Top 10 NETWORK AUTOMATION USE CASES

How to Drive ROI by Prioritizing the Right Use Cases

itential®

Introduction

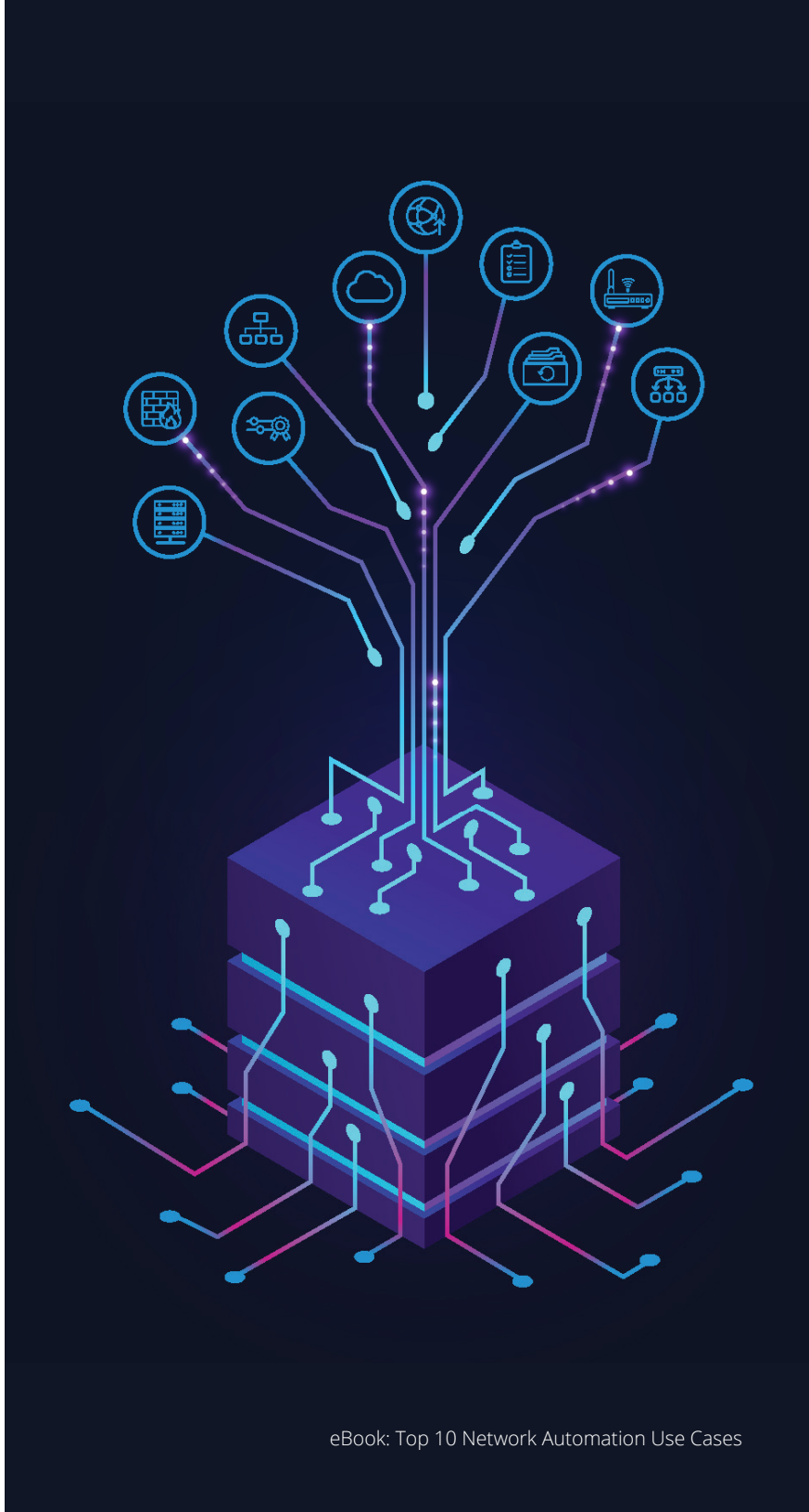
As networks become more complex, the activities necessary to maintain and grow them become exponentially more difficult and time-consuming. Due to the constant pressure put on IT and NetOps teams to ensure their networks meet these growing demands, tasks such as software upgrades, migrations, and provisioning of new network elements in an efficient and compliant manner is critical and network automation is required to accelerate and maintain network operations.

While many IT and Networking teams have just started down the road of network automation, others are still considering their first steps. Both groups face the question of which use cases to tackle first in order to realize the most value. The key to any successful automation project starts with choosing the right use cases. In this eBook, we will dive into how to prioritize the top network automation use cases, how to calculate the ROI and expected time and cost benefits that automation can deliver.

