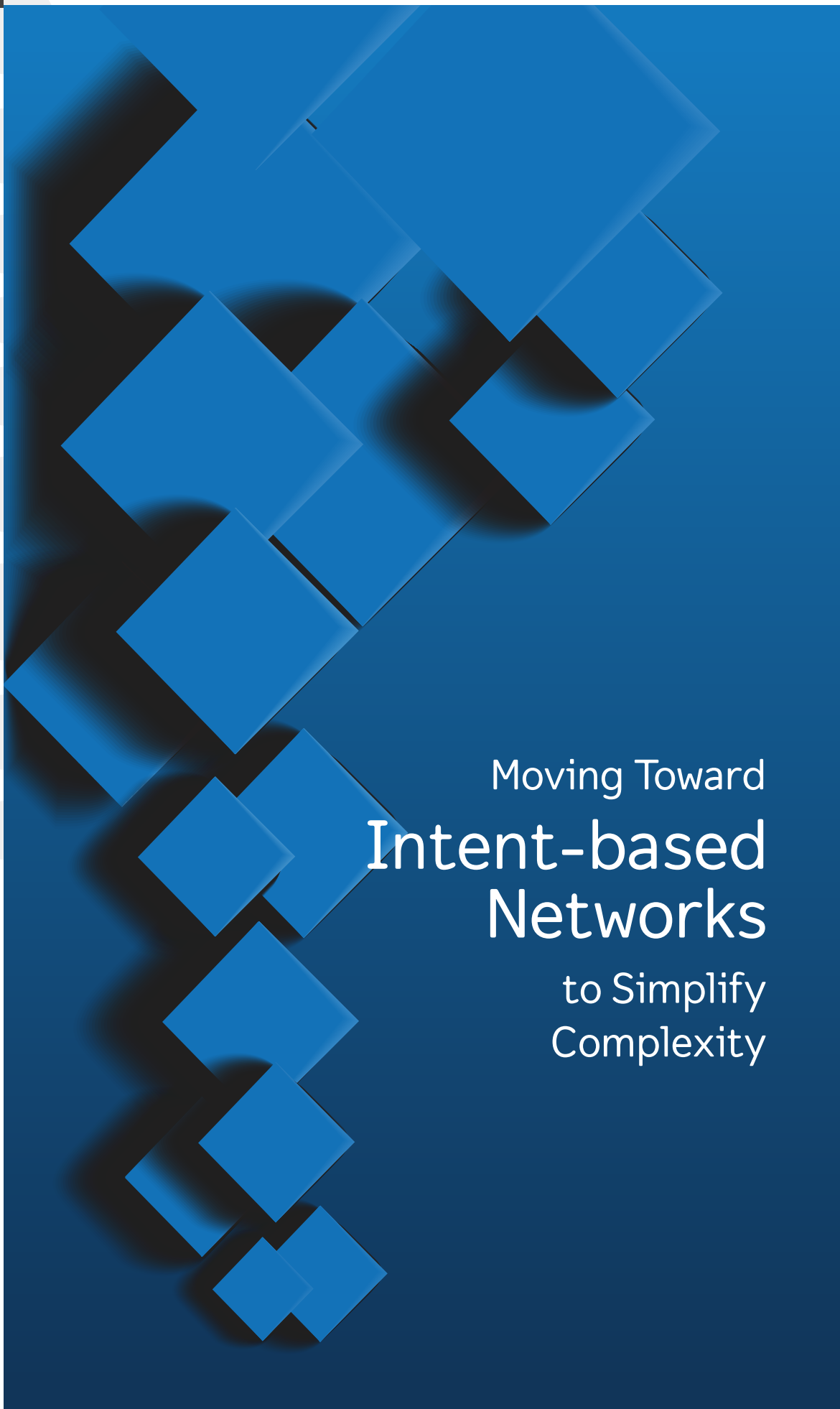
gluware®



Moving Toward Intent-based Networks to Simplify Complexity

Introduction

Executive Summary

Intent-based Networking has emerged as a new paradigm promising to:

Simplify Network Configurations | Reduce Cost | Enable Agility

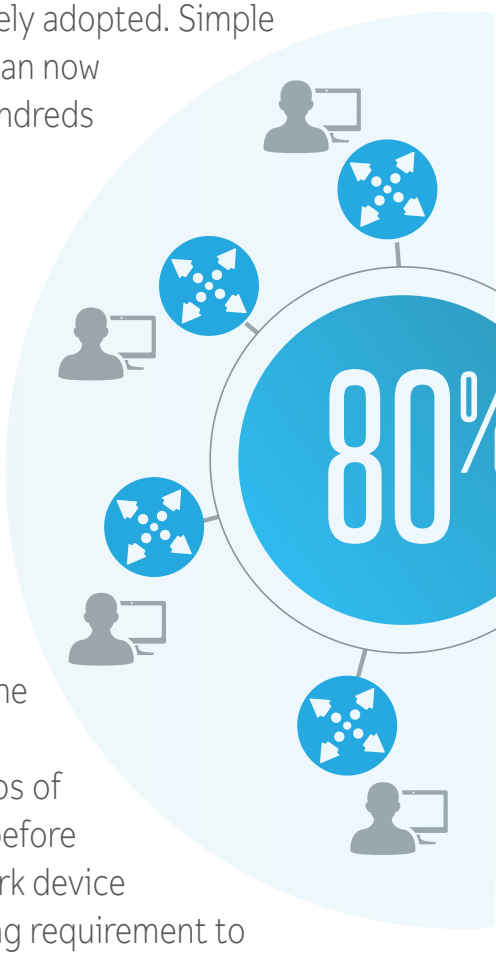
However, many of the initial "intent-based"solutions only deliver on a portion of this promise. The promise includes expressing an "intent" as what a user wants from the network, and relying on an intent-based networking to execute. Gluware has begun to deliver on that promise with an intelligent network orchestration engine capable of consuming abstracted, simplified "intent" and delivering it by configuringmulti-vendor, multi-domain networks.

Several Gluware orchestration solutions have been delivered for common network challenges IT organizations are facing today. As enterprises continue their journey of automation they want to ensure that today's platforms are "intent" capable for future solutions.

We live in exciting times from a technology standpoint. We have virtual assistants, self-driving cars, cloud services, virtual and augmented-reality! However, networking technologies continue to move along at a snail's pace, with only incremental improvements occurring over a span of twenty years.

Currently, on average, over 80% of network changes within enterprises are made manually which is slow and error prone.

The real pain of this was not evident until cloud computing became widely adopted. Simple management systems can now provide control over hundreds (or even thousands) of compute resources, enabling users to "spin-up" virtual machines and deploy applications in minutes. On the other end of the spectrum, deploying new, or changing existing, network services usually takes days or weeks as the change requests move through the isolated silos of expertise for approval before configuring each network device manually. The networking requirement to deliver on a business requirement is now typically the "long-pole in the tent" when it comes to service delivery.



Initial paths to Modernization

SDN and Automation were intended to help provide the reliability and agility needed to propel network technologies into the infrastructure that cloud services can really thrive on top of. SDN is either Controller based or SW only, and Automation is either Scripting or Vendor Mgmt tools.

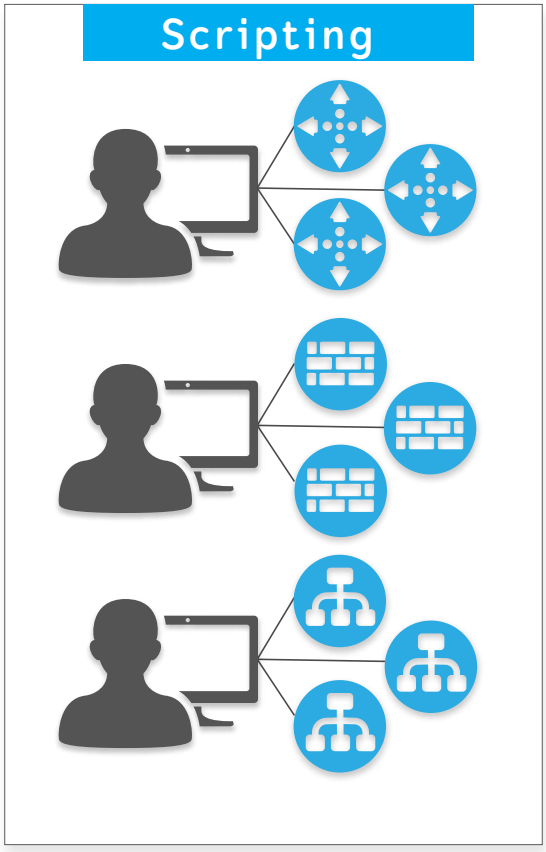
Software-Defined Networking (SDN) and automation were thought to be the answers to problems like these with managing network changes. SDN looked to add a "controller" which talked to all the network nodes and provided centralized access to and management of the control- plane. To date, development for SDN has largely been focused on the data center, where it is being used to control tunneling protocols, known as overlay networks. SDN-like solutions are starting to be used in the WAN with SD-WAN, but they are typically vendor proprietary and often require additional equipment which delivers an overlay to the existing network – not solving most problems completely. Automation has also progressed to help handle configuration and network changes, potentially at scale.

