

LogicVein

EMBRACING THE FUTURE OF NETWORK AUTOMATION

In the rapidly evolving digital landscape, network automation emerges as a pivotal technology, revolutionizing how corporate networks are managed and operated. This whitepaper delves into the essence of network automation, contrasts it with traditional network management practices, and elucidates the myriad benefits of integrating network automation solutions, with a focus on LogicVein's innovative products.

INDEX

1. Overview
2. Traditional vs. Automated
3. Benefits of Network Automation
4. Benefits for IT Teams
5. Must-Have Technical Capabilities
6. Choosing a Solution
7. Impact on Network Security
8. Implementation
9. Implementation Challenges
10. Associated Risks
11. Automating Routine Tasks
12. Change Manage & Governance
13. LogicVein Automation Solutions

THE TRANSFORMATIVE POWER OF NETWORK AUTOMATION

OVERVIEW

Network automation refers to *the use of software to automate the configuration, management, testing, deployment, and operations of physical and virtual devices within a network*. Its primary goal is to enhance efficiency, accuracy, and speed of network management tasks, thereby streamlining network operations and reducing the time it takes to perform tasks. This results in increased productivity and cost savings for businesses.

TRADITIONAL VS. AUTOMATED NETWORK MANAGEMENT

Traditional network management often involves manual configurations and monitoring, which can be time-consuming and prone to human errors. This method lacks the scalability and efficiency required in today's fast-paced digital environment. In contrast, network automation solutions like LogicVein's ThirdEye and Net LineDancer offer several advantages over traditional methods:



Ease of Use: With user-friendly interfaces, LogicVein's solutions simplify network management tasks, making them accessible to engineers without extensive programming knowledge.



Enhanced Monitoring and Alerts: ThirdEye's advanced monitoring capabilities and alerting mechanisms enable proactive identification and resolution of network issues, ensuring optimal network performance.



Automated Configuration and Compliance: NetLD automates device configuration and ensures compliance with industry standards, reducing the risk of errors and non-compliance issues.



Centralized Management: These solutions provide a centralized platform for managing multiple network devices, eliminating the need to individually access each device.

THE BENEFITS OF NETWORK AUTOMATION

Adopting network automation with LogicVein's solutions offers numerous benefits, including:



Increased Efficiency: Automation of repetitive tasks frees up valuable time for network engineers to focus on strategic initiatives.



Reduced Errors: Minimizing manual interventions significantly lowers the risk of configuration errors, enhancing network reliability.



Improved Security: Automated compliance checks and configurations ensure adherence to security policies, reducing the likelihood of vulnerabilities.



Scalability: LogicVein's solutions easily adapt to growing network demands, facilitating seamless expansion and integration of new devices.



Cost Savings: By improving operational efficiency and reducing downtime, network automation leads to significant cost savings over time.

IT TEAM BENEFITS OF NETWORK AUTOMATION

The benefits of network automation for IT teams are extensive and transformative, significantly enhancing the efficiency, security, and scalability of network operations. Here are the key benefits as highlighted across various sources:

- 1. Increased Efficiency and Time Savings:** Network automation streamlines operations by automating routine and time-consuming tasks such as device provisioning, configuration changes, and network management. This automation allows IT teams to focus on more strategic tasks and innovations.
- 2. Enhanced Security:** Automated processes help maintain consistent security configurations across the network, reduce the likelihood of human errors that could lead to security breaches, and ensure timely updates and patches. This consistent application of security policies enhances the overall security posture of the network.
- 3. Reduced Costs:** By automating network management tasks, organizations can better utilize their workforce, reallocating skilled personnel to higher-value projects rather than repetitive tasks. This not only optimizes labor costs but also reduces the likelihood of costly errors and downtime.
- 4. Improved Scalability:** Network automation facilitates the easy addition of new users, applications, and services. Automated systems can configure and deploy new devices quickly, allowing networks to scale with the business without a proportional increase in complexity or manual workload.
- 5. Decreased Risk of Human Error:** Automation reduces the risk of human error, which is a common cause of network failures and security breaches. By automating workflows and validations, IT teams can ensure that changes are applied correctly and consistently.
- 6. Better Resource Management:** Network automation tools provide comprehensive insights and analysis from data across the network, enabling better decision-making and resource allocation. This visibility is crucial for effective management and planning.
- 7. Faster Problem Resolution:** With advanced monitoring and diagnostics, network automation tools can detect and address issues more quickly, often before they impact users. This proactive approach to network management ensures higher availability and performance.
- 8. Compliance and Standardization:** Automation helps ensure that network configurations comply with industry standards and internal policies, reducing the risk of non-compliance and associated penalties. It also standardizes processes across the network, enhancing consistency and reliability.
- 9. Proactive Network Management:** Automated tools can predict potential issues and automate responses, which helps in maintaining network performance and avoiding downtime. This proactive management is crucial in today's fast-paced IT environments.

These benefits collectively contribute to a more agile, secure, and efficient network environment, enabling IT teams to better support organizational goals and adapt to new challenges in the digital landscape.

TECHNICAL CAPABILITIES A NAS SHOULD HAVE

When selecting a network automation tool, it's crucial to evaluate its technical capabilities to ensure it meets the specific needs of your network infrastructure. Based on the provided sources, here are the essential technical capabilities that a network automation tool should have:

1. **Multi-Vendor Support:** The tool should offer broad compatibility with devices from multiple vendors, enabling seamless automation across a diverse network environment.
2. **Configuration Management:** It must provide robust configuration management features, including the ability to automate configuration changes, backups, and restores. This ensures network consistency and aids in quick recovery from issues.
3. **Change Management and Compliance Monitoring:** The tool should facilitate change management by tracking and documenting all changes made to the network. Additionally, it should automate compliance monitoring to ensure network configurations adhere to industry standards and internal policies.
4. **Network Monitoring and Analytics:** Capabilities for real-time network monitoring and analytics are essential. The tool should offer insights into network performance, identify potential issues, and recommend optimizations.
5. **Security Features:** Security is paramount in network automation. The tool should include features for vulnerability assessments, automated security policy enforcement, and remediation actions to protect the network from threats.
6. **Orchestration and Provisioning:** The ability to orchestrate complex workflows and automate the provisioning of network devices and services is crucial for scaling operations and deploying new services efficiently.
7. **API and Scripting Support:** Support for APIs and scripting languages enables integration with other IT systems, customization, and the automation of complex tasks. This flexibility allows for tailored automation strategies that fit specific network requirements.
8. **User Interface and Usability:** A user-friendly interface, possibly with graphical capabilities, can make the tool more accessible to network administrators, reducing the learning curve and improving productivity.
9. **Scalability:** The tool should be scalable to accommodate network growth and complexity without significant performance degradation or the need for complete tool replacement.
10. **Disaster Recovery and Self-Healing:** Features for automated disaster recovery and self-healing mechanisms can minimize downtime and ensure network resilience by automatically addressing failures and vulnerabilities.
11. **Inventory Management:** Automated discovery and inventory management of network devices help maintain an up-to-date view of the network's components, aiding in management and planning.
12. **Role-Based Access Control (RBAC):** RBAC ensures that only authorized users can make changes to the network, enhancing security and accountability.
13. **Integration with Cloud and Hybrid Environments:** As networks increasingly span on-premises and cloud environments, the tool should support automation across these diverse infrastructures.
14. **Customizable Dashboards and Reporting:** Customizable dashboards and comprehensive reporting capabilities are important for monitoring network health, performance, and compliance status at a glance.

Selecting a network automation tool with these technical capabilities will ensure that it can effectively manage and automate your network, improving efficiency, security, and reliability.

