Breaking Free from IT Inefficiency

UNLOCKING VALUE WITH NETWORK AUTOMATION

Hidden within your IT budget lies a significant tangible cost: inefficiency. The main reason is that the critical role IT plays in driving innovation and supporting growth is at odds with today's manual workflows.

A recent study found that 75% of CIOs struggle to strike the right balance between business innovation and operational excellence. This struggle arises because focusing on operational excellence may seem to come at the expense of innovation and growth. For all their excitement about digital transformation, AI, or cloud computing, enterprises spend most of their time simply keeping the lights on.

Network automation is fundamentally changing this predicament culturally to empower IT network and support teams to do more — much more — with less.

This eBook delves into the hidden costs of IT inefficiency, exploring how it impacts business performance and highlighting the critical role of network automation in addressing these challenges.

Table of Contents

CHAPTER 1

The Price of Inefficiency

Beyond the obvious expenses like hardware and software, IT inefficiency carries a significant hidden cost. Let's explore some key areas:

Lost Productivity:

- Network outages and slow response times directly impact employee productivity. When employees can't access critical applications or data, their work grinds to a halt. This translates to lost hours, missed deadlines, and ultimately, reduced revenue.
- Imagine a scenario where a critical network outage disrupts trading operations for a financial institution. The financial impact could be substantial, with lost trades and damaged customer relationships.

Missed Opportunities:

- IT inefficiencies can hinder innovation and slow down time-to-market for new products and services. Manual processes and reactive maintenance can delay the deployment of new applications and services, stifling business growth.
- For example, a lengthy approval process for network changes can delay the launch of new online services, giving competitors a significant advantage.

Reputation and Risk:

- Network outages and security breaches not only disrupt business operations but also damage brand reputation. Customers lose trust in companies that experience frequent service disruptions.
- Security breaches can lead to data loss, financial losses, and regulatory fines.
- A single major outage can have a lasting negative impact on a company's reputation and customer loyalty.
- Consider the impact on a retail company during peak holiday shopping season. A network outage could cripple online sales, leading to lost revenue and frustrated customers.

Impact on Innovation:

- A constant focus on firefighting and resolving operational issues leaves little room for innovation and strategic initiatives. IT teams become so bogged down in maintaining existing systems that they have limited time and resources to explore new technologies, develop new applications, or support strategic business initiatives.
- This can hinder a company's ability to adapt to changing market conditions, respond to new opportunities, and gain a competitive advantage.

