>>> network .toCode()

Maximizing Returns:

The ROI of Network Automation

Part 1

>>> Introduction

Enterprises squander millions of dollars each year by holding on to outdated, inefficient, and ineffective network management models.

When challenges arise, the customary response is to recruit, train, and operationalize more engineers, but this approach often fails. The increasing complexity and scale of today's networks drives demand for engineers ever higher, and the costs are unsustainable.

Thankfully, a compelling alternative has emerged: network automation.

Network automation not only slashes costs by a factor of ten but also substantially reduces error rates and accelerates delivery speeds tenfold. Moreover, it helps networking teams adapt seamlessly to the ever-changing requirements of business.

The network automation market is expected to grow by more than 22% per year until 2030, resulting in a total addressable market exceeding $15 billion. Tasks that previously demanded thousands of labor hours have been reduced to just a few hundred, saving millions of dollars annually. Automation, known for its high predictability and repeatability, is augmenting personnel to provide unparalleled levels of service quality. This collaboration not only enhances outcomes but delights end-customers with great customer experiences and elevates the overall employee experience.

Network to Code has established itself as a front-runner in network automation by embracing the DevOps principles and philosophies that originated in software development and combining them with network engineering best practices. This fusion, termed NetDevOps, is the foundation of our work that drives exceptional outcomes for our clients.

In a recent example, Network to Code facilitated a major retail chain's equipment upgrade at over 900 locations. This initiative saved the retailer over $400,000 and slashed their resource commitment by over 90%, effectively returning thousands of hours to the core operations of the business.

A second example involved consolidating applications at an international brokerage company. This initiative kicked off with a deployment of Nautobot, a purpose-built open source automation and Source of Truth platform, which laid the groundwork for the company to build a full observability stack for their network infrastructure. NTC crafted multiple dashboards showcasing device and interface metrics, NOC perspectives, device uptime, bandwidth usage, and a monitoring framework for their telemetry setup. Customized alerts were also created, using the ingested data. These new tools quickly reduced the duration and frequency of outages, providing an immediate benefit to the customer.

Beyond tailored services and solutions, Network to Code fully embodies the NetDevOps philosophy. NTC's distinctive market position has facilitated the creation of Nautobot; with over 25 pre-built applications, its capabilities can be expanded to rapidly operationalize common automation use cases. Further, it has native integrations with top vendors such as Cisco and Arista, plus an open API architecture allowing it to easily integrate with other enterprise resources such as Ansible and ServiceNow. Furthermore, it offers versatile deployment options, including both on-premises and cloud SaaS solutions, accompanied by a wide array of support choices.

This two-part series eBook will help you build a compelling case for **embracing network automation** by covering these topics in subsequent chapters:

Part 1:

1. The limitations inherent in legacy management practices;
2. The advantages that network automation brings;
3. The financial gains;

Part 2:

4. Strategies for effective implementation;
5. Challenges and misperceptions;
6. How Network to Code is uniquely situated to accelerate your journey.

>>> Chapter 1

>>> *Peering into the Shadows: Drawbacks of Legacy Management Practices*

Legacy network management methods can no longer meet the escalating demands around reliability, accessibility, security, and performance. As the march of progress asks more of administrators, the drawbacks are becoming more evident.

Let’s consider how a typical network operations center functions:

A dedicated team of network engineers allocates the majority of their time to daily maintenance tasks, such as fielding support calls, processing alarm-generated tickets, and responding to user and vendor emails. While these tasks are imperative, little time is left for other essential endeavors like configuration and change management, leading to extended timelines and limited availability for new projects.

When high-impact faults occur, the team's attention quickly pivots to fixing the issue and resuming regular operations. Sometimes, thorough root cause investigations are overlooked, possibly leaving certain business risks unaddressed.

Another challenge is the increasing pace and volume of network operating system upgrades, which are often treated as an afterthought, carried out only in response to critical needs. This approach restricts access to new features and leaves vulnerabilities unaddressed.

When enterprises take reactive approaches and emphasize tactical operations, documentation becomes incomplete and outdated, which confuses engineering teams and leads to inefficiencies and mistakes. Major planning endeavors are understaffed and expedited, resulting in suboptimal solutions. As workloads surge, teams look to hire additional engineers in an increasingly competitive landscape. Remarkably, all of this occurs despite the unwavering diligence of the team. Let’s delve into the specific challenges posed by legacy management practices and shed light on their inherent shortcomings.

>>> Financial Leakage: Uncovering Unnecessary Operating Costs

The primary downside of traditional network management is the extensive human effort demanded by nearly all tasks. Systems administration and software development have devised strategies to address this challenge, but network management lags behind. Whether updating interface descriptions or executing operating system upgrades, each task mandates significant human involvement.

Consequently, as the business grows and new technologies are introduced, the demand for productivity intensifies, necessitating the hiring of additional personnel. Every new role incurs fresh costs, from recruiting and interviewing to onboarding and training, plus ongoing compensation expenses. The networking industry can no longer afford to view these as inherent costs of doing business. Today’s networks include a diverse array of vendors and deployment models, which creates an ongoing cycle of training, retraining, and recruitment.

The proliferation of network-connected devices further introduces interoperability and security concerns.

Meanwhile, teams must continue to contend with the historical challenges of managing geographically dispersed networks by maintaining experts in diverse fields in multiple time zones and overseeing personnel with conflicting schedules, different languages and cultural distinctions. Unfortunately, these factors all further contribute to an increase in expenses.