How to Evaluate & Prioritize Automation Use Cases

Before we dive into each use case, it's important to understand how best to evaluate and prioritize where to start with network automation based on the value your use cases would deliver for your organization. Here are some steps to help you determine which activities may be the lowest hanging fruit:

- Define the following:
  - Activities you are spending most of your day on currently.
  - Activities you are not able to get to as a result of the activities that your day is comprised of currently.
  - Integrations that traverse these use cases.
  - Existing automation efforts in scripts, spreadsheets, etc.
- Segment these activities out by day-to-day maintenance activities (e.g. software upgrade) or revenue-generating activities (ex. provisioning a customer or turning up a new service).
- Quantify the volume of each activity (ex. How many times per day/month/year do we do this activity?).
- Quantify how much time is spent each time you do this activity.
- Quantify how much end-to-end time, including network-facing activities (pushing config, pre/post-checks) and administrative activity across ticket lifecycle, updating sources of truth (IPAM, DNS, Telemetry/Assurance, etc.).
- Break the total out by minutes/hours of hands on keyboard vs. hours/days spent waiting on others, sitting in a ticket queue, etc.



Top 10 Network Automation Use Cases

1. Software Upgrades
2. SD-WAN Branch Management
3. Configuration & Compliance
4. DNS Updates
5. Load Balancing
6. Firewall Configuration Change
7. Virtual Private Cloud Networking
8. Virtual LAN (VLAN) Changes
9. Device Onboarding
10. Firewall Policy Management

1 SOFTWARE UPGRADE

Easily the most common network activity, regular software upgrades are required to maintain operation of network devices. It is important that this process be efficient, accurate, and repeatable in order to avoid network vulnerabilities from out of date software on devices.

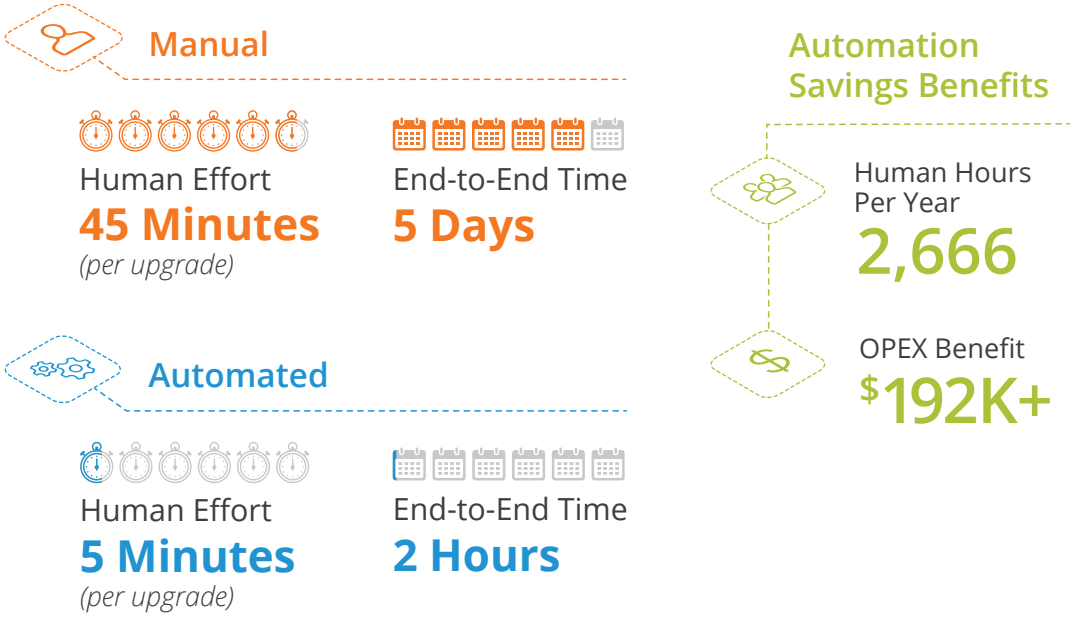
Why Automate Software Upgrades?

- Effectively and efficiently run new technology and software.
- Support new services and architect the network to the desired state.
- Reduce risk for an outage or an intrusion to the entire company by a missed or failed vulnerability patch.

The Value of Automating Software Upgrades

Due to the manual effort required, software upgrades tend to stay in the backlog or only happen once a year. With automation, organizations can automatically discern which devices are vulnerable and upgrade in real-time so, networking teams can focus on bigger projects and security teams can sleep better at night. Automation can:

- Increase the number of devices upgraded in a single 5 hour maintenance window from 2 to 90.
- Decrease cycle time per router from 4 hours to 45 mins.
- Save over $200K+ cost reductions per upgrade cycle.



Assumptions: Devices = 1,000 Frequency = 4/year

2 SD-WAN BRANCH MANAGEMENT

SD-WAN branch management consists of the configuration and activation of connectivity between existing enterprise offices and new locations being brought online. It provides a multi-cloud architecture for businesses to optimize exponential traffic growth, reducing operational costs. How you deploy SD-WAN in Day 0 and 1 has a big effect on how efficient and automatable the management of your SD-WAN network will be in Day 2+.

