PeerPaper™ Report 2022

Based on real user reviews of Cisco Secure solutions

Assembling the Elements of NetOps Strategy

PeerSpot

Contents

Introduction

As digitization continues its inevitable spread, organizations must respond by continually innovating and updating their digital assets and customer-facing offerings. For many organizations, though, the network represents an obstacle to innovation. It's costly and time-consuming to manage and modify. As a result, organizations pay the price for relying on legacy solutions or stopping short of pushing out the latest advancements to their workforce and customers.

To change this, organizations need to make sure that the network is the foundation of digital transformation. If this foundation isn't sound, then the efforts to accelerate innovation and drive outcomes will fall short. Network Operations (NetOps) offers a solution. NetOps aims to improve agility and security by digitizing physical networks while still maintaining full control over them — a fine line to walk, but a critical one for success in a digital world.

NetOps Overview

NetOps is an emerging field that embodies a four-stage cycle, depicted in Figure 1. Like DevOps, NetOps is about deploying new infrastructure to support digital initiatives as rapidly as possible, without compromising quality or security.

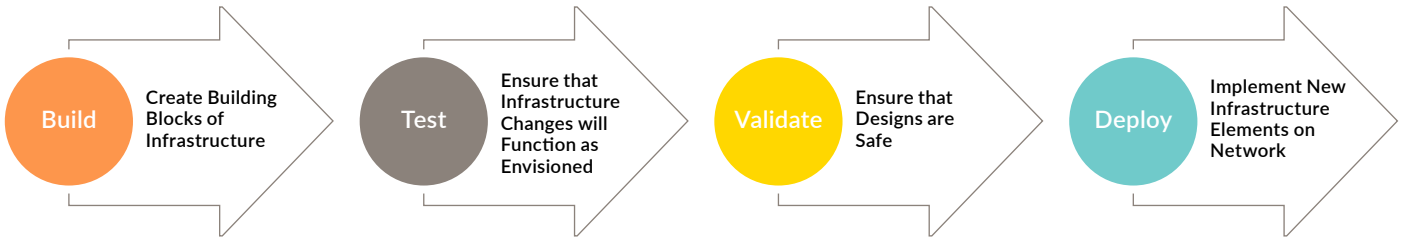


Figure 1 - NetOps cycle, starting with Build and continuing through Test, Validation and Deploy.

The Cisco Portfolio and NetOps

To work, NetOps draws on several key capabilities: virtualization, rapid deployment, flexibility, and orchestration. Figure 2 shows how these capabilities align with the NetOps cycle. Agility and virtualization are needed at the "Build" stage. Security and analytics, while present across the entire cycle, are particularly useful at the "Validate" stage. Fast, effective deployment relies on orchestration and automation.

