Tackling Technical Debt to Modernize Mission Networks

Rev. 10.02.2024

© 2024 Cisco and/or its affiliates. All rights reserved.

Contents

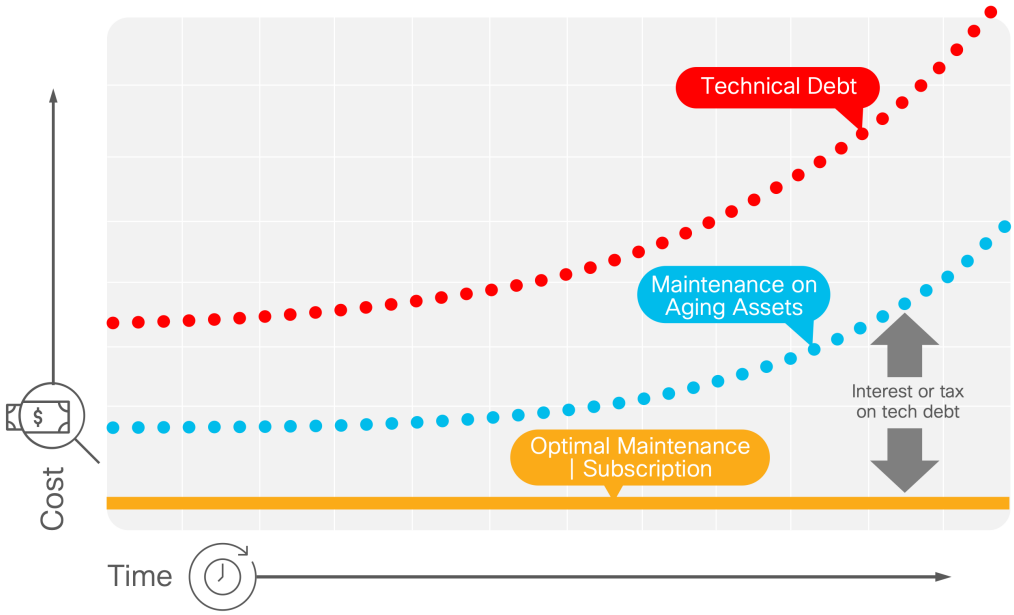
© 2024 Cisco and/or its affiliates. All rights reserved.

Executive summary

In the intricate landscape of federal missions, the network stands as a linchpin for mission execution across various government agencies. Many federal entities recognize the paramount importance of network modernization as a cornerstone in their strategic plans. Envisioning the future of government networks unfolds a proactive and revolutionary approach to tackle technical debt associated with delays in mission-critical network modernization.

Network technical debt stems from outdated devices, old operating systems, incomplete configurations, and legacy operational and consumption models. Addressing this debt is crucial as it amplifies the cost of maintaining and operating the network, hindering adoptions of new capabilities and innovations. In severe cases, it hampers productivity among mission personnel, leading to invisible but substantial costs – think of it as a tax or interest paid on the technical debt (see **Figure 1**). Additionally, it "taxes" next gen innovations in terms of development, deployment and adoption.

Figure 1.
Cost over time in real terms



This debt accumulates for reasons that may have been valid initially, but it's time to proactively address it with a longer term and consistent methodology. Without repayment, it persists as an ongoing cost for Federal Agencies. Let's delve into solutions to take on network technical debt and the interest paid on it to accelerate modernization and a cost-effective future.

Cisco and its partners introduce new and proven methods, combining Network as a Subscription (NaaS), automation, and a modern Concept of Operations (CONOPS). This "dynamic trio" tackles technical debt, speeds up modernization and encourages mission impact and innovation in the following ways.

- **NaaS takes the spotlight with Hardware as a Subscription (HaaS)**, liberating federal agencies from upfront capital expenditures tied to hardware procurement. Subscribing to hardware services

© 2024 Cisco and/or its affiliates. All rights reserved.

enables agility, allowing agencies to scale resources dynamically embracing a modern network platform through subscription services rather than being burdened with maintaining outdated network equipment.

- **Automation becomes the driving force**, eliminating manual bottlenecks and accelerating the modernization of networks. This efficiency surge reshapes the government's approach to technical debt, creating a continuous delivery mechanism. Automation is pivotal in modernizing federal IT networks, transforming them from traditional setups to dynamic, agile entities, and AI-driven operational insights. Shifting towards a "network to code" paradigm streamlines processes, reduces manual errors, and accelerates deployment, enabling federal agencies to foster a resilient and future-ready IT infrastructure.
- **The pivotal component is the meticulously crafted CONOPS**, guiding the orchestrated transformation by aligning technological deployment with mission objectives, and AI-driven automations, security protocols, and compliance requirements. This strategic blueprint not only steers decision-making but also seamlessly integrates emerging technologies into existing infrastructures.

