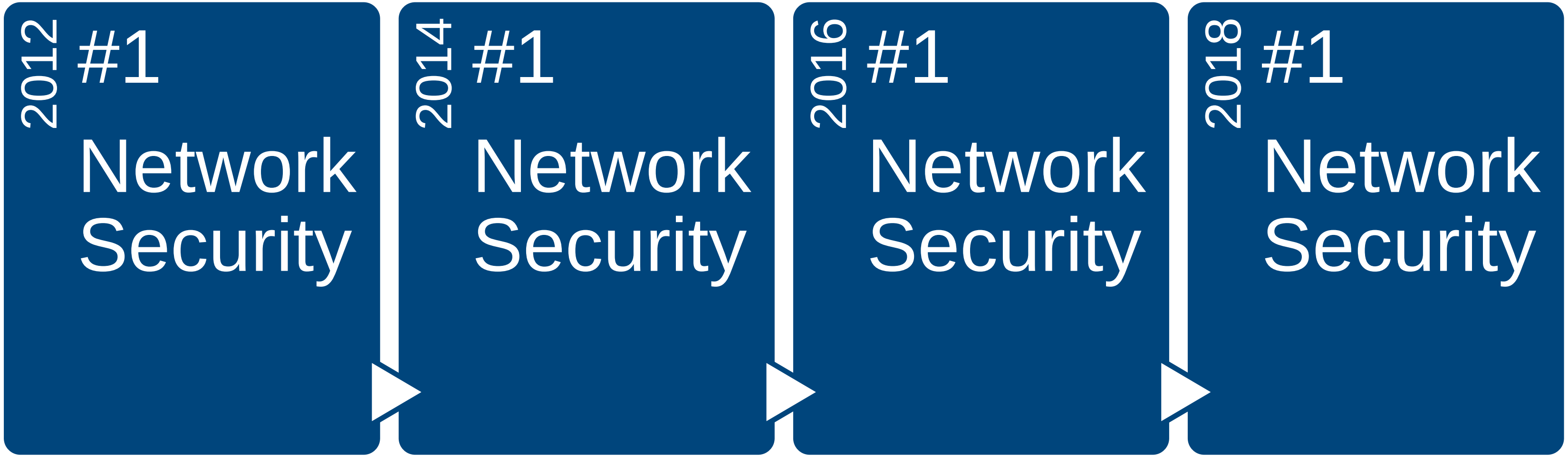
Agenda

- Network pros are security veterans
- NetOps/SecOps Collaboration Becoming Strategic Priority
- Examining NetOps/SecOps Convergence
- Technology Strategies for Collaboration

Network Pros Are Security Veterans

Security Has Been Top of Mind for Years

Networking initiatives that drive decision-making of network managers



2012 #1 Network Security

2014 #1 Network Security

2016 #1 Network Security

2018 #1 Network Security

They Focus on INFRASTRUCTURE, not Cyber Security

- Old school responsibilities:
  - Infrastructure patch management
  - Firewall/IPS management
  - VPNs and secure remote connectivity
  - Access control/guest management
  - Network segmentation

They Focus on Infrastructure, not CYBER SECURITY

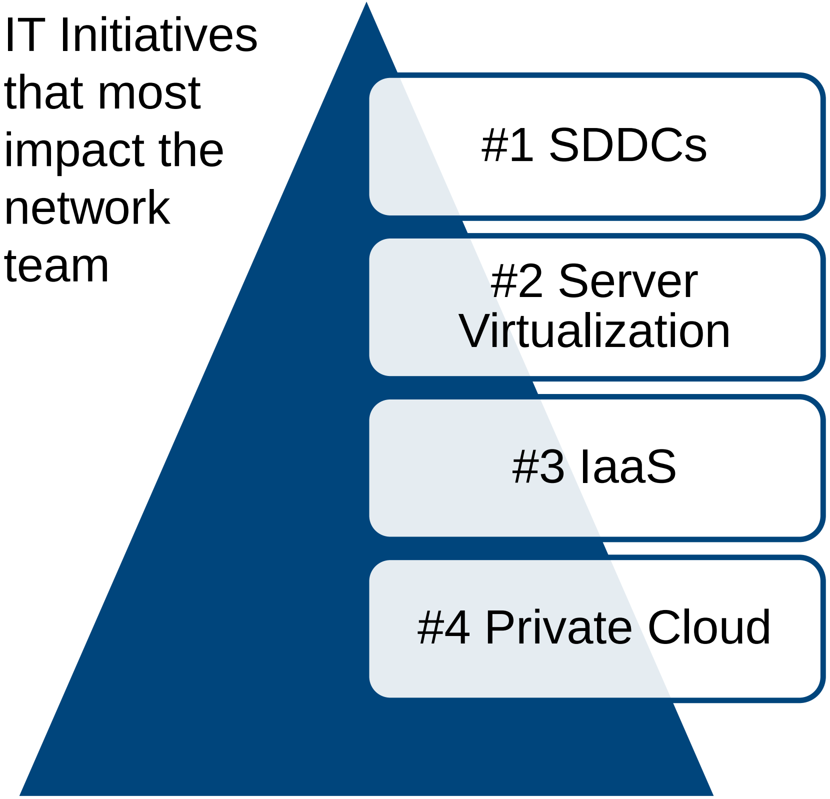
- Hands off attitude toward:
  - Behavioral analysis/security analytics
  - Threat monitoring
  - Malware protection
  - Security incident management

