Executive Guide to Pragmatic Network Security Management

The Demise of Network Security Has Been Greatly Exaggerated

DLP, IPS, NGFW, WAF. Chief Information Security Officers today suffer no shortage of network security tools to protect their environments, but most CISOs we talk with struggle to implement and maintain effective network security programs. They tell us it isn't a lack of technologies or even necessarily resources (not that there are ever enough), but the inherent difficulties in defending a large, amorphous, business-critical asset with tendrils throughout the organization. It's never as simple as magazine articles and conference presentations make it out to be.

> Effectively managing a network security program is a combination of *maintaining visibility* and *adjusting security controls* for the inevitable continuous change.

Managing network security at scale is not easy, but the organizations that do it best tend to follow a predictable, repeatable pattern. This paper distills those lessons into a pragmatic process designed for larger organizations and those with more complicated networks such as medium-sized businesses with multiple locations. We wouldn't claim our process is magical or easy, but it's certainly *easier* than many alternatives. Even if you only pick out a few tidbits, our process should help you refine and operate your network security more efficiently.

Why Network Security Is So Darn Difficult

Networks and endpoints are the two most fundamental pieces of our IT infrastructure, yet despite decades of advancements they still consume a disproportionate amount of our security resources. First the good news: we are *far* more resilient to network attacks than even five years ago. But every CISO knows establishing and maintaining network security is a constant challenge. We have narrowed down a handful of root causes and designed this pragmatic process to address them:

- *Security and operations are divided*. IT Operations is responsible for and manages the network, servers, endpoints, and applications; Information Security is responsible for defending everything. In some cases security doesn't even know how all the pieces of the network are connected, but is still expected to manage firewall rules to protect it all.

- *Networks are dynamic and complex*. Not only are new assets constantly joining and leaving the network, but its structure is never static — especially for larger organizations.

This report created with the Securosis Totally Transparent Research Process and is copyright under a Creative Commons Attribution-Noncommercial-No-Derivative Works 3.0 license by Securosis, LLC

- Organic growth. All networks grow over time. Perhaps it's a new office, extending a WiFi network, or an extra switch or router in the datacenter.
- Mergers and acquisitions require blending resources, technologies, and configurations.
- New technologies with different network requirements are added constantly.
- We mix and match various security tools, often with overlapping functionality, to meet particular project needs.

- *Needs change over time*. Many organizations today are working on consolidating network perimeters, compartmentalizing internal networks, adding application awareness, expanding egress monitoring and filtering for breach and infection defenses, or adapting the network for cloud computing and eventually SDN. Network and network security technologies evolve to meet new business needs and evolving threats.

Our networks are large and complex — sometimes even when our organizations aren't. They change constantly, as do the assets connected to them. Security doesn't manage this infrastructure, but is tasked with protecting it.

From Blocking and Tackling to Integrated Defense

Our primary goal is to adopt processes that are flexible enough to account for an ever-changing network environment, while avoiding the constant firefighting and occasional infighting that waste so much time and energy. The key isn't a technology or security trick, but better integrating defenses into day-to-day management of the enterprise.

We get it — even if you are the CEO there are limits to change. We have collected the best practices we have seen work in organizations, lining them up into a practical and achievable process that takes real-world restrictions into account. Our next sections will dig into the process. As we said earlier, pick and choose those which work for you.

This report is licensed by RedSeal Networks, whose support allows us to release it for free. All content was developed independently.

www.redsealnetworks.com

RedSeal Networks provides the industry's leading network infrastructure security management solution. RedSeal shows you where your network security works, where it doesn't, where your cyber-attack risk is, and what to do about it. The proactive security management solution enables network, security, and risk teams to visualize their end-to-end network, more efficiently manage operations, respond to threats, and analyze risks. It is used by the world's largest governments and enterprises, with the most-complex networks.

The Pragmatic Process

Here is the outline, followed by the details:

1. Know your network.
2. Know your assets.
3. Know your security.
4. Map the topology.
5. Prioritize and fix.
6. Monitor continuously.
7. Manage change and build workflows.

The first five steps ***establish the baseline***, and the next two ***manage the program***, although you will need to periodically revisit previous steps to ensure that your program stays up to date as the business evolves and risks change.

Know Your Network

Many organizations *believe* they have accurate network topologies, but they are rarely correct or complete — for all the reasons in the previous section. The most common problem is simply failure to keep them up-to-date. Topology maps are produced occasionally as needed for audits or projects, but rarely maintained. Work with Network Operations to see what they have and how current it is. Aside from being politically correct, there is no reason not to leverage what is already available. Once you get their data, evaluate it and decide how much you need to validate or extend it.