In summary, the fusion of NaaS, automation, and a forward-thinking CONOPS represents a paradigm shift in government modernization. This approach positions governmental entities as pioneers of technological innovation, overcoming challenges such as technical debt and embracing the dynamic demands of the digital era.

This whitepaper provides a detailed exploration of how federal government agencies can intricately integrate CONOPS into the strategy for modeling and developing the best NaaS model. This involves:

- Strategic alignment
- Executive sponsorship
- Risk mitigation and security measures
- Operational procedures
- Change management
- Training and skill development
- Continuous improvement
- Resilience and recovery planning
- User experience optimization
- Scalability and adaptability considerations
- Performance monitoring and reporting
- A detailed discussion on automation.

In the following pages, we will illustrate that a comprehensive integration ensures that the NaaS model not only meets technical specifications but is also aligned with the overarching vision and expectations outlined in CONOPS for federal operations. It transforms the digital twin into a living representation of federal operational philosophy, evolving in tandem with the dynamic landscape of the federal government’s many missions.

© 2024 Cisco and/or its affiliates. All rights reserved.

Tech debt is a costly national security risk

As noted in the Government Accountability Office testimony before the House Subcommittee on Cybersecurity, Information Technology, and Government Innovation, "Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically reported spending about 80 percent on the operations and maintenance of existing IT investments, including legacy systems."[1] The GAO testimony goes on to note that unsupported legacy IT creates significant risk to federal agencies, including security vulnerabilities, inability to meet mission needs, staffing challenges, and increased costs.

U.S. government policies and mission requirements are driving efforts to eliminate technical debt in U.S. government agencies. The National Defense Authorization Act of 2022 authorized the Department of Defense to study technical debt and make recommendations on its impacts to software-intensive systems.[2]

In a September 2023 speech, Defense Department Chief Information Officer, John Sherman, noted that he is "considering issuing strong, formal guidance to military service branches to get moving faster on the long-sought goal of reducing technical debt throughout the military and particularly on the IT and cybersecurity front," highlighting that near-peer competition is making modernizing critical.

The Biden Administration's 2023 National Cybersecurity Strategy calls for the Office of Management and Budget to lead development of a multi-year lifecycle plan to accelerate Federal civilian executive branch modernization, including identifying "milestones to remove all legacy systems incapable of implementing zero trust architecture strategy within a decade" and "replacing legacy systems with more secure technology."[3]

As agencies work to overhaul their IT systems, the significance of networking and physical infrastructure is critical given the surge of data and the expansion of new applications and software. Adopting financial models and deployment strategies from software and applying them to hardware remains a challenge.

To meet the modernization targets set by federal agencies, **three key changes are imperative**.

- **Financial Model:** Agencies must transition from lifecycle driven technology upgrades and capital expenditures to a predictable, usage-based funding model in the form of Hardware as a subscription (HaaS). This model requires regular payments for service access rather than outright hardware ownership.
- **Automation:** The adoption of a comprehensive automation framework is essential to eliminate outdated practices and facilitate modernization. This framework should integrate with existing workflows, leverage current toolsets, and enforce strict data control to enhance security.

[1] Government Accountability Office (2023). INFORMATION TECHNOLOGY: Agencies Need to Continue Addressing Critical Legacy Systems. Statement of Kevin Walsh, Director, Information Technology and Cybersecurity. Retrieved from https://www.gao.gov/assets/gao-23-106821.pdf

[2] National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81 (2021), https://www.govinfo.gov/app/details/PLAW-117publ81.

[3] See National Cybersecurity Strategy (March 2023), Strategic Objective 1.5. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

© 2024 Cisco and/or its affiliates. All rights reserved.

- **Operational Modernization:** A reevaluation and updating of operational models are necessary to fully benefit from the new financial and automation frameworks. Incorporating contemporary software development methods to manage physical infrastructure is key to this modernized approach to operations.

By adopting these changes – new financial models, automation, and operational modernization – agencies can quickly transition to Network as a Service (NaaS). This subscription-based approach ensures that agencies pay only for the networking capabilities they need, when they need them, leading to increased flexibility, scalability, and cost-efficiency. Such a model supports dynamic allocation of networking resources, rapid deployment of new services, and accommodates the evolving demands of agency operations without the financial burden of owning and maintaining hardware.

Furthermore, the shift to NaaS contributes to the elimination of technical debt, as it replaces outdated systems with modern, up-to-date services that require less maintenance and can adapt quickly to evolving mission needs, keeping agencies at the forefront of innovation.

