KPMG

A 10-part framework for improving security in the modern enterprise

The network segmentation imperative

kpmg.com

Meet the author

Fredrik Lindstrom

Manager in KPMG's CIO Advisory practice.

Fredrik Lindstrom is a manager in KPMG's CIO Advisory practice. He has more than 15 years of experience in global technology consulting, leading information security and information technology projects with companies in a broad range of industries. Fredrik specializes in network architecture, network design, and security services for major companies.

Network segmentation: Why it is time to phase out outdated security approaches

Anchoring the defense

To defend his castle from plunderers and pillagers, a medieval king might have built a wall around the castle and a moat around the wall. It would have been a pretty effective approach, making it extremely difficult to get inside the castle.

The problems would have started if an extraordinarily innovative thief figured out a way through. Once that occurred, the castle became a sitting duck. The sneaky intruder had the keys to the kingdom—there was nothing to stop him from accessing every room, hallway, staircase, turret, tower and parapet in search of the best loot.

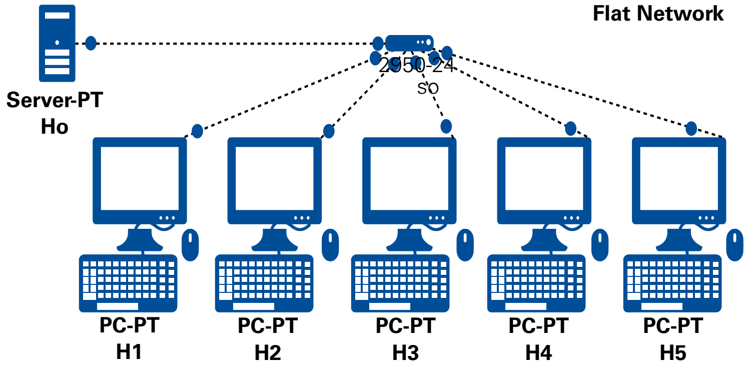
The "moat-around-the-wall-around-the-castle" defense can be likened to the traditional approach to computer network security, which centers on isolating external networks from internal networks with IP addresses and ports. This approach worked fairly well in the early days of the connected enterprise and against the initial wave of security threats. But it cannot effectively secure the complex, interconnected, digitized networks that power today's modern enterprises, nor can it defend against truly elite cyber attackers with a wave of new tricks at their disposal.

In this paper, we examine the realities of today's business and security environment that render old approaches to network security ineffective. Then we will make the case that **network segmentation**—splitting a network into subnetworks—is the most effective way to protect today's enterprises from cyber attack. We will also present a framework to simplify the work of implementing network segmentation, enabling organizations to increase security today and handle unknown and emerging threats tomorrow.

To understand the network segmentation imperative, we will first examine how traditional networks—called "flat networks"—work. These are the kind of networks found in many organizations across industries today.

Flat networks focus on providing reliable and fast connectivity for all devices on the network, meaning all devices have equal access to the network and all services and information that reside on it. Flat networks do not have internal control points limiting the flow of data on the network. Furthermore, the network provides no information on what is traversing the network, or what is connected, including devices under the control of a malicious actor or infected by malicious software.

There are two primary drivers catalyzing organizations to move away from flat networks.



Increased attack vectors

In today's digital world, most enterprise networks are not like isolated castles with a single gate at a single entryway. As organizations move to a more mobile workforce and are relocating IT services to the cloud, there is a blurring line between the enterprise network and the external network. There are more people and information moving in and out of the network at every second.

That means there is not just one gate to the castle, but many, which has increased the attack vector significantly. For example, cyber breaches can now occur not just through servers and ports, but through employee and third-party e-mails, devices and wireless connections.