- But network data can support these tasks

NetOps/SecOps Collaboration Becoming Strategic Priority

Today’s Technology Initiatives Demand Different Approach to Security

IT Initiatives that most impact the network team



#1 SDDCs

#2 Server Virtualization

#3 IaaS

#4 Private Cloud

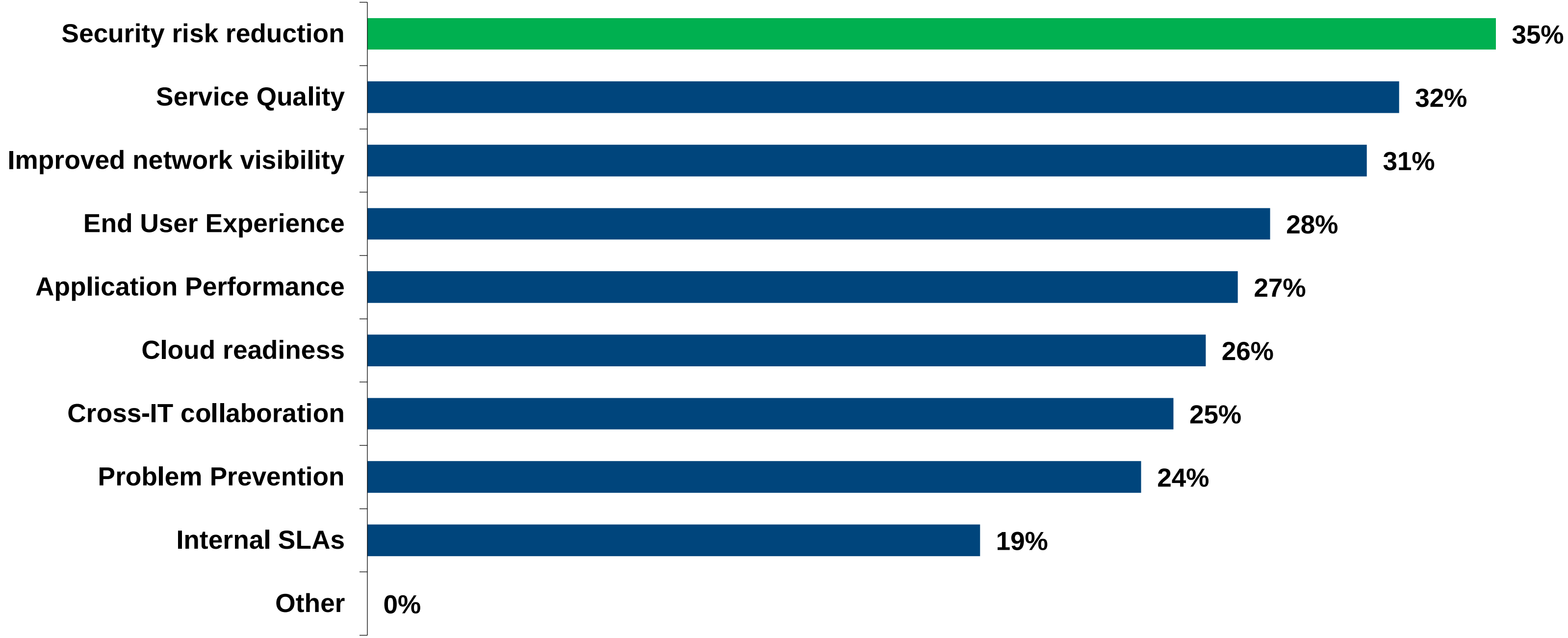
- Perimeter disappears
- Rate of change accelerates
- Endpoint diversity expands
- Critical services vulnerable to disruption, not just penetration

Network Service Assurance and Security are Linked

- Root Causes of Complex IT Service Issues and Outages
  1. Network infrastructure (40%)
  2. Security-related issues (37%)
     - Infected hosts
     - DDoS attacks
  3. End client system or user error (34%)
  4. Security systems (33%)
     - Legitimate traffic blocked
     - Inline security systems oversubscribed

Network Managers Need to Reduce Security Risk

Concepts that are becoming most important to measuring network management success

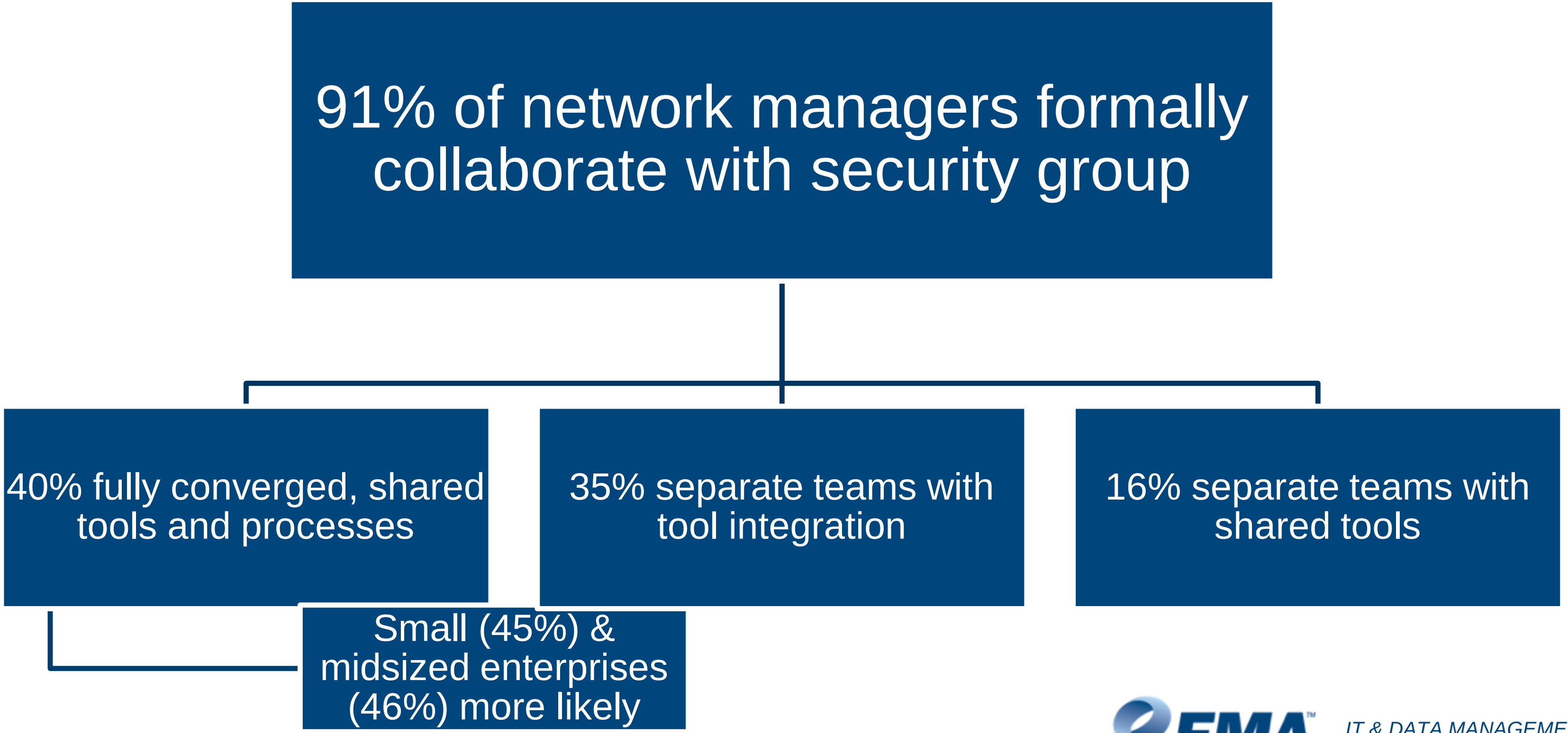


Security is Pulling Network Management in a New Direction

- With whom are you increasing collaboration?
  - #1 IT security/cyber security (46%)
- Which systems do you integrate with network management tools?
  - #2 Security monitoring systems (33%)
- Who uses custom or role-based views into your network management tools?
  - #2 IT security (42%)
- Which network management product features add the most value?
  - #1 Integrated security-related insights (19%)

Examining NetOps/SecOps Convergence

Most Enterprises Report Collaboration Between NetOps and SecOps



91% of network managers formally collaborate with security group

40% fully converged, shared tools and processes

35% separate teams with tool integration

16% separate teams with shared tools

Small (45%) & midsized enterprises (46%) more likely

Most Enterprises Report Collaboration Between NetOps and SecOps

- This collaboration isn't easy
  - IT leadership needs to step up
  - New tools or new integration required
  - New best practices/processes needed

What is Bringing NetOps & SecOps Together?