Network As A Service (NaaS)

Amidst constrained budgets and escalating national security threats, NaaS emerges as a secure, innovative, and predictably priced solution for the U.S. government. Cisco defines NaaS as a cloud-based model that allows users to manage their networks and achieve desired outcomes without owning, constructing, or maintaining the infrastructure. This shift in infrastructure consumption moves towards a model where hardware, software, or services are accessed through subscription-based, usage-driven, or on-demand financial arrangements. This evolution from traditional ownership to NaaS presents a flexible, scalable, and cost-effective methodology for technology utilization.

Hardware as a Subscription (HaaS) is a key element in the architecture of Network as a Service (NaaS). By adopting HaaS, agencies can subscribe to the latest hardware on a pay-as-you-go basis, avoiding large upfront investments. This subscription model aligns with operational expenditure, offering financial predictability and the agility to adapt to changing mission needs. When combined with other service-oriented offerings, HaaS forms the foundation of NaaS, enabling scalable and cost-effective network infrastructure that is vital for meeting the strategic goals of government agencies.

However, implementing hardware-as-a-subscription poses challenges due to the pre-existing hardware that customers already own and operate. Unlike Software as a Service (SaaS) or Infrastructure as a Service (IaaS) solutions, typically deployed in 'greenfield' environments, transitioning to Network as a Service (NaaS) can be challenging due to the ongoing costs and support required for legacy networks.

As customers shift to NaaS, the financial burden can increase as they must cover the costs of new technology while also maintaining their outdated systems. This dual expenditure can drastically increase overall costs. To alleviate this, any HaaS offering should consider the existing install base and provide an effective transition plan. Such a plan would not only account for the current infrastructure but also implement a more economical and efficient migration to NaaS, avoiding unnecessary financial strain during the transition.

This is where a technology leader like Cisco comes into play, providing the expertise and solutions necessary to navigate the complexities of NaaS adoption. In the pages that follow, we will discuss how the

© 2024 Cisco and/or its affiliates. All rights reserved.

vendor-customer relationship can evolve to accommodate this transformation, the financial models underpinning NaaS adoption, and how Cisco can play a pivotal role in empowering organizations to harness the true potential of NaaS.

Vendor relationship

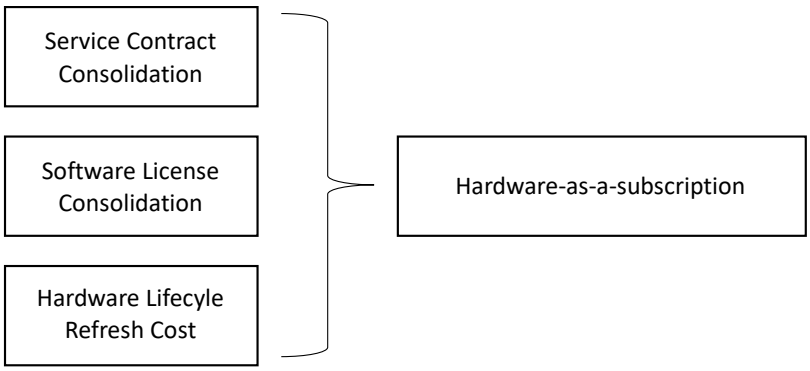
DISA Director and JFHQ-DODIN Commander of the United States Air Force Lt. Gen. Robert J. Skinner emphasized the value of hardware support services when he said, "...the more that I can have hardware-as-a-service and then focus our intellectual capital on the software piece of this the more successful we will be." This statement emphasizes the critical role of a financial model tailored to hardware subscriptions. Cisco excels in crafting such models, starting with a thorough assessment of the customer's existing hardware. This enables us to integrate the benefits of a subscription model against the legacy systems, ensuring a cost-effective and transition.

Our approach involves a close partnership with customers to understand their existing install base and pinpoint opportunities where new technologies can be adopted without imposing additional costs. We align updates with the customer's actual requirements, which means incorporating current software and maintenance expenses into the new model. Our strategy is to craft a clear and straightforward transition plan to HaaS, ensuring it brings value and supports the customer's operational flow while we phase out the older hardware. We can create this model in four phases, as shown below.

Phase One | Inventory Analysis

To begin crafting the financial model, we conduct an inventory analysis. Working side by side with the customer, we review their current infrastructure, software licenses, and service agreements. By aligning our records with the customer's, we establish a detailed and agreed-upon view of their current environment. This step is crucial for any customer, regardless of their interest in NaaS, as it consolidates data from various sources into a single, trusted overview (**Figure 2**). It includes specifics of software licenses, service contracts, and maintenance agreements, along with SLAs. This comprehensive inventory not only clarifies current commitments but also sets the stage for discussions on transitioning to NaaS, providing a clear, informed starting point for those opting to proceed.