More sophisticated attacks

As anyone can see if they read the headlines, there are a seemingly endless string of corporate cyber breaches occurring regularly—and there is no end in sight. In 2016 alone, hackers compromised 500 million accounts from a major e-mail provider, leaked 19,000 e-mails from U.S. political party officials, stole $81 million from a foreign bank, and even brought down major parts of the Internet.[1]

That is because every day, intruders are evolving their mission and their methods to evade old defenses. Once motivated mainly to prove their smarts to the world, today's bad actors are more commonly seeking financial gain. From the installation of ransomware, to the theft of sensitive information such as credit cards or social security numbers, to industrial espionage and sabotage, many network attacks are even backed by large crime organizations. These new bad actors, categorized as "advanced persistent threats" (APTs), are not satisfied simply by penetrating the network through an unsecured port on an external server. Like the sneaky thief pillaging every part of the castle, once APTs compromise one defense and get inside the network, they immediately move to access every system and piece of information they can—an action called "lateral movement."

[1] *Here's how cyber attacks get worse in 2017 (Venture Beat, December 11, 2016)*

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 653415

Why modern enterprises need network segmentation

As businesses become more digital and connected, and cyber attacks become more sophisticated and destructive, it is becoming increasingly clear that enterprises need a new approach to security.

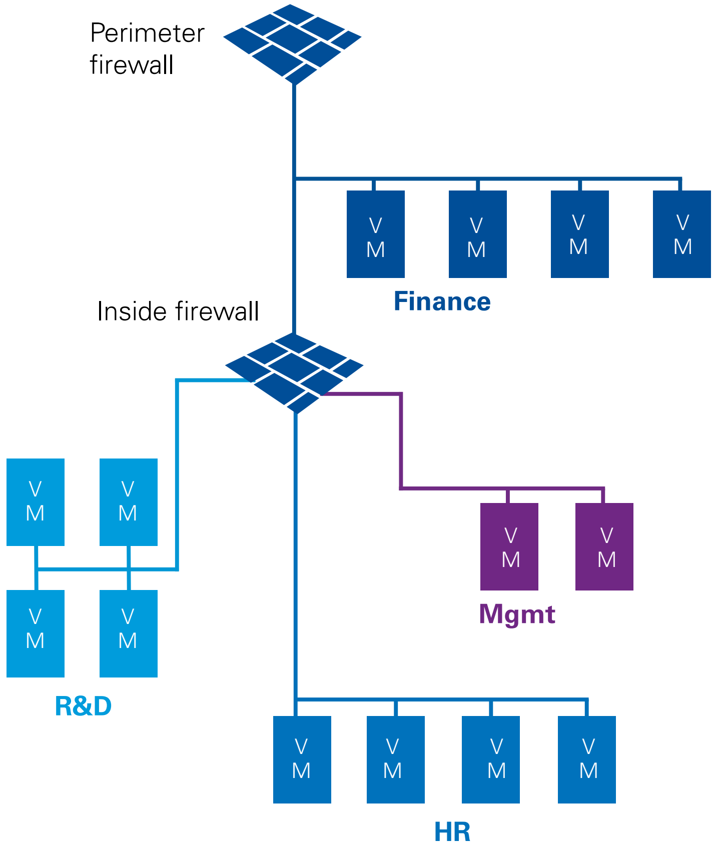
Enter network segmentation.
Network segmentation is one of the most powerful but underutilized security steps and a cornerstone of a successful information security program. It directly addresses the realities of today's threat landscape—that you cannot prevent a cyber breach, but you can isolate one.

Network segmentation focuses on separating parts of the network from one another with barriers or controls. In some cases, the segmentation occurs by function—for example, the finance system is segmented from the HR system. In other cases, the segmentation occurs by data classification—for example, sensitive or regulated data, such as personally identifiable information (PII), is isolated from the rest of the network.

By implementing network segmentation, modern enterprises can help address today's major cyber security challenges far better than with flat networks.

Proper network segmentation lays the groundwork for controls which protect against lateral movement on the network by malicious software and actors, preventing a potential infection or compromise from spreading across the network. It also allows for additional control points across the network, which significantly increases visibility and control over traffic on the network.