SDN Controller Shortcomings

- Provide "lite" features – inflexible
- Require additional HW
- Often vendor or device type specific

Automation Scripting Shortcomings

- New skill set needed separate from networking
- Large efforts for small changes – per vendor/device
- Variables and unique settings needed, but difficult



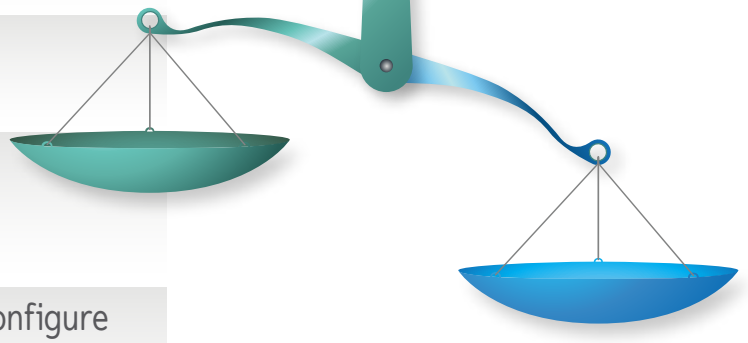
Most IT organizations cobble together a handful of scripts to help with time-consuming networking changes, but often they are not used for the majority of network changes.

Some of the more modern approaches to automation convert the network configuration into software structures, known as data- models, so that intelligent systems can consume those data models and handle configuration changes at scale. This is an important precursor to Intent-based Networking.

Current IBN PROS & CONS for MOST IBNs But not Gluware

Intent Based Networking Solution Benefits

- Expand network scale and complexity to keep pace with business growth
- Increase network agility to keep up with emerging business unit demands
- Reduce manual (device-by-device) configuration changes on devices that account for 80+% of outages currently
- Shrink time and resources needed to configure and troubleshoot the network, freeing engineering time for more strategic activities



Intent Based Networking Solution Issues

- Lack of standardization means there is likely to be fragmented and vendor specific solutions
- [gl] Gluware covers the whole network, and most device vendors and device types at a CLI level
- Low ROI from open-source efforts that show progress, but nontrivial resources and assembly are required to implement and maintain them
- [gl] Config Modeling lets IT immediately automate current features, and Config Drift provides a turnkey approach to config compliance – no coding required
- Significant investments by most IT orgs in existing network equipment and setup make "rip and replace" approaches of many IBN solutions difficult - whether HW or SW based
- [gl] Gluware automates new and existing networks and devices – all HW types supported
- Significant dependencies on "best of breed" mixes of multi-vendor, multi-platform (switch, router, FW, etc), multi-domain (LAN, WAN, Datacenter), and multi-modal (physical and virtual) devices by current IT shops mean large coverage gaps for most IBN solutions
- [gl] Gluware automates from the CLI interface up, meeting the IT "best of breed" challenge
- High saturation in IT orgs of single vendor/single platform network mgmt. tools mean an additional tool for IBN formal validation is often a non-starter
- [gl] Gluware provides integrated feature by feature validation in every Preview and Provisioning cycle from the Orchestration Engine

