Definitive Guide™
to
Next-Generation Network Access Control

Fortifying Visibility, BYOD, and Control
with Continuous Monitoring and Mitigation

Steve Piper, CISSP

CONTRIBUTIONS BY:
Scott Gordon, CISSP

About ForeScout Technologies

ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyberattacks. The company's CounterACT platform dynamically identifies and assesses all network users, endpoints, and applications to provide complete visibility, intelligence, and policy-based mitigation of security issues. ForeScout's open ControlFabric technology allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com.

Definitive Guide™
to
Next-Generation Network Access Control

Steve Piper, CISSP
Contributions by Scott Gordon, CISSP

CYBEREDGE
GROUP

Definitive Guide™ to Next-Generation Network Access Control

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

ISBN: 978-0-9888233-4-1 (paperback); ISBN: 978-0-9888233-5-8 (eBook)
Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Production Coordinator: Valerie Lowery
Contributing Author: Scott Gordon (CISSP), Chief Marketing Officer, ForeScout Technologies
Technical Advisor: Toni Buhrke (CISSP), Systems Engineering Manager, ForeScout Technologies

Table of Contents

Foreword

"Control all access to network assets." Seems obvious, right? Not the most profound tenet of information security. Not exciting. Ranks up there with "maintain patches and anti-virus updates, encrypt sensitive data, and don't forget to back up regularly." But there is more to network access control, commonly referred to as NAC, than meets the eye. NAC has risen like a phoenix from the depths of "Gartner's Hype Cycle," and in its latest incarnation, next-gen NAC has become an infosec game changer — offering tremendous value and delivering advantages that can be applied across a variety of security requirements, policies, and controls. Not only can next-gen NAC optimize resources, but it can also extract better ROI from your security investments.

Now that I have your attention… you may ask, as many others have, "What changed with NAC since a decade or even five years ago? Did I miss something?" Infosec professionals are living in challenging times and it's pretty daunting. Network boundaries are growing even more porous and are extended by mobile apps and cloud environments. Operational dynamics are becoming more complex with global networks, virtualization, and software-defined infrastructure. The days of being confident that only known, fully managed, secure or even corporate-owned devices are on your network are numbered, if not already past. IT consumerization has made anytime, anywhere, any means computing the new normal. Need I mention the more intense, sophisticated, organized, targeted, subversive, and rapidly evolving threat landscape?

What if you could see all users, devices, and applications attempting to access or operate on your network — employee and guest, remote and local, wired and wireless, virtual and embedded, PC and mobile, corporate and personal, authorized and unsanctioned? What if you could easily set policies to allow the wanted, take action against the unwanted, and fix security gaps – with little or no IT intervention? What if you could reduce violations and exposures while preserving user experience and influencing desired behavior?

Next-gen NAC is not a panacea, but it provides the real-time visibility, control, and mitigation needed to resolve numerous next-gen IT challenges. It answers the questions of how to gain greater operational intelligence, reduce risk, efficiently preempt threats, and contain exposures — all without making changes to your network infrastructure or security processes.

Similar to the way other IT tools are procured, next-gen NAC solutions are usually acquired to solve specific problems. Some people want to improve visibility and address rogue devices and applications. Others need to manage guests and enable bring-your-own-device (BYOD) programs. Still others aim to advance endpoint compliance and minimize malware outbreaks. While these are typical problems, next-gen NAC, as the foundation for pervasive network security, offers so much more.

As next-gen NAC dynamically discovers, classifies, and profiles users, devices, and applications — pre- and post-network admission — it can share this intelligence with other network, security, and management systems, providing them greater operational context. Next-gen NAC can also receive information from external systems and invoke network enforcement or remediation actions on endpoints or trigger actions on other systems. These capabilities open the door to a wealth of applications. I am amazed at the ingenuity of our customers who apply ForeScout CounterACT to accomplish tasks we wouldn't have imagined. By leveraging this bidirectional interoperability, next-gen NAC becomes the central network security control platform for many IT organizations.

I am excited to contribute to this book, which serves as a pragmatic resource that demystifies next-gen NAC and examines key features, technologies, and applications. It provides a concise overview of the inner workings of NAC and offers use case sections that best illustrate pertinent purchase drivers, functionality, and advanced capabilities. Furthermore, it shares real-world insight towards successfully implementing a next-gen NAC platform and explores how NAC can be applied to achieve continuous monitoring and mitigation.

So put this Definitive Guide to good use and get a knack for next-gen NAC.

Scott Gordon, CISSP
Chief Marketing Officer, ForeScout Technologies, Inc.

Introduction

Defending our IT infrastructure from cyberthreats is a never-ending battle. With so much emphasis placed on blocking threats, we sometimes forget that another effective and necessary way to manage security risks is to eliminate rogue users, devices, and applications and maintain system defenses and integrity — thus, reducing our networks' attack surface – the available security exposures that can be exploited.

When introduced a decade ago, network access control (NAC) took the security market by storm. Security pundits were excited to have, for the first time, the means to limit network access to "known, managed, and healthy" devices. But these early systems, which focused on device authentication, were cumbersome and costly to fully implement and often disrupted users. They failed to live up to expectations.

Today, broader adoption of wireless, mobile devices, and bring-your-own-device (BYOD) policies has reinvigorated NAC interest and adoption. No longer limited to managed devices and restrictive "grant or deny" network access policies, next-generation NAC offers real-time network visibility, a more accommodating architecture, limitless policy options, and automated endpoint remediation.

If you think you know NAC, think again. NAC has risen to new heights and has now become one of the fastest-growing segments of the information security industry. Want to know why? If so, this is one book you can't afford to miss.

Chapters at a Glance

Chapter 1, "Fundamentals of Network Access Control," sets the groundwork for understanding how NAC works, how it has evolved, and how organizations are leveraging the latest innovations in NAC technology.