KEY CONSIDERATIONS WHEN BUYING

When selecting a network automation tool, several key considerations must be taken into account to ensure that the chosen solution aligns with the organization's specific needs and goals. Here are some of the primary factors to consider, as highlighted in the provided sources:

- 1. Define the Requirements and Objectives:** Clearly define what you want to automate and identify the specific tasks, processes, or systems that need automation. Consider the types of devices, the frequency of changes, and whether the use cases will evolve over time.
 - 2. Evaluate Technical Capabilities:** Ensure that the automation tool or platform has the technical capability to perform the identified tasks. It should be able to handle the complexity and scale of your network and support various domains such as cloud, CLI, policy, service, and SD-WAN.
 - 3. Consider the Tool's Flexibility and Scalability:** The tool should be scalable and flexible enough to meet both current and future network demands. This includes the ability to handle a complex, dynamic, and heterogeneous network environment.
 - 4. Assess Compatibility with Existing Infrastructure:** Check the tool's compatibility with your existing network environment, including hardware, software, and other automation tools. This helps in ensuring seamless integration and operation.
 - 5. Check for Ease of Use and Learning Curve:** The tool should match the skill level of your network team or provide adequate training and documentation. It's important that the tool is user-friendly and accessible to facilitate smooth adoption and usage.
 - 6. Review Costs and Return on Investment (ROI):** Consider both the upfront and ongoing costs associated with the tool. This includes purchase costs, subscription fees, training costs, and any hidden costs like development or maintenance expenses. Evaluate the potential ROI based on the efficiency and benefits the tool offers.
 - 7. Analyze Vendor Support and Community:** Look for strong vendor support and an active user community. Good support can resolve issues quickly, while a vibrant community can offer helpful insights and troubleshooting tips.
 - 8. Security Features:** Ensure that the tool provides robust security features to manage and protect network configurations and comply with industry standards. This is crucial to prevent unauthorized access and data breaches.
 - 9. Automation Capabilities:** The tool should offer comprehensive automation capabilities such as configuration management, network monitoring, compliance enforcement, and possibly self-healing mechanisms.
 - 10. Future-Proofing:** Consider whether the tool is future-proof. This involves evaluating whether the tool can adapt to future technological advancements and changes in network architecture.
- By carefully considering these factors, organizations can choose a network automation tool that not only meets their current requirements but also adapts to future changes and challenges in network management.

IMPACT ON NETWORK SECURITY

The impact of network automation on security:

Security Enhancements: Automated enforcement of security policies and configurations across the network, reducing the risk of human error.

Faster deployment of security updates and patches, improving the network's resilience against threats.

Automated monitoring and anomaly detection to identify and respond to security incidents more quickly.

Improved compliance with industry standards and regulations through automated auditing and reporting.

- **Security Challenges:** Increased attack surface due to the expanded use of APIs, scripts, and software-defined networking.
- **Potential vulnerabilities** in automation tools or scripts that could be exploited by attackers.
- **Difficulty in maintaining visibility and control** over a highly automated network environment.
- **Compliance and accountability issues** if automation tools do not adhere to security and governance requirements.
- **Potential for unauthorized access** or misuse of automation capabilities by malicious actors.

To address these security challenges, organizations should: Implement robust access controls and authentication mechanisms for automation tools.

- **Conduct thorough security assessments** of automation scripts and workflows.
- **Establish clear policies and procedures** for managing and monitoring automated processes.
- **Provide security-focused training** to network engineers to enhance their understanding of automation-related security risks.
- **Integrate network automation tools with security information** and event management (SIEM) systems for centralized monitoring and incident response.