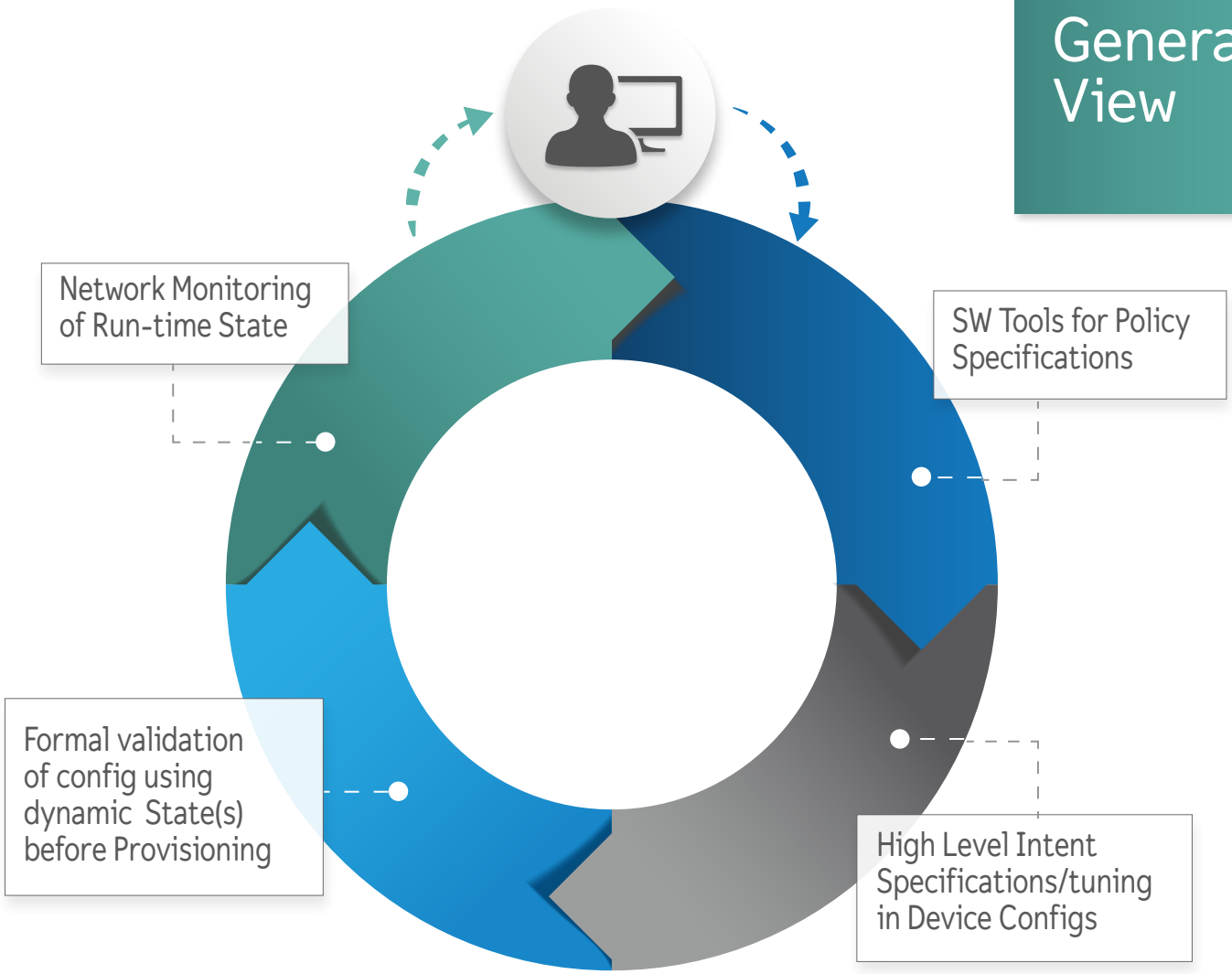
While there is no true single standard specification for Intent-based Networking Systems, quite a few companies are usingthis term in their marketing materials and the networking community is sorting between the reality and the hype.

A More Intentional Approach

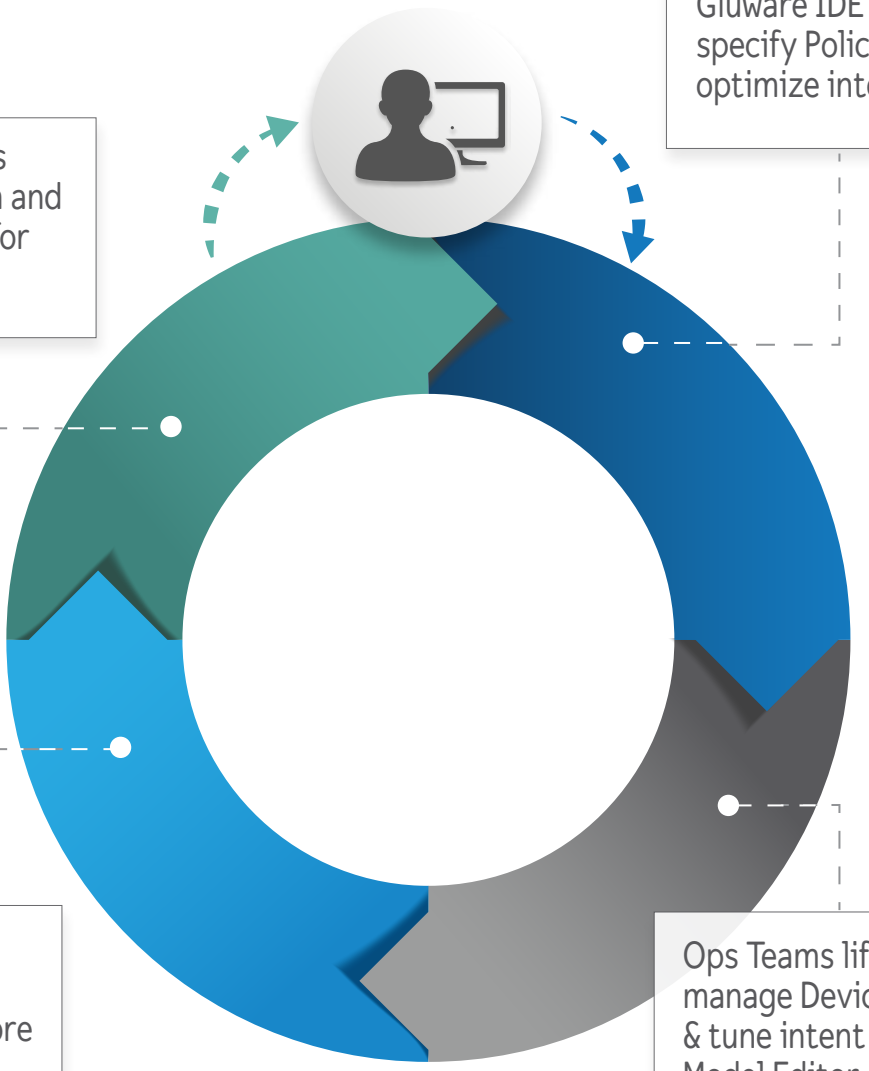
*According to **MIT** and **VMware**, Intent Based Networking is:*