- OpEx reduction (38%)
- Risk reduction (37%)
- Streamlined workflows (34%)
- Responsiveness to change in business (31%
- CapEx efficiencies (31%)

Critical Points of Collaboration with Security

Infrastructure design & deployment

38%

Event/incident monitoring

31%

Incident response

27%

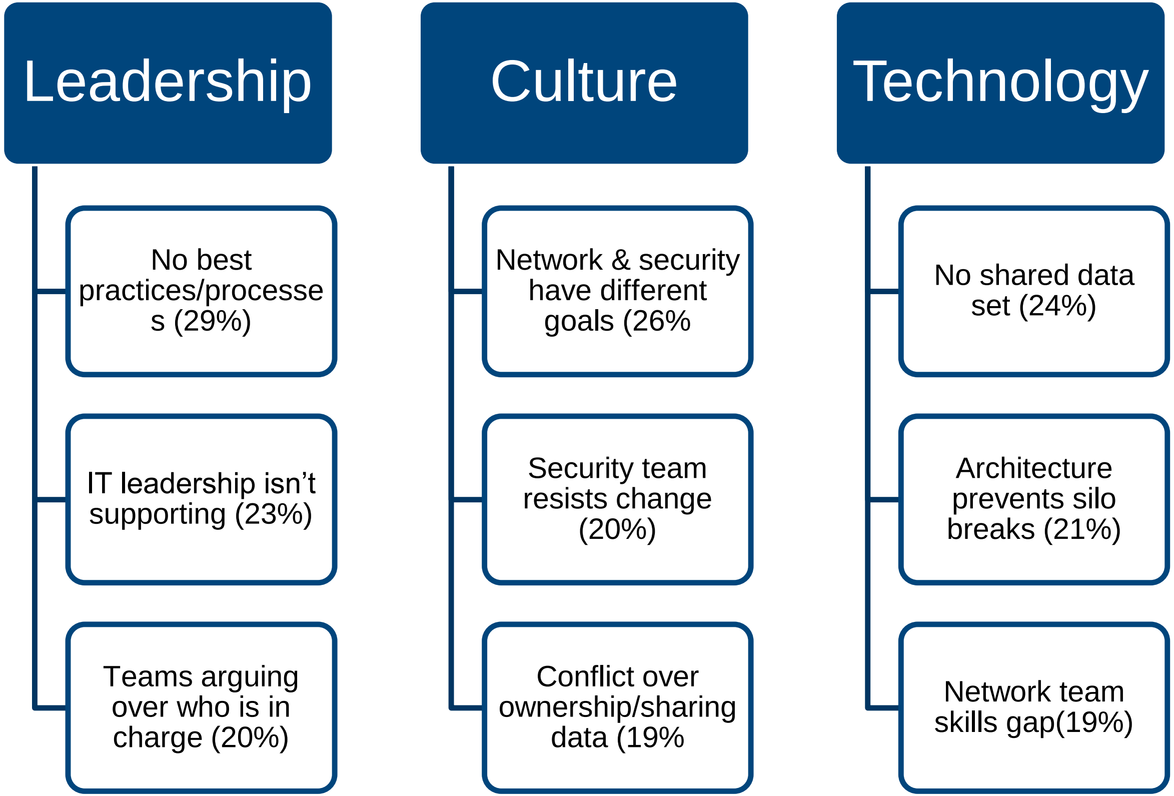
Change management/patch management

26%

Policy verification/validation

24%

Culture, Technology, and Bad Leadership Get in the Way



Leadership

- No best practices/processe s (29%)
- IT leadership isn’t supporting (23%)
- Teams arguing over who is in charge (20%)

Culture

- Network & security have different goals (26%
- Security team resists change (20%)
- Conflict over ownership/sharing data (19%

Technology

- No shared data set (24%)
- Architecture prevents silo breaks (21%)
- Network team skills gap(19%)

Technology Strategy for Collaboration

Critical Tools in Each Silo

- Network managers identify technology that supports collaboration
  - Network management tools
    - Network performance monitoring (33%)
    - Advance network analytics (32%)
    - NCCM (31%)
  - Security management tools
    - Security analytics (31%)
    - SIEM (24%)
    - Threat intelligence feeds (23%)
    - DDoS detection/prevention (21%)
    - NGFWs/UTMs (21%)

Options for Bringing Tools Together

Shared tools

- Integrated workflows
- Collaboration
- Single data set

Integrated tools

- Separate workflows
- Some collaboration
- Shared data

Shared data set

- One data lake feeding separate tools
- No workflow integration
- No collaboration

The Essential Role of Network Automation

- Network teams are focused on automation
  - 92% are expanding their use of network automation
  - 70% say this is a high priority

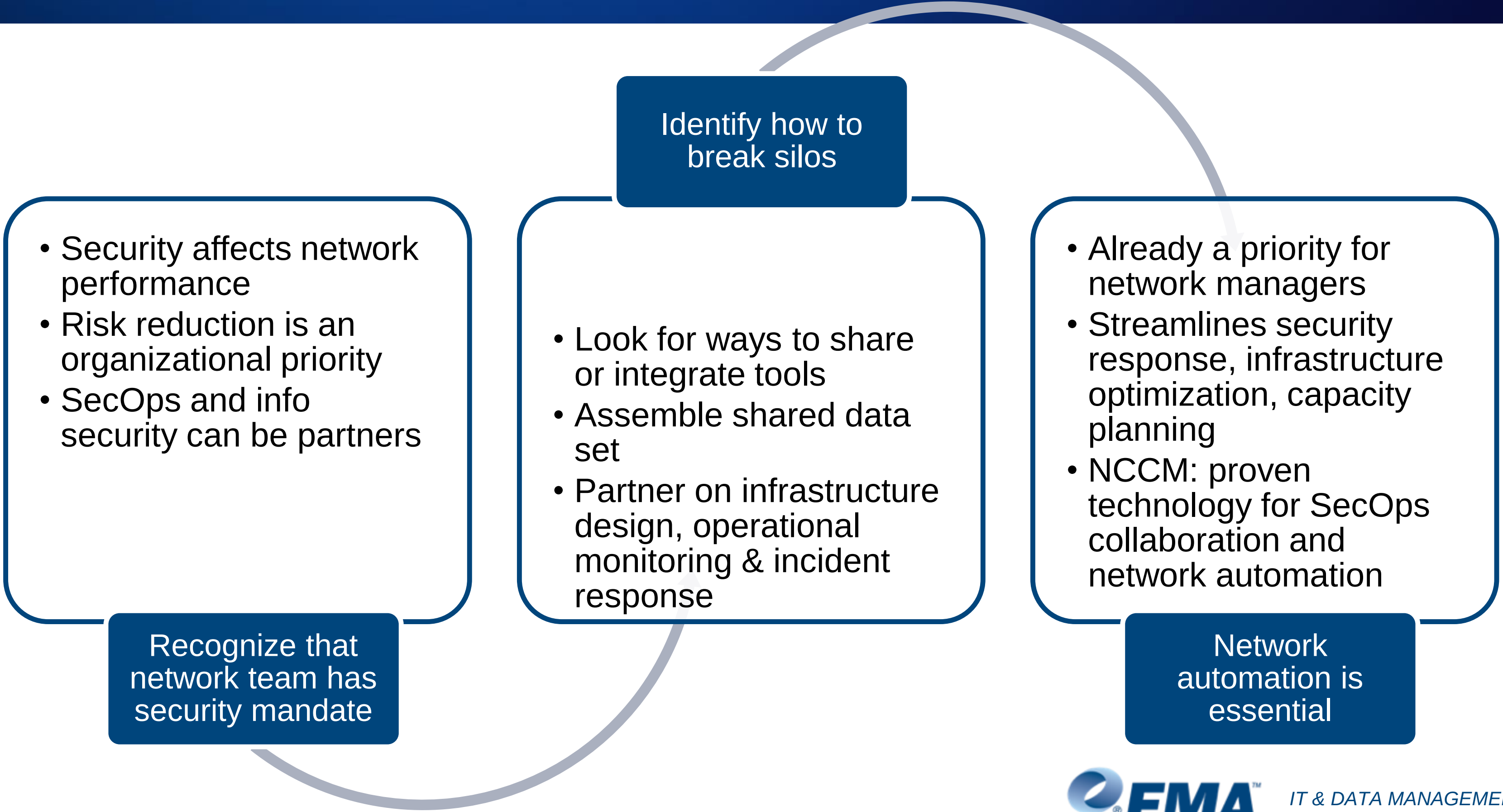
- Top 4 benefits of network automation
  - **Security risk reduction (34%)**
  - Improved collaboration across IT (32%)
  - Rapid response to service problems (28%)
  - Increased network agility (28%)