CHAPTER 2

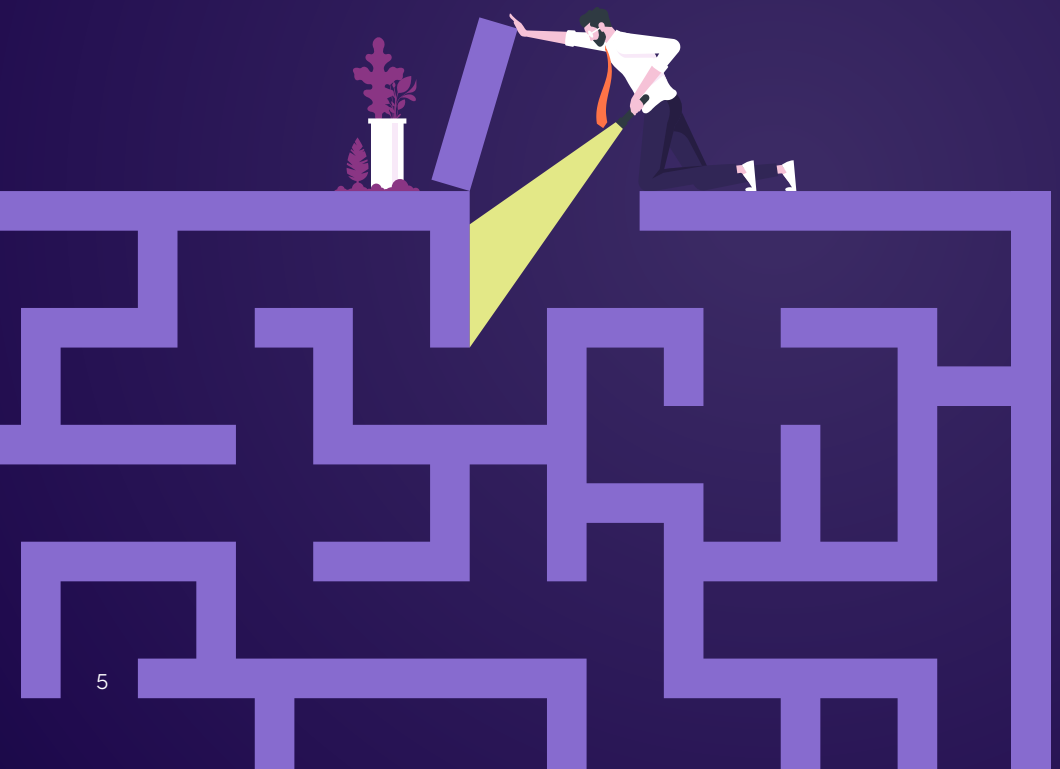
The Root Causes of Inefficiency

THE LEGACY OF INEFFICIENT PRACTICES

Traditional IT operations have often relied on manual processes, reactive maintenance, and siloed teams. These legacy practices can no longer keep pace with the evolving needs of modern businesses.

Manual Processes:

- Managing network configurations, provisioning new devices, and troubleshooting network issues manually is time-consuming, error-prone, and inefficient. This leads to delays, inconsistencies, and a higher risk of human error.
- For example, manually configuring hundreds of switches across a distributed enterprise is not only time-consuming but also prone to human error, which can lead to misconfigurations and network outages.



Reactive Maintenance:

- A reactive approach to maintenance, where issues are addressed only after they occur, can lead to prolonged downtime, increased costs, and a negative impact on user experience.
- This is like waiting for your car to break down before getting it serviced, leading to unexpected expenses and inconvenience.

Siloed Teams:

- When IT teams are siloed, communication and collaboration can be hindered, leading to inefficiencies and delays in resolving issues.
- For example, if the network team and the security team are not working together, security vulnerabilities may go undetected, leading to potential breaches.

THE COMPLEXITY CONUNDRUM

The rise of cloud computing, virtualization, and the proliferation of devices and applications has significantly increased the complexity of IT environments.

- **Hybrid Cloud Environments:** Managing hybrid cloud environments that span on-premises, private, and public clouds presents significant challenges, including increased network complexity, security risks, and the need for robust orchestration and automation.
- **The Internet of Things (IoT):** The proliferation of IoT devices has generated a massive increase in network traffic and created new security challenges. Managing and securing these devices requires sophisticated network management tools and strategies.
- **Edge Computing:** The emergence of edge computing adds another layer of complexity, requiring distributed network management and orchestration capabilities.

This complexity makes it increasingly difficult to manage and maintain network operations using traditional methods. Manual processes and reactive approaches are simply not

CHAPTER 3

Rethinking IT Service Delivery: Embracing Network Automation

SHIFTING FROM REACTIVE TO PROACTIVES

To address these challenges, IT organizations must shift from a reactive to a proactive approach to IT operations. This involves moving away from a break-fix model, where issues are addressed only after they occur, to a proactive model that focuses on preventing issues before they happen.

THE POWER OF NETWORK AUTOMATION

Network automation empowers IT teams to streamline manual tasks, reduce human error, and improve operational efficiency. By automating routine tasks, such as provisioning new devices, configuring network settings, and troubleshooting network issues, IT teams can free up valuable time and resources to focus on more strategic initiatives.

- Increased Speed and Efficiency: Automation can significantly reduce the time required to complete routine tasks, such as provisioning new devices or configuring network settings.
- For example, instead of manually configuring hundreds of switches across a distributed enterprise, automation can automate the entire process, saving significant time and reducing the risk of human error.
- Reduced Errors and Improved Consistency: Automation can help eliminate human error, ensuring that tasks are performed consistently and accurately every time. This can reduce the risk of misconfigurations, improve network stability, and enhance overall network performance.
- Enhanced Network Visibility: Automation can provide greater visibility into network operations, allowing IT teams to identify and address potential issues before they impact business operations.
- For example, automation can collect real-time data from network devices and use this data to identify and predict potential problems, such as network congestion or security threats.

CHAPTER 4

Building a Successful Automation Strategy

KEY COMPONENTS OF AN AUTOMATION STRATEGY

Building a successful network automation strategy requires careful planning and execution. Key components include:

Defining Clear Objectives and Setting Measurable Goals:

- Clearly define the specific business outcomes that you hope to achieve through automation.
  - For example, reduce MTTR (Mean Time to Repair) by 50%, increase network availability by 99.99%, or accelerate the deployment of new services by 20%.
- Set SMART goals (Specific, Measurable, Achievable, Relevant, and Time-bound) for your automation initiatives.
  - For example, "Reduce MTTR for network outages by 20% within the next quarter."