The rapid evolution, growing complexity, and expanding scale of modern networks is surpassing the capacity of the current network engineering workforce. The US Bureau of Labor Statistics foresees a meager 2% growth in the number of network engineers through 2031. The need for a new approach has become evident to numerous industry leaders, prompting major manufacturers to incorporate development environments and training programs that pivot on automation.

>>> Unnoticed Losses: Revealing Inefficiencies in Resource Management

Inefficient network management practices impede operations, stifle innovation, and cause unnecessary delays.

Take into account that 43% of network professionals say they don't have enough time to engage in business initiatives. When these endeavors are sidelined, they can hinder innovation. Not only does the staff find themselves overwhelmed by the existing state of operations, but they also lack the opportunity to do anything about it. It puts their companies at a significant competitive disadvantage.

Routine operations also experience unnecessary delays. When requests are received, they are individually and sequentially processed manually, potentially lasting for days. Certain requests necessitate the involvement of multiple individuals for review, implementation, and verification, creating fresh possibilities for delays at each step. This situation leaves the requester waiting until the entire process is completed, preventing them from carrying out essential job functions.

Let's consider the inefficiencies inherent in a major project like upgrading the operating systems across several thousand devices. The initial phase involves conducting a network audit. Ideally, this process would be scripted, but even in scripted scenarios, creation, execution, and results validation are essential tasks. It's almost inevitable that some systems may have been offline or unresponsive during the audit, necessitating multiple attempts.

Once the audit accurately outlines the scope of work, a team of engineers is assigned to carry out the task. These engineers must manually upgrade dozens of systems each night until the project reaches completion. Following the upgrade, another audit is conducted to identify systems that may not have been upgraded correctly. Due to the manual nature of this process, which is susceptible to human error, it's expected that approximately 3–5% of the systems will have experienced upgrade failures.

These systems require revising by the engineering team for another upgrade attempt.

Overall, a project of this magnitude typically spans several months to half a year to reach completion.

In this model, the demands for team training are substantial. Whenever there's a revision to a business or technical process or the introduction of new compliance standards, team members must be trained for these changes—work that does not significantly contribute to the business's value.

Networks managed under this model also assume excessive technical debt. The presence of disorganized configurations makes management, troubleshooting, and scalability challenging. Inadequate documentation practices make it difficult to understand how the network operates. Engineers are confused by inconsistent naming conventions, requiring them to learn a configuration's purpose each time they encounter it. Undocumented work-arounds are scattered throughout the network, resulting in unnecessary throttling, adjustments, and unpredictable network behavior. Outdated systems with limited functionality and compatibility are prevalent. And inadequate backups and obscure recovery processes complicate disaster recovery operations.

>>> Unanticipated Liabilities: Risks Unconsciously Assumed

With traditional network management practices, organizations assume unnecessary risks. Relying excessively on human labor gives rise to errors and inefficiencies that materialize as security vulnerabilities, network outages, and uncertainties.

Mistakes are a natural part of human-led activities, and certain circumstances increase the likelihood of errors. Tasks performed when engineers are fatigued, distracted, facing a crisis, or dealing with unfamiliar situations tend to have a higher error rate. Unfortunately, these conditions are quite common in the field of network engineering.

Additionally, network engineering tasks are inherently complex. Managing networks involves issuing precise, syntax-sensitive commands, interpreting cryptic outputs, and recalling concepts from dense textbooks and lectures.

Considering these challenges, it's not surprising that human error is a major concern in network management. In fact, it's responsible for 75% of the hours when the network displays degraded or failed conditions, making it the leading cause of network outages.

Human error also poses security risks. Consider a network security standard that isn't consistently applied or an access control list with a single-character error. Such errors can make networks vulnerable to security breaches. Furthermore, when networks are not well understood, it can delay security responses to these intrusions.

Then there's the issue of inadequate documentation. How can an engineer determine if a network is functioning correctly without a documented standard for comparison? To be effective, network documentation must be current, accurate, and easily accessible. Typically, documentation is created during the network's design phase. However, as network changes occur, the network's operation may deviate from its original design.

The manual updating of network documentation can also introduce errors, such as incorrect copying or placing information in the wrong field. This can pose challenges for future engineers in identifying and rectifying these errors. Lastly, when network documentation is dispersed across various platforms, accessibility issues arise, rendering the information less useful.

>>> The Looming Crisis: Future Hurdles for Legacy Management

The prospects for managing networks using traditional methods are bleak. Network-connected technologies are rapidly permeating every facet of business operations. New technologies and vendors constantly enter the scene. The rising frequency and complexity of cyberattacks are complicating security postures and introducing stringent compliance requirements. Relying solely on human-led efforts to navigate the complexities of modern networks is no longer sustainable. Workloads are on the rise, and finding new engineers is increasingly challenging, as only 12.5% of organizations find it easy to hire and retain skilled networking professionals. Enterprises that embrace innovation and break away from the linear relationship between value and workforce size are the ones poised for survival and prosperity.

>>> Chapter 2

>>> Network Automation Unleashed: Transforming Enterprises

NetDevOps practices deliver results that are simply light-years ahead of legacy management approaches.

Productivity is supercharged, streamlining day-to-day operations and enabling common workflows to be completed at speed and scale. Human errors are eradicated. A higher order of business agility is achieved, easing the adoption of new technologies, expediting time to market, and compressing deployment timelines.