Chapter 2, "Exploring Next-Gen NAC Technology," drills into the key capabilities of next-gen NAC solutions and compares them to outdated legacy NAC functions.

Chapter 3, "Achieving Endpoint Visibility and Security," describes methods for discovering and classifying devices, identifying endpoint exposures, and closing security gaps.

Chapter 4, "Enabling BYOD for Employees, Guests, and Contractors," details ways that next-gen NAC can help organizations enable BYOD by role, device, and security requirement.

Chapter 5, "Mitigating Advanced Threats," describes how next-gen NAC can augment your controls to discover issues and coordinate defenses to preempt and contain cyberthreats.

Chapter 6, "Aiding Compliance with Continuous Monitoring and Mitigation," discusses the role NAC plays within standard compliance frameworks and new security operational models that enhance and automate controls.

Chapter 7, "Getting Started," outlines key steps for getting your next-gen NAC selected, up and running, and optimized.

Glossary provides handy definitions for key terminology (appearing in *italics*) used throughout this book.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

Fundamentals of Network Access Control

In this chapter

- Define network access control (NAC) and compare it with next-gen NAC
- Review the key components of next-gen NAC solutions and understand how they work
- Preview four common use cases for adopting next-gen NAC solutions

In today's dynamic and complex computing environment, IT must be an "enabler" to the business, rather than an "inhibitor." Employees and contractors require instant access to company data using both company-supplied and personally owned computing devices, while IT must ensure the confidentiality, integrity, and availability of that data.

Until recently, regulating network access to approved users, devices, and applications was a daunting task. But with innovations culminating in *next-generation NAC*, security practitioners not only have the tools necessary to control network access, but also new capabilities for achieving unprecedented endpoint visibility, detecting exposures, and mitigating threats across a local or global enterprise.

This book is dedicated to next-gen NAC, one of the hottest and fastest-growing IT security technologies on the market today. In the chapters ahead, I describe key capabilities of next-gen NAC solutions, detail four common use cases, and explain how to get the most out of your investment.

But before I get too far ahead of myself, let's first define NAC, follow its evolution to next-gen NAC, understand how leading next-gen NAC solutions work, and briefly explore four common next-gen NAC use cases.

Why NAC, Why Now?

Network access control (NAC) is a network security solution designed to grant, limit, or deny access to network resources through policies defining acceptable or unacceptable users, devices, and application properties. *Pre-connect NAC* (also known as *comply to connect*) takes a "guilty until proven innocent" approach by quarantining devices on a separate VLAN until they are deemed compliant and authorized. *Post-connect* NAC takes an "innocent until proven guilty" approach by granting network access while readily applying policy to take action if a device is or becomes non-compliant or unauthorized.

Many organizations first contemplate pre-connect NAC for wireless access points frequented by guests in conference rooms and lobbies. But as organizations consider broader application in their wired and more distributed environments, post-connect NAC offers a more flexible, easier-to-manage, and less-intrusive approach.

Before considering pre-connect NAC, I recommend that you examine your key use cases and security policies to gauge potential user and device impact, agent management concerns, and infrastructure support requirements. Based on your findings, you may need need a combination of pre- and post-connect NAC deployment.

Regardless of how it is deployed, NAC has emerged as one of the "must-have" information security technologies on the market, with deployments forecasted by IT research firm, Gartner, to increase 45 percent in 2014 and ranked among the five hottest security defenses by 451 Research.

There are three primary reasons why NAC adoption is skyrocketing: infrastructure complexity that introduces control and endpoint visibility gaps; the implementation of *bring-your-own-device* (BYOD) policies; and the need to mitigate advanced threats. The latter is accomplished by reducing your

network's *attack surface* and by detecting and remediating threats that bypass traditional signature-based perimeter defenses. NAC's resurgence is also fueled by major technology advancements, which have culminated in what's now called "next-gen NAC."

What is next-gen NAC?

Next-gen NAC extends the capabilities of (now) legacy NAC products by incorporating a multi-dimensional control platform that offers unprecedented network and security infrastructure interoperability. As depicted in Figure 1-1, next-gen NAC offers three main functions:

- ☑ **Network visibility.** Next-gen NAC affords users unprecedented, real-time network asset intelligence. It classifies all network devices — PCs, laptops, servers, virtual machines, mobile devices, and network infrastructure — and provides device type, user, location, application, and a range of other details.
- ☑ **Granular policies.** Next-gen NAC users can configure anything from broad to highly granular policies based on the specific needs of the organization. Policies can be applied to users (and groups of users), devices (and categories of devices), and application properties. Policies can be set to monitor-only, or to take actions against devices — pre- and/or post-admission until the device has been deemed authorized and compliant per the policy.
- ☑ **Mitigation.** Next-gen NAC users have a myriad of ways to reduce the risk created by unauthorized and/or non-compliant devices. Beyond grant, limit, and deny network access alternatives, next-gen NAC solutions can remediate endpoint issues with little or no human intervention.

Available as physical and virtual appliances, today's next-gen NAC solutions offer agentless inspection and authentication approaches along with broader device classification, profiling, and mitigation capabilities. Next-gen NAC vendors provide different wireless and mobile device security capabilities, including integration with mobile device management (MDM) tools — enabling organizations to support the entire mobile

device lifecycle, including: provisioning, securing, monitoring, and managing company-owned and personal mobile devices. Next-gen NAC solutions also offer integrations with other network and management applications in order to facilitate detection of threats and to remediate or mitigate exposures.

