gluware®
Intelligent Network Automation

Top 10

Network Automation Use Cases in the Financial Services Industry

e-Book

The Network Automation Journey

When financial services companies begin their enterprise network automation journeys, top of mind is enhancing network security, increasing agility and ensuring business continuity. No matter what path they are on as they move from manual and scripted network management to code-free, error-free automation, they share some common ground on what urgent challenges to tackle first.

This collection of network automation use-cases is designed to help financial services companies learn from each other about the common challenges they face, the key learnings they gain along the way, and the benefits they experience as a result of putting intelligent network automation to work on some of their most pressing network challenges.

The Gluware® Intelligent Network Automation software suite delivers the features, simplicity and reliability financial services companies seek today to discover, automate and orchestrate their complex, multi-vendor, multi-domain, multi-cloud network environments. To prevent network outages, ransomware attacks, data breaches, manual errors and security issues, many global enterprises use the Gluware platform for an intent-based and declarative approach to automating their mission-critical networks.

As you explore these top network automation use cases and the IT challenges they present to financial services companies today, you will learn more about the ways that Gluware is solving these problems for customers today.

gluware®
Intelligent Network Automation

#1 Inventory and Assess your Network

Understanding the current status of the network, including vendors, operating systems, OS versions and vendor supportability, is critical to the network automation journey. The inventory should be complete and accurate. If a device or devices are not tracked, it could allow access to the network. In addition to deeply understanding the composition of the network, intent-based network automation allows rogue devices to be identified including unauthorized network hardware, firmware or software, as well as wireless access points and switches under desks. As many network executives, architects and operations teams know, such intrusions can be real-world vectors for enabling dangerous cyber-attacks or data theft. The process of conducting network inventory consists of several steps, typically performed by different systems including device discovery, hardware and software inventory and using the inventory data to drive best practices.

CHALLENGES

- No accurate source of truth
- Lack of standards enforcement
- Keeping up with vendors
- Overlooked fundamental step

GLUWARE SOLUTION

- Run on-demand discovery
- Import or discover devices
- Get to a known state
- Plan OS upgrades to enable features and prevent network risk
- 3rd party API calls for Cisco SmartNet, EOS / EOL, PSIRTs (Cisco), and NIST API integration for multi-vendor CVE's
- Audit for config statements related to known vulnerabilities

Learn More

Discover devices on your network with Gluware

Assess EoX, SmartNet status and vulnerabilities (PSIRTs) with Gluware

Use OS Manager to automate FW / SW updates with Gluware

Monitor network devices for config drift and identify exactly what changed with Gluware

Perform audits of network configurations with Gluware

#2 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.

CHALLENGES

- Avoid costly downtime
- Decrease vendor vulnerabilities
- Improve configuration integrity
- Upgrade and patch at scale for rapid response
- Address compliance

GLUWARE SOLUTION

- Auto-discovery of the network and device configurations for inventory management
- Assess the operating systems running on network devices including integration with Cisco support APIs for knowledge of vulnerabilities (PSIRTs issued), and NIST API integration for multi-vendor CVE's
- Automate OS upgrades, patches and downgrades to ensure that only stable, reliable and approved software are running
- Automate network configuration related to security including authentication, password management, ACL policies, etc.
- Deploy new security features like Network Admission Control (NAC) on switch ports
- Real-time visibility of manual configuration changes through Syslog messages
- View progress towards compliance with dashboards

Learn More

Discover devices on your network with Gluware

Assess EoX, SmartNet status and vulnerabilities (PSIRTs) with Gluware

Automate OS management (upgrades, patches, downgrades) with Gluware

Automate Network Admissions Control (NAC) deployment with Gluware

#3 Minimize Downtime and Outage

Analysts state that approximately 70% of all network outages are traced to human error and Network Operations spends 80%+ 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% 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+%.