Furthermore, the consistent development and application of security policy bolsters network integrity, access control, and availability. The organization has more visibility and can make better business decisions backed by empirical data. Let's explore the triple-win differentiators that make network automation such an exceptionally appealing alternative. We will delve into the advantages it offers to enterprises and their customers and the benefits it brings to personnel.

>>> Fueling Enterprise Excellence: Transformative Benefits

Network automation reduces the costs associated with managing a network to such a high extent that the time it takes to recover these costs is frequently under a year.

Furthermore, because most automations are reusable, the benefits accrue throughout their lifespan. Once a process has been automated, there is no need to revisit it unless there have been changes in the technical or business processes.

Engineers frequently find themselves mired in tedious and repetitive tasks, dedicating a significant portion of their time to basic maintenance. Automations excel at managing these repetitive duties, and computers are more than capable of working continuously without breaks. This liberates personnel to focus on tasks and projects that make the most of their extensive skills. As a result, business initiatives shift from the sidelines to the forefront, enabling enterprises to foster innovation, gain a competitive edge, and bring more responsibilities in-house.

When engineers are empowered to use the full breadth of their skills, engaging with interesting challenges and developing new capabilities, they feel more fulfilled and engaged with the organization's goals.

This leads to a reduction in employee churn, reducing the need to spend time assessing potential candidates and incorporating them into the workforce.

Automation also mitigates operational risks. Networks that operate programmatically ensure they are in their intended state, leading to improved compliance rates. By implementing automated compliance checks, deviations from standards can be identified and addressed. Networks that adhere well to standards experience fewer outages, minimizing disruptions to essential business operations. And when outages occur, they tend to be shorter in duration because the network's desired state is defined, and automated processes can be utilized for diagnosis and remedy. Even if automation doesn't entirely resolve the outage, the process is expedited by applying intelligent diagnostics and attempting common solutions. Moreover, disaster preparedness is improved because operational states can be swiftly reinstated by restoring known functional configurations on both recovered and new hardware. Notably, intent-based networking enables the integration of diverse vendors since configurations are generated based on intent.

These practices create networks that are more scalable, adaptable, and responsive to market dynamics. Managing an influx of orders that impact the network's state no longer necessitates an engineer to execute each individual request. Instead, automated systems can be deployed to manage provisioning. When alterations occur in business or technical processes, there's no need to train personnel; merely modify the automation to reflect the change. Rapid operationalization of new network segments becomes a reality, thanks to automated generation and zero-touch provisioning of equipment requirements and configurations.

Enhancements in responsiveness, compliance assurance, and comprehensive infrastructure patching contribute to improved security postures. Automation plays a role in expediting security incident response times by triggering actions to address common issues. Furthermore, integration with information systems empowers engineers to isolate affected systems more quickly. Data collection techniques ensure that security teams are guided by empirical insights. Automation ensures compliance, guaranteeing consistently accurate configurations and diminishing the number of potential attack vectors. Lastly, the maintenance of operating systems in line with recommended software releases becomes streamlined. Engineering teams can rapidly upgrade operating systems and be confident that their equipment is running the most secure and preferred version.

Operators also benefit from significantly enhanced insight and control. Network information is collected and combined from disparate sources to a unified platform. Automations then draw inferences based on causal relationships that often go unnoticed by engineers, creating a more comprehensive analysis of widely scattered data points. By viewing these relationships in a single pane of glass, engineers can recognize and synthesize them more easily. Furthermore, these systems have the capacity to translate these inferences into action, such as through self-healing network mechanisms.

>>> Creating Astonishing End-Consumer Experiences: Raising the Bar

The advantages of network automation extend to enhance the customer experience as well.

Automation allows customer requests to be addressed 24/7, while ensuring a remarkably consistent process. Requests that previously required days or even weeks due to manual efforts and internal processes can now be swiftly fulfilled through automation, resulting in fewer errors and a highly dependable workflow. This also means fewer customers need to make “chase up” calls to inquire about the status of their request.

Network issues that affect the customer experience are promptly resolved using automation, often before customers become aware of any impact, thus mitigating the more challenging aspects of their experience.

Additionally, customers reap the benefits of reduced costs, as the delivery of value has been decoupled from headcount and manual labor. These advantages establish strong differentiators from competitors, aiding businesses in retaining existing customers and attracting new ones.

>>> Elevating Employee Well-Being: Automation and Enhanced Quality of Life

The employee experience is enhanced through a variety of avenues. Primarily, workloads become more manageable as routine tasks are eliminated from their daily responsibilities.

Additionally, they no longer have to dedicate excessive amounts of time beyond business hours to process changes and address incidents. Consequently, this affords them the chance to allocate more time to deliver outstanding outcomes, bolstering their reputation and offering numerous opportunities for genuine recognition from colleagues and leadership. By extracting the mechanical aspects from human roles, it opens up a pathway for personnel to reach their utmost potential, motivating them to learn, innovate, and pave the way for groundbreaking accomplishments. Furthermore, automation provides the opportunity to re-shore certain operations, and as a result, businesses may find an increase in employee morale. Having operations closer to home can mean improved communication, faster decision-making, and a greater sense of connection to the company’s core values and mission. This can translate into a more cohesive team, enriched company culture, and an overall boost in employee satisfaction.

>>> Chapter 3

>>> *Calculating the Benefits: A Closer Look at Returns*

Having established an overarching understanding of the advantages brought by network automation, let's now delve into the concrete returns that businesses can anticipate. We'll begin by examining select use cases and analyzing their measurable contributions to the business, before proceeding to explore the qualitative returns that automation brings.

