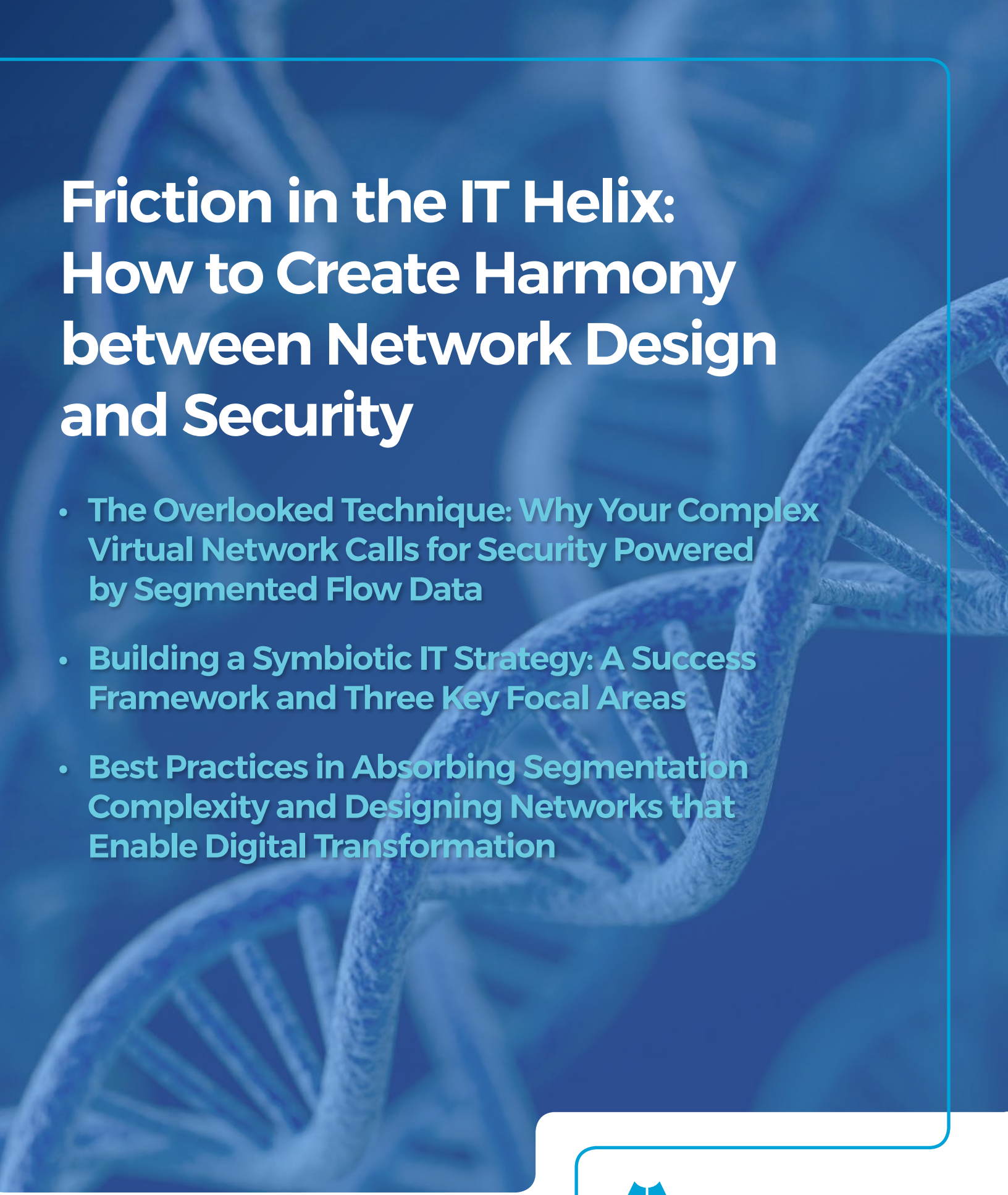


Friction in the IT Helix: How to Create Harmony between Network Design and Security

- The Overlooked Technique: Why Your Complex Virtual Network Calls for Security Powered by Segmented Flow Data
- Building a Symbiotic IT Strategy: A Success Framework and Three Key Focal Areas
- Best Practices in Absorbing Segmentation Complexity and Designing Networks that Enable Digital Transformation