1. SW that creates Policy Specifications and Device Configurations that reflect High level Policy Intent,
2. Then performs formal validation of Intent by modeling/previewing Dynamic States before Provisioning,
3. Then monitors the network/configuration state during runtime, and revisits policy intention as necessary.

General View



How Gluware Stacks Up



Gluware IDE & Control specify Policy and optimize intent

Config Drift provides Run time verification and compliance reports for network config state

Previews modes & Engine fully validate config before provisioning

Ops Teams lifecycle manage Device configs & tune intent using Model Editor

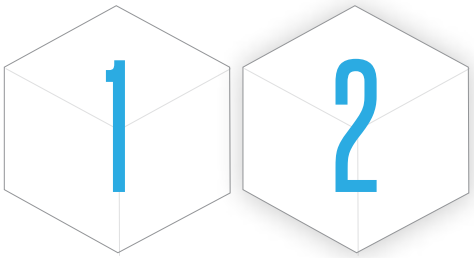
Gluware IDE is used to develop Expert Features and Guided Workflows that integrate and simplify the mapping of network configs to business intentions, and Gluware Control further tunes those intentions.

The Model Editor and intermittent Strategic Syncs on Devices provide fine tuning for the mapping of network configs to business intentions throughout the lifecycle of networks and devices.

Config Drift provides a Runtime Verification mechanism for network config monitoring, and an integrated compliance report generation utility.

Previewing and Provisioning activities leverage the Gluware Orchestration Engine which integrates the Discover/Analyze/Validation process, Contextual Execution, and Strategic Syncs – all of which help validate and abstract device and device type technical execution from business intentions.

As newer solutions emerge, there are two implementation strategies being used.



The first, and most non-disruptive, approach is to implement intent-based networking on the management plane. These solutions attempt to work with the current network and overlay intelligence through state validation and/or orchestration. Implementing on the management plane typically will not require new hardware or a re-design of the network.

The second approach is to build off SDN and expose an intent- based network interface API to leverage the controller, which communicates directly with the network nodes. The SDN approach typically requires a re-design or new deployment of the control-plane, and often an upgrade or replacement of the network nodes. The SDN community has worked on IBN starting with the Open Networking Foundation (ONF). The ONF has since combined with the On.Lab to develop the ONOS SDN controller and are continuing work on an available "intent-based" interface to their controller. The open-source controller OpenDaylight (ODL) also has an active project.

While there are many open-source options out there to start from, most enterprises do not have the budget that the large carriers do to commit resources to participate and contribute to these projects. As commercial offerings of these tools become available, they are expected to be more mature and ready for direct enterprise IT consumption, instead of providing puzzle pieces that an IT operator then has to assemble.