>>> Quantitative Returns: Automation's Tangible Benefits

Automation adds value directly by generating additional revenue and cost savings, as well as by returning valuable hours back to the business. An example calculation of each is covered in this section.

Calculating the value of addtional revenue and cost savings:

Automation can deliver substantial value to businesses by expediting the provisioning and decommissioning of services. Let's take the example of an Internet Service Provider (ISP) where the realization of value from a circuit occurs only after it has been successfully provisioned.

Time Savings - Provisioning

Time saved per provisioning process	x **164 hours**
Activations /month	x **1100**
Cumulative time to value savings /month	**180.4K hours**

New Value - Provisioning

Cumulative time to value savings /month	**180.4k hours**
Revenue per circuit /hour	x **$0.17** ($85 per month)
Total new revenue /month	**$30,869**

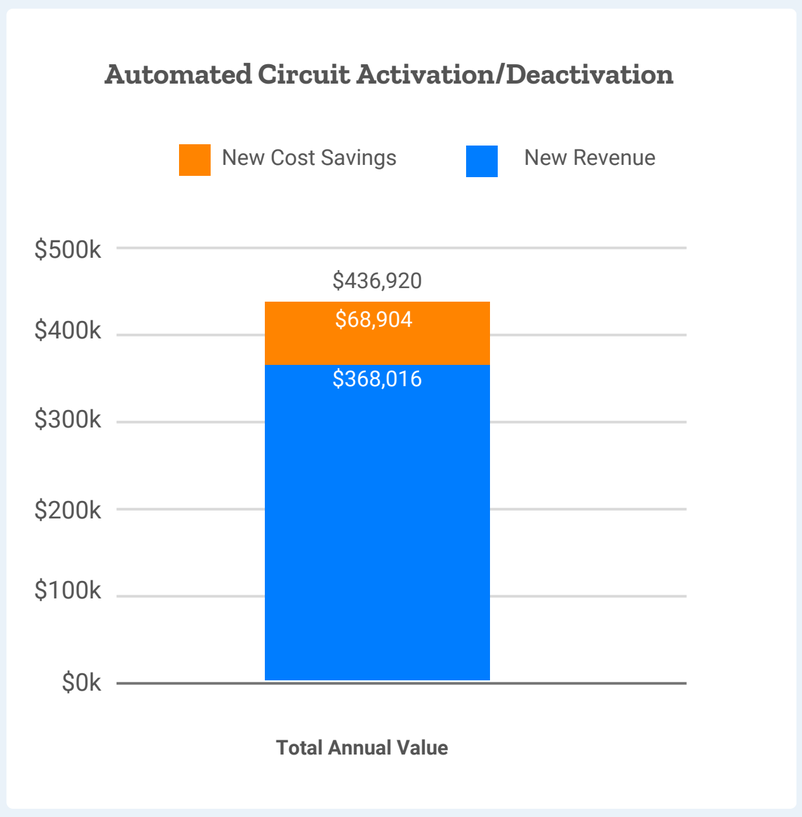
Let's also take into account that the ISP continues incurring expenses related to the circuit until it is deactivated.

Time Savings - Deactivations

Reduced hours per decommission	**116 hours**
Deactivations /month	x **900**
Cumulative hours saved per month	**104.4k**

New Value - Deactivations

Cumulative hours saved per month	**104.4k**
Expense per circuit /hour	x **$0.055** ($40 per month)
Total cost reduction /month	**$5,742**



Annual Value: $436,920

Altogether, this automation initiative would yield a substantial value of $436,920 annually.

Cumulative Value	
Total New Revenue	**$368,016**
Total Cost Reduction	**+ $68,904 (annually)**
Total Solution Value	**$436,920 (annually)**

Calculating the value of workflow automations:

A workflow automation is an automation of a specific process, such as upgrading a device or processing a customer request. It has a well-defined beginning and ending point. The first step in assessing the value of workflow automations is quantifying the number of hours that will be returned to the business upon implementation. By returning hours back to the business, teams can redeploy their engineering resources from routine and less critical tasks to more valuable business endeavors. This value is commonly referred to as full-time equivalent (FTE) hours. Start by estimating the time required to execute the task a single time. Then, approximate the frequency of task execution within a year. Lastly, evaluate the extent to which automation will fully take over the work: Will the entire process be automated, as seen in zero-touch automations, or will engineers be required to intervene at some point? If the latter, be sure to deduct that time from the overall calculation.

Hours Back to the Business	
Manual workflow effort per iteration	**2 hours**
Task frequency per year	**x 1,200**
Automation effectiveness	**x 100%**
FTE hours per year	**2,400**

The next phase involves determining the blended labor rate (**BLR**) per hour. The BLR per hour value will vary based on a wide range of factors, including the skill level and region of the engineer who would typically be performing the task. Remember to encompass the comprehensive expenses related to the engineer, such as benefits, office space, ongoing training, etc. Your cost estimates should also include paid time off and holidays. Lastly, consider non-productive hours, which include activities such as meetings, coffee breaks, and short pauses that provide brief breaks from focused work.

Total Compensation	
CCNA salary	**$89,491**
Overhead costs	**+ $26,847**
Total Cost	**$116,338**

Total Productive Hours	
Maximum possible workdays	**260**
PTO days	**- 15**
Holidays	**8**
Average productive hours per day	**x 7**
Productive hours year	**1,659**

The BLR per hour rate is **$72.12**, and this is the value of an FTE hour returned to the business for CCNA-level processes.