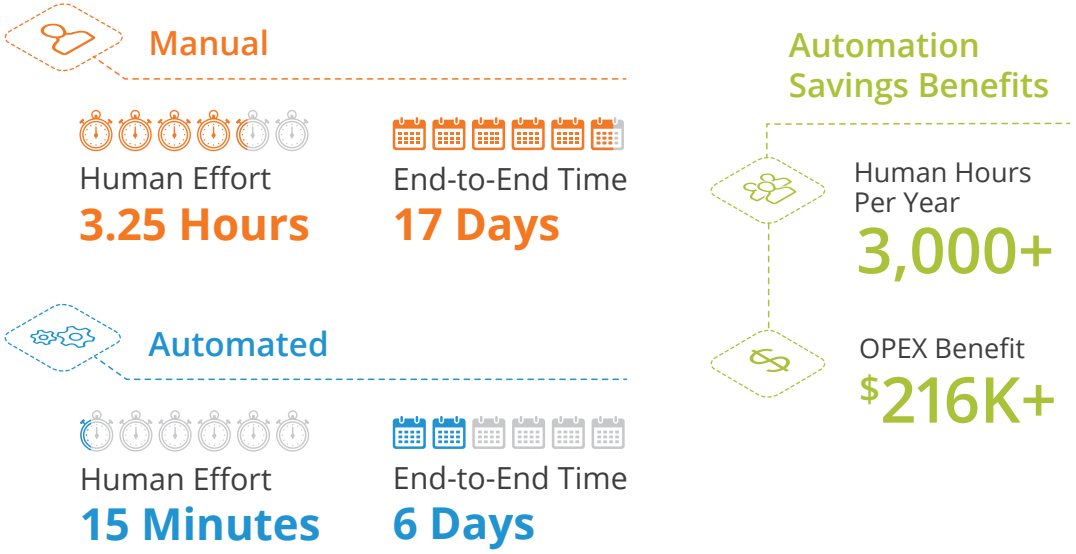
Why Automate SD-WAN Branch Management?

- Increase cloud application performance.
- Integrate siloed operations across distributed multi-domain networks, complex platform interactions.
- Lower operational costs.

The Value of Automating SD-WAN Branch Management

Enterprises need to look at leveraging automation for multi-domain, multi-vendor systems involved in the entire SD-WAN deployment process. Implementation of fallout feedback loops and expansion of active participation to IT and Operations teams will increase rate of change and minimize human errors. Automation can:

- Decrease the number of manual steps from 42 to 3, which saves significant cycle time and reduces operating costs.
- Reduce the time it takes to deploy and manage SD-WAN from 17 days to 6 days, resulting in over 3,000 hours saved on branch management.



Assumptions: Devices = 1,000 Frequency = 4/year

3 CONFIGURATION & COMPLIANCE

NetOps teams are responsible for managing device configurations, including audit and compliance, to avoid and manage configuration drift. Activities also include turn up of network devices, migration of devices, replacement of devices, or auditing and remediation of compliance to a defined standard. Configuration standards and compliance are critical for businesses to ensure accurate representation of networks over time for real-time informed decisions and adhering to security and audit requirements.

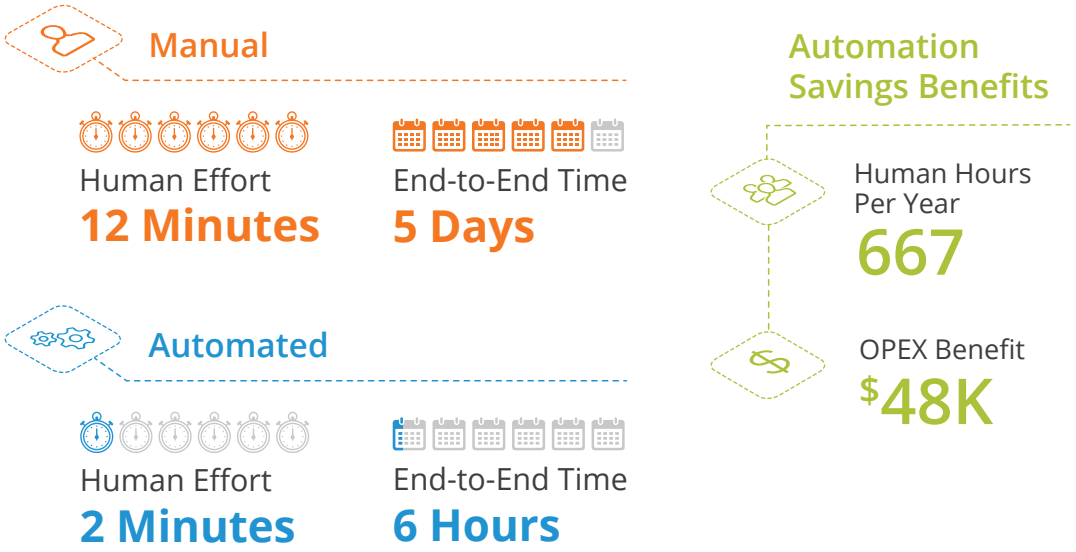
Why Automate Configuration & Compliance?

- Severely reduce performance issues or network outages costing businesses time, money, and lack of customer retention.
- Eliminate interoperability issues and errors updating configurations across any device type or domain caused by lack of configuration standards.