How it all Works

SDWAN/LAN Switching/ Workflow

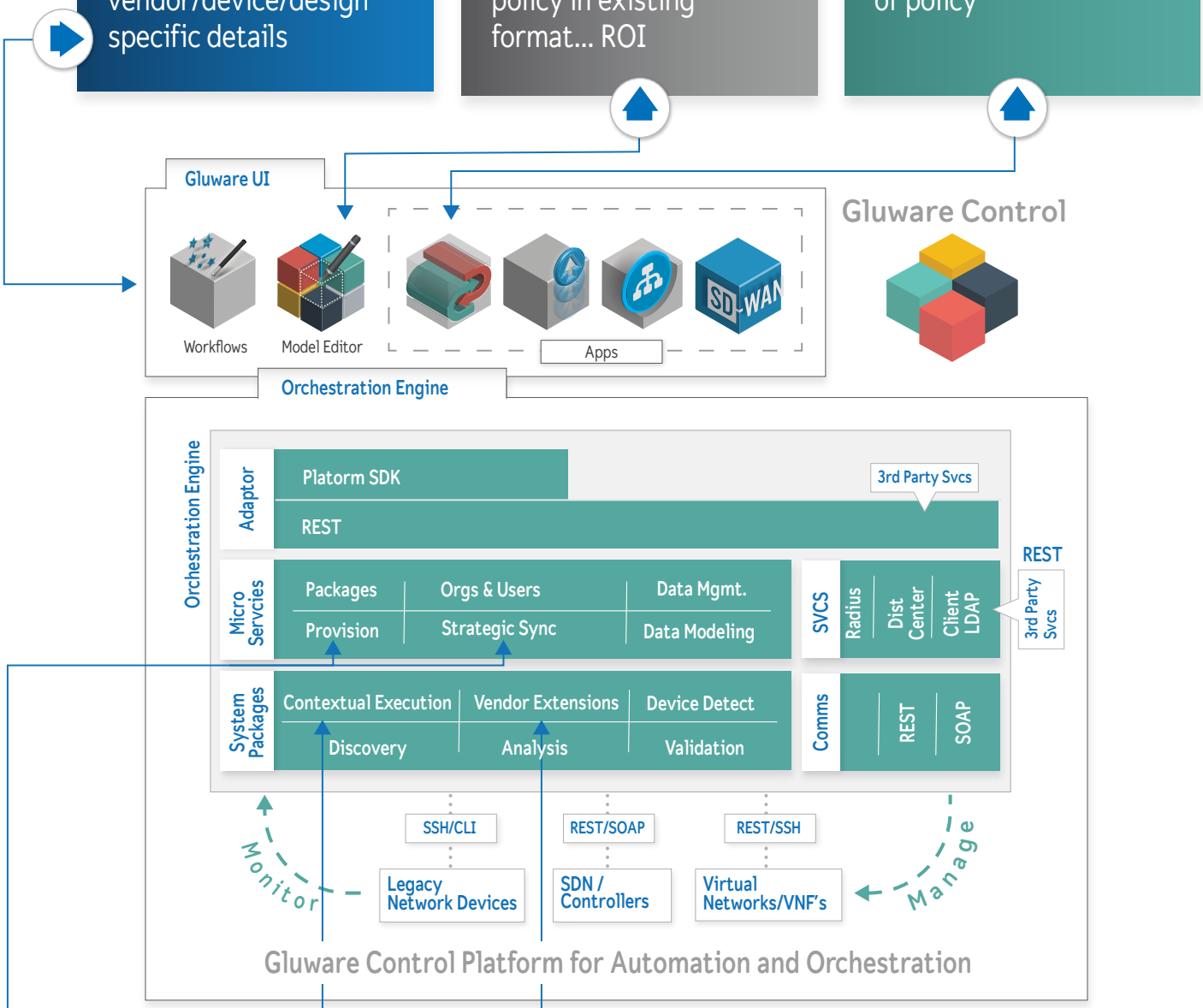
Abstract policy from vendor/device/design specific details

Model Editor/Config Modeling

Add structure to existing policy in existing format... ROI

Config Drift

Run time validation and compliance reporting of policy



Provisioning and Strategic Sync

Discover/Analyze/ Validate – Formal validation of policy

Contextual Execution

"Order matters" – abstract away CLI structure details from policy

Vendor Extensions

Abstract away Vendor specific details from policy

Gluware Advanced Modeling

delivers IT automation and orchestration solutions that are multi-vendor, multi-domain, and support physical and virtual platforms. Gluware Control, as an orchestration platform, offers pre-built solutions as well as config modeled solutions built off of technology base packages. Gluware technology is based on an intelligent orchestration engine which performs discovery, analysis, validation and provisioning of network features. When a network "feature" is onboarded into the Gluware system, it is converted from low- level vendor specific semantics into a data- model combined with policy for analysis and validation. Then, while provisioning the feature, the engine can use the data-model to convert it back to the required CLI or API for each vendors' device.

Built for IT operations, Gluware Control has a web based user-interface which can be consumed as a Software-as-a-Service from a public cloud or installed on the customer premises'. Gluware Control uses RESTful API calls to the Intelligent Orchestration Engine to configure and provision network "features". Users of Gluware Control select a package and then have simplified, abstracted, form-fill based configurations to execute provisioning for network solutions.