IMPACT ON NETWORK SECURITY (CONT)

Network automation tools significantly impact network security in several positive ways, addressing both the enhancement of security measures and the management of potential security risks. Here are the key impacts based on the provided sources:

- 1. Complexity and Interoperability Issues:** Network automation tools can introduce complexity into the network environment. Different tools may have varying features, functions, interfaces, and protocols that need to be integrated and coordinated. Additionally, these tools may not be compatible or consistent with existing network devices, systems, or standards, leading to conflicts, errors, or failures that can affect network performance or security.
- 2. Skill Gaps and Training Needs:** There is often a skill gap among network engineers who may not have the adequate knowledge, skills, or experience to use network automation tools effectively. This challenge is compounded by the need to learn new tools, languages, or frameworks relevant for network automation, such as Python, Ansible, or Netconf.
- 3. Cost and Value Trade-offs:** Network automation tools can involve significant costs, including expensive licenses, hardware, or maintenance. These costs may not always be justifiable against the return on investment (ROI) or the value proposition of the automation tools, especially under budgetary or resource constraints.
- 4. Compliance and Accountability Issues:** Automation tools must comply with relevant rules, regulations, and standards applicable to the network environment. There is a risk that these tools may not adhere to data privacy, security, or governance requirements imposed by organizations, industries, or laws. Additionally, there may be insufficient transparency, traceability, or documentation of the actions or decisions made by automation tools, affecting network operations or outcomes.
- 5. Resistance to Change:** Employees may resist adopting automation due to fears of job displacement, unfamiliarity with new technologies, or concerns about the reliability of automated systems. This resistance can slow down the adoption process, delay the realization of benefits, or lead to limited implementation of automation.
- 6. Integration with Legacy Systems:** Many organizations still rely on legacy systems that may not be inherently compatible with modern automation technologies. Integrating automation with these systems can be challenging and may require additional time and resources, potentially resulting in only partial automation.
- 7. Data Quality and Integrity:** Automation heavily relies on accurate and up-to-date data. Inaccurate data can lead to misconfigurations and operational issues. Poor data quality can result in unreliable automation outcomes, affecting the overall reliability and effectiveness of the automated processes.
- 8. Lack of Standardization:** The networking industry lacks standardized approaches to automation, leading to a variety of tools, frameworks, and methodologies. This lack of standardization can result in interoperability issues, making it challenging to integrate different automation tools seamlessly.
- 9. Perceived Loss of Control:** There is a concern that automated processes might miss something important or that automation will supplant human workers. However, oversights are more likely to occur without automation, and automation does not necessarily eliminate the need for human workers.

Addressing these challenges requires careful planning, skilled personnel, and a strategic approach to the selection and implementation of network automation tools. By acknowledging and tackling these issues, organizations can better harness the benefits of network automation and enhance their network operations.

IMPLEMENTATION BEST PRACTICES

Implementing network automation involves a strategic approach to enhance network efficiency, reliability, and security. Drawing insights from the provided sources, here are some best practices for implementing network automation:

- 1. Define Clear Objectives and Scope:** Before starting with network automation, have a clear vision of what you aim to achieve. Define your objectives, such as reducing manual tasks, improving performance, enhancing security, or enabling new capabilities. Also, delineate the scope of your network automation project, including which devices, services, functions, and processes you want to automate.
- 2. Adopt a Federated Source of Truth:** Embrace a federated source of truth approach to manage network changes across dispersed ecosystems. This involves adopting automation solutions that can integrate with any database, system, or service, providing fresh, accurate information and ensuring network changes are always made correctly.
- 3. Implement Operation Process Automation (OPA):** OPA focuses on automating repetitive operational tasks to improve efficiency and ensure consistency in operations teams. It delivers process automation specifically to IT and network operations teams, improving the mean time to resolve (MTTR) and decreasing the cost of operations.
- 4. Use Version Control:** Implement version control systems to track and record changes to your code, scripts, and configuration files. This allows for reverting to previous versions, comparing differences, and collaborating with other network engineers, thereby improving code quality and documentation.
- 5. Test and Validate:** Ensure thorough testing and validation of scripts and tools before deploying them to your production network. Utilize methods such as unit testing, integration testing, simulation testing, and validation testing to identify and rectify errors, security issues, or compliance violations.
- 6. Error Handling and Logging:** Implement error handling and logging techniques to manage exceptions, errors, or failures that may occur during automation. This prevents your code from crashing or behaving unpredictably and provides alternative actions or solutions. Logging helps in monitoring, troubleshooting, and auditing.
- 7. Follow Coding Standards and Best Practices:** Adhere to coding standards and best practices to ensure your network automation scripts are reliable, secure, and error-free. This includes using descriptive names for classes, variables, and methods; choosing a consistent coding style; organizing code using modules and packages; and leveraging libraries to simplify work.
- 8. Review and Improve Regularly:** Network automation is an ongoing process of improvement and innovation. Regularly review and improve your automation strategies to ensure they meet objectives and scope, as well as adapt to changing network needs. Support features such as performance metrics, feedback mechanisms, updates, and optimization options.
- 9. Educate and Train Your Team:** Invest in developing your team's network automation skills and knowledge through courses, reading materials, videos, webinars, and participation in communities and forums. A well-trained team is crucial for the successful adoption and implementation of network automation.
- 10. Choose the Right Tools and Platforms:** Select network automation tools and platforms based on compatibility, scalability, reliability, security, and usability. Consider tools that offer centralized management, support for multi-vendor environments, and low-code options for bridging the skills gap.

IMPLEMENTATION CHALLENGES

When implementing network automation tools, organizations face several common challenges that can impact the success and efficiency of their automation initiatives. Here are some of the key challenges based on the provided sources.

- 1. Complexity and Interoperability Issues:** Network automation tools can introduce complexity into the network environment. Different tools may have varying features, functions, interfaces, and protocols that need to be integrated and coordinated. Additionally, these tools may not be compatible or consistent with existing network devices, systems, or standards, leading to conflicts, errors, or failures that can affect network performance or security.
- 2. Skill Gaps and Training Needs:** There is often a skill gap among network engineers who may not have the adequate knowledge, skills, or experience to use network automation tools effectively. This challenge is compounded by the need to learn new tools, languages, or frameworks relevant for network automation, such as Python, Ansible, or Netconf.
- 3. Cost and Value Trade-offs:** Network automation tools can involve significant costs, including expensive licenses, hardware, or maintenance. These costs may not always be justifiable against the return on investment (ROI) or the value proposition of the automation tools, especially under budgetary or resource constraints.
- 4. Compliance and Accountability Issues:** Automation tools must comply with relevant rules, regulations, and standards applicable to the network environment. There is a risk that these tools may not adhere to data privacy, security, or governance requirements imposed by organizations, industries, or laws. Additionally, there may be insufficient transparency, traceability, or documentation of the actions or decisions made by automation tools, affecting network operations or outcomes.
- 5. Resistance to Change:** Employees may resist adopting automation due to fears of job displacement, unfamiliarity with new technologies, or concerns about the reliability of automated systems. This resistance can slow down the adoption process, delay the realization of benefits, or lead to limited implementation of automation.
- 6. Integration with Legacy Systems:** Many organizations still rely on legacy systems that may not be inherently compatible with modern automation technologies. Integrating automation with these systems can be challenging and may require additional time and resources, potentially resulting in only partial automation.
- 7. Data Quality and Integrity:** Automation heavily relies on accurate and up-to-date data. Inaccurate data can lead to misconfigurations and operational issues. Poor data quality can result in unreliable automation outcomes, affecting the overall reliability and effectiveness of the automated processes.
- 8. Lack of Standardization:** The networking industry lacks standardized approaches to automation, leading to a variety of tools, frameworks, and methodologies. This lack of standardization can result in interoperability issues, making it challenging to integrate different automation tools seamlessly.
- 9. Perceived Loss of Control:** There is a concern that automated processes might miss something important or that automation will supplant human workers. However, oversights are more likely to occur without automation, and automation does not necessarily eliminate the need for human workers.