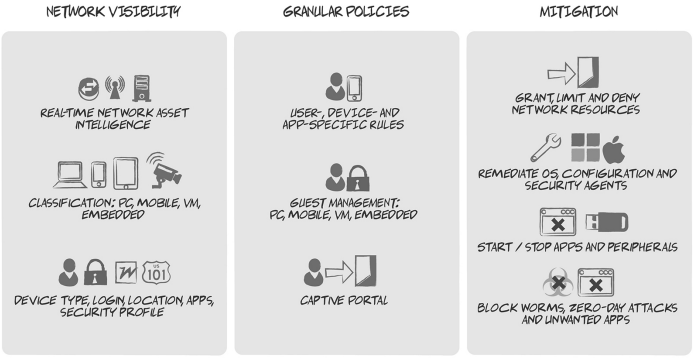

Figure 1-1: Key functions of next-gen NAC solutions

As you'll soon discover, there are now dozens of ways organizations can leverage NAC. However, many IT organizations have explicit requirements for basic device authentication and port-based access control. You can rest assured that next-gen NAC can satisfy these requirements.

Answering market trends

The following trends are changing the way employees use technology and how enterprises secure their IT infrastructure:

- ☑ Explosion of network-enabled mobile devices
- ☑ Consumerization of IT and user demands for IT to support BYOD policies
- ☑ Virtualization and cloud computing environments that bring new risks and uncertainties
- ☑ Cyberthreats that are growing in number, sophistication, and velocity, entering via social engineering techniques but succeeding by exploiting poorly managed systems
- ☑ Increased demands imposed by regulatory compliance mandates for continuous monitoring and mitigation

Common NAC misconceptions

A number of misconceptions about NAC have been fueled by legacy NAC offerings. Let's clear up a few of them now:

Myth #1: NAC adoption is waning. NAC is alive and well. In 2013, Gartner placed NAC in the "Slope of Enlightenment" (adoption) phase of its Hype Cycle for Infrastructure Protection report. In 2014, security research firm, CyberEdge Group, cited NAC adoption by organizations with 500 or more employees at 64 percent in its Cyberthreat Defense Report.

Myth #2: You must re-architect your infrastructure. Actually, upgrading and/or reconfiguring your network infrastructure to support next-gen NAC deployment is more the exception than the rule. Next-gen NAC offers extensive network and security infrastructure support and deployment options negating the need to re-architect one's infrastructure.

Myth #3: NAC requires endpoint agents. Although some vendors require agents, other leading NAC vendors do not require client software. Many offer non-persistent agents that terminate on reboot.

Myth #4: NAC takes months to deploy. Today's next-gen NAC solutions can be fully deployed in a matter of days or weeks — even across distributed environments. Long gone are the days when the entire infrastructure had to be upgraded or reconfigured to support deployment.

Myth #5: NAC requires 802.1X. As you will read in this book, while the 802.1X protocol is an authentication standard often associated with NAC, it is not a required approach to achieve next-gen NAC capabilities.

Myth #6: NAC is built into my network infrastructure. NAC capabilities are not built into all network devices. And when they are, those capabilities are quite limited and pale in comparison to the functionality found in modern day NAC solutions.

Myth #7: NAC appliances are costly for expansive networks. Unlike legacy NAC solutions, next-gen NAC appliances don't require expensive infrastructure upgrades, a SPAN port to operate, or deploying an appliance at each network segment – ensuring a low cost of ownership.

Myth #8: NAC is unnecessary in virtual and cloud environments. NAC enhances visibility and control to handle the dynamics, complexities, and compliance issues introduced by virtual and cloud environments.

NAC is poised to help organizations address these challenging IT market trends and is widely recognized as a core security platform. In a 2014 Cyberthreat Defense Report that surveyed more than 750 IT security practitioners across North America and Europe, key findings include:

- ☑ Of 21 cyberthreat defense technologies listed, NAC is perceived as most effective at mitigating cyberthreats.
- ☑ NAC is the most commonly used technology to identity security misconfigurations within endpoint devices.
- ☑ NAC is the most commonly used technology to identify vulnerabilities and security misconfigurations within transient laptops and mobile devices.

ON THE WEB

To download a copy of the 2014 Cyberthreat Defense Report, connect to www.cyber-edge.com/2014-CDR.

How it Works

Although multiple options exist for deploying next-gen NAC appliances (physical or virtual), they are typically installed *out-of-band* (rather than inline) by connecting to the mirror (or SPAN) ports of your core network switches in order to gain seemless visibility to users and devices (see Figure 1-2).

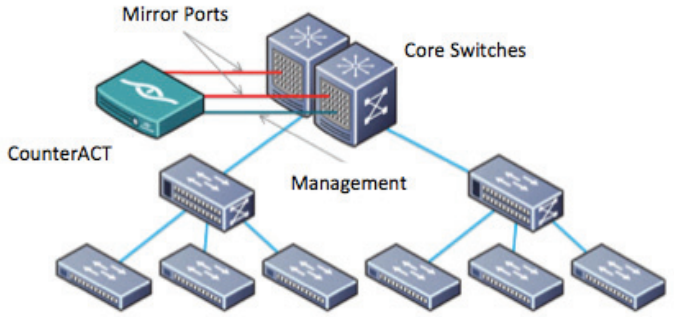

Figure 1-2: Typical next-gen NAC deployment

DON'T FORGET

Deploying a next-gen NAC solution is different than configuring basic 802.1X–based access control, which, as an authentication protocol, provides a fraction of the benefits of a full-fledged NAC solution. (See the "Understanding the limitations of 802.1X" sidebar for more information.)

With your next-gen NAC appliances in place, there are several other considerations when deploying a next-gen NAC solution. The following sections provide insight.

Understanding the limitations of 802.1X

802.1X is a standard that provides a pre-connect NAC mechanism to authenticate devices or users before network resources are provisioned. The 802.1X components include: a supplicant (agent software), an authenticator/network access server (NAS), an authentication server (RADIUS), and optional directory.

The supplicant communicates at Layer-2 from the device to NAS, which then encapsulates and forwards connection requests to the authentication server, which accepts or denies access. The advantages of 802.1X are that it is based on standards, is supported by most NAS vendors, and supplicants ship in many devices.