Using Advanced Modeling, users can to rapidly onboard network features into the system. When a feature is "onboarded" each of the engine components "learns" about the feature so that it can perform discovery, analysis and validation. The feature is also made up of JSON (JavaScript Object Notation) based data-models to expose as much, or as few, options to IT Operations as required for a configuration. Network features can then be easily configured and provisioned across hundreds or thousands of nodes concurrently.

To handle multi-vendor support, the Gluware engine is populated with Vendor Extensions for each vendor platform supported. These engines can convert the data-model to the appropriate CLI (and semantic) that each vendor uses as well as read in current state of the features from the network nodes upon discovery.

The idea of Intent-based Networking is that the intent (what I want) is translated into how (how I do it). While it is still up for debate how high up the intent is abstracted, Gluware provides pre-packaged solutions to address common IT requirements that simplify configuration and lifecycle management.

3 Themes of Gluware Intent

1 Simplify Network Configurations

Validation of Policy: Discover/Analyze/Validate each feature; Ordered execution of CLI – improves success % thru validation

2 Reduce Cost

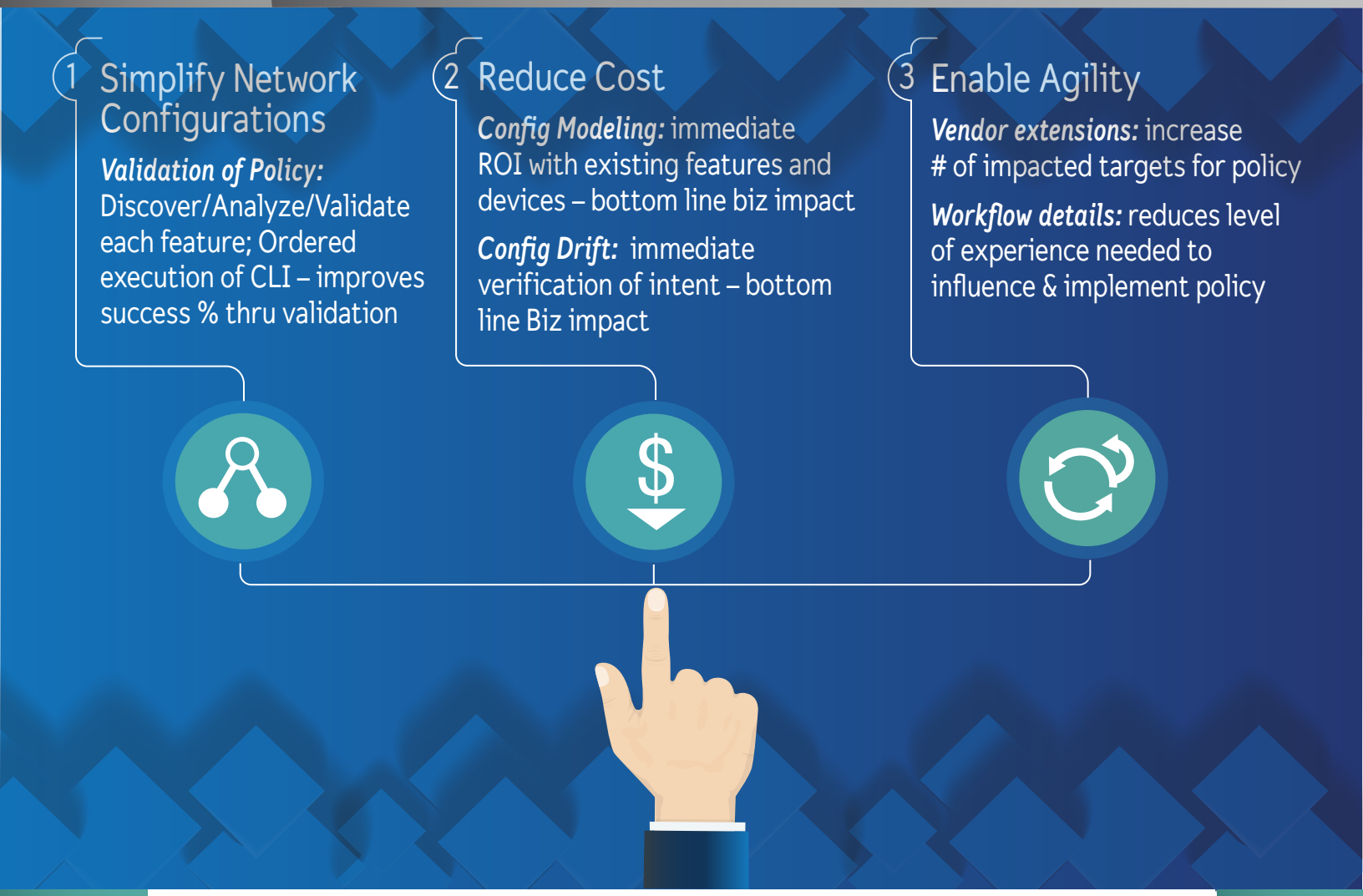
Config Modeling: immediate ROI with existing features and devices – bottom line biz impact