MASERGY

MASERGY

Friction in the IT Helix: How to Create Harmony between Network Design and Security

The relationship between network design and security is tightly intertwined, and with the onset of artificial intelligence (AI), the internet of things (IoT), bring your own device (BYOD), and guest Wi-Fi, today's IT environments are expanding with an ever-growing number of segmented virtual networks that can complicate operations, creating friction and misalignment between network and security teams. How should your security practices stay in sync with your increasingly complex network, and what are the areas of intersection where alignment is most critical? This white paper explores network trends and challenges, an overlooked technique and three focal areas to strengthen IT synergies and reduce the tension amidst digital transformation initiatives.

The IT Helix: Digital Transformation and Network Segmentation

Network design and IT security are much like the spiraled double helix structure in DNA. They are two frequently connected strands, intrinsically linked. Together, this "IT helix" is the laddered backbone of the enterprise that constructs the genetic instructions for data exchange, establishing a foundation for digital transformation.

DNA's distinctive shape also creates a plethora of individually segmented areas inside the helix. Segmenting and separating network environments is a key strategy, because it breaks the IT infrastructure into small components for more effective data safeguarding. These isolated zones (VLANs) create layers of protection with incremental gates that help limit the attack surface for hackers, strengthening the enterprise security posture. As one of the strongest security strategies, network segmentation improves access control, monitoring, and containment, but the number of segmented environments your network should have is a topic of much discussion.

Smart Network Design: Flat vs. Layered

The security advantages of segmentation keep network design top of mind for IT leaders. In fact, executives often debate the questions: Should our network environment be flat or a richly layered topography? With today's rapidly evolving security landscape and our company's changing needs, which type of network is best and how much segmentation do we need?

As the owner and operator of the largest independent software defined platform in the world, Masergy sees customers increasingly moving toward richly segmented environments; most customers maintain at least six discrete virtual networks. Masergy's experts agree that a richly segmented environment is increasingly the best approach. Here's why.

The "IT helix" is the laddered backbone of the enterprise. With the network and security working in unison, it creates the genetic instructions for data exchange, establishing a foundation for digital transformation.

Most Masergy® customers maintain at least

6

discrete virtual private networks

CONTACT US: USA +1 (866) 588.5885 | UK +44 (0) 207 173 6900 | sales@masergy.com

Friction in the IT Helix: How to Create Harmony between Network Design and Security

Most people design their network with a flat environment for two reasons. First, that is how the service is sold. Many network providers don't offer an unlimited number of virtual environments (without additional costs). Second, flat architectures reduce the complexity of network visibility and management—particularly when legacy IT architectures are in place.

The problem with these default design approaches is that they don't start with the business need in mind and therefore don't accurately reflect what enterprises actually create when unrestricted by providers and technology. "Without the constraints of legacy network platforms, we consistently see enterprises creating segmented architectures around each initiative, department, location, project, and user group. This organic approach, in which you can spin up and spin down discrete virtual networking environments, aligns the network design with enterprise requirements," said Chris Werpy, Senior Vice President, Masergy, explaining that grouping applications, workflows, and user groups provides the foundation for optimal network design. "During discovery and design consultations, it's key to start the whiteboarding process at the application layer," he advised. These lessons reveal a critical best practice: Stop designing networks around service offerings and technology limitations and let function drive form. More often than not, that means additional segmentation.