Network Automation Strategies

- Technology options
  - SDN (40%)
  - NCCM (38%)
  - SD-WAN (38%)

- Tasks network managers want to automate
  - Network optimization (49%)
  - Security incident response (47%)
  - Network capacity planning (40%

Roadmap for NetSecOps Success



Recognize that network team has security mandate

- Security affects network performance
- Risk reduction is an organizational priority
- SecOps and info security can be partners

Identify how to break silos

- Look for ways to share or integrate tools
- Assemble shared data set
- Partner on infrastructure design, operational monitoring & incident response

Network automation is essential

- Already a priority for network managers
- Streamlines security response, infrastructure optimization, capacity planning
- NCCM: proven technology for SecOps collaboration and network automation

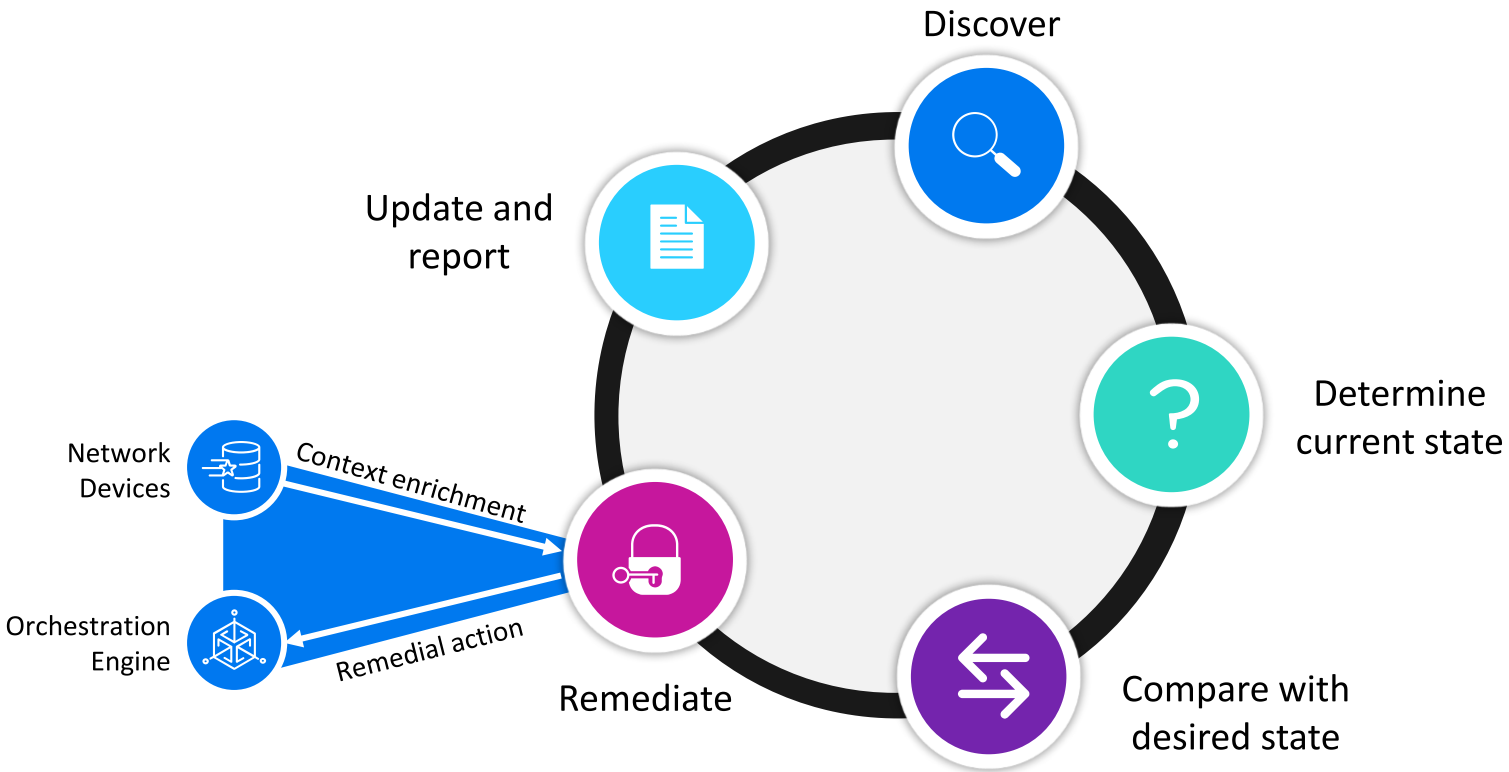
MICRO FOCUS®

Automation is the key to driving NetSecOps

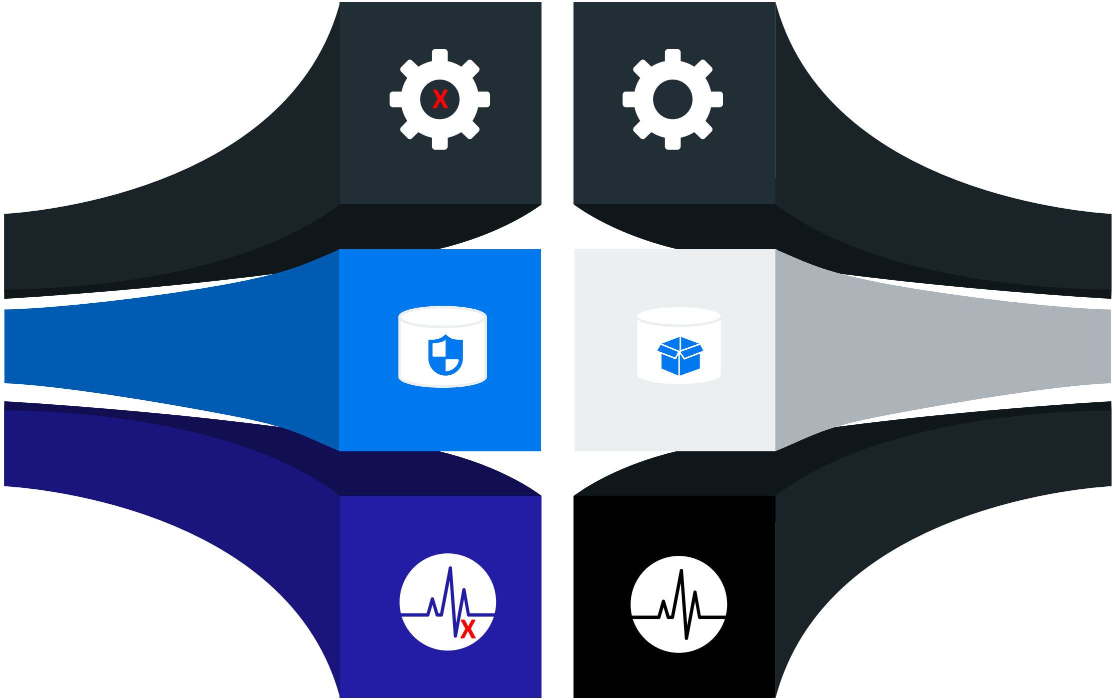
Jon Kies

Manager, Network Operations Management

Security compliance & automated remediation



Overlaps and gaps



IT Security

