Transforming Network Security: How to Win Against Cyberthreats

Securing your network from new challenges and emerging threats

Highly efficient. Agile. Effective. Such traits are often valued by today's enterprise organizations.

Yet, when it comes to securing their networks against the latest cyberthreats, there are many who would not use these same terms to describe their own levels of organizational readiness.

It's easy to see why. Securing one's network has become an increasingly thorny dilemma with no easy answers.

On one side, there's simply too much of what you don't want:

- Too many threats
- Too many endpoints (both known and unknown)
- Too much data to analyze – with a shortage of qualified people to do so
- Too many security point products
- Way too much complexity

On the flip side, there's not enough of what you do want – an air-tight, secure network that can effectively block and contain today's stealthy digital intruders.

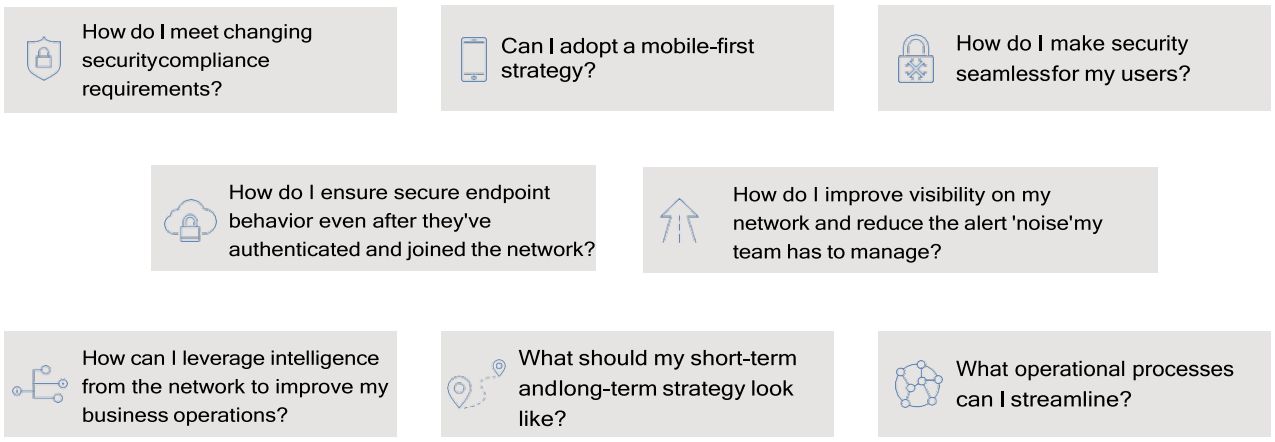
Is there a way forward? Is there a way for today's enterprise to reset this balance and start to successfully win the game against today's (and tomorrow's) bad actors?

At En Pointe ITS, we think there is. And, while this paper won't promise a magic wand to remove all risk, it does offer a better way forward. Built upon real-world insight from our work with enterprise clients and industry leaders, this paper offers key advice and approaches that can help you win your own long and short game towards better network security.

Many questions, but are there answers?

At En Pointe ITS, clients come to us with a number of questions. They need answers and we are happy to provide them. Figure 1 gives just a small sampling of the questions we field in the area of network security.

Figure 1. Common questions organizations ask about security.



Part 1: First business, then technology

As it turns out, answers to common questions about network security lie as much with the business-side as they do with the technology you choose to deploy.

Amidst vendor talk of hot new features and products for such areas as next-generation firewalls, network segmentation, or Network Access Control (NAC) are the very real business issues that continue to impede many organizations' network security efforts.

For that reason, Part 1 of this paper first tackles the most common business challenges companies face in their efforts to shore up their defenses. Part 2 then covers some of the technology-side questions and recommendations to help companies move forward.

> "No single strategy, technological solution, or approach will solve all of the challenges that our adversaries throw at us. It takes a comprehensive and unified approach across people, process, technology, and policy."[1]

Blog announcing results from the Cisco 2018 Annual Cybersecurity Report.