Since the vast majority of breaches are thought to occur toward the network periphery, it is clear that proper network segmentation should be the starting point for protecting modern enterprises. In fact, one of the most infamous corporate data breaches to date—the massive hack of a major retailer in 2015—was partially blamed on improper network segmentation. According to *Computerworld*, hackers broke into the retailer's network using login credentials stolen from a third-party contractor. They then leveraged that access to move through the network, eventually accessing the company's point-of-sale systems (POS), which handled sensitive consumer payment card data[2].



[2] *Target breach happened because of a basic network segmentation error (Computerworld, February 6, 2014)*

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 653415

A framework for implementing network segmentation

According to research commissioned by Avaya, although virtually all information technology professionals believe network segmentation is an essential security measure, less than one-quarter of organizations actually implement it. The biggest stumbling block? Complexity.

There is no getting around it: Implementing network segmentation is a vital but incredibly significant organizational effort. Businesses may need to add or replace hardware and software. They may need to integrate existing solutions in different and new ways. The people who manage the network may need to change, as may the processes governing the network. Even the users of the network may need to transform.

KPMG's CIO Advisory team understands the key components of a successful network segmentation program as the team has led complex network projects across the globe that improved enterprise security. **Below, we describe 10 components of KPMG's framework for network segmentation.** Businesses challenged to phase out outdated network infrastructure and update their network to handle the security challenges of today and tomorrow can use this framework as a basic guide to getting started on network segmentation.

1 Strategy

The plan of action

The network segmentation strategy is essentially the guiding document for the entire network segmentation effort. The strategy documents the organization's goals and defines the segmentation. For example, the network segmentation can start at the regional level (i.e., creating subnetworks based on geographical location), move down to the functional level (i.e., dividing HR systems from finance systems) and finally segment at the data level (i.e., keeping sensitive data types like intellectual property in well-protected zones).

2 Network architecture

The blueprint

The network architecture is the foundation of network segmentation or the implementation blueprint of the network segmentation strategy. The network architecture shows the number of segments and the number and type of control points between segments.

3 IT asset management

Defining who is on the network

To be able to validate and authorize devices for the network, a comprehensive IT asset management program must be in place. With IT asset management, the network segmentation effort can define the requirements for segmentation and network authorization levels based on the user, device and location.

4 Network access control, firewalls and intrusion prevention systems

The core security controls

A number of technology solutions work together to prevent malicious actors and malware from entering and moving through the segmented network. Intrusion prevention systems monitor and detect the presence of bad actors on the network. Firewalls control the traffic between segments based on user and device criteria. Finally, network access control limits admission to the network based on compliance to the organization's security policies. For example, it validates that only authorized users and devices—those which meet the network segment's security requirements—are allowed on that particular network segment.

5 Behavior-based protections

Dynamic, next-generation security controls

Leveraging advanced user analytics, today's organizations can make behavioral analysis a next-level control on the network, enabling more sophistication in how the network prevents, detects and responds to cyber threats. User analytics enable the organization to map out a baseline profile of each user—i.e., who they are, what device they use, where they connect from, and how they authenticate their identity. Once the profile is in place, the network can spot deviations from normal user behavior—even if it is within the allowed traffic—and dynamically adjust how they treat that user based on that change in behavior. For example, if a user who normally never transmits any data externally suddenly starts transmitting large amounts, it may be a valid action—or it may indicate a breach, malware infection or insider threat. Having detected this change in behavior, the network would automatically quarantine the potentially compromised user to allow for further investigation, prevent a possible breach in progress, and expedite any required remediation effort.

6 Network policy management tools

Automating security rule improvement

Network policy management tools continuously analyze the traffic on the network and compare it to the control rules. Based on this analysis, the tools suggest improvements to the rules to provide more granular filtering. This enables the migration to a strategically segmented network by first leveraging a relatively open rule base and then automatically defining more granular rules based on traffic flows.