However, there are several distinct disadvantages to 802.1X. One challenge is taking on the unique supplicant configuration management required across the spectrum of device types. Other implementation considerations include certificate management requirements, client deployment efforts, managing non-802.1X device exceptions, and resolving directory authentication concerns. 802.1X network configurations also require authentication timers, failure backup configuration, RADIUS management, and directory replication. Also, 802.1X excludes endpoint classification and security compliance assessment, and it does not account for guest devices.

In summary, all 802.1X devices must be known, managed, configured, and have credentials to connect, resulting in lots of moving parts and significant network reconfiguration.

Infrastructure interoperability

Leading next-gen NAC solutions are designed to interoperate with heterogeneous and distributed computing environments, including the following:

- ☑ **Network devices** – Switches, routers, firewalls, VPN concentrators, wireless access points, printers
- ☑ **Network services** – Active Directory, LDAP, DNS, DHCP, RADIUS
- ☑ **Endpoints** – Windows, Mac, Linux/UNIX, mobile devices, and virtual devices
- ☑ **Endpoint management** – Patch and system management, mobile device management (MDM)
- ☑ **Endpoint protection**– Anti-virus, data leakage, host IPS, encryption

- ☑ **Security Management** – Security information and event management (SIEM), vulnerability assessment, IDS/IPS, advanced threat detection

Be wary of NAC solutions from network infrastructure providers as their interoperability depth and breadth with third-party platforms may be limited.

Authentication and authorization

Next-gen NAC enforces role-based access policies, ensuring that only the right people with the right devices gain access to the right network resources. Most next-gen NAC offerings support standards-based authentication and directories, such as Active Directory, LDAP, Oracle, and RADIUS.

Endpoint discovery, classification, and profiling

Unbeknownst to many next-gen NAC buyers is the rich endpoint intelligence derived from the solution once in production. As endpoint devices of all types connect to wired and wireless networks, next-gen NAC appliances discover them, classify them, and profile them against dozens of attributes, including unpatched vulnerabilities, unsanctioned applications, outdated anti-virus signatures, and other security risks, including the identification of unknown, rogue devices.

Monitoring and mitigation

Today's next-gen NAC solutions afford its users flexible policy enforcement options. Examples include:

- ☑ **Alert and inform** – Open trouble ticket, send email, hijack HTTP browser, trigger SNMP traps or syslog messages, update console data and self remediate
- ☑ **Limit access** – Reassign the device to a VLAN with restricted access, DNS hijack (captive portal), move the device to a guest network, and update access control lists (ACLs) on network switches, firewalls, and routers

- ☑ **Move and disable** – Reassign a device to a quarantine VLAN, block access with 802.1X, turn off a physical switch port, block Wi-Fi, intercept network traffic communications, stop application processes, and disable USB devices

Endpoint remediation

When a device connects to or is on the network and is flagged as non-compliant — say, it's missing a critical Windows patch — the next-gen NAC solution can be configured to facilitate device remediation in three ways:

- ☑ **Self-remediation** – The user is informed of the security issue and presented with instructions on how to self-remediate
- ☑ **NAC-instigated remediation** – The next-gen NAC solution executes a script to install the patch
- ☑ **Third-party remediation** – The next-gen NAC solution sends a request to an external system, such as Microsoft SCCM, to deploy the missing patch

Common Use Cases

NAC technology has evolved considerably over the past decade — so much so that there are now dozens of ways organizations can leverage NAC. Don't worry. I'll spare you the obligatory "Swiss army knife" analogy. Rather, I'll simplify the use of next-gen NAC technology into the following four core use cases:

Achieving endpoint visibility and security

As you'll learn in Chapter 3, next-gen NAC yields unprecedented endpoint visibility. The solution is ideal for identifying endpoint exposures and closing endpoint security gaps — through the next-gen NAC appliances themselves and by coordinating with third-party security systems.

Regulating access and enabling BYOD

NAC, as the name suggests, clearly is used to ensure that devices are secure, as per policy, before accessing network resources. By enabling real-time endpoint visibility and control, security practitioners can rapidly implement BYOD policies for all types of users. Chapter 4 explores how next-gen NAC can support even the most liberal BYOD policies.

Mitigating advanced threats

Innovative next-gen NAC solutions not only help organizations mitigate the risk of advanced threats by reducing the network's attack surface, but also by monitoring device activity and by integrating with advanced threat detection products, as you'll discover in Chapter 5.

Aiding compliance with continuous monitoring and mitigation

Maintaining adherence to industry and regulatory security standards is never an easy task. But with advancements in *continuous monitoring and mitigation* (CMM) fueled by next-gen NAC, as discussed in Chapter 6, organizations gain new methods to meet their compliance obligations while increasing security and reducing risk.

Now that you've grasped the fundamentals of network access control, the next chapter explores the standard and advanced capabilities of today's leading next-gen NAC solutions.

Chapter 2

Exploring Next-Gen NAC Technology

In this chapter

- Review the standard features found in today's NAC platforms
- Discover advanced features found in next-gen NAC

The purpose of this chapter is to explore the key capabilities of next-gen NAC solutions and contrast them against those found in basic NAC offerings, as depicted in Table 2-1.

Key Capabilities	*Basic NAC*	*Next-Gen NAC*
Policy Engine	Basic	Advanced
Third-party interoperability	✓	Advanced
Authentication	✓	✓
Network enforcement	✓	Advanced
Guest networking	✓	✓
Visualization and reporting	✓	✓
Agentless operation	✗	✓
Endpoint compliance	✗	✓
Guest management	✗	✓
Automated remediation	✗	✓
Advanced threat mitigation	✗	✓

Table 2-1: Comparison of legacy and next-gen NAC capabilities

Standard NAC Features

Let's begin our exploration into modern NAC functionality by reviewing standard features found in virtually all NAC solutions today.