Define network security-related wants and needs

En Pointe ITS experts are often called in to consult with organizations about their networking environments and their network security-related needs. For some, the issue may be more clear-cut: such as the need to meet a network security requirement in order to do business with a new client. Some may have many of the right resources but struggle with issues surrounding staff shortage or overly slow deployments. Still others may need immediate help to triage or remediate a recent, suspected security breach or post-audit findings.

For many organizations, however, the need to secure their network is often much fuzzier and less well-defined. This is one of the common places we see many organizations struggle. Many companies say they want better security but don't really understand the specific business drivers or goals surrounding this need.

When such customers are then asked to analyze and assess a hot, new network security technology or vendor offering, they may find themselves agreeing to move forward – without knowing whether or not that technology will help them achieve specific business goals. We call this falling into the "buzzword" trap. Just because something's hot doesn't mean it's necessarily right for the organization.

Some of the practices we use to crystallize an organization's network security needs and challenges include:

- Meeting with business units to extract each unit's specific business goals toward security.
- Conducting detailed interviews with stakeholders to determine their goals from a network security or operations standpoint.
- Identifying the types of network security drivers (i.e., internal drivers like corporate compliance goals vs. external drivers like agency or third-party regulations).
- Identifying current and future network security challenges to the organization. (For instance, many organizations remain concerned with managing and securing data as it traverses such evolving frontiers of IoT, containers, the cloud, and mobile devices.)

Getting to the root of security challenges, business drivers, and expected business outcomes is a critical first step on the road to success with an organization's network security.

According to CyberEdge,[2] the top three most-cited barriers to adequately defend an organization from cyberthreats are: too much data to analyze, a lack of skilled personnel, and a low security awareness among an organization's employees. Cisco survey respondents also cite personnel shortages, budget, and interoperability as key challenges to managing security.[3]

2018 Cybersecurity Reports from CyberEdge and Cisco

Understand where you are now

Another area we look at is organizational and technological maturity or "readiness" in regard to network security. Some of the questions we seek to answer here might include:

- What security tools and equipment are currently in use? How effective are they?
- What is the state of the current network?
- How well does the organization and infrastructure follow network security best practices?
- What is the nature of the skill set of current staff?
- Is the security team integrated with the networking team or operating in its own silo?
- How equipped is the organization to deploy and manage emerging network security technologies, such as next-generation firewalls or software-defined networking?

Translate business needs into technical requirements

After completing the first few steps, it becomes much easier for En Pointe ITS to define an organization's important business outcomes and successfully translate those into technical requirements. This goes as far as identifying specific policies and practices a solution should follow in order to meet the network security needs of one group over another.

This translation process sets the stage to then better assess, compare, and select the right network security technologies —at the right time.

Close the gaps and break down barriers

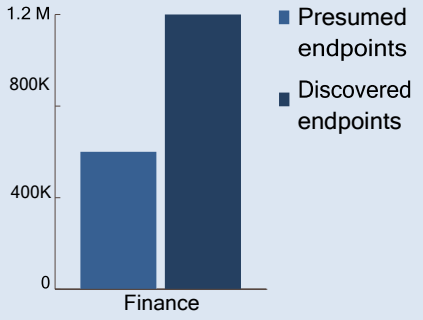
A number of issues make it difficult for organizations to strengthen their network security posture. Part of the answer lies in identifying and resolving key gaps and barriers to moving forward. Once plans are in place to close such gaps, network security efforts can become more streamlined.

> "Much of the...cybersecurity industry...will be focused on bringing machine learning, artificial intelligence, and big data analytics to their products. In addition, there will be more focus by the industry on integrating the various tools into consolidated platforms that will require fewer people to operate..."[4]
>
> **Bill Crowell, Cybersecurity Expert**

EN POINTE IT SOLUTIONS
Making Technology Work for You

Potential gaps:

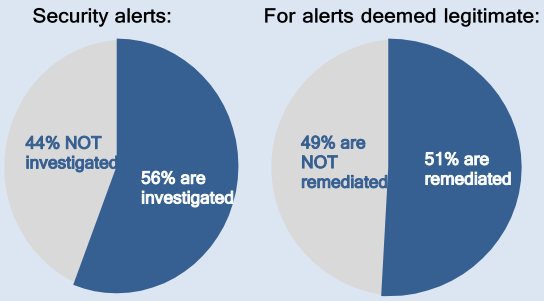
Closing "leak paths." According to the Cisco report,[5] a leak path occurs with unauthorized or misconfigured connections to the Internet. It can also occur with some type of violation of policy or segmentation process. Surprisingly, the report's research in this area indicates a wide gap between the number of endpoints presumed to exist in an organization and the actual number of endpoints discovered. For instance:



Finance organizations thought they had 600,000 endpoints. In reality, 1.2 million endpoints were discovered. Healthcare organizations did not fare much better. They presumed about 60,000 endpoints, when the reality was nearer to 90,000.

Such leak paths highlight a common – but serious – issue we see as well: incomplete security installs and deployments that don't follow network security best practices.

Too much log/alert data, not enough people. The network security staff shortage is not likely to improve much in the short term. Yet, security products continue to send a growing mountain of daily data needing analysis and follow-up action. Unfortunately, in too many instances, much of this data remains unknown, uninvestigated, or unaddressed.



According to Cisco,[6] organizations that received daily security alerts did not investigate 44% of them. In situations where alerts were investigated and deemed legitimate threats, nearly half of those still went unremediated.

En Pointe ITS experts and industry veterans have begun to see promising new ways to close this gap. Increasingly, these have started to incorporate interesting elements of automation, AI, and machine learning. The use of outsourced or managed security services to bridge potential shortfalls is also on the rise.

EN POINTE IT SOLUTIONS
Making Technology Work for You

Potential barriers:

Too many point products. Depending on which source you follow, organizations can have as few as 10-15 separate security solutions[7] or as many as 50 separate security vendors[8]. This grows complexity and data exponentially. Part of the answer may lie in transforming and streamlining network security operations – through potential consolidation, better integration, and unification.

Separation between networking and security. This is both an organizational issue as well as one of infrastructure. In the past, we would often see security teams owning one set of policies while the network team was in charge of implementingthem. Yet, there remained a wall between them and little collaboration.

There is power in breaking down the organizational silos that have traditionally separated network teams and their securityteam counterparts. Progress toward digital transformation means it's no longer effective to operate in separate silos. Today, En Pointe ITS is seeing greater efficiencies, greater collaboration, and progress on the security front after organizations' network/ security teams start to collaborate and begin to jointly own more integrated, network security solutions.

Mapping a course forward

The legwork performed on the business-side helps us develop a viable, working plan and transformational roadmap to followon the road to better security. This enables organizations to more successfully meet their network security needs – in both the short term and the long term.

> "Cybersecurity is not solely an IT issue. The most senior membersof a company's management team must engage and be at least conversant with this dynamic risk. In your organization, can the CEO, the CFO, or the GC answer the following three questions:
>
> - What are your company's principal cyber vulnerabilities?
> - What are your key strategies for mitigating those risks?
> - Are adequate resources being devoted to the task at hand?"[9]