7 Data center micro segmentation

Protecting the highest-priority systems

The security of data centers, which house the network's most critical systems, is a top priority for organizations. Traditionally, data centers are one segment of the larger network, protected by perimeter security technologies. Only authorized devices are allowed to access the data center. However, inventive cyber attackers have now demonstrated the ability to compromise even authorized devices. Once inside, they can often wreak havoc across the data center. Micro segmentation helps to prevent the spread of intrusions by dividing the data center into even smaller zones, enabling organizations to stop intruders from moving freely about the data center and contain breaches within the most important enterprise systems.

8 Data classification

Enabling data center micro segmentation

Network segmentation based on data classification, a common approach in the data center, requires a comprehensive data classification program. With the data classification program, it is possible to not only define micro segments, but also define different authorization levels based on the user, device, location and data being accessed.

9 Program management office (PMO) and architecture management office (AMO)

Keeping everything on track

A dedicated program management office (PMO) and an architecture management office (AMO) are critical pieces of a network segmentation project, in place to keep the project on track from the get-start-go. These functions provide governance over network architecture decisions throughout the course of the project. They develop and maintain the program charter, provide quality assurance, maintain schedule, budget and resources, and provide status reporting for stakeholders.

10 Organizational change management (OCM)

Getting the organization aligned

Implementing network segmentation is really about transforming the network from a flat network to a modern and secure network. As with any technology transformation, the people and processes connected to the network have to transform, too. These changes should be handled through an organizational change management (OCM) function, which drives the changes throughout the organization. The OCM function helps ensure end users are informed, engaged and able to make the required behavioral changes. It also develops strategies, plans and tactics to obtain key stakeholder buy-in, communicate effectively, mitigate stakeholder resistance, and train and educate impacted people.

[3] *End-to-end network segmentation research (Avaya, August 2016)*

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 653415

Case study:

Protecting a manufacturer's IP with network segmentation

The situation

A high-tech manufacturing company had a stitched-together network infrastructure due to organic growth and through acquisition over the past several decades. As such, the network had also been stitched together and did not provide the required segmentation to protect significant investments in research and development. This left the manufacturer's most valuable assets vulnerable to cyber attackers seeking to steal intellectual property. To make matters worse, this company operates in countries and locations that are not friendly to the United States where the company is headquartered.