We can’t automate remediation

We maintain a security configuration DB

We monitor the environment, find issues, but can’t fix them

IT Operations

We have automation tools

We maintain an asset configuration DB

We monitor the environment, find issues and fix them

Zero-day exploits aren’t the issue!

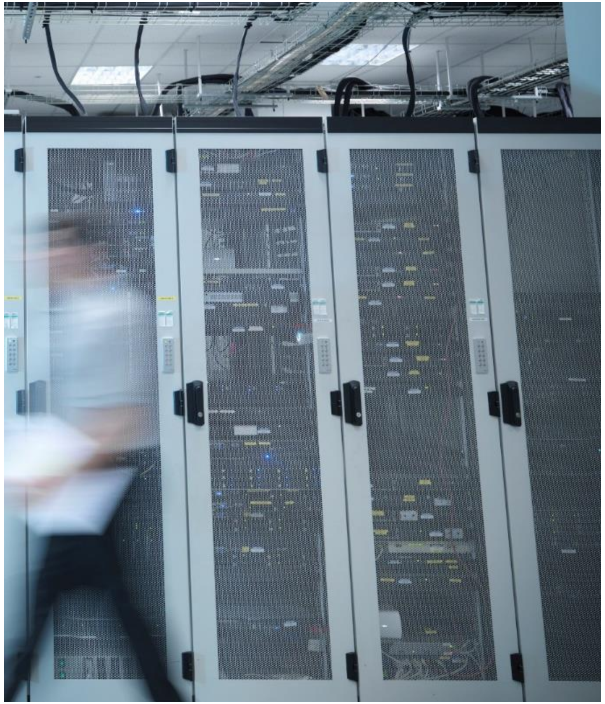
The top 10 *known vulnerabilities* account for 85% of successful exploits.

verizon✓

Source: Verizon’s 2016 Data Breach Investigations Report

Vulnerabilities are overwhelming network teams

Multi-vendor networks and the high rate of vulnerabilities



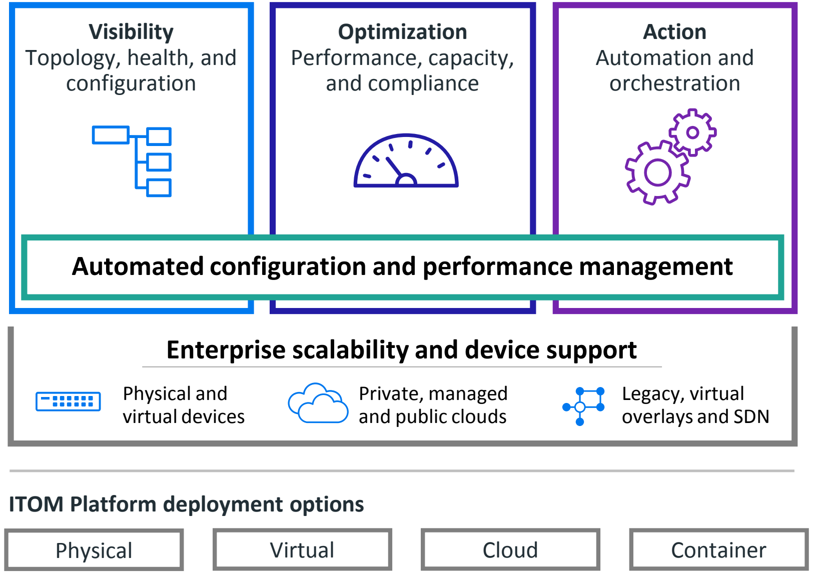
- Even single-vendor networks can result in hundreds of vulnerabilities/year
  - As of April 16, 2018 CISCO alone has identified 1,200+ CVEs[1]
- NIST has listed 4,700+ CVEs[2] for same time period

[1] Source Cisco Security website search through April 16, 2018. Includes multivendor CVEs (Common Vulnerabilities and Exposures)

[2] Source NIST website search through April 16, 2018.

Network Operations Management

Manage, automate, and ensure compliance for traditional, virtual, wireless and software-defined networks