Addressing these challenges requires careful planning, skilled personnel, and a strategic approach to the selection and implementation of network automation tools. By acknowledging and tackling these issues, organizations can better harness the benefits of network automation and enhance their network operations.

POTENTIAL RISKS

When selecting a network automation tool, it's crucial to evaluate its technical capabilities to ensure it meets the specific needs of your network infrastructure. Based on the provided sources, here are the essential technical capabilities that a network automation tool should have:

- 1. Complexity and Interoperability Issues:** Network automation tools can introduce complexity into the network environment. Different tools may have different features, functions, interfaces, and protocols that need to be integrated and coordinated. This complexity can lead to interoperability issues, making it challenging to ensure seamless operation across various network components.
- 2. Security Vulnerabilities:** Network automation tools often require high-level access to network equipment, sometimes needing "super administrator" privileges. This makes them prime targets for attacks. If compromised, these tools can be used to alter security settings or steal sensitive configuration data, posing significant security risks.
- 3. Theft of Sensitive Data:** Automation tools that store sensitive configuration data or personal customer information can be targeted by attackers. If compromised, this could lead to data theft, which can be used for larger attacks or blackmail, especially concerning data protected under regulations like the General Data Protection Regulation (GDPR).
- 4. Overreliance on Automation:** There is a risk that overreliance on automation could lead to gaps in monitoring and response. Automated systems might miss new, unforeseen threats (zero-day threats) or fail to adapt to evolving threat landscapes. This could result in security breaches if not properly managed.
- 5. Data Quality and Integrity:** Poor data quality can lead to automation errors, such as misconfigurations and operational issues. Automation relies heavily on accurate and up-to-date data, and any discrepancies can affect the reliability and effectiveness of the automated processes.
- 6. Resistance to Change:** Employees may resist adopting automation due to fears of job displacement or concerns about the reliability of automated systems. This resistance can slow down the adoption process, delay the realization of benefits, or lead to limited implementation of automation.
- 7. Integration with Legacy Systems:** Many organizations use legacy systems that may not be inherently compatible with modern automation technologies. Integrating automation with these systems can be challenging and may require additional time and resources, potentially resulting in only partial automation.
- 8. Lack of Standardization:** The networking industry lacks standardized approaches to automation, leading to a variety of tools, frameworks, and methodologies. This lack of standardization can result in interoperability issues, making it challenging to integrate different automation tools seamlessly.

These risks highlight the importance of careful planning, robust security measures, and ongoing management to ensure that network automation tools are implemented effectively and securely.

ROUTINE TASKS THAT CAN BE AUTOMATED

Network automation can significantly streamline routine tasks, enhancing efficiency and reducing the likelihood of human error. Here are some examples of routine tasks that can be automated with network automation, as highlighted in the provided sources:

- 1. Complexity and Interoperability Issues:** Network automation tools can introduce complexity into the network environment. Different tools may have different features, functions, interfaces, and protocols that need to be integrated and coordinated. This complexity can lead to interoperability issues, making it challenging to ensure seamless operation across various network components.
- 2. Security Vulnerabilities:** Network automation tools often require high-level access to network equipment, sometimes needing "super administrator" privileges. This makes them prime targets for attacks. If compromised, these tools can be used to alter security settings or steal sensitive configuration data, posing significant security risks.
- 3. Theft of Sensitive Data:** Automation tools that store sensitive configuration data or personal customer information can be targeted by attackers. If compromised, this could lead to data theft, which can be used for larger attacks or blackmail, especially concerning data protected under regulations like the General Data Protection Regulation (GDPR).
- 4. Overreliance on Automation:** There is a risk that overreliance on automation could lead to gaps in monitoring and response. Automated systems might miss new, unforeseen threats (zero-day threats) or fail to adapt to evolving threat landscapes. This could result in security breaches if not properly managed.
- 5. Data Quality and Integrity:** Poor data quality can lead to automation errors, such as misconfigurations and operational issues. Automation relies heavily on accurate and up-to-date data, and any discrepancies can affect the reliability and effectiveness of the automated processes.
- 6. Resistance to Change:** Employees may resist adopting automation due to fears of job displacement or concerns about the reliability of automated systems. This resistance can slow down the adoption process, delay the realization of benefits, or lead to limited implementation of automation.
- 7. Integration with Legacy Systems:** Many organizations use legacy systems that may not be inherently compatible with modern automation technologies. Integrating automation with these systems can be challenging and may require additional time and resources, potentially resulting in only partial automation.
- 8. Lack of Standardization:** The networking industry lacks standardized approaches to automation, leading to a variety of tools, frameworks, and methodologies. This lack of standardization can result in interoperability issues, making it challenging to integrate different automation tools seamlessly.