Figure 2.
Consolidation of existing data to develop an initial HaaS offering



© 2024 Cisco and/or its affiliates. All rights reserved.

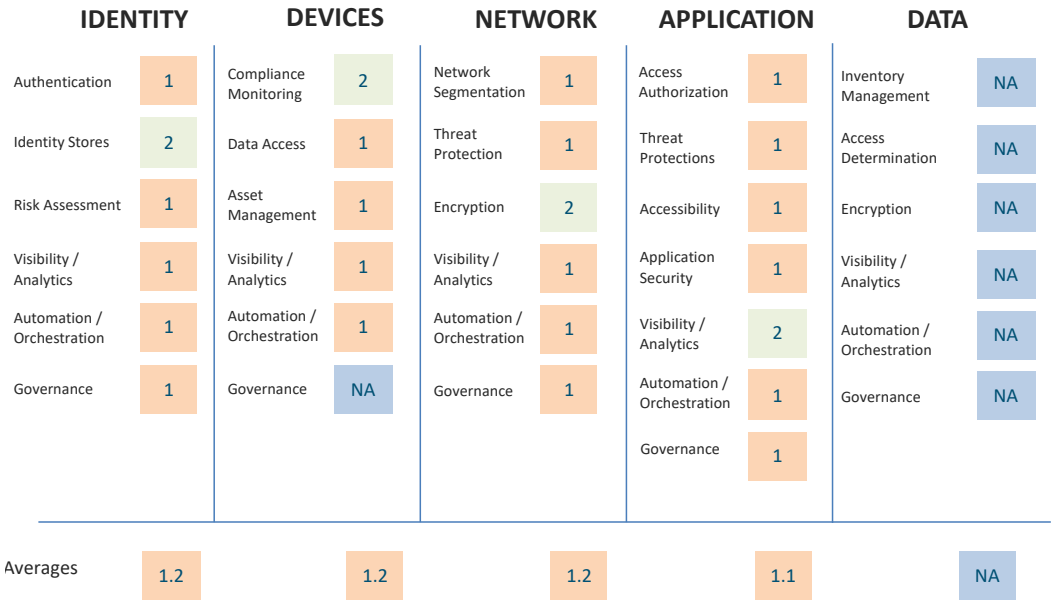
Phase Two | Requirements Alignment

The second phase is about identifying requirements, which involves a deeper dive into systems outside of Cisco inventory. It starts with identifying critical applications that support the agency's core mission, encompassing both older legacy systems and newly modernized apps. This phase aims to grasp the full scope of the existing architecture and the desired outcome after modernization.

The result is a set of clear metrics tailored to guide our financial model. For example, Figure 3 shows a customer aiming to transition to a zero-trust framework, as per the CISA guidelines. To formulate precise metrics and scores, we must understand the entire technological ecosystem, not just the networking aspect.

Figure 3.

Customer requirements scorecard using CISAs zero trust framework



Phase Three | Immediate Action Plan

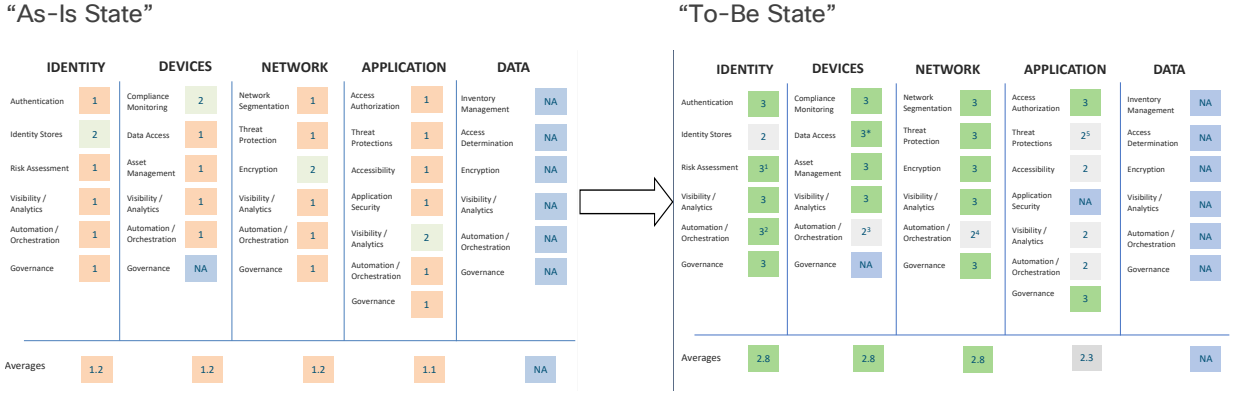
In the third phase, we leverage the findings from the previous assessments to craft an immediate action plan that capitalizes on the customer's existing investments. This strategy focuses on activating available functionality that can have an instant impact on their success metrics, thereby accelerating progress towards their mission goals.