Excerpt, 2017 Cyber Risk Report, Marsh & McLennan Companies

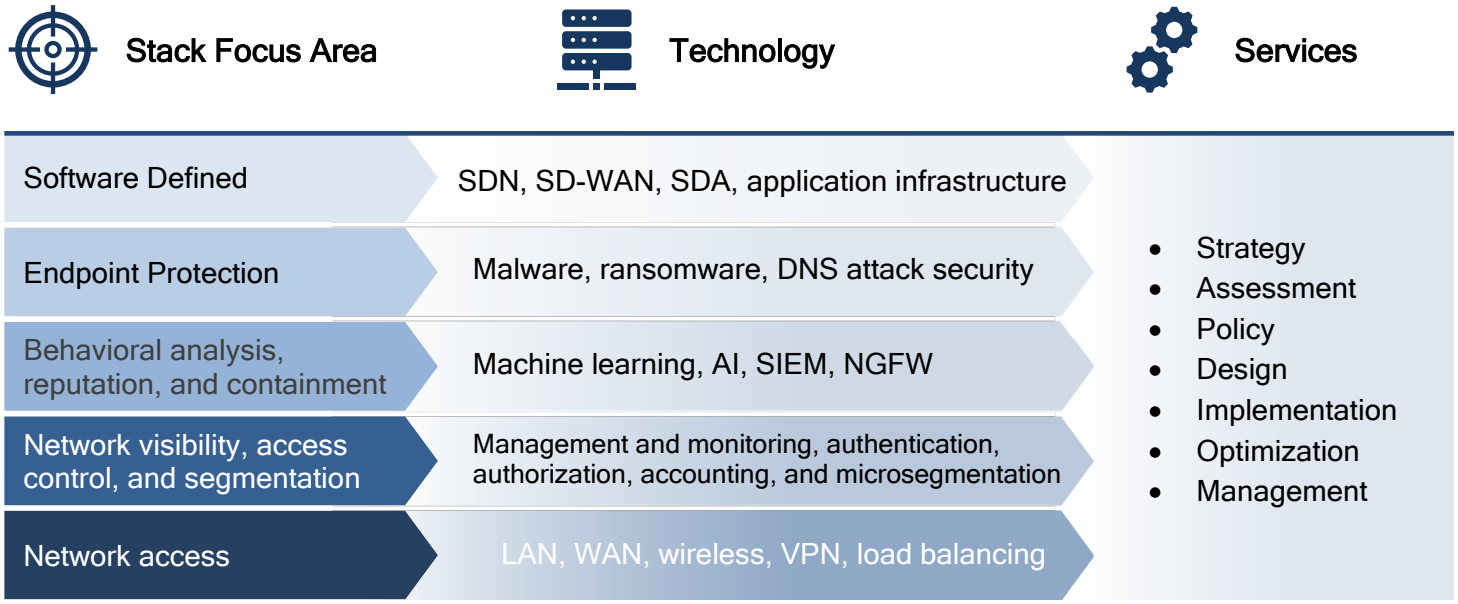
EN POINTE IT SOLUTIONS
Making Technology Work for You

Part 2: Assessing network security technologies

Once network security-related business drivers are clearly established and translated into technical requirements, this clears the way to focus more on network security technologies or solutions that best match an organization's requirements.

At En Pointe ITS, we work with organizations to effectively secure areas within what we call the "secure network solution stack." Figure 2 shows some of the solution stack's focus areas and their related technologies. It also describes the services – from strategy to implementation, optimization, and management – that En Pointe ITS is able to offer in order to meet organizations at their specific level of need.

Figure 2. En Pointe ITS services and secure network solution stack.



This section highlights the evolution of a few, key technologies and practices that have begun to gain the attention of organizations. These include:

- NAC
- Network segmentation
- Software-Defined Networking (SDN)
- AI and machine learning

The following table covers a few of the developments and advice for these areas.

Table 1. Technology highlights

Technology	Evolution & Recommendations
Network Access Control (NAC)	In the past, early solutions associated with NAC often would result in a negative impact on user productivity. In addition, traditional NAC solutions were very basic and inefficient. Today's NAC solutions, however, are changing at a pace the market demands in order to accommodate new requirements and regulations. In this area, it's important to maintain current systems according to best practices and accepted procedures. It's also important to keep pace with the latest developments. Deploying and managing NAC correctly is a unique technology which can require specialized skill sets. Here, it might make sense to consider engaging one of En Pointe ITS's NAC experts to help in the critical, early phase of NAC implementation. This is involved in defining initial requirements then translating those into the best, correlated design and approach.
Network segmentation	Early network segmentation efforts tended to involve a lot of manual work surrounding VLANs along with configuring and monitoring Layer 2/Layer 3 boundaries on the physical network. Modern network segmentation practices and technologies rely more on logical, dynamic groupings of different users with different access rights to company systems. When deployed correctly, these types of robust systems make it easier to automatically grant access to only those systems that are needed for different groups – from corporate executives to human resources and on down to guests and contractors who may access the network from their own, external devices. The level of granularity of network segmentation now available also allows organizations to deploy fine-grained microsegmentation of different groups and resources.
Software-Defined Networking (SDN)	SDN has become one of the latest terms to generate interest in the field of emerging, modern networks. This is for good reason as this area is poised for the most potential growth in future. There are many components in emerging SDN architectures. These will even include elements of logical network segmentation. Rather than define the various facets here, we'll focus instead on the general goals behind SDN: SDN is all about bringing greater automation, optimization, and efficiency to an organization's corporate network. This includes more efficiently deploying security policy on the network. If you have questions on how SDN architectures can better support your organization's security needs, consider getting input from an En Pointe ITS SDN expert.
AI and Machine Learning	AI and machine learning have already been mentioned earlier in this paper. While still in its infancy, this technology is already showing great promise at processing large volumes of security data logs or alerts and flagging those events that don't fit a predefined pattern.