Decreases troubleshooting time

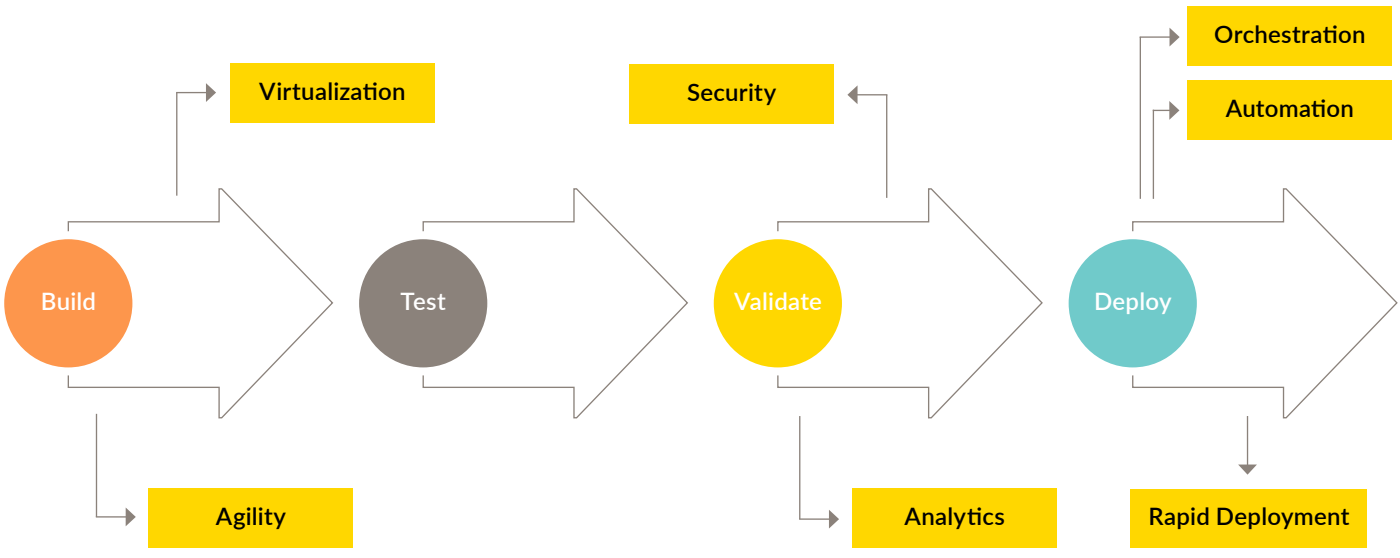


Figure 2 - How the capabilities of the Cisco Security portfolio align with the NetOps cycle.

> "I've found that to be incredibly valuable because it's a lot easier to get to some points of data now."
>
> Read review »

All these elements are featured in Cisco Secure products. Cisco Secure offers network managers and security teams the components to build a NetOps strategy. As Cisco Secure users on PeerSpot explain, the portfolio gives them the virtualization, rapid deployment, flexibility, automation and orchestration they need to pursue NetOps in their organizations without sacrificing security or control. It also helps save time and money, which can instead be allocated to transformative projects. Cisco Secure's open, interoperable approach to security helps make the potential of NetOps more achievable than ever before.

The Cisco Secure portfolio comprises a range of solutions that work together as a team to deliver seamless interoperability with an organization's security infrastructure, including third-party technologies. When used together via the integrated Cisco SecureX platform, the benefits of this approach are stronger security, accelerated threat investigation and response, automation, and unified visibility.

For example, a systems engineer at a small tech services company liked how Secure Firewall offers Layer 7 visibility. He explained, "...if you have a Layer 4 firewall, it is clear that a Layer 7 firewall gives you more visibility, and you can see the packets that the application connection is using, meaning which application is using them. It's not how much visibility you get but, rather, the fact that you get Layer 7 visibility."

An IT technical manager at a healthcare company with over 10,000 employees appreciated that the 7.0 version of Secure Firewall allows his team to "see much more granularly into the packet."He continued by saying that, "this gives us much more granularity into what is exactly happening on our network and snapping in the Cisco StealthWatch piece gives us the end-to-end way of monitoring our network and making sure that it's secure."

For an engineering services manager at a tech services company with more than 200 employees, "One of the most valuable features of Cisco Secure Firewall software version 7.0 is the 'live log' type feature called Unified Event Viewer." In his experience, that view has helped his team get to data faster, decreasing the amount of time it takes to find information and fix problems faster. He added, "I've found that to be incredibly valuable because it's a lot easier to get to some points of data now."

"The hardware list of the products ranges from, I think, 20 sensors and up to 500. Depending on your needs, you can scale it."

Read review »

"reduced our operational costs because it is faster to deploy configurations to firewall... deployment time has been reduced from five to 10 minutes down to two to five minutes."

Read review »

Virtualization

Another critical way to make the most of a NetOps strategy is through virtualization. When it comes to virtual deployment, a lead network security engineer at a small security firm liked that "you have a couple of choices depending on your needs and how much bandwidth you have that needs to be inspected."