For instance, the given example (**Figure 4**) would illustrate how the metrics have improved from the initial assessment by deploying existing but underutilized technologies. This phase is about getting quick wins by optimizing current resources to deliver tangible benefits and set the stage for more extensive modernization efforts.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 4.

Before and after technology matrix based on the success of a transformational roadmap



Phase Four | Technology Roadmap and Gap Analysis

The final phase uses all the information gathered to formulate a comprehensive future state, complete with a proposed architecture and a migration strategy. This plan is aligned with mission outcomes to ensure that every technological enhancement and architectural decision directly supports the agency's objectives.

It also incorporates a financial analysis that compares the costs of maintaining the current legacy systems against the investment in new technology, offering a clear, strategic view of the economic impact and benefits of the migration. This phase is pivotal as it delivers a clear, actionable blueprint that guides the customer through the transition from their current state to the desired technological and operational environment.

Financial Model

After gathering all pertinent data and understanding the customer's long-term mission objectives, we establish a financial foundation by consolidating all hardware, software, and services into a single fixed-price contract. This contract incorporates bundled services and a built-in lifecycle refresh, providing a consistent and predictable cost structure. With this baseline, we then work closely with the customer to identify the specific technologies they'll require to achieve their goals.

By offering a comprehensive HaaS solution, we ensure alignment with their critical mission objectives. Furthermore, recognizing the need for adaptability in technology solutions, we emphasize the importance of flexibility in consumption. One size doesn't fit all; thus, our diverse consumption models are designed to evolve as mission objectives change, guaranteeing an efficient and responsive infrastructure.

© 2024 Cisco and/or its affiliates. All rights reserved.

Automation

The true benefit of a subscription-based model, as previously highlighted, becomes apparent when the technology is seamlessly integrated and functional within the customer's existing environment. The key to achieving this is a robust automation framework.

This framework ensures that subscription services are not only delivered but also fully operational and aligned with the customer's workflows, thereby unlocking the full potential of the technology investment. To make this possible in existing environments, it is essential to separate the data that defines the infrastructure from the infrastructure itself and manage it as software.

Model-Driven Automation Framework

To successfully consume Network as a Service (NaaS), an automation framework that meets several requirements is necessary.

- **Integration into Legacy Systems:** The framework must have the capability to integrate with and automate both legacy and brownfield infrastructure. This approach is crucial for systematically eliminating technical debt and phasing out outdated systems, facilitating a smoother transition to modern, service-based offerings while maintaining operational continuity.
- **Alignment with Existing Tools and Processes:** It's imperative that the automation framework aligns with the organization's current tools and processes. This is especially important for organizations already using Agile or DevOps methodologies for software management.

  By treating hardware and infrastructure as programmable entities, and incorporating them into continuous integration and delivery pipelines, hardware management can evolve alongside software practices, resulting in a more agile and responsive infrastructure.
- **Infrastructure as Data (IaD):** The adoption of IaD is critical for maintaining flexibility in how environment data is managed. Defining infrastructure through vendor-agnostic data models allows organizations to version, track, and store their infrastructure configurations securely, akin to software code. This practice ensures greater consistency and accountability and offers the flexibility to choose storage solutions that meet security and compliance needs.

Implementing the Automation Framework

The implementation of this automation framework is divided into three phases:

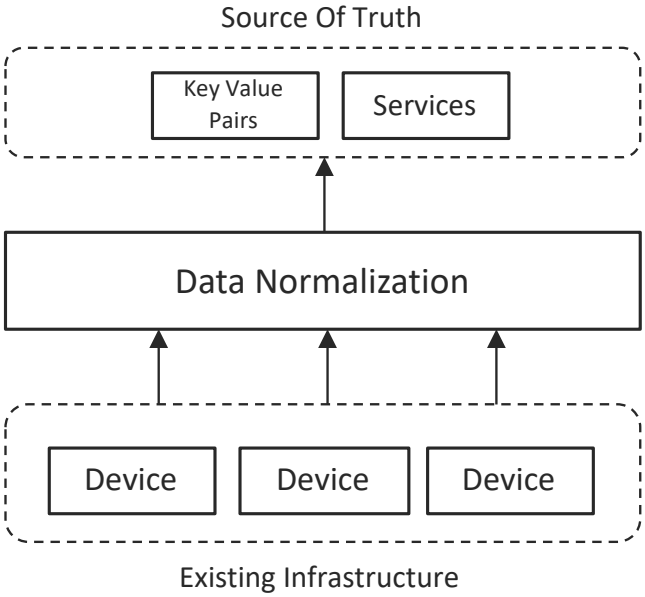
- **Onboarding:** The process begins with establishing a centralized, reliable source-of-truth by systematically gathering device data across the network. This involves using a combination of open-source and commercial tools to communicate with multi-vendor devices, storing configurations as standard data models. This step is crucial in creating a uniform API for cross-vendor communication and scaling automation practices.

  As illustrated in **Figure 5**, data is pulled from the infrastructure and subjected to a normalization and separation procedure. Configurations specific to devices are converted into standardized data

© 2024 Cisco and/or its affiliates. All rights reserved.

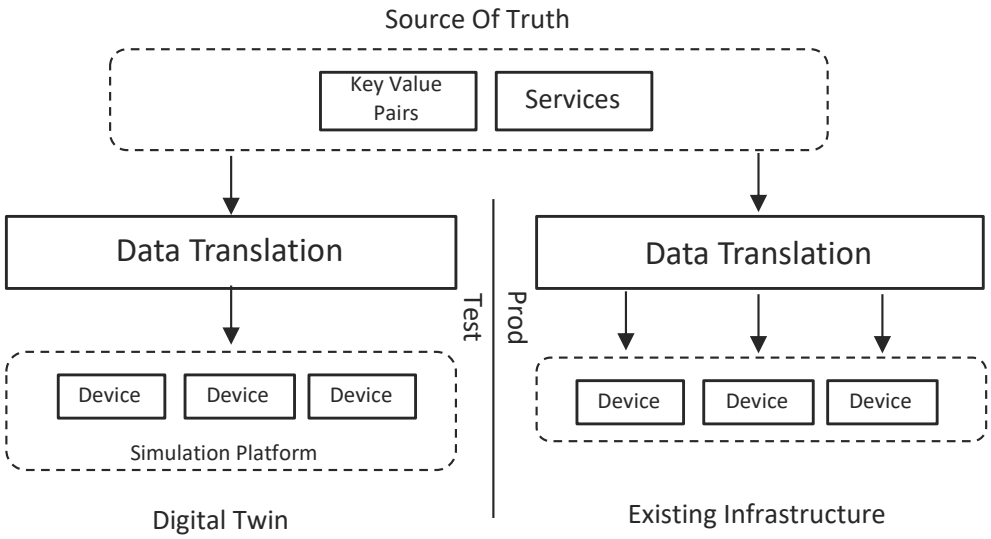
models that depict the services on each device, such as routing protocols and security policies. This simplification enhances the ease of managing and editing the network data.

Figure 5.
The harvesting of data from the existing infrastructure



- **Digital Twin Creation:** Leveraging the tools from the onboarding phase, a digital twin of the network is programmatically generated. This accurate virtual model of the network serves as a valuable resource for simulation, testing, and planning, allowing validation of configurations and assessment of potential changes before implementation in the live network.

Figure 6.
A single source of truth used to control the digital twin and existing infrastructure



© 2024 Cisco and/or its affiliates. All rights reserved.

In **Figure 6** above we can see the single source of truth being applied to both the digital twin and production network. This structure is what enables us to minimize risk through testing and validating data before its deployed into our live infrastructure.

- **Data Standardization:** The transformation of existing infrastructure into accurately represented data models, coupled with the use of a digital twin for testing, sets the stage for the next critical step: standardization. This is accomplished by distinguishing unique device characteristics – identified as key-value pairs – from the general data models. The standardized models are then applied as reusable network services, which become the default templates for infrastructure operations.