The features in this section are found in all NAC solutions. If you feel you're already grounded in the basics of NAC technology, then skip ahead to the "Advanced Next-Gen NAC Capabilities" section later in this chapter.

Device discovery

Unlike first-generation NAC offerings that required endpoints to be managed and running NAC client software, most modern NAC solutions use multi-factor active and passive monitoring techniques to detect devices as they enter the network and to manage them post admission.

Device authentication

NAC solutions support standards-based authentication services and directories. Regardless of how a user or device authenticates, the moment his or her device connects, it should be instantly profiled and assessed against the NAC policy associated with that network segment or user role for provisioning.

Whereas next-gen NAC incorporates additional system, network and external sources to enhance properties that ensure a complete risk profile is included in the policy decision – pre- or post-admission (see next section).

Basic policy engine

At the heart of any NAC solution is its policy engine. This is where NAC administrators decide which devices with what appropriate level of security protection (e.g., active personal firewall, current anti-virus, necessary patches, encryption enabled) and other attributes (e.g., virtual machine, mobile, laptop) belonging to which users can connect to which network resources. Better NAC solutions offer policy wizards with built-in templates (see Figure 2-1) to make constructing and tuning NAC policies quick and easy.

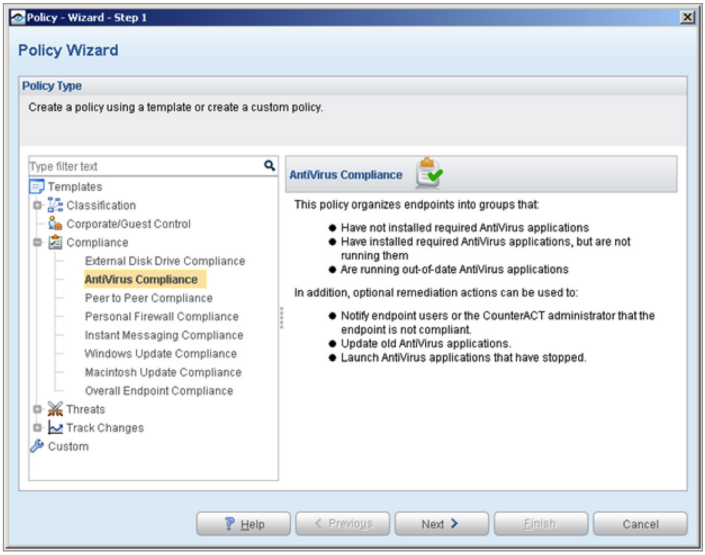

Figure 2-1: Sample next-gen NAC policy wizard

Network enforcement

NAC offerings provide pre-connect and/or post-connect NAC network enforcement options, as briefly described in Chapter 1. In a post-connect deployment, non-compliant and unauthorized device connections can be reassigned (quarantined) to a VLAN with restricted access or simply terminated at the switch. In a pre-connect deployment, all devices connections begin in a quarantined VLAN and are moved into production once they have been assessed for compliance and authorization.

Guest networking

NAC solutions are ideal for identifying and registering guest devices as they connect to the network, wired or wirelessly. Guests can be transitioned to a VLAN configured only for Internet access, or they can be relocated to a captive portal where they are given the opportunity to authenticate (if provided with appropriate credentials) or become authorized to gain limited network access.

Endpoint compliance

Endpoint compliance comprises the required system configuration, applications, and security posture of a device depending on user role, device, and risk. Security-conscious enterprises often develop endpoint compliance policies, but few have controls to effectively enforce them. NAC helps to fill this void by monitoring endpoints for the presence of:

- ☑ Active, up-to-date security software and services
- ☑ Unauthorized applications
- ☑ Operating system patches

Visualization and reporting

The best NAC solutions offer comprehensive and customizable dashboards and maps with intuitive visualizations (see Figure 2-2) that make it easy to view NAC policy compliance across the enterprise and on any given network segment. Users can drill down from any dashboard or map element to obtain more details or investigate specific areas of concern.

Better NAC solutions come equipped with a library of report templates and data extraction options that facilitate operational, audit, and compliance reporting.

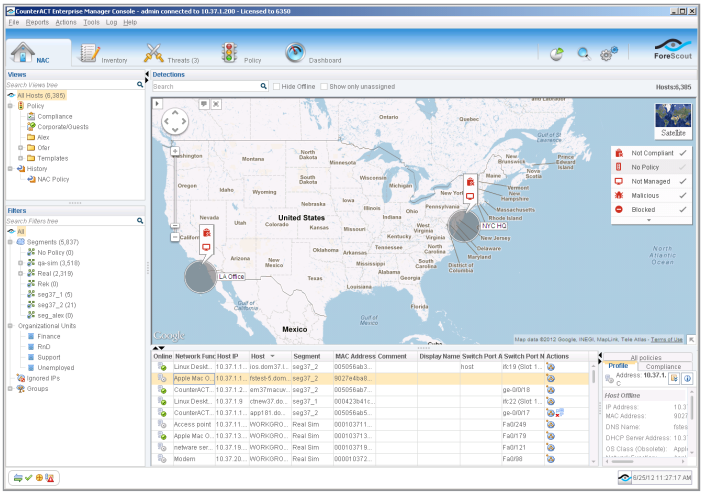

Figure 2-2: Sample next-gen NAC dashboard visualization

Basic integration

Integration with your existing IT infrastructure is generally limited with basic NAC offerings. All modern NAC systems can integrate with network infrastructure devices and can leverage directory services such as Active Directory. Like other security solutions, NAC can export log data to SIEM platforms and send messages to trouble ticket applications. Depending on the NAC solution, infrastructure integration may be limited. You'll need a next-gen NAC solution to reap the full benefits of more advanced NAC integration, as you'll discover at the end of the next section.