These risks highlight the importance of careful planning, robust security measures, and ongoing management to ensure that network automation tools are implemented effectively and securely.

CHANGE MANAGEMENT AND GOVERNANCE

In the context of network automation, effective change management processes are crucial to ensure that network changes, whether manual or automated, are properly planned, tested, and implemented without disrupting critical business operations.

Some key considerations for change management and governance in network automation:



Establishing a centralized change management process to review, approve, and track all network changes.



Implementing robust testing and validation procedures to ensure the reliability and safety of automated changes.



Defining clear roles, responsibilities, and approval workflows for network automation tasks.



Maintaining comprehensive documentation and audit trails of all network changes, including those made through automation.



Regularly reviewing and updating the change management process to adapt to evolving network requirements and automation capabilities.

By addressing these security and change management aspects, organizations can more effectively harness the benefits of network automation while mitigating the associated risks and ensuring the overall security and reliability of their network infrastructure.



ThirdEye

ThirdEye is a comprehensive network monitoring system designed to offer various functionalities necessary for effective network failure monitoring and management.



Performance Monitoring



Mib Browsing & Compiler



Threshold Surveillance



Custom Dashboards



Topology Mapping



Vendor Agnostic



Alert Engine



Reporting

Net LineDancer

Net LineDancer (netLD) is a sophisticated and easy-to-use network automation suite designed to help network engineers manage the configurations of network devices.