Config Drift: immediate verification of intent – bottom line Biz impact

3 Enable Agility

Vendor extensions: increase # of impacted targets for policy

Workflow details: reduces level of experience needed to influence & implement policy



Proof Points Gluware Intent Proof Points

Proof Points

- Multivendor Whitelist ACLs allow simple execution for new Business apps
- Multi-vendor = Enabling Agility via Vendor Extensions
- Business App support = direct impact on business need
- Executed using Orch Engine = assured validation while executing

Proof Points

- Network Isolation using multiple mechanisms on multiple device types and vendors
- Isolation = abstraction of business intent to ACL, Ports, Interfaces, Firewalls
- Multi-vendor/device = broader impact and agility

Use-Case

1

"Whitelist Applications Explicit Permit" Policy for Network Security through Access-List/Rule management across multi-vendor routers and Firewalls

Problem

Enterprise customers are constantly making changes to their network, deploying new branch offices and turning on and off applications. One specific use case enterprise customers deal with on almost a daily basis is updating an Access-Control- List (ACL) across their network to enable a new application. Most enterprise customers block all traffic and "whitelist" only approved applications. Enterprise IT does not want to waste time determining the correct syntax for a new ACL rule for each of their vendors in their network when a new application needs to be deployed across all their branch locations. Enterprise IT wants to specify the "intent" of permitting a new application and have that automatically pushed across their network.

Solution

Using Gluware, an enterprise IT person can enable new applications across their entire network or a subset of their network. With Gluware' s solution an IT operations person can select the application they want to enable, (example: MS Office 365, Google Services, or Salesforce) and the group of target devices, (example: Cisco routers, Juniper routers, Fortinet firewalls and Palo Alto firewalls). Gluware will translate the "explicit permit" of enabling the application into the vendor specific commands and apply them to all specified devices. Gluware's solution greatly reduces the time it takes to enable new applications and eliminates the need for IT personnel to manually log in to multiple devices to make ACL changes, which is very time consuming and error prone.

Use-Case

2

"External Network Lock Down" Intent for Network Security

Problem

Many enterprise customers have large networks that can span across the globe. The number of security threats are growing, and being a victim of a security vulnerability can have devastating effects on a company. Enterprise customers want the ability to "lock down" their network when a vulnerability has been identified. The lock-down can be used to isolate specific branch locations that may be compromised, or for shutting down WAN connections to isolate branches and protect the core network. Enterprise customers need a simple automated method to quickly apply a lock-down.

Solution

Gluware enables a solution that allows an enterprise customer to initiate a "lock down", protecting their network during a security event. A user can define one or multiple lockdown policies, which can include shutting down ports, interfaces, updating router/switch ACL rules and firewall policy. These lockdown policies can be pre-defined and made available to IT operations or to network security personnel. When a security event occurs, these predefined lockdown policies can be selected and deployed on the targeted areas of the network. Gluware will push the appropriate configuration to the targeted routers, switches, and firewall devices, essentially applying a lock-down of the network and potentially averting catastrophic impact to the network and the company's business, which is very time consuming and error prone.

Summary

Intent-based Network networking is in a nascent state; however, they are emerging to redefine networking as we know it, and provide the agility that businesses demand. Early technologies that are implementing these capabilities are providing useful tools to analyze and verify the current network state – and possible alternate states. These will enable IT operations to spend less time trouble-shooting and more time performing strategic work. Gluware has developed a platform to automate and orchestrate multi-vendor IT networks. Using solution packages, many of the benefits of Intent-based Networking can be realized today - including simplifying operations, automating mundane tasks, eliminating manual errors and reducing cost and network downtime. As the requirements for IBN progress, solutions will follow until we are telling our virtual assistant to make a network change while riding in our self-driving car.

Goals of Simplifying Configs, Reducing Cost, and Enabling Agility combined with the Continuous Intent Cycle described by MIT/VMWare delivers on the slope illustrated in the diagram below.