The Value of Automating Network Configuration & Compliance

Automating network configuration and compliance allows enterprises to easily standardize configurations across their network infrastructure. Successfully implementing Golden Configurations provides a uniform centrally defined way to view and manage configurations and policies, audit them for compliance, and remediate across all different types of devices and domains. Automation can:

- Reduce the end-to-end time for configuring devices, from opening an IT ticket to the completion of the configuration check and remediation from 5 days to 6 hours.
- Save up to 667 manual hours per year, resulting in a $48,000 OPEX cost savings.



Assumptions: Devices = 1,000 Frequency = 4/year

4 DNS UPDATES

Maintenance and updating of Domain Name System (DNS) records such as host names, IP address, and zone is essential as business websites rely on multiple servers to manage their services. Out of date, incorrect, or slow manual migrations can cause outages to these desired services. These issues are time consuming and complicated to resolve, involving cross team cooperation and ultimately costing businesses additional overhead costs, and delayed time to market and time to revenue.

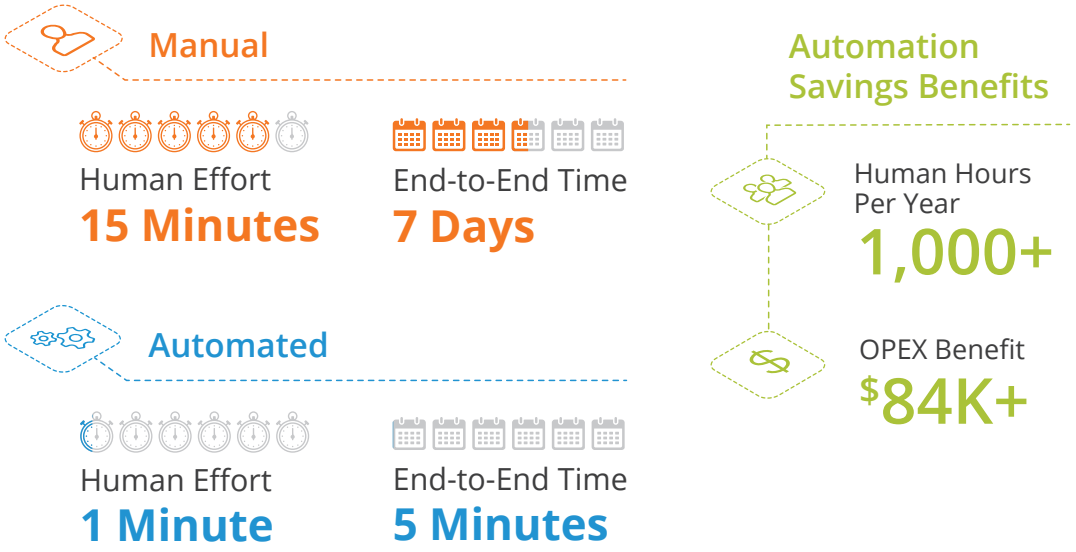
Why Automate DNS Updates?

- Accelerate the fulfillment of DNS update requests, so other teams can quickly provide new applications, services, or functionalities to customers.
- Avoid duplicating records and correctly assign resources.
- Stay on top of critical security updates.

The Value of Automating DNS Updates

By automating pre and post-checks, you can eliminate manual errors and tie together a holistic, safe guarded operational process. Automation can:

- Decrease the length of customer wait times from 24 hours to 5 minutes, reducing operating costs and improving customer retention and satisfaction.
- Reduce deployment time from 7 days to 5 minutes.



Assumptions: Devices = 1,000 Frequency = 5/year

5 LOAD BALANCING

Load balancer management includes the configuration of load balancing rules, virtual IPs (VIP), creation of load balancer pools, and the onboarding of new servers or devices. These activities are critical for businesses as they not only enable efficient distribution of incoming network traffic but also ensure the reliability of services that reside on them by quickly responding to failovers.

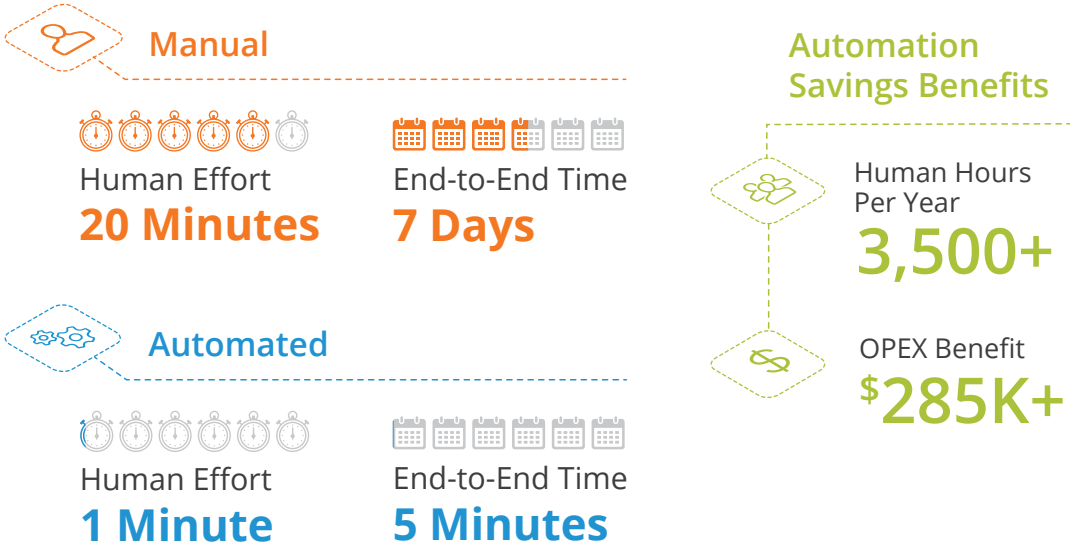
Why Automate Load Balancing?