The approach

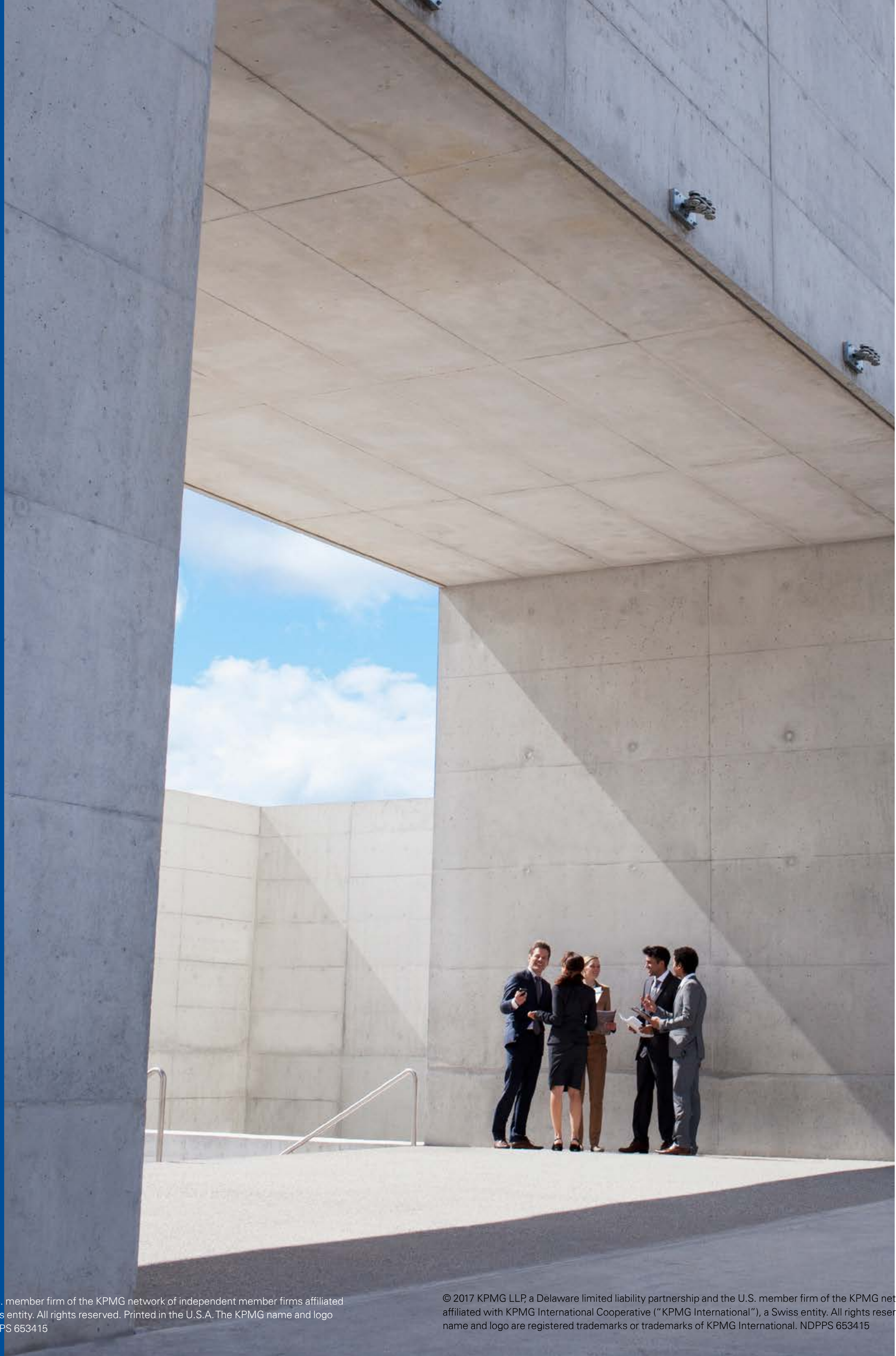
Assessment and goal-setting: Through IT infrastructure architecture review, requirements gathering, and several workgroup sessions, KPMG's CIO Advisory team helped the company assess security gaps in its IT infrastructure and develop specific goals to meet the needs of the company, as well as an approach and time line for a network transformation program.

Building the business case: KPMG worked with a core team of sponsors to develop the business case to gain approval and support from the manufacturer's board of directors to invest in a multiyear program to increase network security and operational efficiency with a network segmentation implementation as the key building block. A key component of this effort is to educate the stakeholders on the risks and mitigation strategies available.

Strategy and planning: KPMG led planning sessions to identify and document individual projects that would quickly deliver against the identified goals and requirements, including developing a network strategy, long-term road map, and prioritized implementation plan. Working with client leads and vendors, KPMG also guided the breakdown of the network transformation program into smaller projects and led development of charters for each project, including: project description; business and technical requirements; high-level and low-level design; cost estimations for hardware, software and resourcing; project plan and timeline; project interdependencies, assumptions and risks; implementation plans, and the required organizational changes to be successful with the program.

The outcome

Under the guidance of KPMG, the client was able to create a formal network transformation program, with the board of directors and business stakeholders aligned to the success of the program. The network transformation program was designed to help the manufacturer address network security deficiencies across its global network increase security, automation, and operational efficiency to meet the needs of the company today, and enable future business requirements with a more flexible, scalable, and secure IT Infrastructure.



Final thoughts

If your organization has not implemented network segmentation, now is the time to consider it.

Just as the smart king would never depend on a single gate to secure his kingdom, a smart business leader would never rely on a single control point to protect the organization's assets.