Selecting the Right Tools and Technologies:

- Evaluate different automation tools and technologies based on your specific needs, budget, and technical requirements.
  - Consider factors such as ease of use, scalability, integration capabilities, vendor support, and the availability of skilled resources.
  - Research and compare different automation platforms, such as those offered by NetBrain, Cisco, Juniper, and other leading vendors.

Developing a Skilled Workforce with the Necessary Automation Expertise:

- Invest in training and development programs to upskill your existing IT staff.
  - Consider hiring new talent with automation expertise.
  - Implement a knowledge sharing program to encourage collaboration and knowledge transfer within your team.
  - Organize workshops, training sessions, and certifications to help your team develop the necessary automation skills.

Building a Strong Data Foundation to Support Automation Initiatives:

- Ensure that your network data is accurate, complete, and readily accessible for automation tools to consume.
- Invest in data quality initiatives and implement data governance processes to improve data accuracy and consistency.
- Develop a centralized data repository to store and manage network data.
- Use network discovery and mapping tools to gain a comprehensive understanding of your network topology and dependencies.

Prioritizing a Phased Approach to Implementation:

- Start with small, manageable projects and gradually expand the scope of automation over time.
- This phased approach will help you minimize risk, build momentum, and demonstrate the value of automation to your organization.
- Begin with simple automation tasks, such as automating routine configuration changes or generating basic reports.
- Gradually increase the complexity of your automation initiatives, such as implementing automated network

CHAPTER 5

The Bottom-Line Impact of Modern O&M Approaches

Where to Find Significant Cost Savings

- **Reduced Labor Costs:** Automation can significantly reduce the amount of time IT staff spend on mundane tasks, such as provisioning new devices, configuring network settings, and troubleshooting network issues.
  - This frees up valuable IT resources to focus on more strategic initiatives, such as innovation, security enhancements, and improving the overall user experience.
  - A study by Gartner found that organizations that have implemented network automation have seen an average of 20% reduction in operational costs.
- **Lower Energy Consumption:** Automation can optimize network utilization, reducing energy consumption and associated costs.
  - For example, by automating power management features, you can reduce energy consumption during off-peak hours and minimize your carbon footprint.
- **Reduced Hardware and Software Costs:** By improving network efficiency and reducing the need for manual intervention, automation can help you optimize your IT infrastructure and reduce hardware and software costs.
  - For example, by automating capacity planning, you can avoid over-provisioning of network resources, leading to cost savings on hardware and software licenses.

Improved Efficiency and Productivity:

- **Faster Response Times:** Automation can significantly reduce the time required to resolve network issues, leading to faster service restoration and minimizing downtime.
  - For example, automated troubleshooting scripts can quickly identify and resolve common network problems, reducing the time spent on manual troubleshooting.
- **Increased Network Availability:** By proactively identifying and addressing potential issues, automation can help ensure that your network is always available and reliable.
  - This translates to increased employee productivity, as employees can rely on a stable and consistent network connection to perform their work effectively.
- **Enhanced User Experience:** Improved network performance directly translates to a better user experience for employees and customers.
  - Faster application response times, improved network stability, and reduced latency can lead to increased employee productivity and satisfaction.

Enhanced Agility and Responsiveness:

- **Faster Time-to-Market:** Automation can accelerate the deployment of new services and applications, enabling businesses to respond more quickly to market demands and gain a competitive advantage.
  - For example, automating the provisioning of network services for new applications can significantly reduce the time it takes to bring new services to market.
- **Improved Business Agility:** Automation can help businesses adapt more quickly to changing business needs and market conditions.
  - By automating routine tasks, IT teams can quickly respond to changing business requirements and support new initiatives.
- **Enhanced Business Continuity:** Automation can help ensure business continuity by enabling rapid recovery from network outages and other disruptions.
  - Automated failover and disaster recovery mechanisms can minimize the impact of outages and ensure that critical business operations can continue uninterrupted.