Blended Labor Rate = $72.12

Now that we know the total number of FTE hours the task requires and the BLR per hour rate, we can determine the value of the automation.

Value to the Business

FTE hours per year	**2,400**
BLR cost	**x $72.12**
Automation value	**$173,088**

Other considerations when calculating ROI

The value of an automation should also take into account any factor which may influence value, for example:

- Human error rate: the impact of error prevention in a given process;
- Overtime rates: the savings incurred when automation diminishes the need for overtime wages;
- On-site dispatches: the expenses avoided when automation reduces the likelihood of dispatching personnel on-site;
- Automation efficiency improvements: advances in the effectiveness of the automation as a consequence of ongoing development efforts;
- Rapid operationalization: When infrastructure is brought online more quickly, such as in stores and call centers, revenue can be realized more quickly.

Factors like these necessitate additional calculations to comprehensively evaluate the return on investment of automation.

Qualitative returns: Beyond the numbers

There are additional advantages to automation that hold significant value but are not as straightforward to measure because of uncertain probabilities or unquantifiable worth. Consider, for instance, the worth of preventing a security breach that leads to the theft of sensitive customer data or the expenses incurred from customer defections. Let's delve into a few of these qualitative benefits. Curbing the frequency of customer defections is a direct advantage of delivery enhanced service, and automation paves the way to achieving excellence that would otherwise be unattainable. According to Harvard Business Review, the longer a customer remains loyal to a company, the greater their value becomes.

Even a minor reduction in customer defections, such as by five percentage points annually, has the potential to result in a twofold increase in profits.

Improved service offerings can also result in fewer customer refunds. Self-service portals empower customers to select precisely what they require, while automation guarantees the prompt and accurate delivery of their orders. Furthermore, by integrating customer communications, it becomes feasible to keep customers informed throughout the transaction's progress. For example, by automating the resolution of network faults, less time is spent corresponding with the customer, and resolution is expedited. This, in turn, translates into heightened customer satisfaction.

By reducing the frequency of service interruptions and security breaches, automation has the capacity to enhance an enterprise's reputation. This, in turn, attracts prospective clients and instills confidence in potential investors regarding the company's operational stability and dependability. Ultimately, this plays a pivotal role in fostering the company's growth.

Enhanced compliance and maintenance practices prevent network faults and reduce the time spent analyzing failures. In instances of high-impact faults, stakeholders rightfully seek root-cause analyses and post-incident reports. Regrettably, investigations of this kind demand substantial engineering time. The integration of automated procedures aids in preventing such scenarios altogether—a twofold advantage for the business. Organizations that embrace automation methodologies take a proactive stance in their operations and place innovation at the core of their practices. As internal engineers evolve into automation specialists, unanticipated advantages for the business will naturally surface. This empowers organizations to retain their competitive edge as they forge ahead in ever more competitive markets.

>>> Returns in Practice

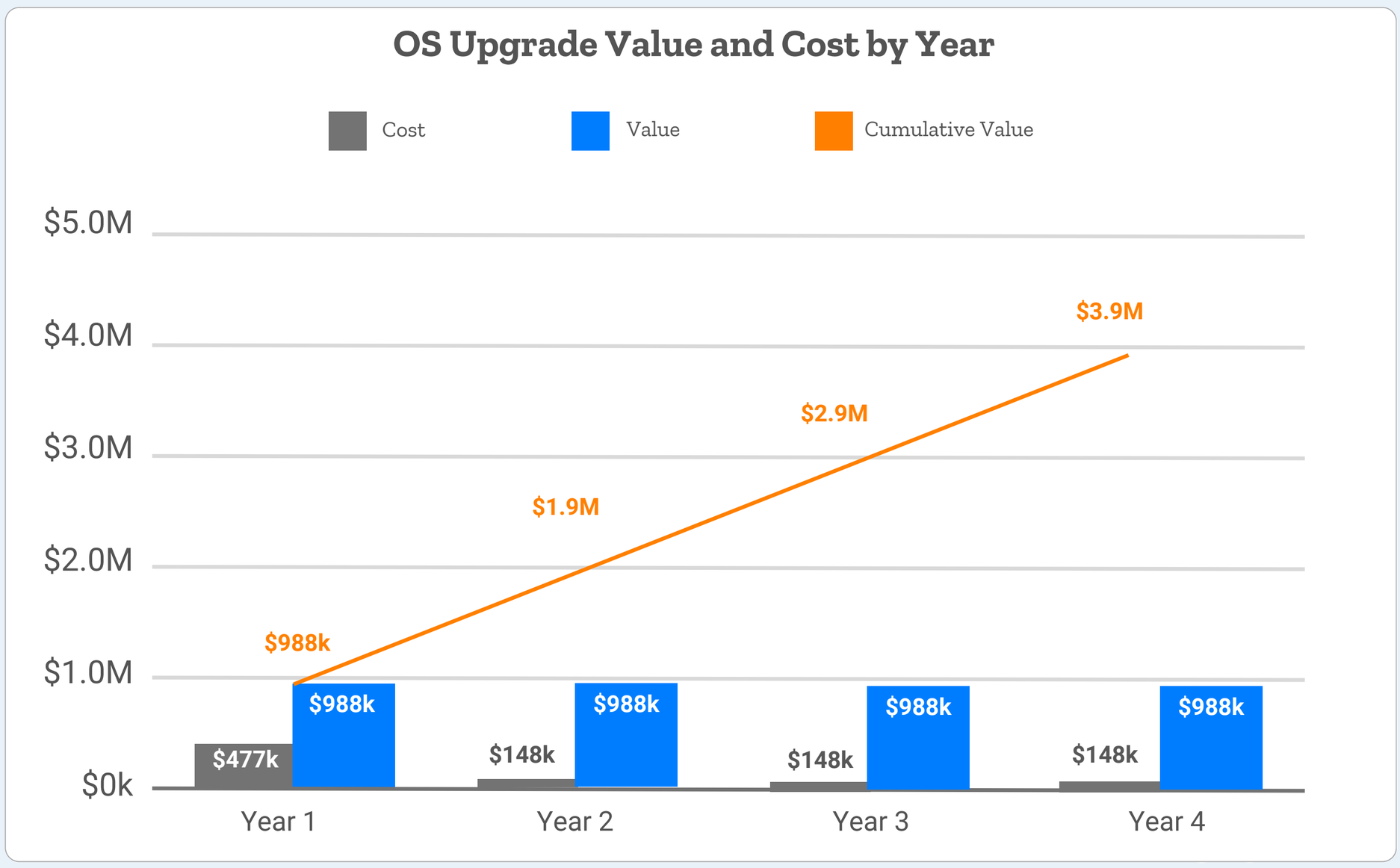
To simplify the calculations for the below scenarios, it is assumed that an orchestration system exists in the customer environment before NTC's engagement. In each of these scenarios, NTC provides the following in addition to the automated task mentioned:

- A strategic assessment and architecture plan
- Nautobot deployment, population, and synchronization
- An initial year of Network Automation as a Service Basic Tier—Fully managed solutions by NTC to deploy the automation; then subsequent years of managed services to continue the benefits of the automation

The benefits of the automations detailed below are realized in the first year, while the examples below demonstrate typical multi-year use cases to illustrate the compounding results of automation's value.

Operating System Upgrades

Network automation solutions have the capability to automatically upgrade operating systems, from pre-upgrade network readiness validations to the upgrade process itself and post-upgrade checks to confirm success. From start to finish, upgrades can span from 30 minutes to several hours per system. In a network with 5,000 devices that require annual updates, the cost of manual updates can exceed $1 million per year. Automation can carry out this task more efficiently with fewer errors, requiring engineers only to review the completion summary reports. Over the course of four years, by adhering to the industry's recommended practice of updating software annually, the business can achieve a remarkable **329%** return on investment, which amounts to **$3.95 million** in added value.



Anticipated:

4-Year Cost: **$920k**

4-Year Value: **$3.95M**

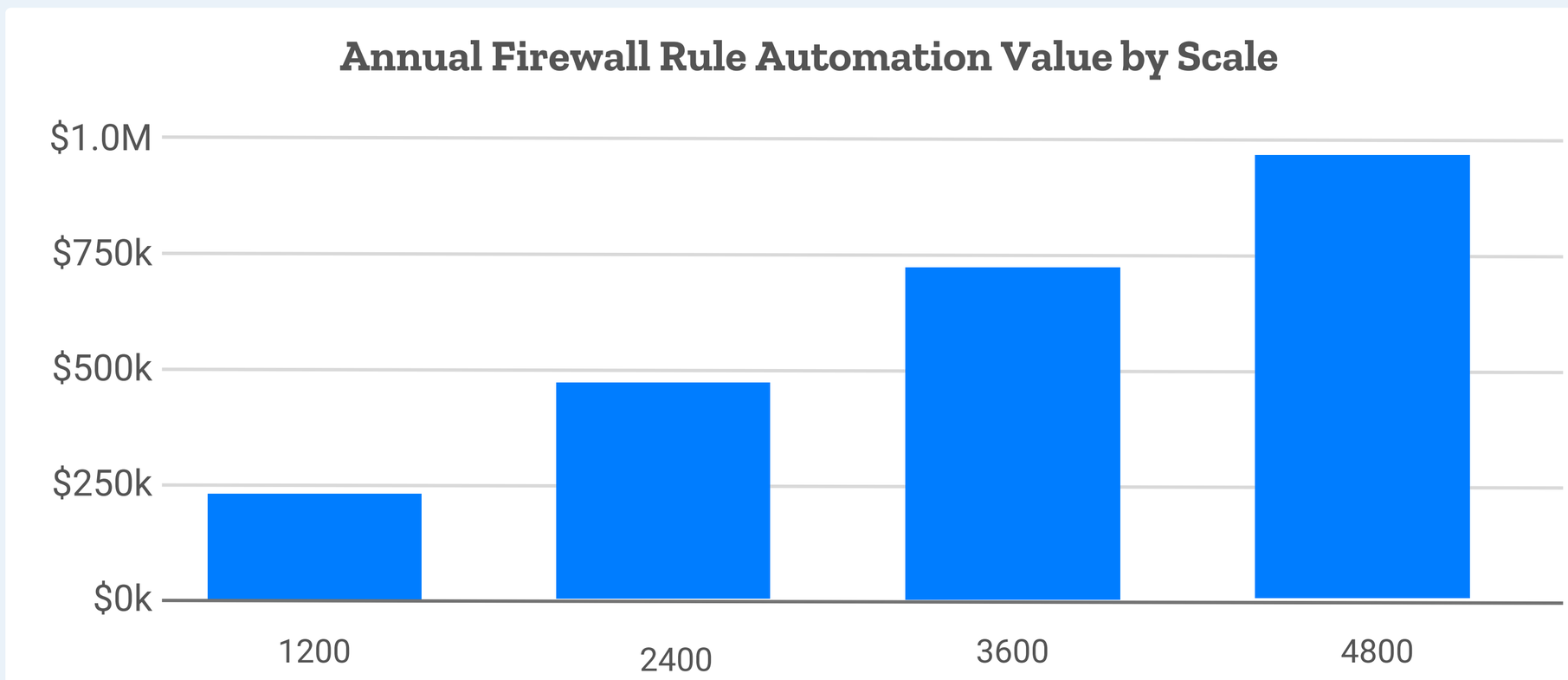
ROI: **329%**

Assumptions:

- CCNP Loaded Labor Cost per Hour: **$93.13**
- Manual upgrade effort per device: **131 Minutes**
- Automated effort per device: **3.7 Minutes**

Firewall Rule Automation

As much as 80% of firewall rule requests can be implemented with little or no interaction from engineering teams. Let's assume a team receives 400 requests per month, and the total time spent on each request is two hours. Over a span of four years, accounting for process failures unique to the human-led effort, the business has the potential to realize an impressive **219%** return on investment, equating to a value of **$3.9 million.**



Anticipated:

4-Year Cost: **$1.22M**

4-Year Value: **$3.90M**

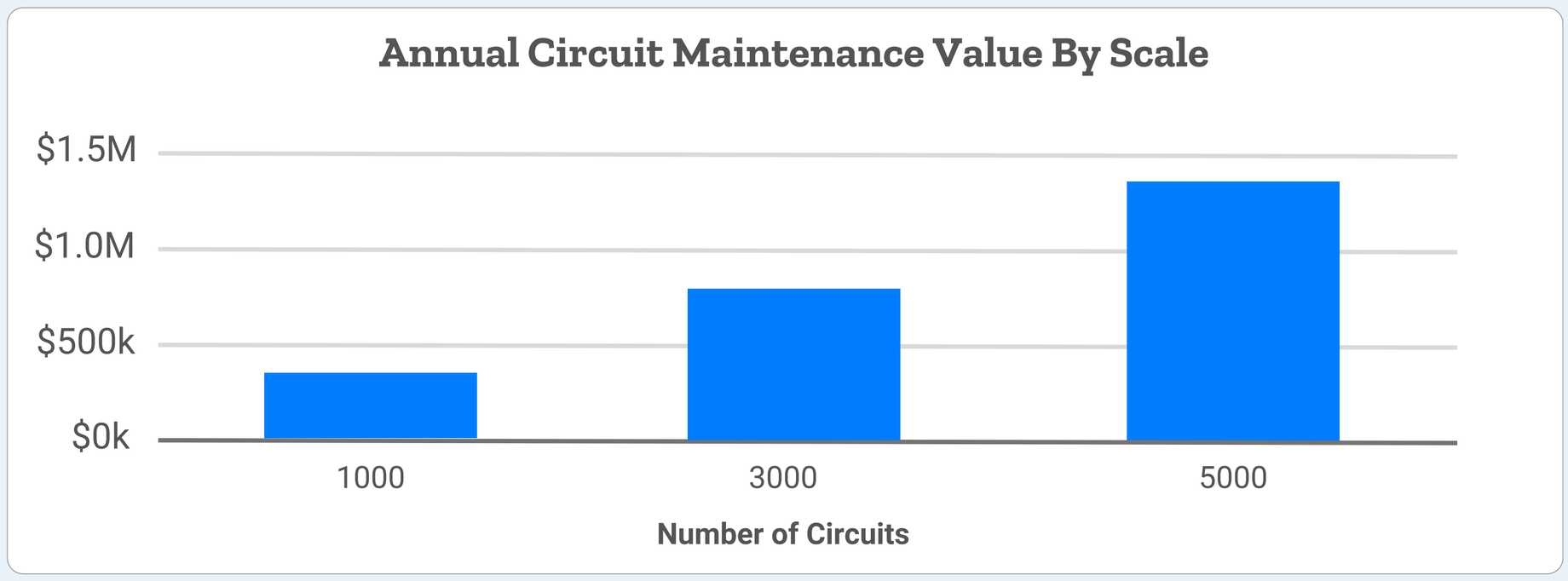
ROI: **219%**

Assumptions:

- **4800** Requests per Year
- Security Engineer Loaded Labor Cost per Hour: **$100**
- Manual upgrade effort per device: **131 Minutes**
- Automated effort per device: **3.7 Minutes**

Circuit Maintenance Management

Automation can also streamline circuit maintenance management—specifically, it can field incoming notifications from carriers and perform device-level actions. After four years, in an environment with 5,000 circuits, each receiving an average of 2.5 maintenance notifications per year, an astonishing **514%** return on investment could be realized, returning **$5.22 million** in value to the business.