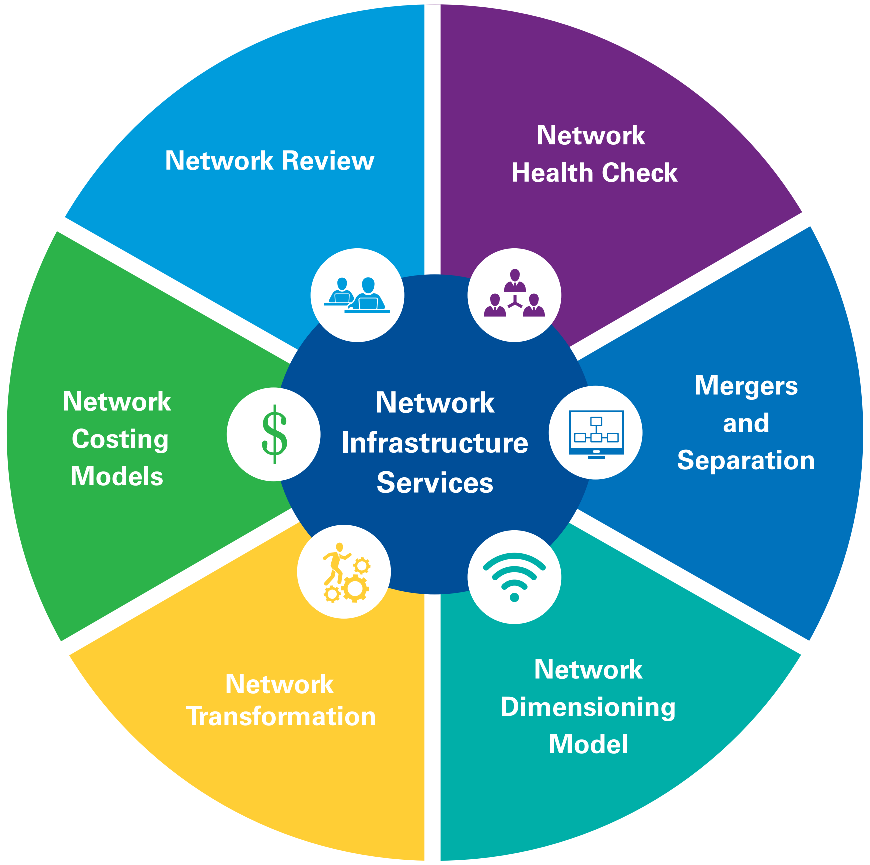
Network segmentation—which limits the damage of a breach—is arguably the leading defense against the latest, sophisticated security threats. As corporate hacks become more frequent and devastating, impacting large and small businesses in every industry, network segmentation has become an imperative for the modern enterprise.