EN POINTE IT SOLUTIONS
Making Technology Work for You

Part 3: How En Pointe ITS can help you win against cyberthreats

Remember when we mentioned winning against cyberthreats and bad actors? At En Pointe ITS, we believe the key to successful network security starts by helping clients identify their challenges and business drivers, then mapping a transformational path to successfully move forward.

Toward that end, we have been able to help many midrange and enterprise organizations succeed. Table 2 offers a few examples.

Table 2. Successes with the secure network solution stack.

Technology	Evolution	Recommendations
Public Utility Company	*SDN* *Network segmentation* *Network access*	Developed next-generation secure network fabric at new HQ
Multinational Conglomerate	*Behavioral analysis* *Network segmentation* *Network access*	Compliancy mandate for enhanced network visibility and segmentation
Large U.S. Bottler and Distributor	*SDN* *Network segmentation* *Network Access*	Complete infrastructure transformation involving the complete En Pointe ITS services stack
Large U.S. Bottler and Distributor	*Network segmentation* *Network access*	Displaced an incumbent infrastructure service provider and platform
National Grocery Chain	*Behavioral analysis* *Network access*	Enabled widespread business transformation through next-generation wireless/wired network access platforms
Energy Company	*Network segmentation* *Network access*	Took ownership of network refresh lifecycle
Large County Government	*Network segmentation* *Network access*	Partnered with OEM to deploy a service provider-grade network core for the 6th largest U.S. county

EN POINTE IT SOLUTIONS
Making Technology Work for You

Getting help and more information

You probably have questions of your own about network security. You may even need guidance in a specific area. We help businesses like yours define security-related gaps, alleviate emerging threats, and increase organizational defense against today's digital intruders.

We are always happy to speak with you, reach out to your representative at any time.

Your representative –

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at our website: www.enpointeits.com

1. "Setting the Cybersecurity Bar Higher – Announcing the Cisco 2018 Annual Cybersecurity Report," by John Stewart, Feb. 21, 2018, https:// blogs.cisco.com/security/cisco-2018-annual-cybersecurity-report.
2. "2018 Cyberthreat Defense Report," by CyberEdge Group, https://www.paloaltonetworks.com/resources/research/cdr.
3. "2018 Annual Cybersecurity Report," by Cisco Systems, Inc., https://www.cisco.com/c/en/us/products/security/security-reports.html.
4. "3 Top Cyber Experts Speaking Out," by Jeremy King, Jan. 10, 2018, CSO Online, https://www.csoonline.com/article/3245802/security/3-top- cyber-experts-speaking-out.html.
5. "Defenders Must Remediate 'Leak Paths,'" p. 34, Cisco 2018 Annual Cybersecurity Report.
6. Cisco 2018 Annual Cybersecurity Report, p. 49.
7. "What's Really Driving The Cyber-Security Workforce Shortage?" by Gabi Reish, May 16, 2018, Information Security Buzz, https://www.informationsecuritybuzz.com/articles/whats-really-driving-the-cyber-security-workforce-shortage/.
8. Cisco 2018 Annual Cybersecurity Report, p. 48.
9. "2017 Cyber Threats: A Perfect Storm About to Hit Europe?" by FireEye and Marsh & McLennan Companies, January 2017, Marsh McLennan Companies, https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Fireye%20Cyber%20Report-01-2017.pdf.

EN POINTE IT SOLUTIONS
Making Technology Work for You