WHAT EVERY EXECUTIVE NEEDS TO KNOW AND DO TO ACHIEVE NETWORK TRANSFORMATION

A practical guide to predictable outcomes

Abstract

IT Networks are the platform for profitable growth. But network transformation is required for network assurance and affordable support. This report outlines steps IT leaders need to take to achieve transformation using network automation and remediation technology.

Stephen White

Founder / CEO

Viking Technology Advisors, LLC

Infrastructure and Operations Transformation

AI and Hybrid multi-cloud environments are increasing the pressure on legacy network and cyber security architectures to deliver scalable, secure, flexible, and cost-effective operating environments. Infrastructure and Operations (I&O) teams must adapt by continuously transforming their people and processes to accelerate business-enabling digital transformation. By 2027, 70 percent of I&O leaders who fail to transform their teams to an Infrastructure Platform Engineering operating model will be managing only legacy infrastructure services.[1] To be successful I&O leaders must transform their operating models to adopt new strategies that will deliver today's digital transformation and a roadmap to support future requirements. This is not simply a matter of technological change, it is a transformative process that requires executive sponsorship, business buy-in, and a strategic, holistic approach.

I&O leaders are facing significant challenges that are impacting their ability to keep pace with the rapidly changing business requirements and adopt an Infrastructure Platform Engineering operating model. These challenges include:

- Keeping pace with new service requests using manual ticketing and platform administration.
- Managing technical debt across Data Centers, Offices and Branches is time consuming, impacting I&O teams' ability to support digital transformation initiatives.
- Ensuring alignment with business objectives, since legacy infrastructures are not designed to support the accelerated pace of change associated with Hybrid Cloud journeys.
- Inconsistent technology, process and procedures across cloud and on-premises infrastructure increase complexity and risks.
- Network and Cyber Security teams lack Software Development Life Cycle (SDLC) skills necessary to develop and maintain multi-vendor intent based automation.

Network Infrastructure and Cyber Security Architectures must be aligned to support the digital transformation journey. This will require a holistic redesign of the Network Infrastructure and Cyber Security Architectures supporting integration of physical infrastructures with hybrid multi-cloud environments. Automation is a foundational capability that will accelerate Network Infrastructure and Cyber Security transformations. Gluware is the only turn-key multi-vendor network automation platform on the market. By adopting Gluware I&O leaders can accelerate automation benefits across the enterprise network supporting business enabling digital transformation.

[1] Statistic provided by Gartner at the Infrastructure Operations and Cloud Strategy Summit December 2023

Gluware, Enabling Business Outcomes

- **Inventory and asset management automation, delivering annual cost savings improvement**. An accurate inventory is a foundational requirement for effective management of a complex enterprise network. An important outcome of an accurate inventory is automating maintenance renewals delivering cost savings that can be re-invested in the digital transformation program.

- **Enhance Security,** ensuring network security is paramount for network automation. Intent-based and declarative automation works on many levels to ensure security for the network. Intent-based network automation solutions identify potential security and configuration issues with drift, compliance and audit detection and can remediate configuration changes and accelerate OS upgrades, downgrades, and patching. When automating a network, it is important to work with a solution that can actively interrogate the network to find violations and make changes using each vendor's unique CLI with common policy enforcement for features like authentication, access control lists, SNMP, password management, and more.

- **Minimize Downtime and Outage,** analysts state that approximately 70 percent of all network outages are traced to human error and Network Operations spends 80+ percent of their time trouble-shooting these issues. This is because networks are built over many years and most have significant technical debt, including aging, end-of-life equipment, and unnecessarily bloated configurations. Since most network changes are still performed manually or through template pushes, companies are increasingly vulnerable and more prone to costly network outages. Any downtime for a financial services company can have a significant economic impact. Research shows that ransomware attacks on banks increased 1318 percent in 2021 and that the average loss per incident was $5.72 million (Nasdaq 2022). Implementing network automation to inventory, audit, update, and enforce consistent configuration policies can eliminate errors and reduce outages by 90+ percent.

- **Deliver sustainable compliance reporting and automated remediation,** supporting compliance and regulatory requirements in financial services and health care industries. The services include enabling audit self-service risk and control testing reducing impacts on I&O staff and addressing the following challenges.
    - Paper policies and standards not implemented on the network.
    - Requirement for 3rd party compliance (OCC, SOX, GLBA, PCI DSS, and FDIC mandates)
    - Need for ad-hoc audits related to vulnerabilities.
    - Ability to continuously audit hardware inventory, operating systems, and configuration on each device.
    - Enable audit control testing self service automation.

- **Driving Digital Transformation and Accelerating Cloud,** adoption from on-premises services, like mail servers and storage, to SaaS based services, like Microsoft 365, can mean significant changes to network traffic patterns. This will require network re-architecture, or at least a reconfiguration, and most likely an iterative reconfiguration process to improve end-user performance. Gluware automation can accelerate cloud transformation timelines by automating network infrastructures on-premises and in the cloud. Improvements include but are not limited to the following.
    - Time to market Direct impact on network.
    - Traffic pattern changes.
    - Internet breakout changes.
    - Distributed security changes.
    - Managing network policy as it extends into public cloud infrastructures.