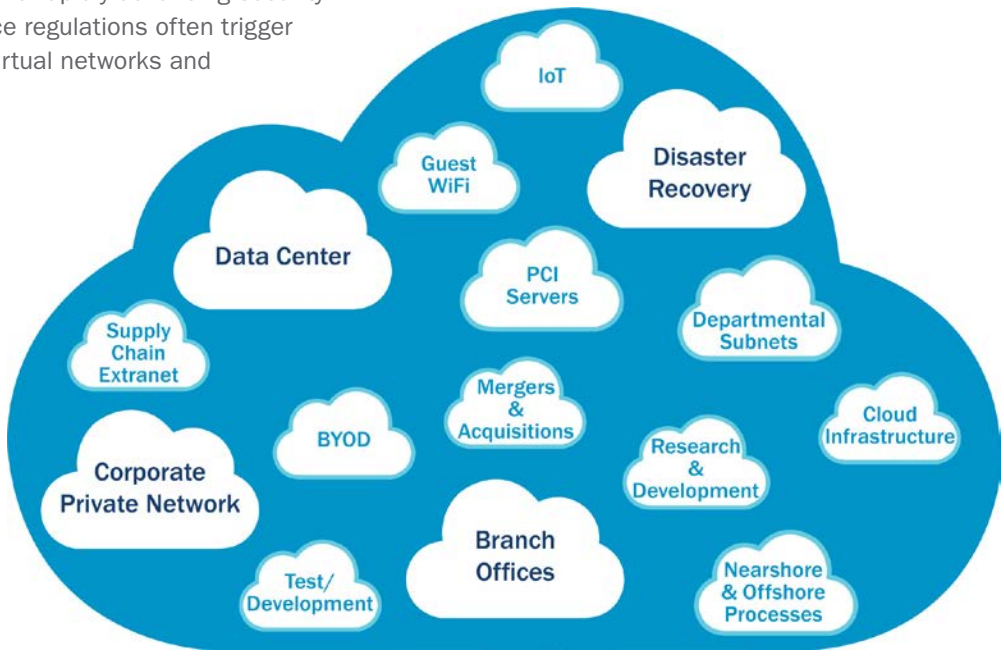
NETWORK DESIGN BEST PRACTICE

Most people design a flat network because that's how connectivity services are sold or because flat networks reduce complexity. Instead, you should let the business need drive the network design. More often than not, that means more segmentation.

Driving Factors behind Segmentation

The increasing need for highly segmented environments is the result of many driving factors in the IT world today. Trends such as AI, IoT, big data, workforce mobility and BYOD policies, guest WiFi, the increasing and rapidly advancing security threat landscape as well as new compliance regulations often trigger IT leaders to create yet more segmented virtual networks and Layer 3 VPNs.

Trends such as AI, IoT, BYOD policies, and regulations trigger IT leaders to create highly segmented networks



In addition to traditional environments such as the corporate network, data center replication, and branch location connectivity, use cases for segmentation include:

- Cloud migration strategies run on premise software inside a public or private cloud service provider's infrastructure
- Research and development, where segregated networks are needed for testing applications
- Mergers and acquisitions, where newly acquired companies are brought into a separate network during a gestation period
- Nearshore and offshore business processes, where security concerns are elevated

The Challenges: Segmentation Complexity and Misalignment across the IT Helix

Most people shy away from the highly segmented network, because it causes logistical barriers. It starts with poor management. Many times, segmentation is inadequately documented and not managed from a central place or repository. Technological limitations add to the challenge. Rigid, legacy carrier technologies and multiple technology stacks are commonly the root problem. Interoperability is lacking, making it difficult to manage multiple networks. Typically, IT teams are unable to rapidly deploy and provision new networks, gain clear visibility into performance and security, and manage the vast number of security analytics reports that increase exponentially with each newly added network.

Another formative IT challenge adds complexity: designing the network and the security strategy together. All too often, the network is designed without considering security design and its operations. IT teams fail to make the security blueprint part of the network blueprint when, in fact, the two go hand-in-hand. As a result, the two function as leader and follower rather than as equal partners in the IT helix. This misalignment becomes multiplied in highly segmented, complex network environments.

With the challenges of complex networks and network-security misalignment at play, the end result is friction, which significantly dampens the effectiveness of transformation initiatives. In response, IT executives aim to eliminate the operational constraints around the concept of limitless networks and bring network and security strategies into tighter alignment.

Rigid carrier networks make it difficult to manage highly segmented networks. Additionally, the corporate network is often designed without considering security and its operations.

As a result, IT executives should aim to eliminate operational constraints, establish IT environments that allow limitless segmentation, and align network and security strategies.

Creating IT Harmony: Software Defined Networking with Segmented Flow Data

To solve these problems, first IT leaders need a seamless software defined networking platform that absorbs the complexity of their segmented environments, removing this primary source of friction. Software defined networking principles allow unlimited VPNs while still providing deep visibility into the performance of each and offering a unified control panel across all. This foundational upgrade helps enterprises leap some of today's most plaguing IT hurdles, ushering in agility that keeps them dynamic in the face of rapid change and under the pressures of digital innovation.