Advanced Next-Gen NAC Capabilities

Now that we've covered key features shared with basic NAC products, let's shift into high gear by discussing advanced capabilities only found in modern, best-of-breed next-gen NAC solutions.

Unobtrusive, flexible deployment

As I mentioned in Chapter 1, one of the most common misconceptions about NAC is that it requires infrastructure upgrades and network re-architecting to successfully deploy. Although this was certainly true with legacy NAC offerings, this is no longer the case with next-gen NAC.

Next-gen NAC solutions can be installed with existing equipment and with few, if any, changes to your network infrastructure. NAC appliances can be deployed centrally or distributed throughout a network to support the largest of enterprises with the most complex network architecture.

As you embark on your NAC project, capture your infrastructure details to determine key component integration requirements and estimated concurrent devices to manage by subnetwork. Select a vendor that offers broad infrastructure support and multiple appliance models to choose from to accommodate your environment.

Enterprise-class scalability

The scalability of a security solution is just as important as its effectiveness. Today, it's not uncommon for geographically dispersed enterprises to experience a great deal of unplanned growth. Your next-gen NAC deployment should easily expand to accommodate new network segments and/or endpoints.

For networks that require a higher level of continuity, next-gen NAC appliances can be configured to support an active/passive high-availability (HA) design. To address disaster recovery concerns, cold spare appliances should be available for deployment.

Agentless operation

A key differentiator of next-gen NAC solutions is the ability to operate without agents in order to conduct more extensive device inspection, authentication, and compliance assessment. An agentless approach expedites deployments, lowers initial deployment cost, and reduces on-going management burden for your NAC investment. It also simplifies supporting the multitude of devices connecting to your network, including BYOD devices and specialized equipment.

In some instances, agents facilitate communications or enable additional controls for managed devices — although added control is usually offset by operational impact and cost. When NAC agents are required, it's best to know what devices a vendor's agent will support and to select a NAC solution that offers both persistent and non-persistent agents.

Advanced policy engine

Policy engines found in next-gen NAC solutions offer high-speed processing of both synchronous and asynchronous data obtained from network, device, and application sources, as well as automated resolution of conflicting network, device and application properties. They cross-correlate this data to determine accurate classification, authentication, profile, and state change details.

Next-gen NAC policy engines also analyze data against pre-defined and user-defined policies that result in device classifications and triggered actions. Policies should be agile

enough to accommodate all device types, new data sources, new actions, and a wide range of response options. Next-gen NAC solutions also permit the means to take ad hoc actions on an endpoint without having to create a policy to address urgent situations.

Extensive network visibility

Today's next-gen NAC solutions provide real-time, multidimensional network visibility, allowing you to track and control users, devices, applications, services, processes, ports, external devices, and more. The value of this rich network asset intelligence extends beyond NAC policy, as it can be leveraged by other IT departments (e.g., help desk, network, security and operations) and can provide greater context for the controls within other network and security tools (described in chapters 3-6).

Examples of host data values aggregated and recorded by next-gen NAC solutions include:

- ☑ **Physical layer:** Physical switch, VLAN, switch port, 802.1X, number of devices sharing a port, location
- ☑ **Device information:** IP address, MAC address, hostname, device type (e.g. PC, mobile, printer, wireless router, attached peripherals)
- ☑ **OS integrity:** OS fingerprint, anti-virus update status, unpatched vulnerabilities, open services, running processes
- ☑ **Applications:** Applications, versions, registry values, file information
- ☑ **Users:** Username, workgroup, authentication status, email address, role/department
- ☑ **Device behavior:** Network policy violations, malicious activity

Guest management

Beyond the basic guest networking capability discussed earlier in this chapter, next-gen NAC solutions provide more-extensive guest management features, including registration, authorization, sponsoring and monitoring.

With *guest registration*, users are transitioned to a captive portal where they are prompted to log in to register for access. Figure 2-3 depicts a sample smartphone guest registration interface. Next-gen NAC allows IT to set up designated business users who, according to policy, can authorize guest access without any IT intervention. Guest devices can be required to have minimum endpoint security standards. Once a guest is granted access, device access can be restricted and the device can be closely monitored against NAC policies.

Figure 2-3: Sample next-gen NAC mobile guest registration interface

Flexible policy enforcement

NAC solutions provide a broader set of options for enforcing policies on non-compliant devices — whether they are connected to the network via a wired, wireless, or VPN connection— including:

- ☑ Notifying the user and logging the violation within NAC, SIEM, ticketing, or other systems
- ☑ Reassigning the device to a different VLAN

- ☑ Automatically updating network router and switch ACLs or firewall rule settings
- ☑ Automatically moving the device's connection to a pre-configured guest network
- ☑ Automatically disabling the physical or logical switch port
- ☑ Triggering a "virtual firewall" that isolates the device by intercepting IP communications
- ☑ Blocking the device using 802.1X
- ☑ Notifying the user via hijacking the HTTP session and displaying system messages

Automated endpoint remediation

Unlike legacy NAC solutions that require users or IT personnel to manually remediate compliance issues, next-gen NAC solutions can remediate many endpoint security issues automatically without human intervention. Examples include initiating remediation of vulnerable systems; installing, activating, or updating host-based protections; terminating a process; or triggering another tool to remediate an issue.

Advanced threat mitigation

When it comes to mitigating modern cyberattacks, such as *advanced persistent threats* (APTs), the most effective approach is to reduce one's attack surface and coordinate processes and controls that optimize layers of network and endpoint defenses.

As you'll discover in Chapter 5, better next-gen NAC solutions offer behavioral threat detection capabilities and provide bidirectional integration with other tools to preempt and contain exposures.