CHAPTER 6

The Future of IT: A Vision for Efficiency and Innovation

The Rise of AI-Powered Operations:

- Explore the potential of AI and machine learning to further enhance network operations.
  - Discuss how AI can be used for predictive maintenance, anomaly detection, and autonomous remediation.
  - Provide examples of how AI-powered tools can help identify and resolve network issues before they impact business operations.
  - For example, AI-powered tools can analyze network traffic patterns to identify and predict potential bottlenecks or security threats.
- Discuss the use of AI for network optimization, such as traffic flow optimization and capacity planning.
  - AI algorithms can analyze network traffic patterns and dynamically adjust network configurations to optimize performance and resource utilization.

The Network of the Future:

- Paint a picture of the future of IT operations, where automation and AI play a central role in enabling dynamic, self-healing, and intelligent networks.
- Discuss the potential for self-configuring networks, autonomous troubleshooting, and AI-driven network optimization.
- Describe the benefits of this vision, such as increased agility, improved resilience, and enhanced business outcomes.
- Imagine a future where networks are self-healing, anticipate and resolve issues before they occur, and continuously optimize themselves to meet the evolving needs of the business.
- Discuss how this vision can enable organizations to unlock new levels of innovation and achieve their business goals.

HOW AUTOMATION ENHANCES NETWORK OPERATIONS

Speeding Up Troubleshooting

Automation facilitates faster troubleshooting by disseminating knowledge across the organization. This efficiency allows experienced engineers to focus on critical issues rather than being bogged down by routine tasks.

Preventing Configuration Drift

Regular automated assessments of configurations—such as router settings, switch port access, and ACLs—help identify potential issues before they escalate into outages. While NetOps teams may lack the time for frequent manual checks, automation allows for daily or even hourly assessments.

Reducing Human Error

Human error is a significant contributor to outages, with studies indicating that 45% of outages stem from configuration and change management mistakes. Automated verification processes can ensure that configurations are correct before and after changes, minimizing the risk of service disruptions.

Achieving Cost Savings

Ultimately, these improvements translate to fewer network outages and reduced IT costs, making a compelling case for the adoption of automation within NetOps.

STRATEGIES FOR FACILITATING A CULTURAL SHIFT

Sharing Knowledge Across the Organization

To foster a culture of automation, NetOps teams should prioritize sharing their expertise throughout the organization. This can enhance consistency and scalability in operations.

Shifting Responsibility to Automation

Encouraging team members to consider automation as a first response can help shift the burden of tasks from people to machines, leading to more efficient workflows.

Showcasing Successful Automation Projects

Demonstrating the early successes of automation initiatives can help garner support from engineers and management, showcasing tangible benefits and encouraging further investment in automation.

Collaboration Beyond Network Automation

Automated network assessments yield valuable insights with minimal effort. Leveraging these assessments whenever possible can streamline operations significantly. Additionally, collaborating with other teams—such as Cloud Operations and Security Operations—can identify automation opportunities that benefit multiple departments.

In summary, building a culture of automation within Network Operations can vastly improve operational efficiency, reduce mean time to recovery, and lower the risk of service delivery issues. By scaling processes without increasing staff, organizations can harness the full potential of their NetOps teams. For example, one large corporation reported saving over 16,000 hours annually through network automation, illustrating the profound impact of this cultural transformation.

CHAPTER 7

5 Networking Tasks that AI Can Help NetOps With, And 5 It Can't

In today's fast-paced digital landscape, the complexity of network infrastructure is growing rapidly. With an increasing volume of network traffic and devices, managing networks efficiently is becoming more challenging than ever. Despite the availability of various tools, Gartner reports that two-thirds of network tasks still require manual intervention. As organizations pivot towards cloud computing and virtualization technologies, the demand for flexible and scalable network management solutions is more pressing. Enter AI, particularly generative AI, which has emerged as a game-changer in the networking space.

5 NETWORKING TASKS AI CAN HELP NETOPS TEAMS WITH

1. Infrastructure Discovery and Configuration Analysis

Identifying and cataloging an organization's IT infrastructure components is a labor-intensive process. Traditionally, this task could take hours per week when done manually. AI, equipped with a comprehensive Digital Twin of the network, accelerates this process dramatically. For instance, identifying a BGP tunnel issue can be reduced from two hours to just ten minutes. This allows NetOps teams to quickly access vital information on device hardware, software, configurations, resources, performance, and security risks.

2. Dynamic Mapping

Dynamic mapping is essential for network visualizations, monitoring, and troubleshooting. AI can automatically discover, document, and update relationships between various network devices and components. While traditional mapping methods can take hundreds of hours, AI can create dynamic network topologies in minutes, ensuring that maps remain current and relevant to ongoing queries or issues.