The Overlooked Technique

Second, your security strategy should take the same segmented approach as your network, matching your unlimited virtual environments with multi-data-flow security monitoring. IT leaders need to keep their strategies parallel across the two sides of the IT helix, so you should maintain segmentation across both the network *and security.*

To illustrate, the diagrams on the next page contrast traditional security strategies with a multi-data-flow security approach. Traditional strategies that track activity across all subnets collectively are appropriate for networks with fewer subnets. However, as influencers in our modern world drive complex segmentation, a

multi-data-flow security monitoring strategy that tracks activity across each subnet individually may make more sense for your enterprise, because it aligns the IT helix and offers many benefits (more on those later).

This overlooked technique might feel like a forward-thinking suggestion, but it is possible with the technologies we have today. Just like you can segregate networks from both a logical and physical perspective, you can also create a different span for each network by which you can apply security policies and run managed detection and response services. To monitor individual networks, security systems must ingest segmented flow data from each discrete virtual network environment. Multiple virtual networks based on virtual routing and forwarding tables (VRFs) generate separate flow data and metadata for each network, allowing independent security monitoring.

MULTI-VRF SECURITY: HOW IT WORKS

Segmenting a network using VRFs allows multiple isolated routing tables to exist on a routing system. Monitoring segmented networks requires security systems to ingest flow data from each network, including its associated router, firewalls, and other virtualized functions. This is made possible through multiple VRFs, which generate separate flow data and metadata for each network. Once the network is set up, the segmented data is ingested into the security system for additional visibility and monitoring.

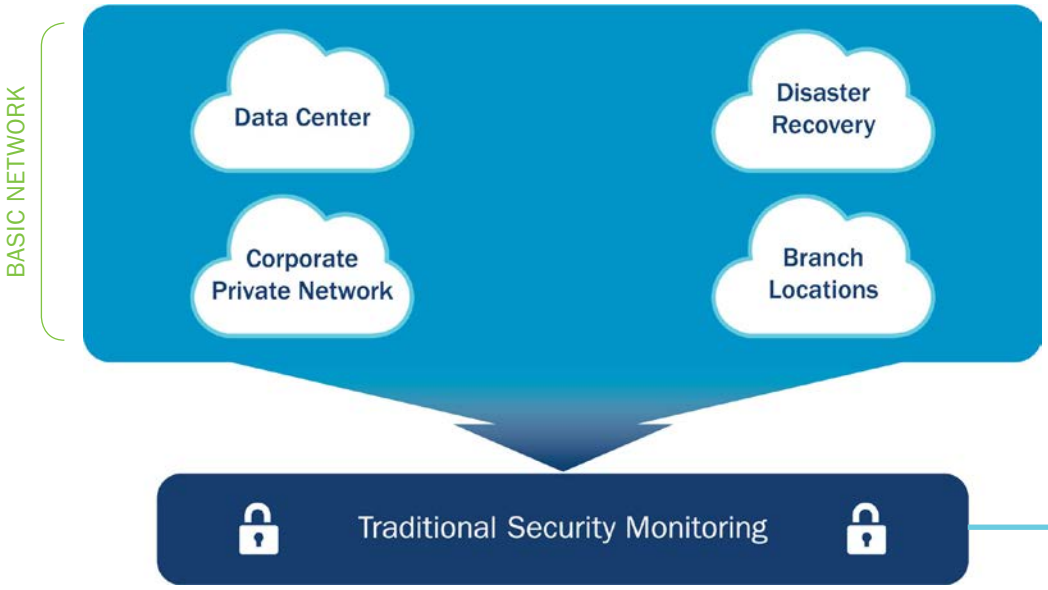
Here's an example. If users in your engineering department is not allowed to have access to the finance server, the system will flag any engineering user traffic as a violation of policy. Network rules, policies, and segmentation zones define which traffic is allowed to commingle. Then, the security system monitors multiple data flows to ensure the rules are followed.