- Avoid performance issues for customer facing and internal services.
- Customer retention.
- Stay ahead of maintaining pace with server security updates as infrastructure continuously changes.

The Value of Automating Load Balancing

A consistent strategy for management of load balancing and VIPs customized to the evolving network infrastructure will look to meet requirements across all teams involved and reduce inconsistencies and cycle times. Automation can:

- Decrease human hours spent per year by almost 4,000.
- Reduce inconsistencies and cycle times while improving customer retention and satisfaction to see a 95% savings and increased throughput capacity.



Assumptions: Devices = 1,000 Frequency = 25/year

6 FIREWALL CONFIGURATION CHANGES

Firewall configuration changes includes the validation, management, and configuration of policy rules across the network. Accurately maintaining and updating organizations' policies across their network is critical for avoiding network outages, and adhering to security and audit requirements.

Why Automate Firewall Configuration Changes?

- Eliminate long maintenance windows and network outages.
- Ensure the right traffic is let through while the wrong traffic is not.

The Value of Automating Firewall Configuration Changes

Automated deployment and validation of firewall configuration ensures changes are executed safely, with limited to no downtime, while reducing the time spent on this activity during a finite number of change windows. Automation can:

- Decrease the number of failed configuration changes from 1 in 3 to see an 80%+ increase in accuracy and mitigate downtime.
- Reduce annual OPEX spend by almost $275,000.

Manual

Human Effort
20 Minutes

End-to-End Time
2 Days

Automated

Human Effort
1 Minute

End-to-End Time
5 Minutes

Assumptions: Devices = 1,000 Frequency = 12/year

Automation Savings Benefits

Human Hours Per Year
3,800

OPEX Benefit
$274K+

7 VIRTUAL PRIVATE CLOUD NETWORKING

Virtual Private Cloud Networking encompasses provisioning cloud infrastructure with configuration of the subnets, route tables, internet gateways, ACLs, and security access groups. As businesses continue to expand or migrate towards leveraging cloud infrastructure, private cloud networking provides self-service, customizable controls for application performance, and security policies.

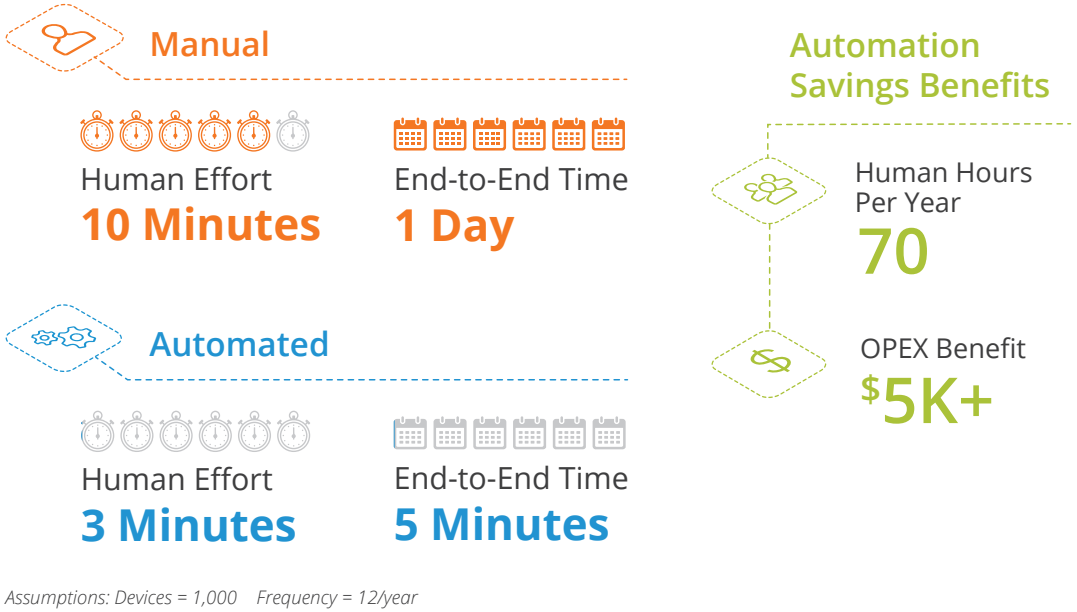
Why Automate Virtual Private Cloud Networking?

- Rationalize the investments made in cloud infrastructure.
- Full control over security settings such as routing policies that can suffer application performance due to excess congestion outside of a private network.