There are a few ways to validate your network topology, and you should rely on automation when possible. Even if Network Operations provides a map or CMDB, you need to verify that it is current and accurate. One issue we see is that Security uses a different toolset than Network Operations, because security tools are tuned to scan for weaknesses rather than build a topology.

Know Your Assets

Once you have a picture of the network start evaluating the assets it contains: servers, endpoints, and other hardware. Security tends to have better tools and experience for scanning and analyzing assets than for underlying network structure, especially workstations.

Depending on how mature you are at this point, either prioritize your scanning to particular network segments or use the information from the network map to target weak spots in your analysis. Endpoint tools such as configuration/patch management and endpoint protection platforms offer some information, but you also need to integrate a security scan (perhaps a vulnerability assessment) to identify problems. Assessment should be continuous, with at least an effort at prioritization.

Know Your Security

You need to collect detailed information on three major aspects of network security:

- *Base infrastructure security*. This includes standard perimeter security, as well as anything deployed internally to enforce any kind of compartmentalization or detection. Think firewalls (including NGFW), intrusion detection, intrusion prevention, network forensics, Netflow feeds to your SIEM, etc. Things designed primarily to protect the core network layer. Even network access control, for both of you who use it.
- *Extended security tools*. These are designed to protect particular applications and activities, such as your secure mail gateway, web filter, web application firewalls, DLP, and other "layer 7" tools.
- *Remote access*. Security tends to be tightly integrated into VPNs and other remote access gateways. These aren't always managed by security, but unlike network routers they have internal security settings that affect network access.

For each component collect location and configuration. You don't need all the deep particulars of a WAF or DLP, beyond what they are positioned to protect, but you certainly need complete details of base infrastructure tools, including firewall rulesets.

Map the Topology

This is the key step, when you align your network topology, assets (focusing on bulk and critical analysis, not every single workstation), and existing security controls. Then there are two kinds of analysis to perform:

- A *management analysis* to determine who manages all the security and network assets, and how. Who keeps firewall X up and running? How? Using which tool? Do you feed IDS alerts to the SIEM? The objective is to understand the technical underpinnings of your network security management, and who is responsible.
- A *controls analysis* to ensure the right tools are in the right places with the right configurations. Again, you probably want to prioritize by assets. Do you use application-aware firewalls (NGFW) where you need them? Are firewalls configured correctly for the underlying network topology? Do you segment internal networks? Capture network traffic in the right places to detect network attacks?

The first analysis focuses on implementation of management processes and workflow. The second is all about preventing and detecting attacks and aligning controls. Once you map assets to the network topology, to the security defenses, and to the management infrastructure, two pictures emerge: how your defenses are really aligned, and how you manage them.

Prioritize and Fix

By now you have a deep understanding of your network topology, a decent understanding of where important things are on the network, and a solid idea of how your security is configured around and within it. So it's time to start fixing things. The goal is to improve how you manage your security over time — not just to plug a few holes until you need to start all over again.

This involves:

- *Repositioning network security tools*. Ensure you have the correct preventative or monitoring control in the right physical location. This isn't about buying new things, but understanding and best using the ones at your disposal.
- *Reconfiguring network security tools*. Adjust rules and configurations to provide the desired protection.
- *Consolidating network security management*. So you can maintain visibility and implement changes more efficiently in the future.
- *Position new tools as needed*. You may already be using application-aware network security, egress monitoring, command and control monitoring, DDoS protection, cloud web filtering, and malware gateways. But if you weren't, now you have much better information for integrating them effectively into your program, as well as positioning and configuring them.

Continuous monitoring doesn't necessarily mean *real-time*. Figure out the best schedule based on your rate of change and security needs.

This is still the "initial fix" phase. In a moment we will discuss continuous change management. Most organizations fix some immediate things while they begin adjusting their management processes and workflow. There is no reason you must hop through these steps one at a time.

Continuously Monitor

This phase moves past *baselining* into *managing the program*. There are four key pieces to track:

1. *Network topology changes,* such as routing changes and network additions. Security can monitor for these directly or establish stronger collaborative workflows with network operations. Regardless, topology needs to be revalidated periodically, using active and passive tools, to catch errors and omissions.
2. *Asset changes*. Use security scanners, especially vulnerability scanners, to track asset movement and configuration changes.
3. *Network security tool changes*, including both uses and configurations — which is why we emphasized consolidating network security management infrastructure.

You notice we skipped the part about *monitoring for bad guys*. That's because this report is focused on managing your overall program — not the details of daily defenses and incident response.

The last piece of this phase is creating reports for auditors and executives. Ideally you can quickly create these reports without undue effort because you already have all the required data, constantly updated and accessible.