MASERGY

Friction in the IT Helix: How to Create Harmony between Network Design and Security

Traditional Security versus Multi-Data-Flow Security

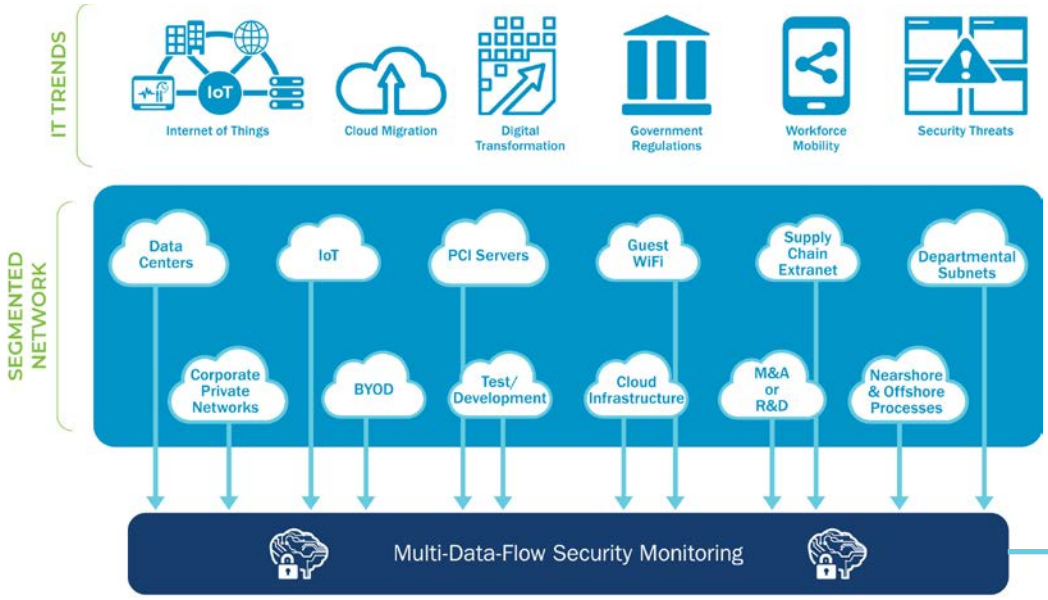
Traditional Security Monitoring



- Takes a single, broad and comprehensive viewpoint
- Tracks activity across all subnets collectively
- Normal network behavior is widely defined
- Recognizing irregularities in behavior is more difficult because definitions can be obscure

Multi-Data-Flow Security Monitoring

Mega-trends spur IT leaders to create segmented networks and adopt a multi-data-flow security approach that maintains tight harmony between the network and security. It also fine tunes security.



- Takes a multiple, segmented viewpoint
- Tracks activity across all subnets individually
- Normal network behavior is more narrowly defined
- Recognizing irregularities in behavior is easier because definitions are more precise
- Requires machine learning and behavior analytics

CONTACT US: USA +1 (866) 588.5885 | UK +44 (0) 207 173 6900 | sales@masergy.com

The Benefits: Harmony and Fine-Tuned Security Intelligence

Maintaining segmentation across both the network and security is an approach that Masergy uses to simplify digital transformation for its customers. Applying parallel approaches with multi-data-flow security monitoring can result in a symbiotic relationship between the network and security operations, which serves innovative companies well given the backdrop of today's accelerating velocity of change and the pressure to rapidly adopt advancing technologies. Those who strive for this synergy can recognize benefits including:

- The virtualized segmentation of workloads and workflows
- Customized design and implementation to create the best application experience for the end user
- Visibility into those individual workloads and workflows (by business unit or virtual routing and forwarding)
- The ability to apply security policies specific and relevant to those virtualized environments or business units
- Security benefits including finely tuned security intelligence that takes into account accurately defined normal behavior (see sidebar)
- An IT ecosystem where network design and security work together in harmony

How to Build a Symbiotic IT Strategy

The Success Framework

Implementing a symbiotic strategy between network and security requires enterprises to tackle the multi-network logistical challenges and build multi-VRF security monitoring practices in sync. Several prerequisites create a framework for success, including

Foundation: Software Defined Network Platform

A software defined network platform enables unlimited virtual networks, simplifies provisioning and management, grants deeper WAN visibility, and supports multiple VRFs.

SEGMENTATION FINE TUNES SECURITY

Segmenting applications, workflows, and user groups into discrete virtual networks allows security learning models to derive more accurate predictions of normal behavior. It sharpens the precision of anomaly detection, which is a key technique for detecting advanced persistent threats and zero day attacks. Using painting as an analogy, when security takes a comprehensive approach, it tracks activity from all environments collectively, establishing a norm that takes into account behavior from a variety of different networks. This normal is painted with a single, broad stroke. But when security takes a segmented approach, it tracks the activity of each network individually, painting each normal with many small strokes and creating a high-resolution "image." For the purpose of analysis, this fine-tunes security intelligence tools to make irregularities less obscure.