He also appreciated that the Cisco Secure IPS solution is scalable, going on to say, "You have two different virtual appliances, one is for managing up to 25 sensors and the bigger one is up to 300 sensors. The hardware list of the products ranges from, I think, 20 sensors and up to 500. Depending on your needs, you can scale it."

A technical consultant at a tech services company with more than 500 employees also acknowledged Cisco's virtualization capabilities. He elaborated, saying, "They have multiple products that fit in multiple areas. They also have virtual firewalls, which are working well in virtualization systems. They have the data center firewalls feature for data centers. It's scalable enough to cover most of the use cases that might arise."

Saves time and money

Rapid Deployment

The speed with which a digital transformation happens is a measure of success for a NetOps strategy. An infrastructure engineer at a media company with over 10,000 employees spoke to this issue. He commented on Cisco SecureX's fast setup. He said, "We needed something like 45 minutes, maybe an hour, to run the initial setup. That was really fast."

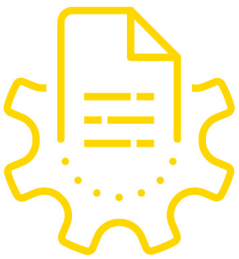
A technology director at an educational organization with more than 200 employees discussed the ease with which his team was able to set up the SecureX solution. He explained, "it was very easy because we could push it out using various systems. The biggest one was our mobile device management system that supports Macs and iPads. We could just upload the software to that and push it out. On the PCs, because we use Active Directory here, we could do it through group policy. We might have manually touched some of the PCs, but the deployment was very fast and easy."

A tech services systems engineer saved money from a quick deployment with Cisco Secure Firewall that it "reduced our operational costs because it is faster to deploy configurations to firewalls.... The amount of time it saves when deploying configurations depends on how often you deploy policies or how many changes you have. But if you compare 7.0 to earlier versions, deployment time has been reduced from five to 10 minutes down to two to five minutes."

Agility

Agility is a critical factor to consider when developing a NetOps strategy. Agile networks help organizations quickly overcome roadblocks and create the right conditions for digital transformation to take root. In this context, the flexibility of the Secure Firewall solution stood out to an administrator at a university with over 1,000 employees, who said it "can be easily integrated with your network hardware."

"It is very easy to integrate additional firewalls or even nodes on appliances. Whenever needed, they are stackable," said a technical specialist who uses Secure Firewall at a computer software company with over 10,000 employees. He added, "They are very flexible in that sense." An information security manager who uses Secure Firewall at a financial services firm with more than 500 employees had a similar sentiment. He mentioned, "It's a flexible solution and is well-known in the community."



Helps gather data faster

Automation

Automation is essential for success with NetOps, as it allows companies to take advantage of dynamic solutions that can allocate network resources based on business needs. To this point, an information security operations expert at a comms service provider with over 1,000 employees expressed that the most valuable feature of the Cisco Sourcefire SNORT solution is its ability to automatically learn the traffic in their environment, and change the merit recommendations based on that information. Specifically, he said, the intrusion rule recommendations feature "can tune its IPS rules automatically based on what it has learned. This feature is not available in other IPS solutions, so it is very beneficial for us. Manually tuning the IPS rules is difficult because we have thousands of them."

Meanwhile, the media company infrastructure engineer who uses Cisco SecureX "would rate it a 10 out of 10." He loved that the team "can aggregate the data from all our security products." It gives them the option to automate many of the tasks that they had to do manually before which is a "really huge time saver."

A lead program manager who uses Cisco Secure IPS at a computer software company with over 10,000 employees similarly acknowledged the value of users having access to intelligent security automation. He went on to say, "It can easily automate your event impact assessment and your IPS policy tuning can be done as well as your network behavior analysis. They introduced this intelligent security automation as part of that and then you can do a real-time contextual awareness. Basically, you can see a correlation of events that are created on your application, user devices, operating systems, or vulnerabilities. All of this real-time data can be captured including on your apps and port scans."