Figure 7.
The source of truth data represented as a set of network services

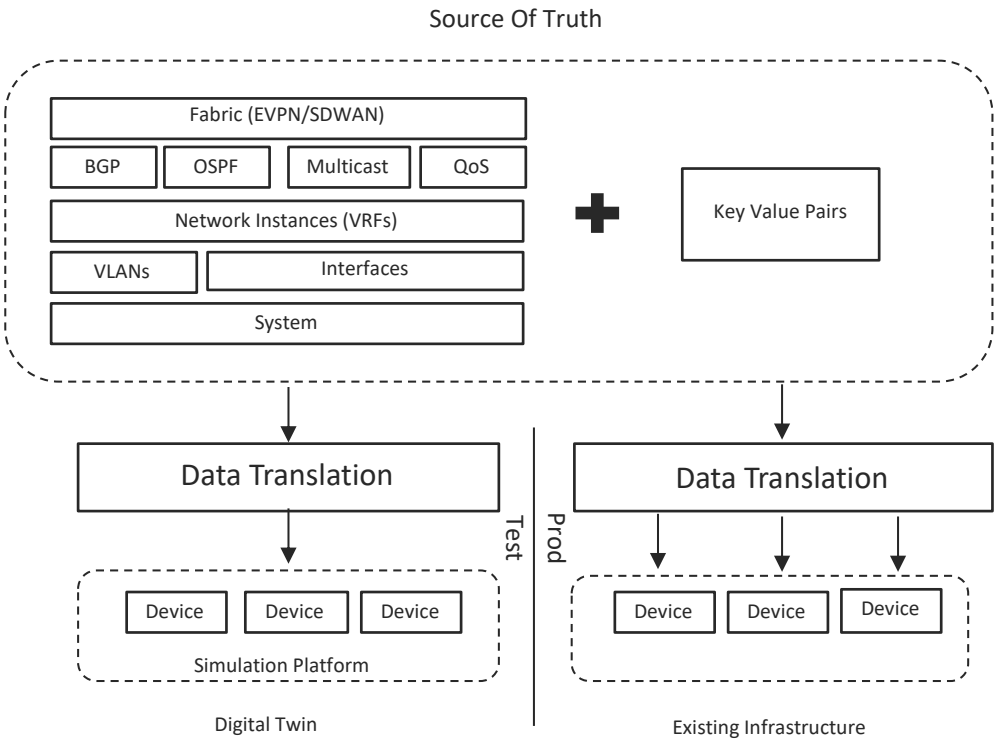


Figure 7 above visualizes this process. It shows the Source of Truth as the central repository for network configurations, integrating both general network protocols and device-specific key-value pairs. This informs both the digital twin for safe testing and the existing infrastructure for live deployment, reflecting the standardization of data models across the network.

By separating the data from the physical hardware, we create a distinct division between the network's operational data and its underlying hardware. This separation is critical as it enables updates, changes, or enhancements to be applied at the data level, leading to a more efficient and agile network management process.

Such a method is integral to enabling hardware as a subscription, where the hardware's function can be updated or changed as quickly as new data configurations can be applied. This separation of data and infrastructure provides customers with the control to manage their networks with the flexibility and speed of managing software, fully realizing the potential of HaaS.

© 2024 Cisco and/or its affiliates. All rights reserved.

Continuous Integration and Continuous Deployment (CI/CD)

With the transformation of our network into a manageable data format, we introduce Continuous Integration/Continuous Deployment (CI/CD) as the final step in our automation strategy. This critical implementation leverages existing tools used in software development, now adapted for network management. By treating our network data with the same agility and precision as software, we significantly enhance the management process.

Continuous Integration (CI) ensures regular, consistent integration and testing of changes to network configurations. This phase is pivotal in minimizing the risk of errors and conflicts, thereby enhancing network stability. Once changes pass the CI phase, Continuous Deployment (CD) comes into play, automatically applying these tested and validated changes to the network. This rapid deployment keeps the network aligned with both operational needs and technological advancements.

The integration of CI/CD using software development tools and methodologies marks a substantial advancement in our approach to network management. It represents a shift towards a more dynamic, responsive, and future-focused infrastructure. As we proceed, our modern Concept of Operations (ConOps) will fully utilize this CI/CD framework, ensuring an agile, efficient network ready to meet the evolving demands of the digital landscape.

Concept of Operations

As previously discussed, the transformative financial model supporting Network as a Service (NaaS), backed by Hardware as a Subscription (HaaS), is reshaping network infrastructure management within government agencies. This approach enables more dynamic, scalable resource deployment. Central to this transformation is the role of automation, enabled by separating data from physical infrastructure. This separation not only facilitates rapid hardware deployment but also enhances risk management by giving agencies complete control over their data, fundamental to their infrastructure. Moving forward, the emphasis is on managing this evolved network environment effectively.

By adopting a modern Concept of Operations (ConOps) that integrates DevOps and Agile principles into the management of network data, we aim to equip government agencies with the capability to adapt seamlessly to their evolving missions while ensuring the integrity and security of their operations.

Continuous Improvement

The automation framework we have implemented brings immediate benefits, notably a significant increase in the efficiency of the current operating environment. The CI/CD pipeline, central to this framework, is crucial for enhancing network performance and enabling rapid, reliable deployment processes. This system streamlines the implementation of updates and network stability through continuous testing and validation.