CHALLENGES

- Outages caused by manual errors
- Unauthorized changes
- Manual configuration changes
- Time-consuming troubleshooting
- Manual processes including outdated scripts

GLUWARE SOLUTION

- Standardize the operating systems running on network devices, ensuring only approved software images are running
- Continually monitor network for configuration changes and notify when, and exactly what changes have been detected
- Perform initial audit for 'out of policy' configurations
- Automate network policies by feature to ensure approved configurations
- Preview automated changes before applying
- Automate troubleshooting processes
- Convert manual procedures and processes to automated workflows
- Data model managed configuration features deployed with a declarative and intent-based engine at scale

Learn More

Automate OS management (upgrades, patches, downgrades) with Gluware

Monitor network devices for config drift and identify exactly what changed with Gluware

Perform audits of network configurations with Gluware

Automate network troubleshooting with Gluware

Automate repeated processes and procedures with Gluware

#4 Enable Compliance

Compliance and regulatory requirements to meet OCC, SOX, GLBA, PCI DSS, and FDIC mandates are critical to financial services companies, as is achieving ISO certification to comply with data regulation laws. Implementing the ability to audit and ensure compliance is an integral component to satisfy 3rd party auditors to meet requirements.

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 audit hardware inventory and operating systems running as well as the configuration components running on each device

GLUWARE SOLUTION

- Use Gluware Topology to generate site documentation
- Audit the hardware inventory and current operating systems
- Easy to create CLI and RegEx based rules
- Internal, 3rd-party and ad-hoc audits
- Automate ongoing configuration audits
- Automated ongoing monitoring of configuration changes
- Implement standards-based configurations
- Zero Touch Provisioning (ZTP) to implement correct configurations from the start
- Automate changes across the network
- Remediate devices that fail audits
- Real-time visibility of manual configuration changes through Syslog messages
- View dashboards showing progress toward compliance (configuration / policy changes, OS upgrades)

Learn More

Audit your network inventory with Gluware

Perform audits of network configurations with Gluware

Monitor network devices for config drift and identify exactly what changed with Gluware

Implement standard network configurations with Gluware

Automate OS management (upgrades, patches, downgrades) with Gluware

Automate multi-cloud infrastructure with Gluware

#5 Driving Digital Transformation And Accelerating Cloud

Financial services companies are accelerating "cloud-first" strategies, consuming Software as a Service (SaaS) and moving workloads to the cloud via Infrastructure as a Service (IaaS). SaaS and public cloud infrastructures have proven to drive agility, scalability, availability and align cost with consumption. Enabling a financial services company to move 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 a network re-architecture, or at least a reconfiguration, and most likely an iterative reconfiguration process to improve end-user performance.

CHALLENGES

- Time to market
- Direct impact on network
- Change in traffic patterns
- Internet breakout
- Distributed security
- Managing network policy as it extends into public cloud infrastructures

GLUWARE SOLUTION

- Perform a network inventory
- Network-wide QoS policy automation for critical apps at scale
- Iterate on QoS changes as traffic patterns change
- Get to a known good configuration state
- Plan OS upgrades to enable features
- Automate OS upgrades / downgrades
- Automate with Gluware Config Modeling:
  - Network-wide QoS for backhaul
  - SNMP and NetFlow for monitoring
  - Local-breakout for Internet
  - Distributed firewall rules and device access lists
  - Public multi-cloud network infrastructure

Learn More

Perform a network inventory with Gluware

Automate configurations and get to a known good state with Gluware

Automate OS management (upgrades, patches, downgrades) with Gluware

Automate configuration policy like QoS to enable your move to the cloud with Gluware

Automate multi-cloud infrastructure with Gluware

#6 Accelerate Mergers and Acquisitions

Network technical debt is the accumulation or acquisition through consolidation / M&A of aging devices, old operating systems, unnecessary or partial configurations, and variances in deployments. This technical debt increases the cost of maintaining and operating the network. In some cases, technical debt decreases productivity across the entire organization, which can be expensive. Often financial services companies are forced into unnecessary hardware upgrades to achieve automation, which is another financial impact of technical debt. Automating is a critical step to optimizing the network by inventorying all the devices running on the network, standardizing platforms and operating systems, and minimizing configuration complexity while enforcing standards.

CHALLENGES

- Consolidation and M&A
- Ongoing inventory of all devices on the current and growing network, resulting from consolidation
- Change in traffic requiring configuration change
- Internet reachability and policy
- Distributed security

GLUWARE SOLUTION

- Build Gluware Network RPA workflows to accelerate discovery, inventory, and audit phase of M&A
- Inventory and assess the network
- Implement configuration standards
- Plan OS upgrades to enable features
- Automate OS upgrades / downgrades
- Automate configuration management
- Automate network-wide QoS
- Automate SNMP and NetFlow for monitoring
- Automate local-breakout and related configuration for internet access
- Automate distributed firewall rules

Learn More

Perform a network inventory with Gluware

Automate configurations and get to a known good state with Gluware

Automate OS management (upgrades, patches, downgrades) with Gluware

Automate configuration policy like QoS to enable your move to the cloud with Gluware

#7 Make NetOps More Agile

Financial services requirements are constantly changing, and IT organizations must have the ability to be responsive to not just common and standard change requests, but to unplanned changes as well. Network changes implemented manually or that require the development and testing of scripts will significantly impede the agility of an organization. Outsourcing network changes also comes with significant delays and cost. Enabling the network team with advanced networking automation technology that does not require all the manual building and skill set development will accelerate changes, enabling agility to meet business needs.