3. Root Cause Analysis and Anomaly Detection

Root cause analysis and anomaly detection are crucial for maintaining system stability and security. In the past, this required extensive expertise and manual intervention. AI can streamline this process by suggesting diagnostic logic based on training from subject-matter experts. As AI continues to evolve, the hope is that it will reliably replicate and scale automation across all network devices.

4. Recommended Actions

When issues arise, the remediation process often demands expert knowledge and experience. AI can help bridge the gap by cataloging years of expertise and distributing this knowledge to engineers of all experience levels. Once a diagnosis is made, AI can recommend corrective actions, next steps, and follow-up procedures, significantly reducing response times.

5. Dashboards and Reporting

Real-time observability and actionable insights are vital for effective NetOps management. While traditional dashboard creation can be time-consuming, AI can streamline this process by assisting in the development of custom dashboards and reports tailored to specific use cases. Imagine an AI transforming vast amounts of network telemetry data into glanceable visuals that highlight urgent issues, allowing for quick decision-making.

5 NETWORKING TASKS AI DOESN'T HELP NETOPS TEAMS WITH

1. Approve Network Changes

Network changes carry significant risks, and while AI can suggest actions, it lacks the judgment needed to approve changes. Given the complexity of enterprise networks, a mistake can result in costly downtime. Currently, trust in AI for such critical decisions is lacking.

2. Design Complex Networks

Designing enterprise networks requires human intuition and expertise to consider unique requirements and constraints. While AI may one day assist with simpler designs, the intricacies of complex networks demand human oversight to make informed decisions about protocols, latency, and bandwidth.

3. Make Choices

NetOps professionals are continually faced with critical decisions regarding traffic management and performance optimization. AI can provide information but lacks the contextual understanding needed to weigh trade-offs and make tough calls, especially in high-stakes environments like healthcare and government.

4. Take Accountability

NetOps teams are measured on uptime and performance, and accountability is paramount. As AI becomes integrated into operations, the question remains: who is responsible when things go wrong? Relying on AI for accountability is unlikely to be accepted by stakeholders.

5. Innovate

Innovation is a uniquely human trait, driven by creativity and understanding of complex networks. While AI can enhance efficiency and performance, it cannot generate original ideas or solutions tailored to specific organizational challenges. The ability to think outside the box remains a human domain.

CHAPTER 8

Why Are NetOps Teams Struggling to Deliver on Their Network Automation Strategy?

Despite years of investment in network automation, many organizations still struggle to implement effective strategies. A report by Enterprise Management Associates reveals that while 95% of organizations use a combination of DIY and vendor solutions for network automation, only 28% believe they have successfully executed their strategies.

THE FIVE STEPS TO NETWORK OBSERVABILITY

Understanding Network Observability: The Equation

Let's begin with a math problem: solve for "X."
Network Observability = Monitoring + X

The answer is "Context." Network observability is more than just monitoring; it encompasses the vital context that explains why issues arise in the network. While monitoring informs the Network Operations (NetOps) team that a problem exists, observability provides clarity on the underlying causes. This insight enables NetOps to operate more efficiently, which translates to lower Mean Time to Repair (MTTR), improved network performance, reduced downtime, and ultimately enhances the performance of the applications and businesses reliant on the network.

In an era where networks are increasingly complex and IT budgets remain static, observability has become paramount. Over the past two years, the term has gained traction among engineers and practitioners, with Gartner predicting a 15% growth in the market for network observability tools from 2022 to 2027.

Step 1: Network Discovery and Data Accuracy

The journey to observability begins with **Network Discovery and Data Accuracy**. NetOps must compile an accurate inventory of all network devices, including device pairs and clusters, along with their configurations. Achieving this at an enterprise scale often necessitates some form of auto-discovery. Additionally, accurate data must be collected from logs,

traces, traffic paths, and SNMP, which may require aggregating telemetry from various systems. This foundational layer supports all subsequent steps in the observability process.

Step 2: Network Visualizations

The second step is the creation of **Network Visualizations**. This involves mapping the topology of the network and illustrating the connections between devices. Historically, this has been a manual process, often involving the creation of Visio diagrams, which can be time-consuming and quickly become outdated. For effective observability, an automated method to generate and update these maps is essential, ensuring accuracy and relevance in real-time.