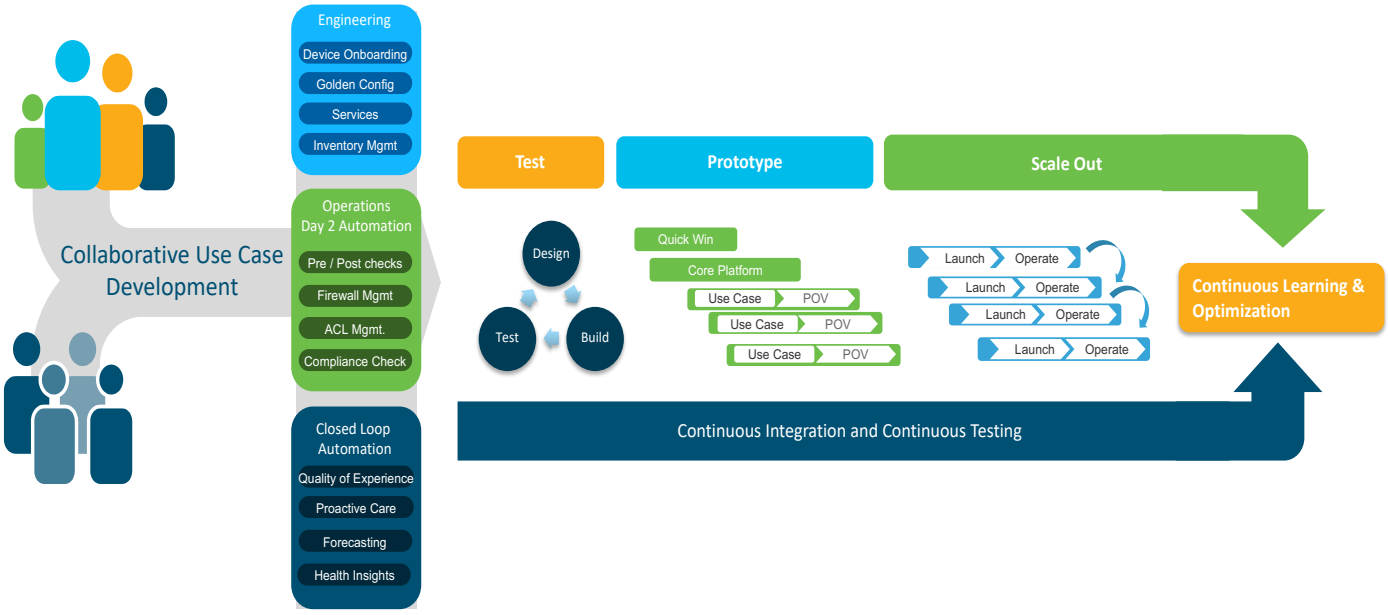
These enhancements are crucial for maintaining a robust, fully operational network, and they come with the additional benefit of zero downtime during maintenance and upgrades. This phase lays a solid foundation for ongoing optimization of network operations, setting the stage for the introduction of new features and capabilities.

© 2024 Cisco and/or its affiliates. All rights reserved.

New feature deployment

In our Concept of Operations, Cisco collaborates closely with agency personnel in a structured, Agile process to identify and deploy new network features and functionalities (see **Figure 8**). It illustrates the key steps from the initial creation of use cases to scaling solutions.

Figure 8.
The process to identify and deploy new features delivered as a service



The process includes critical stages such as testing and prototyping, essential for validating the functionality of network enhancements before their wide-scale implementation. This focused, iterative approach ensures that network improvements are consistently aligned with agency objectives, resulting in an infrastructure that is adaptable and resilient to the evolving requirements of national security.

© 2024 Cisco and/or its affiliates. All rights reserved.

Conclusion

In conclusion, this paper has articulated a strategy for transforming government agency network infrastructures, pivoting towards Network as a Service (NaaS) supported by Hardware as a Subscription (HaaS). By embracing a model that integrates automation, financial strategies, and a modern Concept of Operations, agencies are equipped to navigate the complexities of today's digital landscape.

The implementation of Continuous Integration/Continuous Deployment (CI/CD) signifies a transformation, aligning network management with the agility of software development. This approach not only enhances operational efficiency but also ensures the flexibility and security necessary for meeting evolving national security demands.

As we move forward, the successful adoption of these strategies will play a crucial role in maintaining the robustness, adaptability, and innovation at the core of government agency operations, positioning them at the forefront of technological advancement and operational excellence.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2024 Cisco and/or its affiliates. All rights reserved.