CHALLENGES

- Days, weeks or months to complete broad network changes
- Manual and reactive processes
- Siloed expertise, serial workflows
- Delays due to outsourcing
- Delays due to script development, testing and maintenance

GLUWARE SOLUTION

- Build automation policy from current configurations using interrogative modeling tools
- Rapidly automate reference features
- Native CLI support for config standards
- Quickly transition from test to production
- Automate configuration management
- Automate network-wide changes
- Preview changes before writing to network
- Automate repeated tasks with workflows
- Customized stepwise execution of common tasks

Learn More

Intelligent network automation and dynamic creation of policy with Gluware

Automate standard network configurations with Gluware

Automate repeated processes and procedures with Gluware

#8 Manage Network Lifecycle

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.

CHALLENGES

- Initial provisioning of devices
- Management of devices resulting from consolidation / M&A
- Staging of OS
- Ongoing moves, adds and changes
- Upgrade / swap of devices
- New site deployment
- Site refreshes

GLUWARE SOLUTION

- Automate network configuration management
- ZTP or "advanced" provisioning
- Model entire configuration, or start small
- Centralized control of policy
- Version control
- Ability to automate vendor / device swap
- Automate OS upgrades
- Advanced network-wide updates
- Build no-code drag and drop process automation with Gluware Network RPA
- Customized stepwise execution of common tasks

Learn More

Automate network configuration management with Gluware

Automate OS upgrades with Gluware

Automate repeated processes and procedures with Gluware

#9 Manage OS

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, multi-vendor, multi-operating system, and multi-domain networks. For example, IT organizations may try to limit firmware / software changes such as OS upgrades on their network equipment to once a year, or security patching on an as-needed basis only. 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.

CHALLENGES

- 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

GLUWARE SOLUTION

- Device management to inventory and assess
- Automate operating system updates and security patches quickly and at scale
- Centralized organization and control
- Elimination of manual, error-prone processes
- Pre-checks and post-checks performed
- Integrate drift snapshots and state assessment
- Track progress using OS upgrade dashboard view

Learn More

Use Device Manager to inventory and assess your network devices with Gluware

Use OS Manager to automate FW / SW updates with Gluware

Monitor network devices for config drift and identify exactly what changed with Gluware

#10 Consolidate and Integrate

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.

CHALLENGES

- Too many multiple legacy tools that don't meet current needs
- Too many manual processes
- Home-grown scripts
- Management systems to integrate

GLUWARE SOLUTION

- Multi-vendor, multi-platform
- Unify management across vendors
- Ability to co-exist
- Automate as much, or as little as needed to get started
- API integrations with products like Ansible
- Ability to rapidly integrate 3rd party API (for example with IPAM or ticketing systems)
- Published APIs so 3rd party systems can interact programmatically
- Automate third party open-source integrations through Gluware Service Connectors (GSCs) and external integrations with StackStorm

Learn More

Leverage the GluAPI to automate your network programmatically with Gluware

Understanding and using the Gluware API

Automating with Ansible and leveraging API integration with Gluware

Gluware Solutions for the Financial Services Industry

STARTING THE JOURNEY

When your team is ready to begin it's network automation journey towards code-free, error-free security and agility, Gluware® Intelligent Network Automation delivers the capability many of our financial services customers require:

- Flexible Automation: On-premises or cloud-delivered; One app or more
- Expanded Vendor Support: Growing list of more than 40 platforms
- Inclusive Environments: Multi-vendor | Multi-domain | Multi-cloud
- Quality User Experience: Enterprise-class features and dashboards
- Multiple Payment Offerings: Get started your way

WHEN YOU ARE READY TO GET STARTED, OUR TEAM OF AUTOMATION SPECIALISTS ARE HERE TO HELP
SALES@GLUWARE.COM

gluware®
Intelligent Network Automation

2020 L Street, Suite 130, Sacramento, CA 95811 | www.gluware.com