Step 3: Network Design and Assurance

Next, we delve into **Network Design and Assurance**. At this stage, NetOps must establish baselines for normal network performance. Understanding how the network should behave involves adhering to security best practices, such as determining which ports should be open and configuring backup firewalls. This is a complex task, as enterprise networks are vast and intricate, often shaped by decades of operational quirks. The loss of senior engineers can further complicate efforts to retain this institutional knowledge, necessitating a reverse-engineering approach to understand existing policies.

Step 4: Automation

Automation plays a crucial role in enhancing observability in three significant ways:

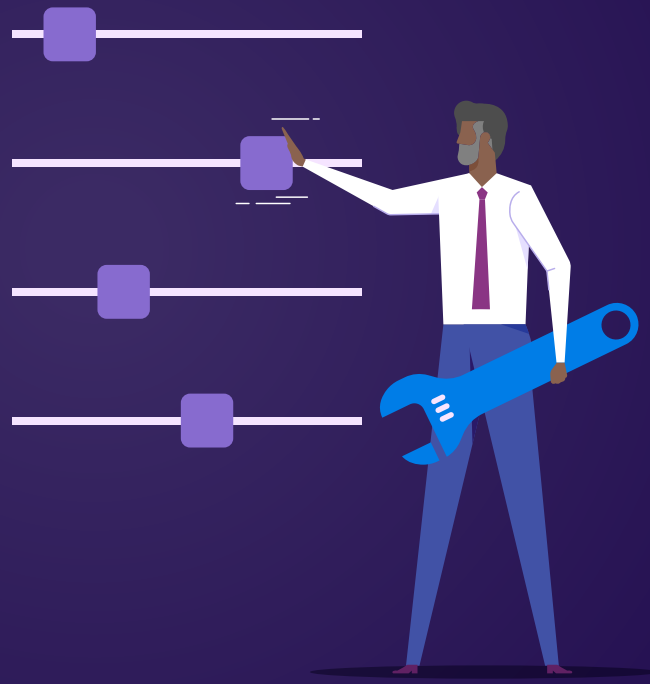
1. **Diagnosis Automation:** This automates common tests and diagnoses issues when NetOps receives a trouble ticket.
2. **Change Automation:** This involves automating tests before and after a network change to verify success and identify any unintended consequences.
3. **Assessment Automation:** Regularly checks actual network performance against the established baselines from Step 3.

By leveraging these automated processes, NetOps can gain critical context without adding to their workload. Engineers have immediate access to diagnostics, can review the impacts of recent changes, and monitor deviations from normal performance. This shift towards proactive monitoring allows for early problem detection before users even report issues.

Step 5: Observability

Finally, we arrive at Observability, the culmination of all previous steps. Each layer builds upon the last: accurate data fosters reliable mapping, which facilitates the measurement of network design and intent, and this knowledge empowers NetOps to create automations for ongoing assessment and enforcement. Ultimately, these automations yield deeper insights into network performance.

Contrary to popular belief, network automation is a cornerstone of observability. By following these five steps, NetOps teams can enhance their capabilities in proactive issue detection, root cause analysis, performance optimization, and security compliance. This comprehensive approach to observability equips NetOps to respond agilely to evolving network conditions and requirements, an essential strategy in the ever-changing landscape of networking.



CHAPTER 9

Leveraging No-Code Automation for Efficient Network Operations

In an interview with Help Net Security, Lingping Gao, CEO at NetBrain, highlights the pressing challenges faced by NetOps teams. As infrastructures expand, these teams often struggle to maintain production services due to outdated processes and increasing demands.

Challenges Facing NetOps Teams

NetOps teams are stretched thin, overwhelmed by remedial tasks and the repetitive operations necessary to resolve user service requests. The challenge is one of scale; as infrastructures grow and more critical services depend on them, service requests increase exponentially. The traditional manual approach to service restoration requires an ever-expanding workforce, which is no longer sustainable given current economic conditions. This leads to longer repair times, rising incident reports, and an increased risk of catastrophic failures that can erode customer confidence.

Outdated Processes

Many NetOps teams still rely on processes established decades ago, such as manual command-line sequences and individual ad-hoc scripts. This antiquated methodology limits efficiency and prevents engineers from focusing on more complex problem-solving tasks.

CHAPTER 10

Merging Network Operations and Security Operations: Key Benefits and Challenges

As cybersecurity becomes increasingly vital, the merging of Network Operations (NetOps) and Security Operations (SecOps) presents both significant benefits and challenges. Understanding the interplay between these two domains is crucial for organizations aiming to enhance their infrastructure security.