> "can be easily integrated with your network hardware."
>
> Read review »

"It can easily automate your event impact assessment and your IPS policy tuning can be done as well as your network behavior analysis."

Read review »

Orchestration

NetOps strategy also requires orchestration. Orchestration allows companies to interconnect various processes, data, and information. For instance, a technical team lead who uses SecureX at a small tech services company noted, "The orchestration allows us to say, 'Well, if this happens here, then we should take an automated action.' For example, if an email is received on a machine and malware is being executed, it can be put into lockdown mode. It should only be accessible by the investigators. It cannot connect with any other resources within the company anymore. It cannot send or receive any files."

This user then related, "SecureX takes all the separate pieces of security within your company, adds in intelligence from different sites and services on the internet, and makes them work together." A cyber security practice lead who also uses Cisco SecureX at a small tech services company echoed this sentiment, saying orchestration is "a very positive thing and one that will help us to scale as a managed service provider."

Security

NetOps strategy can help companies mitigate the impact of threats by building security into everything they do. Cisco Secures portfolio includes technologies to help teams achieve this goal. Secure Firewall's intrusion policy, for example, stood out as the most valuable feature for the tech vendor's lead network security engineer. He said, "...I cannot shy away from giving kudos to all of the other features such as AVC (Application Visibility and Control), SSL Decryption, Identity policy, Correlation policy, REST API, and more."

> "This enables us to have all the threat intelligence and threat event data in one place."
>
> Read review »

The policy ruleset available in Secure Firewall is what mattered most to a Senior Network Engineer at a retailer with over 1,000 employees. He shared, "The majority of what I do is create rules and work with the customers to make sure that things are getting in and out of the environment."

Data Analytics

Making NetOps work means having awareness and insight into how a network's many elements are functioning. This takes data and analytics. Analytics for NetOps involves tracking data through an array of sources like logs, user behavior, network performance monitoring, and other areas. For the cyber security practice lead, Cisco SecureX offers both security and analytic features. He explained, "We've integrated it with a number of Cisco security technologies, though we're primarily using it for Network Analytics right now."

Flexible and integrates easily

In his case, SecureX provides contextual awareness throughout their security ecosystem. It allows his team to integrate multiple threat intelligence feeds, as well as multiple security appliances and platforms. He said, "This enables us to have all the threat intelligence and threat event data in one place."

Additionally, a director of IT security at a wellness and fitness company with more than 5,000 employees said, "The telemetry that it generates gives Cisco unparalleled visibility, and Talos steps into that. They are able to apply their analytics over that data and identify emerging threats before practically anyone else, but Microsoft. From that perspective, my organization appreciates what Talos is able to do."

Conclusion

PeerSpot members are making progress toward the realization of NetOps strategies. The Cisco Secure portfolio provides them with virtualization, along with the orchestration and automation of processes. The portfolio delivers speed to deploy and agility, as well as the kind of data analytics network managers need to implement NetOps, and users can also build security into every element of their NetOps strategy. With these capabilities, users of the Cisco Secure portfolio gain the ability to realize the network side of digital transformation.

About PeerSpot

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. PeerSpot provides technology professionals with a community platform to share information about enterprise solutions.

PeerSpot is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.peerspot.com

About Cisco Security

Cisco has long established itself as the networking leader, while building an open, integrated portfolio of cybersecurity solutions along the way. Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, easy to manage, and easy to use – and that it all works together. We're driven by the fact that people and our customers are at the heart of what we do.

Cisco Secure empowers the security community with the reliability and confidence that they're safe from threats now and in the future on the SecureX platform. We help 100 percent of the Fortune 100 companies protect what's now and what's next with the most comprehensive, integrated cybersecurity platform on the planet. Learn more about how we simplify experiences, accelerate success, and protect futures at www.cisco.com/go/secure.

Cisco Secure Firewall | Cisco Secure IPS | Cisco Secure Access by Duo | SecureX | Cisco StealthWatch