Manage Change and Build Workflows

This is the most important phase of the entire process. Until now you have focused on understanding your infrastructure and developing the security controls around it. But all that is impossible to maintain unless security works closely with both IT Operations and business units. The key is not only to refine internal processes, but to create *minimal-friction workflows* for working with the rest of the organization. The easier it is for *them* to go through an approved process, the less likely they are to try to circumvent it.

In this section we cover the security change management process, and in the next section we will offer examples of common workflows for coordinating with other areas. For detailed processes for network security operations, we recommend our own Network Security Operations Quant Report.

- **Trigger:** Either a change request or a change in the operating environment (such as a routing change detected by security which didn't go through a change request process).
- **Process change request and authorize:** Examine the unapproved change to determine the security response, or process the internal or external change request. Determine requirements, impact, security risks, and priority; then slot the change into a maintenance window. Priority reflects both business and security needs, especially when threats are a factor.
- **Test and approve:** This step includes development of test criteria, any required testing, result analysis, and approval of the signature or rule change for release once it satisfies requirements.
- **Deploy and confirm:** Deploy and verify that changes were successful, including both installation and operation. This might include use of vulnerability assessment tools or application test scripts to ensure there is no disruption of production systems or attack surface added as a result of the change.
- **Audit/validate:** This entails validating the change to ensure policies were properly updated and matching it to a specific request. This closes the loop to make sure there is documentation, as well as an audit trail, for every change.
- **Emergency updates:** In some cases, including data breach lockdowns and imminent or active zero-day attacks, a change to the network security device's configuration must be made immediately. An 'express' process should be established and documented in advance as an alternative to the normal full change process, ensuring authorized approval for emergency changes, and a rollback capability in case of unintended consequences.

Workflows: from Sec and Ops to SecOps

Even mature organizations occasionally struggle to keep security aligned with infrastructure. But low-friction processes that don't overly burden other areas of the enterprise reduce both errors and deliberate circumvention.

The problem often manifests as a lack of communication between Network Security and Network Operations. Not out of antagonism but simply due to different priorities, toolsets, and issues to manage on a day-to-day basis. A seemingly minor routing change, or the addition of a new server, can subtly expose the organization to new risks if security defenses aren't coordinated. On the other hand security can easily break things and create an operational incident with a single firewall rule change.

Efficient programs don't just divide up operational responsibilities — they implement workflows where each team does what they are best at, while still communicating cleanly and effectively with each other. Here are examples of four integrated operations workflows:

- **Network topology changes:** Changes to the topology of the network have a dramatic impact on the configuration of security tools. This workflow consists of two tracks — *approved* changes and *detected* changes. For approved changes the network team defines the change and submits it to

security for review. Security analyzes it for impact, including any risk changes and required security updates. Security then approves the change for Operations to implement. Some organizations even have Network Operations manage basic security changes — mostly firewall rule updates. A detected change goes through the same analysis process but is more likely to require an emergency fix or communications with the network team to roll back the change — and obviously requires ongoing monitoring for detection in the first place. In both cases it can be helpful to integrate the process into your change management or workflow tool to route tasks automatically.

- **Business exemption or change requests:** Occasionally a business unit will need a network security change. Many of these come through Network Operations, but quite a few come directly from application teams or business units for particular projects. The same basic process is used: the change request comes in, is analyzed for risks and required changes, and then approved, implemented, and validated. As before, you should plan to monitor for and manage unapproved changes, which is where application-aware monitoring is particularly useful. Consider creating a portal for business units to submit and track requests, rather than handling them through email or spreadsheets.

- **New assets and applications:** Similar to a business exemption or change request, but focused on new projects and assets rather than creating an exemption to existing policy. There may be more planning, earlier in the process, involving many more people. Develop a two-track process: one for new applications or assets that are fairly standard (*e.g.,* a business unit file server or basic web application) which can be more automated, and a second for larger programs such as major new applications.

- **New security tools or policy changes:** Adding a new security tool or policy change reverses the workflow, so the responsibility is now on the security team to initiate communications with Network Operations and other affected teams. Security should first analyze the change and potential downstream impacts, then work with other teams to determine operational risks, timelines, and any other requirements.

Conclusion

Network security management isn't easy, but there are more and less efficient ways to handle it. Knowing your posture and maintaining visibility are key, as are developing core workflows to bridge gaps between different operational teams. Network Security Operations monitors the environment and change requests to adapt the security posture as needed in a timely manner. It monitors for changes that slip past approval processes, develops workflows to handle the unexpected, and responds quickly when changes are requested to support other business areas. Finally, Network Security Operations understands that security policy changes impact other operations, and that it needs to analyze and communicate the potential implications.

It is not always easy, but it is far more efficient and effective than the alternatives, and frees up the Security team to focus on what they are best at.

Rich Mogull is an Analyst and the CEO of Securosis. Prior to founding Securosis he was a Research Vice President at Gartner.