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

ITOM Platform deployment options

Physical

Virtual

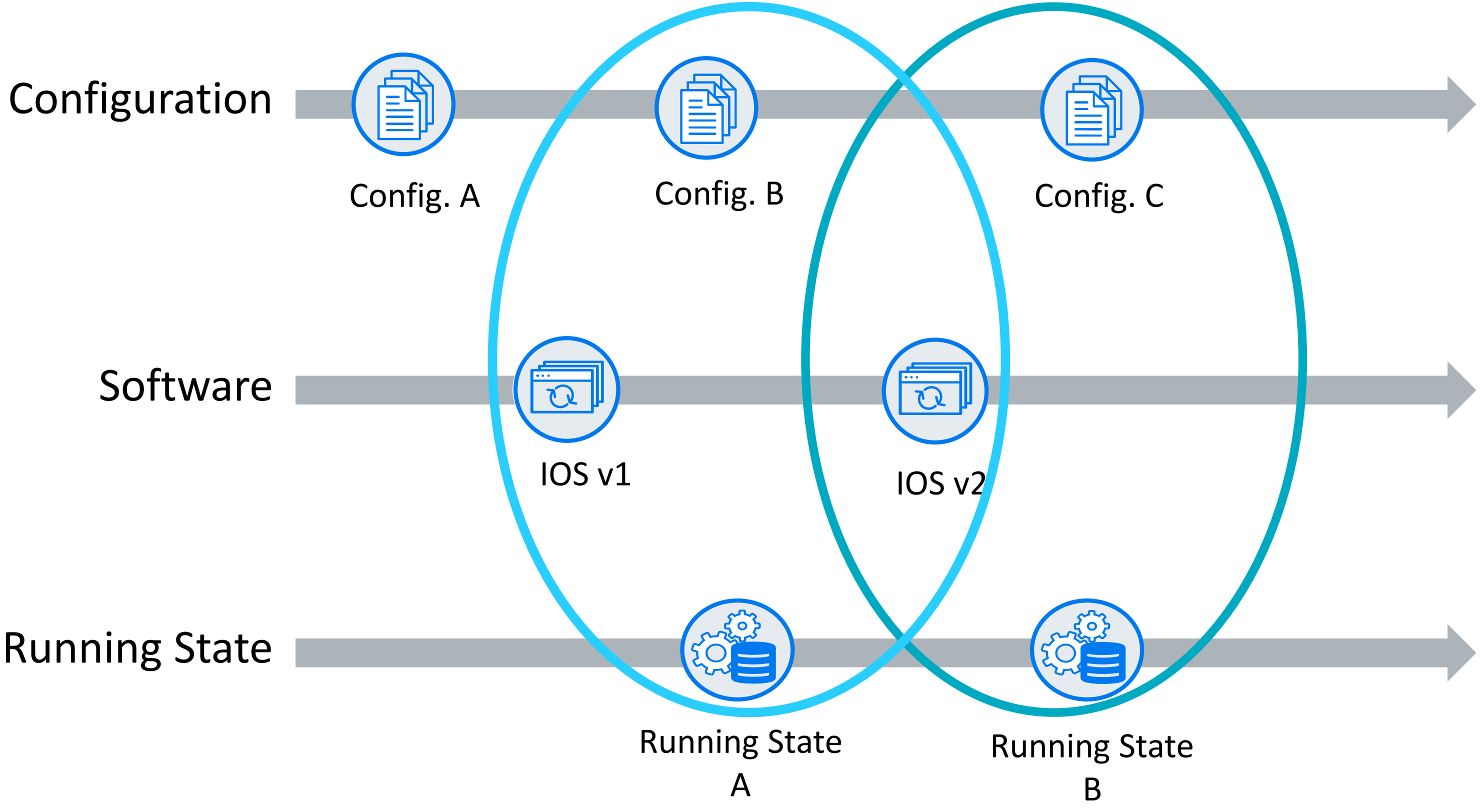
Cloud

Container

- Industry-leading support for physical, virtual, wireless, and SDN-enabled devices
- Single toolset delivers performance management and configuration
- Network-focused orchestration content speeds service delivery
- Policy-based audit and remediation drives security compliance
- Capacity and configuration modeling tools enable effective planning

3-dimensional compliance model

Device is fully compliant when the 3 dimensions are examined together

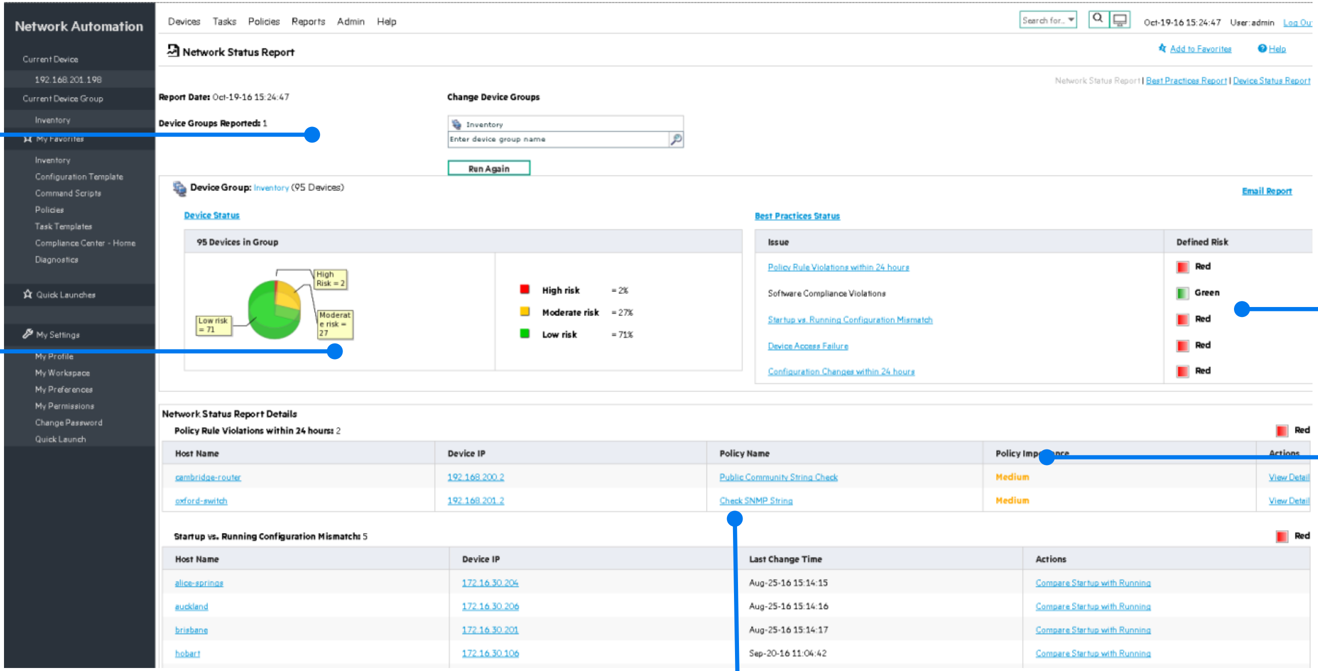


Decreasing risk and improving operations

Policy-based audit and remediation drives security compliance

Groupings allow compliance granularity

Easy-to-read charts provide compliance risk at a glance



Network Status Report

Report Date: Oct-19-16 15:24:47

Device Groups Reported: 1

Change Device Groups

Device Group: Inventory (95 Devices)

Device Status

95 Devices in Group		
🟥	**High risk**	= 2%
🟨	**Moderate risk**	= 27%
🟩	**Low risk**	= 71%

Best Practices Status

Issue	Defined Risk
Policy Rule Violations within 24 hours	🟥 Red
Software Compliance Violations	🟩 Green
Startup vs. Running Configuration Mismatch	🟥 Red
Device Access Failure	🟥 Red
Configuration Changes within 24 hours	🟥 Red

Network Status Report Details

Policy Rule Violations within 24 hours: 2 🟥 Red

Host Name	Device IP	Policy Name	Policy Importance	Actions
cambridge-router	192.168.200.2	Public Community String Check	Medium	View Detail
oxford-switch	192.168.201.2	Check SNMP String	Medium	View Detail

Startup vs. Running Configuration Mismatch: 5 🟥 Red

Host Name	Device IP	Last Change Time	Actions
alice-springs	172.16.30.204	Aug-25-16 15:14:15	Compare Startup with Running
auckland	172.16.30.206	Aug-25-16 15:14:16	Compare Startup with Running
brisbane	172.16.30.201	Aug-25-16 15:14:17	Compare Startup with Running
hobart	172.16.30.106	Sep-20-16 11:04:42	Compare Startup with Running