THE ROLE OF INFRASTRUCTURE SECURITY

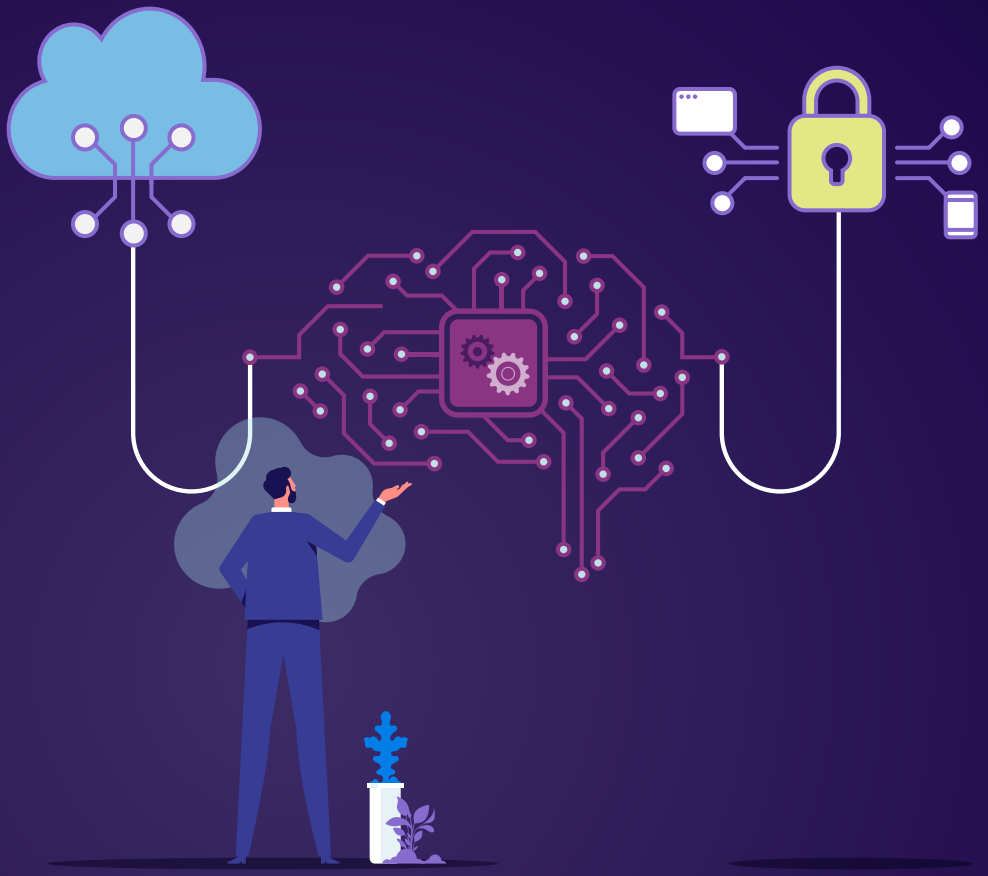
At its core, infrastructure security is intrinsically linked to the network. Every device containing information is connected to the network, accessible from both internal and external sources. This connectivity creates various attack surfaces that need to be addressed.

Responsibilities of SecOps and NetOps

SecOps teams define essential security requirements, such as:

- Coordinating firewall policies
- Establishing access rules
- Ensuring password compliance
- Managing firmware versions

While SecOps outlines these requirements, it is the NetOps team that is best positioned to implement them effectively. For instance, the NetOps team can automate the design and operational status assessments needed to adhere to SecOps guidelines, ensuring continuous compliance and security.



THE ROLE OF AIOPS IN NETWORK PERFORMANCE MANAGEMENT

Addressing Data Overload and Complex Infrastructures

AIOps, which has evolved over decades, promises to enhance network performance management by providing automated solutions to complex issues. However, many NetOps teams already possess the knowledge necessary to address these challenges. The primary limitation is scaling this expertise across the organization.

The Future of AIOps

While AIOps may offer potential solutions, the existing knowledge of subject matter experts (SMEs) often surpasses what AIOps can provide. By combining the ability to capture SME knowledge through no-code solutions with the capability to execute that knowledge, organizations can minimize their reliance on AIOps. Network automation can replicate SME expertise at scale, presenting a more effective solution for ongoing network management.