Key Enabler #1: Managed Security Service with Machine Learning and Behavior Analytics

Look for a fully managed security service capable of ingesting and effectively monitoring multi-VRF dataflows, and make sure they have the latest machine learning and data analytics tools to reduce millions of security alerts down to a short list of meaningful actions. Due to the large amount of data on a network, the ideal method for evaluating network flow data is to use machine-learning-based models that look for abnormal patterns of traffic. This helps enterprises understand normal behavior on their network, and more importantly, detect and alert on malicious activity within segmented environments.

Key Enabler #2: A Partner who Does Both

Partners best suited for the work outlined above will be proven experts in both capabilities and will be able to successfully deliver them as a unified and fully managed service—rather than ad hoc tools and services.

Generating Harmony: Three Key Focal Areas

Developing a symbiotic IT strategy also compels enterprises to take a closer look at the precise intersections where security and networking join together. Any misalignment at these junctures can quickly create consequences for the organization. It comes down to these three primary focal areas:

1. **Segmentation:** Consistency from the LAN to the WAN and into the security strategy
2. **Hybrid Networking and SD-WAN Strategies:** Public connectivity and security concerns
3. **Multi-Faceted Devices:** Virtualization, SD-WAN, and bundled capabilities blur the line between network and security

Anytime you are engaging in one of the activities listed above, collaboration is needed to address security, monitoring, and cohesive strategies. Here are some ideas on how to stay aligned.

To absorb IT complexity, adopt software defined network platforms for limitless segmentation and put multi-data-flow security into practice to keep strategies aligned between the network and security.

Partners best suited to lead the charge will have mature software defined network offerings and will provide managed security services with machine learning and behavior analytics.

Segmentation: Consistency from the LAN to the WAN and into Security

Most of the time, enterprises don't consider mapping LAN segmentation across the WAN because with most providers they can't. Segmentation technologies in the LAN, WAN, data center, and cloud can all be different. As a result, enterprises build totally separate networks. But ideally, data protected inside the LAN should also be isolated and protected in the WAN—as one unified strategy.

Strict adherence to RFC standards for MPLS/VPLS backbone architecture combined with a common global service delivery fabric make it possible to more easily maintain LAN-WAN segmentation. It also makes it possible to overlay emerging technologies such as

SD-WAN and hybrid networking while maintaining both traffic separation and performance as well as full visibility to traffic flows, service creation, capacity, and performance management.

LAN-WAN segmentation can also be mapped into a pervasive security posture by monitoring multi-tenant infrastructure through one, centralized managed detection and response security deployment across multiple instances of virtual routing and forwarding (VRFs) and LAN segmentation.

Ideally, data protected inside the LAN should also be isolated and protected in the WAN—as one unified strategy.

Then, LAN-WAN segmentation should be mapped into security.

Hybrid Networking and SD-WAN Strategies: Public Connectivity and Security Concerns

Everyone's talking hybrid networks and SD-WAN, but no one talks about how they secure it from a perimeter perspective. Enterprises often forget that hybrid networks and SD-WAN projects require alignment between security and network teams, because they often introduce public Internet connectivity. When introducing public-facing customer premises equipment (CPE) to the network, new security monitoring must be added.

Security and network teams should work together to identify how security will be handled. They may choose to isolate access to the edge SD-WAN device and create policies to ensure it is part of the broader enterprise security strategy. At the end of the day, you either need to ingest the security alerts into your existing solution, or you need to partner with a managed security provider who can ingest and monitor the alerts for you. Ideally, you want a partner who covers both playing fields, offering managed network and security services that always stay in sync.

Hybrid networking projects typically require tight alignment between security and network teams.

Multi-Faceted Devices: Virtualization, SD-WAN, and Bundled Capabilities Blur the Line between Network and Security

Virtualization and SD-WAN are blurring the line between network and security, making responsibility for each a gray area and alignment even more critical. For example, networking solutions now come with security functions bundled in, making multi-faceted devices much more commonplace. Such is the case with SD-WAN connectivity, which may include integrated routing and firewalls and associated unified threat management. As a result, roles and responsibilities become confusing. Network teams find themselves asking questions such as, "Does that mean our internal IT security team is responsible for managing the SD-WAN devices on our corporate network?"