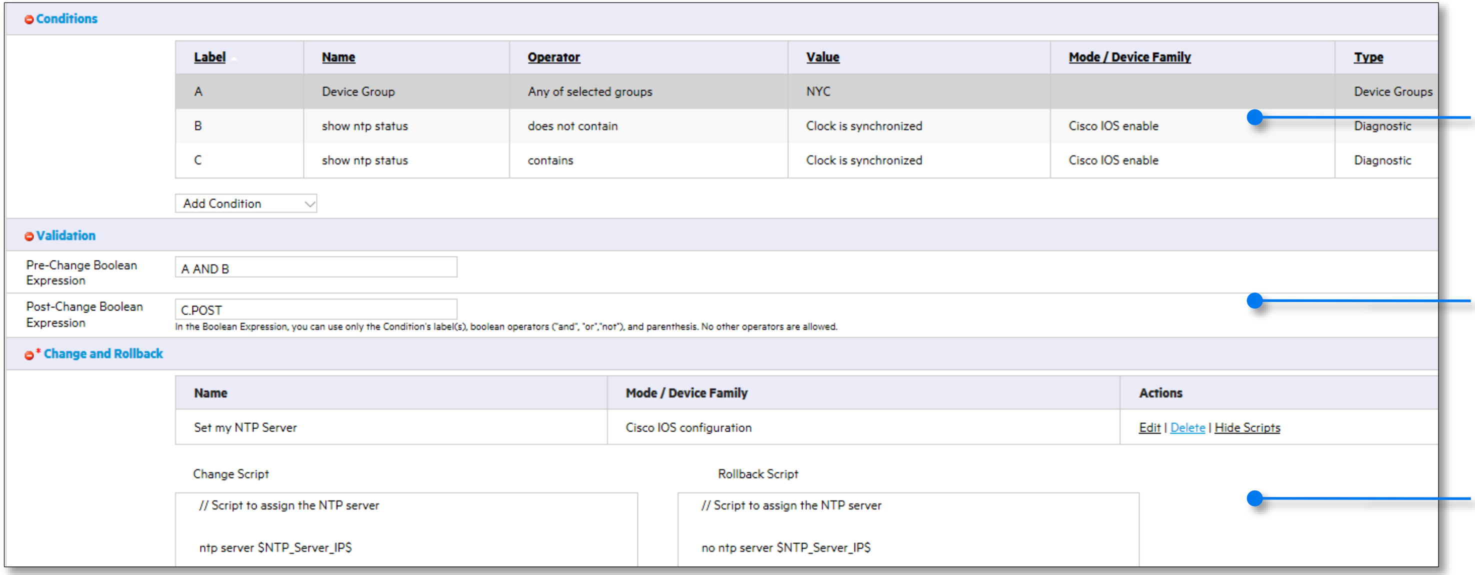
Quick view shows recent changes and config events

Policy importance levels allows for prioritization

Subscription service delivers ongoing security policy

Change Plans

Automated configuration change driven by logic



Conditions

Label	Name	Operator	Value	Mode / Device Family	Type
A	Device Group	Any of selected groups	NYC		Device Groups
B	show ntp status	does not contain	Clock is synchronized	Cisco IOS enable	Diagnostic
C	show ntp status	contains	Clock is synchronized	Cisco IOS enable	Diagnostic

Add Condition

Validation

Pre-Change Boolean Expression	A AND B
Post-Change Boolean Expression	C.POST

In the Boolean Expression, you can use only the Condition's label(s), boolean operators ("and", "or","not"), and parenthesis. No other operators are allowed.

*** Change and Rollback**

Name	Mode / Device Family	Actions
Set my NTP Server	Cisco IOS configuration	Edit | Delete | Hide Scripts

Change Script

```
// Script to assign the NTP server

ntp server $NTP_Server_IP$
```

Rollback Script

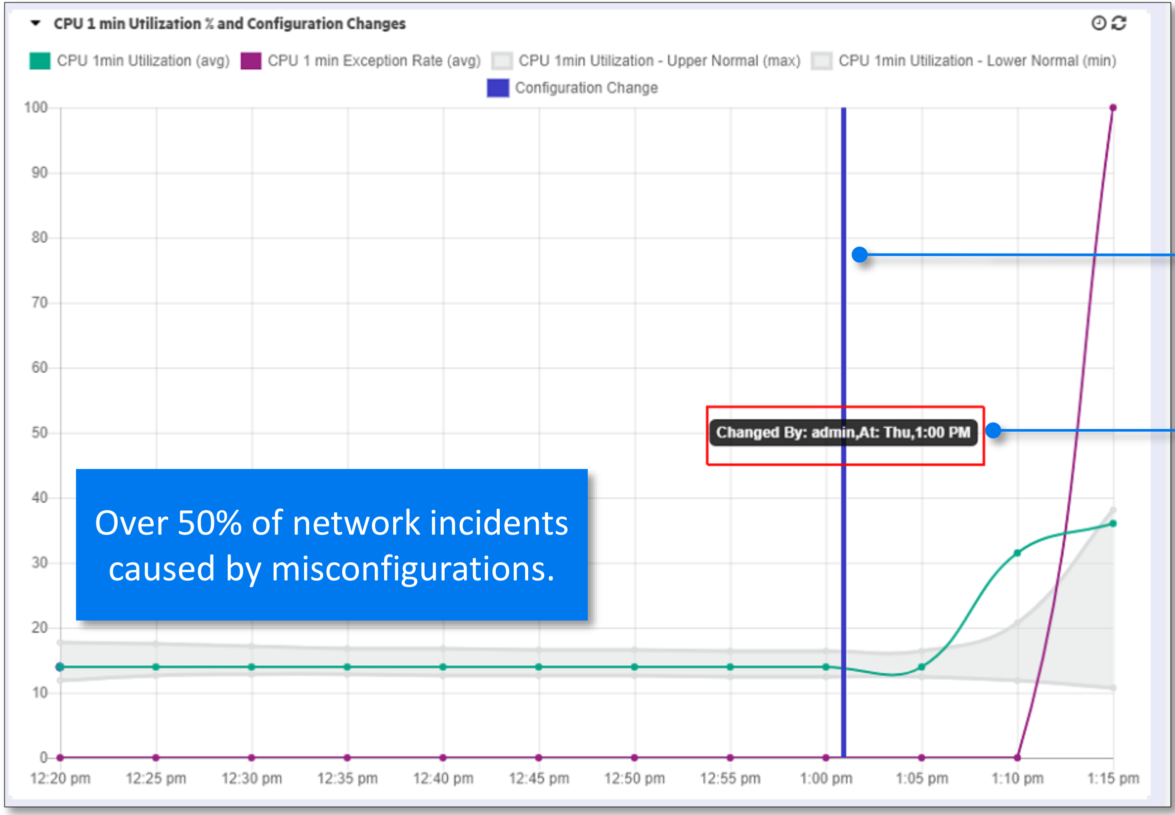
```
// Script to assign the NTP server

no ntp server $NTP_Server_IP$
```

Conditions

Validation

Change or Rollback

Change-correlated performance views



Changed By: admin,At: Thu,1:00 PM

Over 50% of network incidents caused by misconfigurations.