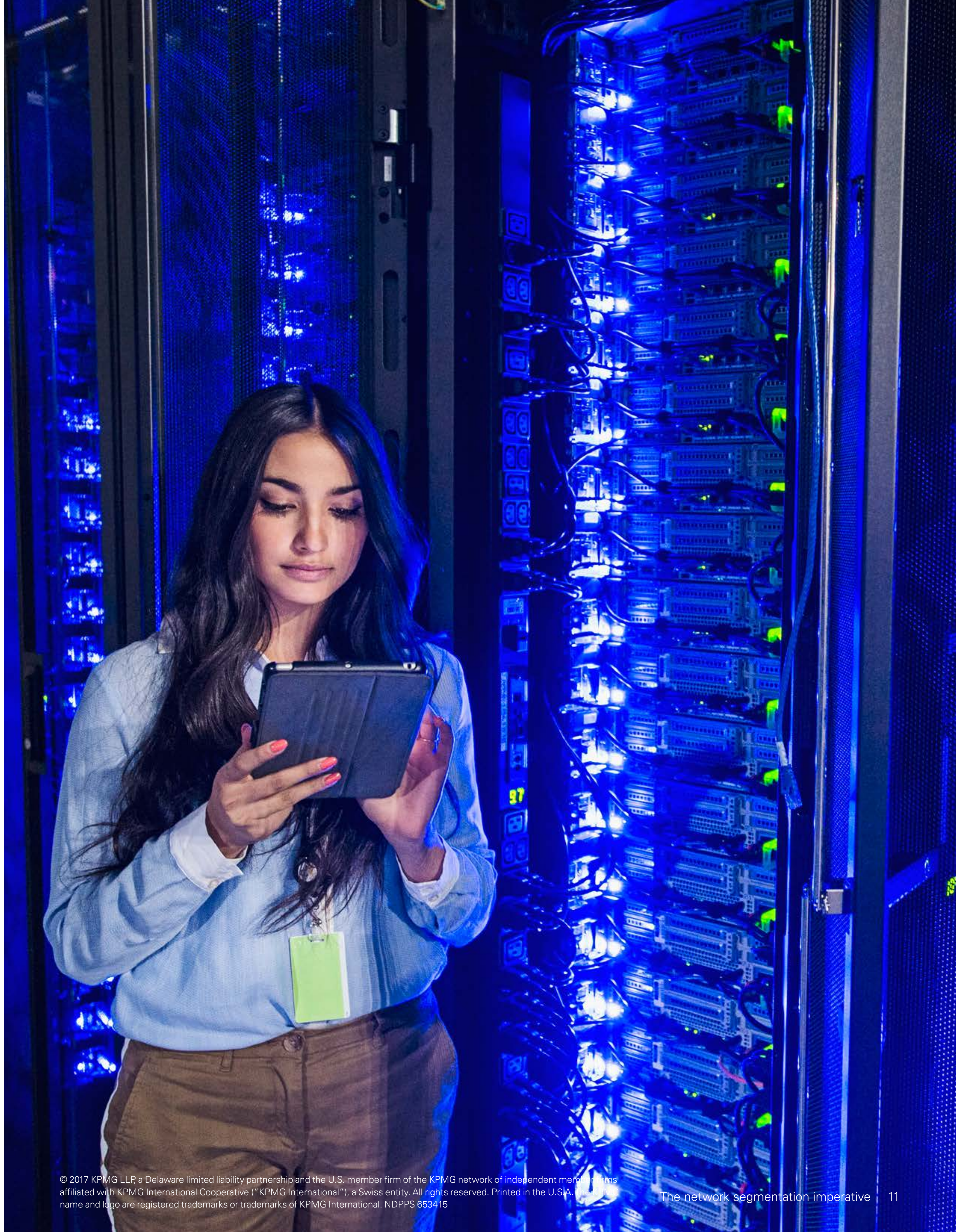
Effective network segmentation is a huge undertaking. But if you break it down to its basic pieces—the 10 components in the KPMG framework—it becomes significantly more manageable to implement proper network segmentation to better protect your enterprise.

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 653415

Need help with network segmentation?

KPMG's CIO Advisory team consists of network specialists with deep network knowledge in wired and wireless solutions, network service providers, and network security. Our experienced team has a tested track record and has having successfully assessed, designed and implemented network projects across the globe. As trusted and independent advisors who serve client interests rather than our own, we offer vendor- and technology-neutral advice about the evolution of more secure and modern enterprise networks.





© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 653415

Learn More

KPMG recognizes that today's CIOs face increasingly complex demands and challenges in becoming the strategic technology partner their businesses require.

KPMG's CIO Advisory practice helps CIOs, technology leaders and business executives harness technology disruption, more effectively manage technology resources to drive agile and improved business performance, enhance strategic position, and improve the strategic value of their technology investments.

If your IT organization is seeking ways to leverage technology as a source of innovation and competitive growth, KPMG member firms can help.

For more information on CIO Advisory's service and capabilities, please visit www.kpmg.com/us/CIOagenda and www.kpmg.com/us/IT

Contact us

Fredrik Lindstrom
Manager,
CIO Advisory
T: 214-840-4447
E: fredriklindstrom@kpmg.com

Timothy Williams
Managing Director,
CIO Advisory
T: 720-573-7071
E: timothywilliams@kpmg.com

Michael Dawson
Director,
CIO Advisory
T: 202-533-3096
E: michaeldawson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.