Anticipated:

4-Year Cost: **$851k**

4-Year Value: **$5.22M**

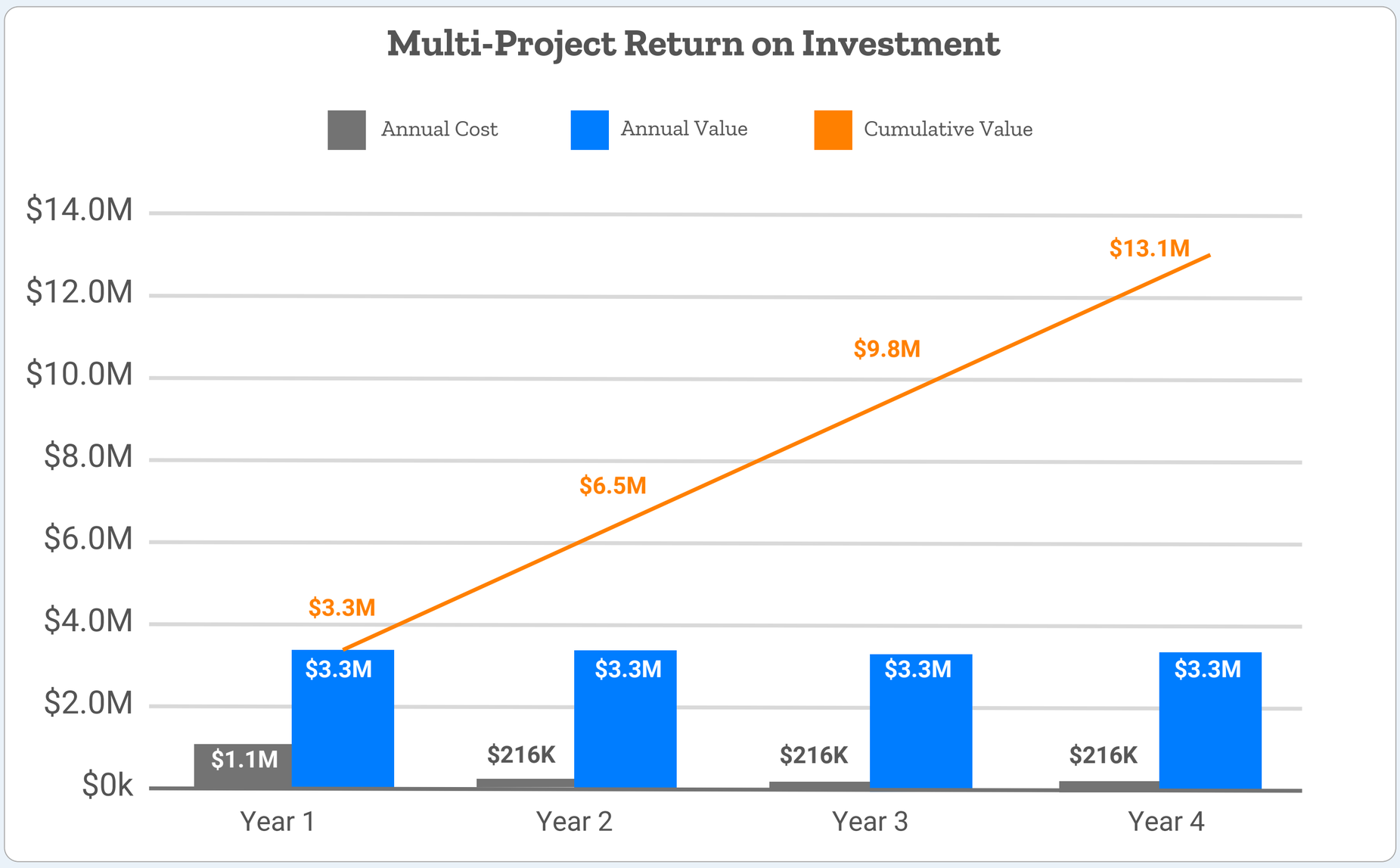
ROI: **514%**

Assumptions:

- CCNA Loaded Labor Cost per Hour: **$70**
- Maintenance Events per circuit per year: **2.5**
- Manual process duration: **88 Minutes**
- Automated process **recovers 100%** of manual effort

Multi-Project Return on Investment

While the returns demonstrated in the previous examples are remarkable, the real magic happens when we harness the foundational architecture to drive multiple projects. When these three solutions are combined, the result is an exceptional **628%** return on investment over four years, yielding a staggering **$13.1 million** in value.



Anticipated:

4-Year Cost: **$1.8M**	4-Year Value: **$13.1M**	ROI: **628%**

Assumptions:

- CCNA Loaded Labor Cost per Hour: **$70**
- Maintenance Events per circuit per year: **2.5**
- Manual process duration: **70 Minutes**
- Upgrade to NAaaS Enhanced Tier

>>> Conclusion

In the first part of this two-part series covering the ROI of network automation, we've considered the drawbacks of legacy management, uncovered its financial shortcomings, and recognized its long-term unsustainability. We've considered NetDevOps as an answer to these challenges given its potential to transform business outcomes and elevate both the customer and employee experience, and how it can yield tangible quantitative and qualitative returns.

As we wrap up this first conversation, it's important to note that the exploration is far from over. In the second part of this series, we will dive deeper into the foundation of network automation, address the challenges and misperceptions that come with adoption, and highlight some of the key approaches to achieving network automation success.

Thank you for joining us on this journey, and we look forward to continuing it with you in the next eBook.

Eager to unlock the full potential of network automation and accelerate your ROI? Don't wait for the next eBook—take action now! Click here to schedule a conversation with one of our network automation experts today and gain valuable insights into achieving rapid returns on your investment.

About Network to Code

Network to Code is a network automation services and solutions provider that helps companies transform the way their networks are deployed, managed, and consumed. Through managed and professional services, Network to Code enables enterprises across all industries and geographies to deploy data-driven network automation based on NetDevOps principles to improve reliability, efficiency, and security while reducing costs.

NTC is the sponsor of Nautobot, an open source Network Source of Truth and Network Automation Platform with a growing ecosystem of integrations and partners. Nautobot is the leading Network Source of Truth for enterprises looking to adopt a data-driven approach to network automation and a platform that complements any network automation journey.