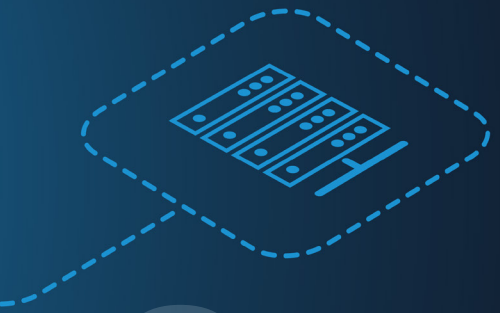
The Value of Automating Virtual Private Cloud Networking

This enables faster deployments, mitigates risks of configuration errors, and provides an audit of changes. Automation can:

- Reduce the end-to-end time by 99.6%.
- Save 70 human hours per year.



Assumptions: Devices = 1,000 Frequency = 12/year



8 VIRTUAL LAN (VLAN) CHANGES

As a result of virtualization, the data center environment has quickly transitioned from static to dynamic. As applications and workloads grow, shrink, and shift based on client demands, the network team must also make changes to the VLAN configuration on their devices to match these changes.

Why Automate VLAN Changes?

- Increase quality of service for customers' who require a VLAN change.
- Improve customers' ability to use the application.

The Value of Automating VLAN Changes

Automation of VLAN changes to the data center network in coordination with workload and application changes significantly reduces the turnaround time to complete a VLAN change, ensuring customers stay satisfied. Automation can:

- Reduce the end-to-end automation time of a VLAN change from 7 days to 5 minutes.
- Save over $200,000 in OPEX cost annually.

Manual

Human Effort
15 Minutes

End-to-End Time
7 Days

Automated

Human Effort
1 Minute

End-to-End Time
5 Minutes

Assumptions: Devices = 1,000 Frequency = 12/year

Automation Savings Benefits

Human Hours Per Year
2,800

OPEX Benefit
$201K+

9 DEVICE ONBOARDING

Device onboarding consists of the configuration and activation of a new device in the network. It requires consistent application of standard configurations to meet the quality goals of most network operators. This is critical for businesses to rapidly extend their networks, provide services to and activate new customers, as well as improve quality of service. Proper management is needed for the application of Day 0 configurations for network connectivity, Day 1 configurations for operational settings, and management of device configuration over time.

Why Automate Device Onboarding?

- New customer revenue.
- Increase customer retention as businesses exceed customers' expectations of service.

The Value of Automating Device Onboarding

Automation replaces manual operational processes, reducing swivel chair and touch points for expedited provisioning and activation times. Automation can:

- Decrease customer onboarding time from 45 days to 2 days, which improves customer retention and increases realization of new customer revenue.
- Turn a 20 day end-to-end process into a 5 day process resulting in $270k+ annual OPEX saving.

Manual

Human Effort
4 Hours

End-to-End Time
20 Days

Automated

Human Effort
15 Minutes

End-to-End Time
5 Days

Automation Savings Benefits

Human Hours Per Year
3,000+

OPEX Benefit
$270K+

Assumptions: Devices = 1,000 Frequency = 12/year

10 FIREWALL POLICY MANAGEMENT

Firewall policy management is needed to ensure the continuous monitoring and maintaining of the compliance of policy rules across the network. Complex networks require a significant time investment to manually ensure, monitor, and update policies. Constant change of requirements outpaces the time it takes to discover and remediate out of compliance policies. Accurately maintaining and updating organizations' policies across their network is critical for avoiding network outages and adhering to security and audit requirements.

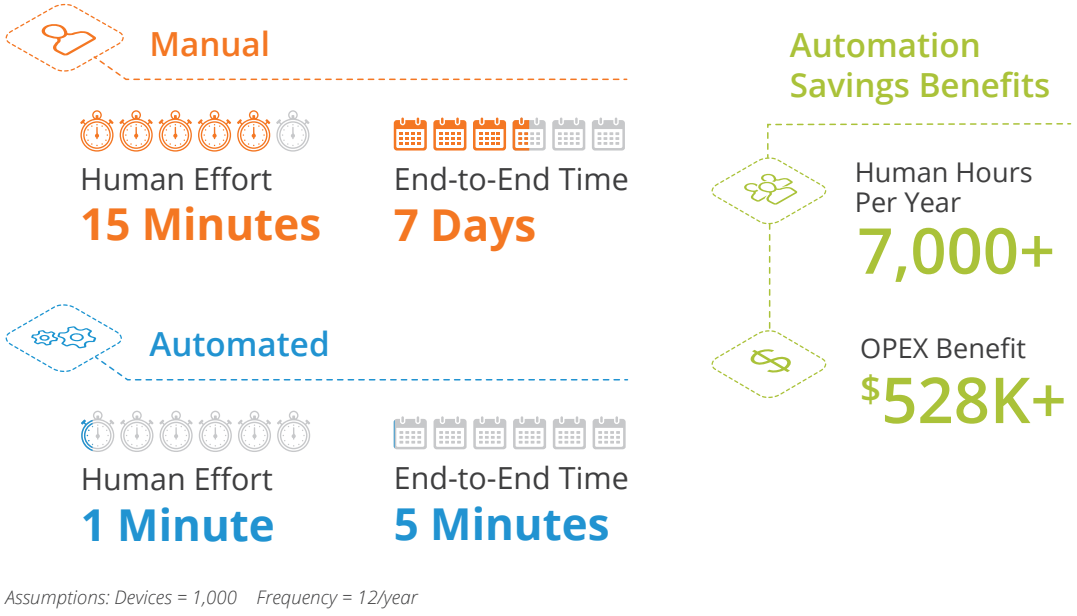
Why Automate Firewall Policy Management?