Component integration

Legacy NAC offerings are sometimes packaged using a piecemeal approach that require organizations to buy individual NAC components for asset discovery, guest management, device profiling, and more. This can increase the cost of ownership and make integration more difficult. Fortunately, next-gen

NAC vendors wrap all core NAC components into one platform that also facilitates centralized monitoring and administration.

Advanced interoperability

Beyond sources sending event logs to SIEM platforms, most tools and controls within your network operations, secure asset management, and security risk management organizations often operate using a siloed approach (see Figure 2-4).

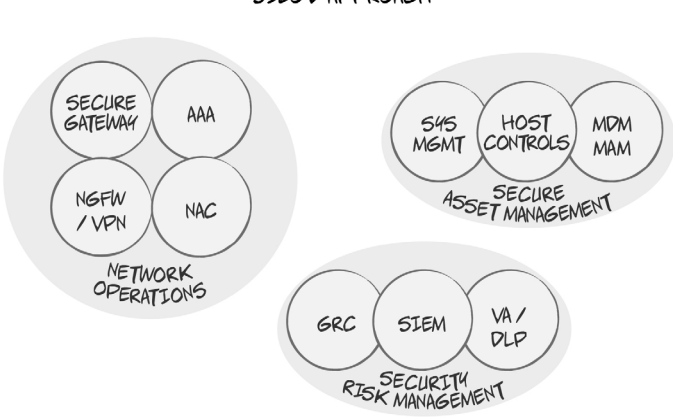

Figure 2-4: Basic NAC offerings provide few integration options

In contrast, the rich endpoint intelligence aggregated by next-gen NAC systems can be utilized by a multitude of IT and security systems (see Figure 2-5). Likewise, these systems can leverage NAC mitigation capabilities whereby NAC receives data from these systems triggering NAC policy actions. As a result, IT organizations can improve security, reduce risk, reduce mean time to mitigate non-compliant or infected endpoints, and decrease operational costs.

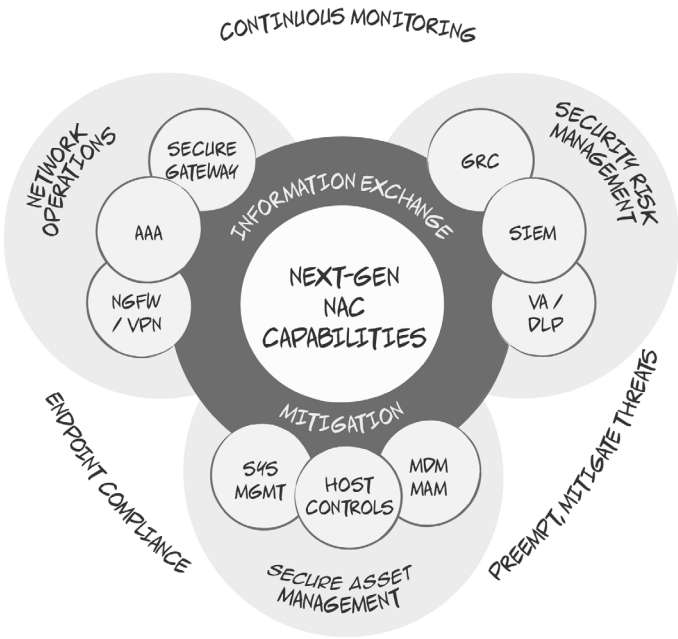

Figure 2-5: Next-gen NAC provides advanced interoperability

In summary, next-gen NAC solutions are straightforward to implement and integrate seamlessly with your existing environment, including endpoint devices and your security and network infrastructure. Today's next-gen NAC solutions are simple to administer and are easy to scale out. They are flexible, yet effective in enforcing policy while ensuring minimal disruption to the end user experience. And lastly, modern next-gen NAC offerings leverage and enhance your network and security investments while improving operations.

Now that you've gained insight into next-gen NAC technology, let's explore common use case applications.

Chapter 3

Achieving Endpoint Visibility and Security

In this chapter

- Explore the first of four primary use cases for next-gen NAC
- Discover how next-gen NAC can dramatically improve the security posture of your managed and unmanaged endpoints

If I asked you "How many devices are on your network?" you would likely respond with a range of numbers, perhaps with a margin of error of between 10 and 30 percent. But how would you respond if I asked you "How many unmanaged, non-compliant, and/or rogue devices are on your network?" Would you even have a clue?

Unfortunately, modern networks are dynamic and complex. The diversity of devices, connections, users, applications and activities adds to this complexity. Research studies indicate that companies typically know approximately 80 percent of what is on their network, and at any given time, as many as 50 percent of those devices have a security or configuration issue.

In this chapter, I explore the first of four next-gen NAC use cases described in this book. I discuss how next-gen NAC enables visibility of network users, devices and applications, including rogue devices and unsanctioned applications, through passive and active discovery; how it discovers endpoint security risks; and how these risks can be automatically mitigated with or without human intervention.

But first, Figure 3-1 provides a bit of context for this chapter by illustrating what a full-fledged next-gen NAC solution can see and control — in real time — including visible and non-visible endpoints, network devices, applications, and users.

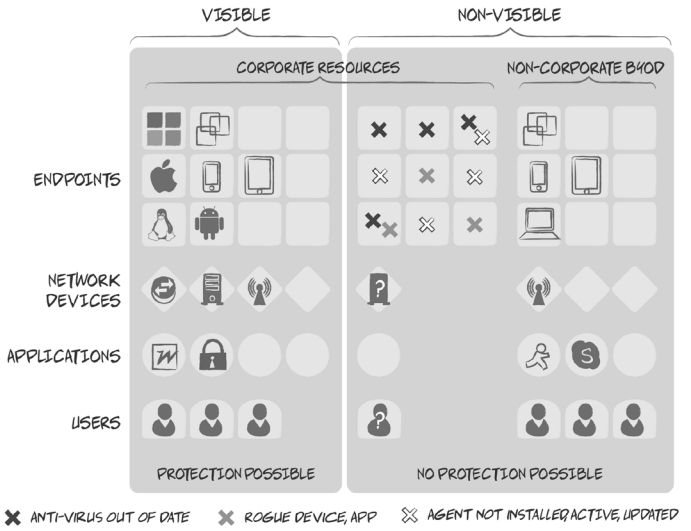

Figure 3-1: Next-gen NAC sees "everything" in real time

Achieving Real-time Network Visibility

Today's next-gen NAC solutions are well equipped with sophisticated passive and active network discovery techniques, affording security professionals unprecedented, real-time network visibility.