- **Accelerating Mergers and Acquisitions,** through automation improving efficiencies with the following
    - Manage inventory of all devices on the current and growing network, resulting from consolidation
    - Quickly identify and remediate configuration compliance gaps.
    - Identify and remediate lifecycle concerns.
    - Automated integration changes supporting device authentication, SMMP and log management.
    - Automated implementation of Internet reachability and policy
    - Automated distributed security
    - Accelerate business integration and reducing integration complexity.

- **Improve NetOps agility,** while reducing the level of effort and timeline for network platform support.
    - Reduce time to deliver broad network changes eliminating dependencies on SMEs to script changes.
    - Transition from manual and reactive processes to automated proactive management.
    - Transition from siloed expertise to serial workflows, improving team agility.
    - Improve outsourcing efficiencies.
    - Reduce delays associated with script development, testing and maintenance.

- **Network Lifecycle Management,** network automation is sometimes thought of only in the context of an initial configuration or a limited, scripted day 2 change. Automation should be thought of in the context of full lifecycle management of each network device and the services running on top of the network. The most challenging task is automating the currently deployed “brownfield” network and getting to a known, good state. Lifecycle management involves automating the initial deployment along with all related moves / adds / changes the business requires. This ranges from low-level policy changes to new end-to-end service deployments. Network automation is the key enabler to lifecycle management.
    - Initial provisioning of devices.

  - Management of devices resulting from consolidation / M&A.
  - Ongoing moves, adds and changes.
  - Upgrade / break fix device replacement.
  - New site deployment.
  - Site refreshes.
  - De-risk and accelerate hybrid cloud adoption.

- **Operating System Vulnerability Management – Operating System Currency.** Upgrading network device firmware / software is a complex and challenging task for IT operations, given that it introduces change and therefore risk. It requires a highly coordinated effort to minimize downtime, especially when dealing with complex, multivendor, multi-operating system, and multi-domain networks. Security vulnerabilities are the most urgent requirement and are the top priority for IT leadership because of the current high-profile hacks that are negatively impacting financial services companies operationally, financially, and publicly. This drives the requirement for network management teams to automate network OS changes and security patching at scale much more frequently to minimize risks.
  - Vendor vulnerabilities.
  - Upgrading equipment to use new features.
  - OS going EOS / EOL.
  - Risky and complex manual processes for upgrades that differ on a vendor and a platform basis.

- **Consolidate and Integrate management tools.** There is no shortage of tools and systems for NetOps teams to use when performing network management. This is a significant part of the challenge when managing networks since there are so many fragmented solutions for specific vendors or purposes including commercial legacy / vendor tools and home-grown solutions that have been built over years. These existing legacy tools and processes often impede the ability to implement change when it comes to network automation. With the current demand on IT operations, it is time to consolidate and modernize network management and automation. Modern technologies like intent-based networking, data-modeling and API integrations must be embraced to meet business needs for agility and security with stability improving network management and addressing the SME attrition risks.
  - Multiple legacy tools supported by a limited SME.
  - Manual undocumented processes dependent on institutional knowledge
  - Home-grown scripts managed by a small number of SME.
  - Management systems to integration.

The time is now to adopt an automation strategy for the brown field enterprise network and cyber security infrastructure that will enable hybrid cloud adoption. The level of effort associated with a DIY script-based automation approach will fail to meet these demands. The adoption of a purpose-built intelligent automation solution from Gluware will deliver sustainable automation capabilities quickly enabling I&O leaders to meet the demand of this fast-paced, digital-first world.

About the Author

Stephen J. White
Founder / CEO
Viking Technology Advisors, LLC
sjwhite@vikingtechadvisors.com
978 500 1492

Stephen White is a Senior IT executive with 25+ years of IT leadership experience in the Financial Services and Consulting sectors. Stephen has held a variety of roles in his career including 14 years building and leading the State Street Corporation global network infrastructure. Stephen spent 6 years at Citizens Bank building the Network, Voice and Security Architectures supporting the Citizen's digital transformation journey while insourcing the network. Stephen is the Founder/CEO of Viking Technology Advisors, LLC a strategic professional services firm empowering organizations to successfully navigate their digital transformation journey. Stephen has a unique breadth and depth of business and technology skills. He is trusted for integrity and the ability to use creativity and innovation to guide organizations through technology-enabled digital transformation.

Viking Technology Advisors LLC

Viking Technology Advisors, LLC (VTA) is a strategic professional services firm empowering organizations to successfully navigate their digital transformation journey. VTA services focus on the transformation of Network Infrastructure and Cyber Security Architectures supporting the integration of physical infrastructures with hybrid multi-cloud environments. They help executive teams see the totality of these projects, unlocking new opportunities to enhance customer and colleague experience.
Viking Technology Advisors has established a portfolio of services designed to support I&O Managers by accelerating their adoption of an Infrastructure Platform Engineering operating model. These services focus on meeting the customer where they are, understanding their business strategy, identifying the gaps and defining a path to sustainable success. We do this by automating management of their multi-vendor on-premises environments, freeing resources to focus on Infrastructure Platform Engineering transformation supporting digital transformation.

VTA leverages a comprehensive approach focused on enabling business outcomes. These services include network and cyber security infrastructure supporting Data Center, Hybrid Cloud, Office, Branch and Retail infrastructures.

- Network & Cyber Security Hybrid Cloud Readiness Assessments
- Network & Cyber Security Hybrid Cloud Architecture Roadmaps
- Network and Cyber Security Engineering & Service Delivery
- Organizational Transformation
- Risk Management and Control Process Automation
- Mergers & Acquisitions