- Severely reduce long maintenance windows.
- Reduce network outages and security risks that cost businesses time, money, and their reputations.

The Value of Automating Firewall Policy Management

Greatly reduce labor efforts and cycle times by implementing automation of firewall policy management. Automating the business systems and policy management tools instills greater trust in accuracy level of rule replacement. Automation can:

- Reduce cycle times from days to just minutes.
- Save over 7,000 manual hours, resulting in over $500,000 OPEX saved annually.



Assumptions: Devices = 1,000 Frequency = 12/year

How to Calculate the Value of Automation

Now, let's do the math. By comparing your current manual state to the future automated state for each use case, it's easy to rank them in order of benefits your organization can achieve by automating each use case. But there are a few things to consider when making sense of the savings to build your business case:

- OPEX isn't always hard cash flowing in or out of the business but does represent a significant value to any organization. In the model below, it estimates productivity improvements which may show in the form of backlog reduction, enhanced capacity, and more.
- The sum total of the results may be difficult to believe at first and you may be skeptical of your own results. However, the estimates used in this ebook are based on real world examples, and should be viewed as good representations of one organization's results - yours may vary.
- You shouldn't overlook the importance of end-to-end time improvements as this is where your organization can see real value (customer satisfaction, reduced time to revenue, etc.) by completing tasks more quickly.

While value can be perceived in many different facets, the scope of this eBook presents a simple model (improvement x task volume) with a handful of estimated metrics to start building your business case and understanding the value automation can deliver.

Human Effort Saved

=

(Human Manual Time - Automated Time) x (Device Count x Frequency Per Device)

Automation OPEX Benefit

=

Hours of Human Effort Saved x Hourly Labor Rate (FTE)

End-to-End Time Saved

=

(Manual End-to-End Duration - Automated End-to-End Duration) x (Devices x Frequency Per Device)

Realizing the Value of Automation

Here's a few example calculations of top use cases and the benefit automation can deliver:

Software Upgrades

1,000 devices upgraded 4 times per year currently require 45 minutes of human effort and spans 3 days (7,200 minutes) of end-to-end duration (prep, scheduling, pre-check, install, post-check). Automation reduces this process to 5 minutes of human effort within a 2 hour (120 minutes) end-to-end duration. Assume a loaded FTE rate of $72.11/hour ($150,000 on 2,080 hour work year).

Human Effort Saved: (45 minutes – 5 minutes) x (4 times annually x 1,000 devices) = 160,000 minutes saved or ~2,666 hours

Automation Benefit: ~2,666 hours x $72.11 = $192,245

End-to-End Time Saved: (7,200 minutes – 160 minutes) x (4 times annually x 1,000 devices) = 28,320,000 minutes (472,000 hours / 53 years of duration reduced)

Load Balancing

500 devices configured, created, or onboarded 25 times per year currently require 20 minutes of human effort and span 7 days (10,080 minutes) of end-to-end duration (prep, scheduling, pre-check, configure, post-check). Automation reduces this process to 1 minute of human effort within a 5 minutes end-to-end duration. Assume a loaded FTE rate of $72.11/hour ($150,000 on 2,080 hour work year).

Human Effort Saved: (20 minutes – 1 minute) x (25 annually x 500 devices) = 237,500 minutes saved or ~3,958 hours

Automation Benefit: ~3,958 hours x $72.11 = $285,456

End-to-End Time Saved: (10,080 minutes – 5 minutes) x (25 times annually x 500 devices) = 125,937,500 minutes (2,098,958 hours / 239 years of duration reduced)

Device Onboarding

1,000 devices onboarded 1 time per year currently require 4 hours of human effort and span 20 days (28,800 minutes) of end-to-end duration (prep, scheduling, pre-check, onboarding, post-check). Automation reduces this process to 15 minutes of human effort within a 5 days (7,200 minutes) end-to-end duration. Assume a loaded FTE rate of $72.11/hour ($150,000 on 2,080 hour work year).

Human Effort Saved: (240 minutes – 15 minutes) x (1 time annually x 1,000 devices) = 225,000 minutes saved or ~3,750 hours

Automation Benefit: ~3,750 hours x $72.11 = $270,432

End-to-End Time Saved: (28,800 minutes – 7,200 minutes) x (1 time annually x 1,000 devices) = 21,600,000 minutes (360,000 hours / 41 years of duration reduced)

The total value of automating these three use cases can deliver:

- **Human Effort Saved:** ~10,374 Hours
- **Automation Benefit**: $748,195
- **End-to-End Time Saved:** 175,857,500 minutes (2,930,958 hours / 333 years of duration reduced)

Jumpstart Network Automation Use Cases with Itential

Itential is intelligent automation for multi-domain networks. Our automation platform provides an easy on ramp for customers to rapidly adopt network automation for all use cases. Our Pre-Built Collection enables organizations to start fast and stay fast by providing out of the box, customizable, and reusable components that simplify and accelerate network automation initiatives.