Manage All Configs From a Single Instance



Config Backup and Restore



Lifecycle Management



Span Multiple Subnets



Realtime Compliance For Policy Violations



Bulk Firmware/IOS Updates



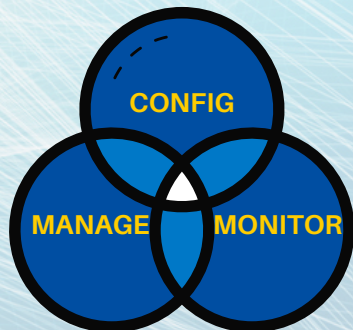
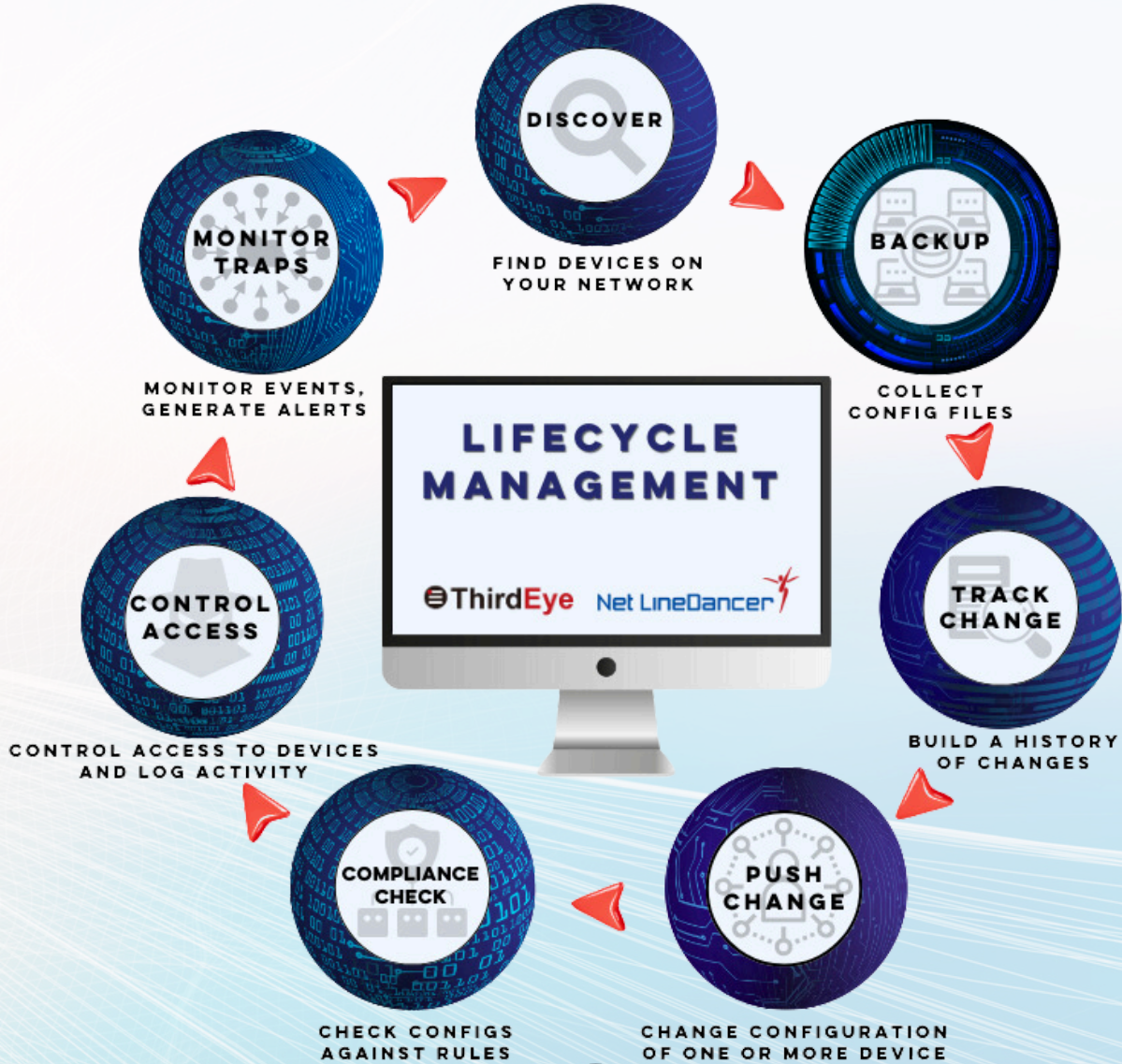
Cisco PnP Hands-Free Operation



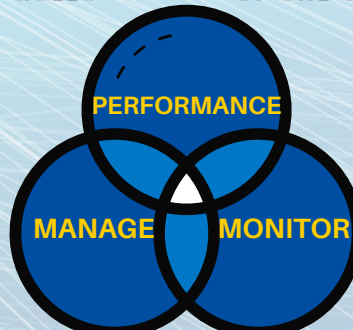
Vendor Agnostic



NETWORK AUTOMATION TOOLS



1ST STEP IN NETWORK AUTOMATION



NMS MADE EASY



FROM A SINGLE PANE OF GLASS

DOWNLOAD A FREE TRIAL



Download the 30 Day Free Trial to see firsthand how our easy-to-use network automation tools perform.

We provide easy to follow instructions as well as short videos to follow.

SCHEDULE A LIVE DEMO



Schedule a Live Demo With your LogicVein rep today by emailing sales@logicvein.com.

Tell them what you want to see and they will show it to you in a live demo.