Configuration change indicators

Hover to view who made the change and when

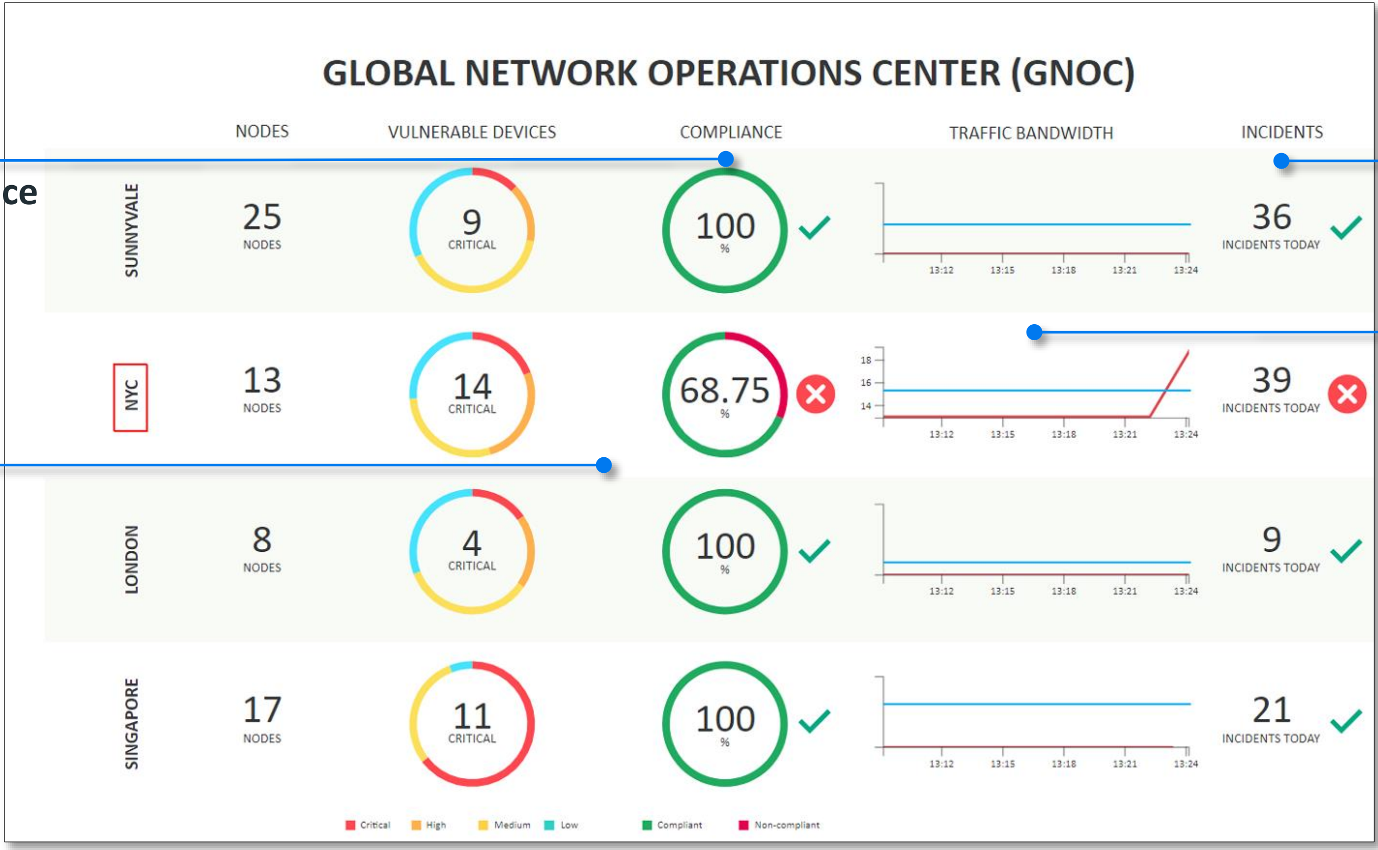
Executive Dashboards

Compliance Data

KPIs provided by NOM

Root Causes

Improvement Opportunity



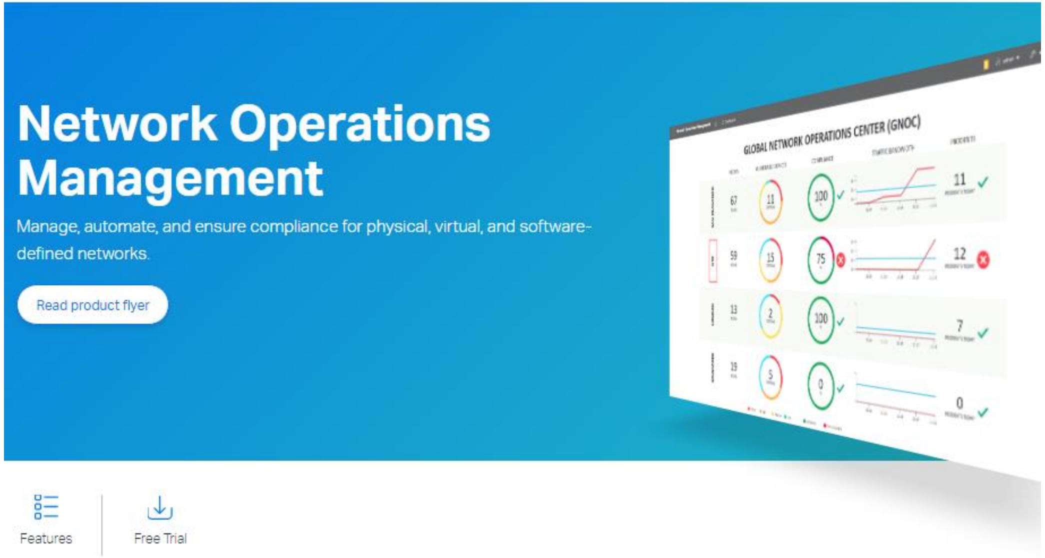
GLOBAL NETWORK OPERATIONS CENTER (GNOC)

	NODES	VULNERABLE DEVICES	COMPLIANCE	TRAFFIC BANDWIDTH	INCIDENTS
SUNNYVALE	25 NODES	9 CRITICAL	100 % ✓		36 INCIDENTS TODAY ✓
NYC	13 NODES	14 CRITICAL	68.75 % ☒		39 INCIDENTS TODAY ☒
LONDON	8 NODES	4 CRITICAL	100 % ✓		9 INCIDENTS TODAY ✓
SINGAPORE	17 NODES	11 CRITICAL	100 % ✓		21 INCIDENTS TODAY ✓

🟥 Critical 🟧 High 🟨 Medium 🟦 Low 🟩 Compliant 🟥 Non-compliant

For more information

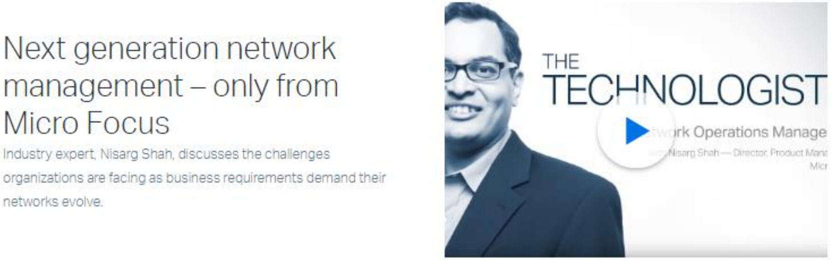
- **Network Operations Management:** Brochures, Case Studies, Videos, Whitepapers, Trials, … www.microfocus.com/nom
- **Blog:** [Join the discussion!]()
- **LinkedIn:** [MF Network Mgmt Group]()



Network Operations Management

Manage, automate, and ensure compliance for physical, virtual, and software-defined networks.

Read product flyer



Next generation network management – only from Micro Focus

Industry expert, Nisarg Shah, discusses the challenges organizations are facing as business requirements demand their networks evolve.

MICRO®
FOCUS