Pre-Built Automations

With Itential's Pre-Built Automations, organizations can start fast, onboard automation principles quickly and stay fast, mitigating manual management and reducing errors. Our Pre-Built Automations are packaged and self-contained, and include all the relevant documentations, files, scripts, dependencies, and logical components that are needed to execute the automation such as workflows, forms, Golden Configuration tree, command templates, and more.

Explore Our Library of Pre-Built Automations >

Pre-Built Integrations

The Itential Automation Platform is an API first, vendor-agnostic solution that connects to everything and acts as an aggregated network API, transforming and federating functionality and data from existing northbound and southbound systems. With over 50+ out of the box adapters as well as the ability to auto-generate your own to any system using our Adapter Builder, Itential simplifies integration, mitigating vendor lock-in and custom development hurdles for network automation.

Explore Our Library of Pre-Built Integrations >

By utilizing Itential's Pre-Built Automations and Integrations, you can:

- Expand on your automation strategy by addressing new use cases.
- Customize Pre-Built Automations to meet your requirements and needs.
- Mitigate integration hurdles, stop swivel-chairing and avoid proprietary vendor lock-in.
- Follow embedded best practices in driving an end-to-end automation strategy.
- Enable DevOps and NetOps teams to onboard automation principles quickly.
- Eliminate the backlog and focus resources on new growth and innovation opportunities.

Experience the Power of End-to-End Network Automation

Simplify & accelerate network automation with Itential

Automate Any Network Domain

Today's networks require automation capabilities that span multiple domains from traditional physical networks, next-generation programmable networks, SD-WANs, cloud networks, and more. With Itential, seamlessly automate across any network domain and any network vendor.

Automate Any Network Change

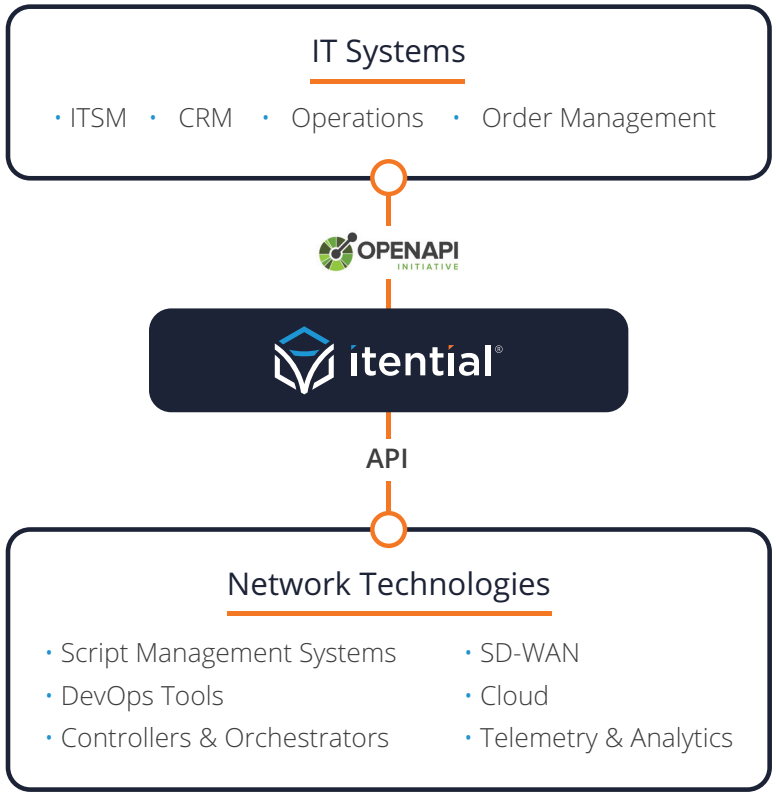
Automate any network change from routine operations tasks such as software upgrades to managing device configuration and compliance to service lifecycle and policy management. Itential's purpose-built applications simplify and automate network management, reducing the scope of human errors.

Connect to Everything

Itential simplifies your network automation ecosystem by providing a single, aggregated network API that connects all of your IT systems with your orchestrators and controllers, configuration tools and custom-built scripts to enable true end-to-end network automation.

Enable Automation For All

Enable network engineers, software developers, and IT operations to participate in network automation. Itential's low-code environment enables developers and network engineers alike to easily design, build, and visualize flexible and reusable workflows to drive rapid network automation deployments.



Resources

Explore Itential Developer Hub >

Watch On-Demand Webinars >

Request Custom Demo >

Read the Itential Blog >

About Itential

Itential is purpose-built for today's complex, multi-domain and multi-vendor networks. From cloud-based networks to branch, data center, and cloud networks and from NFV to distributed WANs – our powerful network automation software is used within some of the largest networks in the world to automate complex, business-critical changes at breakneck speeds. From Fortune 500 telecommunications and financial service companies to enterprises of all sizes, our world-class products accelerate the move toward software-driven networks and next generation, agile network operations.

itential®

itential.com

developer.itential.io

info@itential.com