This situation makes it necessary to take a holistic approach, integrating security architecture with network infrastructure. Security and network teams must work together to determine who will own the capital resource and the CPE administration, associated configuration, and support. They need to address questions around policy, ownership, and expenses.

The intersections between network and security are increasing as the network takes on multi-faceted devices that should now be considered as part of the overall security strategy.

Conclusion

In summary, as networking environments become more segmented and complex and as advances in technology obscure the roles and responsibilities of IT, the convergence of networking and security is a powerful force certain to continue. The intersections between network and security are increasing, and a symbiotic strategy with collaboration at each junction is critical for innovation agendas. Today's fast-paced development requirements alongside the ability to effectively manage technological disruptions means only the tightest of partnerships and the most synergistic teams will be able to effectively drive digital business transformation. IT harmony will soon become an underlying factor for success.

How Masergy Helps You Create Harmony between Network Design and Security

Hybrid networking partners are helping enterprises build symbiotic strategies across networking and security with unified solutions and software defined platforms. Take Masergy for example, which has unlimited virtual private networks at no additional charge as well as managed network and managed security services which can be integrated seamlessly. Here's how Masergy's platform delivers synergistic value:

Unlimited Virtual Environments: Software defined VPNs and network function virtualization mean you can quickly and easily deploy and provision an unlimited number of discrete virtual environments. Spin up or down as many as you need to support your unique business objectives, and enjoy seamless integration with our Managed SD-WAN and Network Function Virtualization.

Embedded Analytics and Control Systems: Unlike other providers that bolt on tools at the perimeter, our platform provides an embedded analytics and service control panel. Our tools provide deep security, network, and application visibility across each VPN. These advanced capabilities empower IT administrators to monitor network traffic, analyze bottlenecks and threats, and make network modifications and security escalations.

Security Powered by Custom and Segmented Flow Data: Masergy provides multi-VRF capabilities at no additional charge and exports flow data from virtualized environments into our managed detection and response service. Our Unified Enterprise Security solution is powered by sophisticated machine-learning capabilities and behavior analytics.

Managed Detection and Response: Other providers put firewalls on your network or on the perimeter and sell them with monitoring services. But that doesn't address the constantly growing number of threat vectors and the need to protect corporate data no matter where it resides (e.g. in the cloud or on an employee's laptop). Masergy offers true managed detection and response (MDR) that goes beyond the perimeter defense model. With patented technologies and comprehensive integration capabilities, Masergy generates a holistic security picture of your core infrastructure. Masergy's UES solution ingests multiple data sources such as logs, network traffic (both raw and flow based), vulnerability scan, cloud security alerts, endpoint detection and response (EDR), and SaaS-based security data via CASB from our customers environments, further enhancing monitoring and the connections between network and security.

Learn about Masergy's Hybrid Networking Solutions

24-7 Monitoring for both Network and Security Operations: With fully managed services providing 24-7 monitoring, Masergy customers expand their team with the watchful eye of certified network and security experts. Masergy has two distinct and separate operations centers (NOC and SOC). These standalone, isolated units in North America, Asia, and Europe continuously monitor network performance and ingest and analyze security alerts to combat advanced threats.

A Network and Security Partner in One: Best of all, customers get a partner who offers both network and security services--a rarity in the marketplace today. Better still, we have proven experience in helping customers align security and network operations to enable the highest performance alongside strongest data security possible.

About Masergy

Masergy owns and operates the largest independent Software Defined Platform in the world, delivering hybrid networking, managed security, and cloud communication solutions to global enterprises. Our patented technology, customizable solutions, and unmatched customer experience are why a growing number of leading organizations rely on Masergy to deliver performance beyond expectations.

ADDITIONAL SUGGESTED READING

The Hybrid Network Buyers Checklist

Time to Recharge Your Cyber Security Strategy

Conversational SD-WAN: What SD-WAN Is, How It Works, and Deciding If It's for You

The SD-WAN Wave: Cost Savings Hype and MPLS Misconceptions