IMPLEMENTING NETWORK AUTOMATION: COMMON STARTING POINTS

Identifying Repetitive Tasks

Organizations should begin their automation journey by identifying tasks that are performed regularly. Starting small is crucial—attempting to create a comprehensive automation strategy at the outset can lead to prolonged project timelines and missed opportunities for immediate value.

Example: Firmware Assessment

A practical example of network automation is the continuous assessment of firewall firmware versions. Regular updates from manufacturers can be overlooked by engineers, leading to vulnerabilities. Automating this task can significantly reduce the risk of breaches due to outdated firmware.

CHAPTER 11

Future Trends in Network Automation and NetOps

The Rise of No-Code/Low-Code Solutions

One notable trend is the increasing adoption of no-code and low-code platforms, which democratize automation for all network engineers. This approach allows engineers to automate repetitive tasks without extensive programming knowledge.

Benefits of No-Code Automation

No-code automation eliminates bottlenecks, enabling non-technical staff to automate NetOps procedures that were previously limited to skilled engineers. The applications are numerous, including:

- Outage prevention
- Network security enhancements
- Automated diagnostic tests
- Configuration drift detection
- Network discovery and mapping

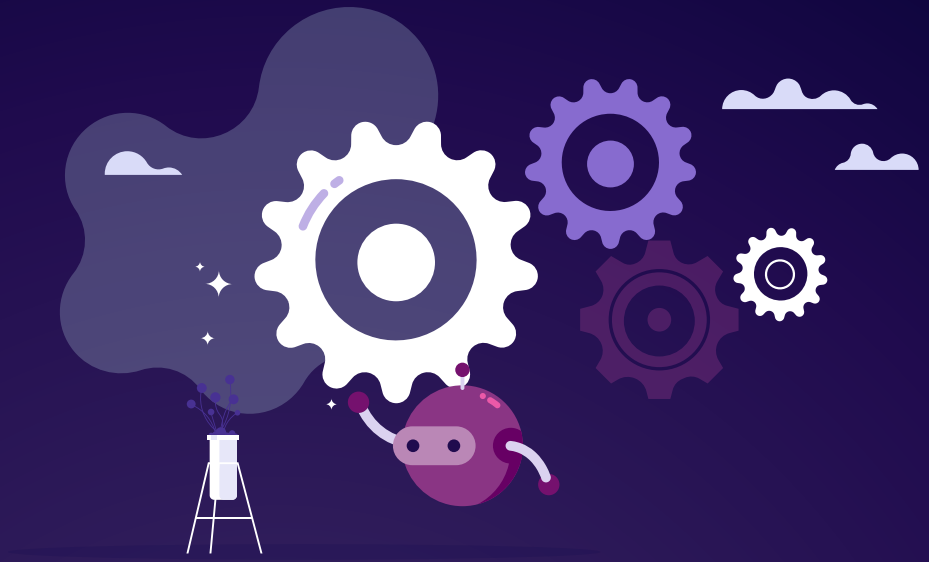
By empowering non-technical users, organizations can streamline processes and enhance operational efficiency. Engineers can then focus on more complex problem-solving tasks, thereby increasing productivity and innovation.

Merging NetOps and SecOps not only strengthens an organization's security posture but also improves operational efficiencies. By leveraging AIOps and embracing no-code automation, organizations can effectively navigate the challenges of cybersecurity while harnessing the full potential of their network operations. As the landscape of network management continues to evolve, staying ahead of trends will be essential for success.

Conclusion

Network automation has transitioned from a nice-to-have to a must-have. Embracing automation and leveraging AI allows organizations to tackle IT inefficiencies head-on, unlock valuable opportunities, and secure a competitive edge in the market.

Schedule a Demo



About NetBrain

A pioneer since 2004, NetBrain is democratizing network automation through GenAI. With its intuitive no-code automation platform, NetBrain empowers network architects, operators and engineers to harness the power of AI and automation, transforming complex operational processes into efficient workflows. By automating network troubleshooting, change, and assessment workflows, NetBrain helps organizations boost operational efficiency, reduce MTTR and mitigate risk. Unifying GenAI and human intelligence, NetBrain provides comprehensive hybrid network observability through continuous network assessment automation and visualization technology, enabling IT organizations to be proactive, make informed decisions and drive innovation.

15 Blue Sky Drive
Burlington, MA 01803 USA
+1 (888) 688-5496
netbrain.com