Passive discovery techniques

The following passive discovery techniques are particularly useful for discovering endpoint devices (e.g., laptops, tablets, and smartphones) not managed by IT. These techniques make it possible to guard your network while simultaneously supporting BYOD policies.

In Chapter 1, I explained that next-gen NAC appliances (physical or virtual) can be configured to inspect network traffic from mirror (or SPAN) ports on network switches. This enables next-gen NAC to inspect all network traffic it receives, which makes it ideally suited for discovering endpoint devices through passive discovery techniques.

Passive authentication monitoring

Next-gen NAC passively monitors authentication traffic of endpoints connecting to servers to learn usernames, authentication statuses, and device IP and MAC addresses.

Passive Nmap

Next-gen NAC incorporates an Nmap scanning engine to inspect network- and transport-layer data to inventory operating systems and services running on each host.

DHCP and ARP request monitoring

Next-gen NAC identifies endpoint devices the moment they connect to the network by analyzing data from DHCP (dynamic host configuration protocol) message packets and ARP (address resolution protocol) admission events to determine their attributes, such as device operating system, class, and other host configuration information.

Passive banners

Next-gen NAC collects banner information by examining traffic on the network and uses it to classify endpoint operating systems.

Active discovery techniques

To extend visibility into network segments for which they're not yet configured to monitor traffic, next-gen NAC appliances typically incorporate multiple active discovery techniques.

Network infrastructure integration

Next-gen NAC appliances can be configured to integrate directly with network infrastructure devices (e.g., firewalls, routers, switches, VPNs) to obtain MAC and IP address information via ARP and CAM (content addressable memory) tables or to receive switch notification traps.

LDAP, RADIUS, and 802.1X

Next-gen NAC appliances integrate with multiple authentication services to actively determine the authentication status of every device and user on the network.

NAT device detection

Next-gen NAC appliances include a sophisticated NAT (net-

work address translation) detection analysis engine designed to detect network devices sharing the same IP address, which makes them difficult to profile and manage.

External scan

Nmap active scanning software is built into leading next-gen NAC appliances to profile new hosts identified through active and passive discovery techniques. This software enables the appliances to obtain a wealth of endpoint intelligence, including operating systems, services, applications, processes, and sometimes files.

Active banners

Next-gen NAC appliances actively collect banner data by opening a connection to hosts and reading the banner returned; this aids in fingerprinting operating systems and applications.

Minding Endpoint Exposures

Once a host has been profiled through passive and/or active discovery techniques, it is instantly evaluated against user-defined next-gen NAC policies. These policies are designed to uncover various endpoint exposures that, if uncorrected, may lead to a successful network data breach. Examples of such endpoint exposures follow.

Unpatched vulnerabilities

Mobile, transient devices are rarely present during periodic (usually monthly or quarterly) full-network active *vulnerability* scans, which are often conducted during evenings and weekends. And at organizations that conduct vulnerability scans on a quarterly or annual basis, even vulnerabilities on desktop computers may go unchecked for weeks or even months.

Based on user-defined policies, next-gen NAC solutions can be employed to uncover unpatched operating system and application vulnerabilities on all endpoint devices as they connect and often in between periodic scans.

Security misconfigurations

Endpoint *security misconfigurations*, when exploited, can be just as damaging to a network's security posture as an unpatched vulnerability. Next-gen NAC solutions can identify, inform the user of, and attempt to remediate endpoint security misconfigurations, including:

- ☑ Unnecessarily opened ports
- ☑ Misconfigured device settings
- ☑ Improper file and directory permissions

Unsanctioned applications

The more unsanctioned applications running on your network, the greater the risk for exposure. Enterprises may furnish employees with documented *acceptable use policies* (AUPs) for corporate computing resources. These AUPs may even specify types of applications that are forbidden on company-owned computers and mobile devices. However, most organizations lack the capability to monitor and enforce AUPs.

Next-gen NAC helps IT security staff monitor and enforce organizational AUPs by reporting AUP violations, terminating processes associated with unsanctioned applications, and coordinating with other systems (e.g., next-gen firewalls) that are capable of blocking associated application traffic at the perimeter.

Missing host-based defenses

Although host-based defenses provide company-owned endpoints with protection against malware and ensure data is always encrypted, they're only effective when they're actually installed and running. One of the challenges faced by IT organizations is to ensure that all company-owned devices — and, in some instances, employee-owned devices — are equipped with the company's chosen host-based defense software.

Next-gen NAC solutions help IT organizations meet this challenge by eliminating common host-based security software omissions. And, as you'll learn later in this chapter, the

endpoint protection software can usually be installed or reactivated on such devices without IT intervention.

Closing Endpoint Security Gaps

Despite your best efforts to standardize desktop, laptop, and even mobile device configurations, there will always be security gaps pertaining to vulnerable and misconfigured devices — especially those not managed by IT (more on that in Chapter 4).

The previous section described the types of endpoint exposures that cause IT headaches. This section describes three ways that next-gen NAC can be used to help close these endpoint security gaps.

Policy monitoring

As I mentioned in Chapter 2, the policy engine is at the heart of every next-gen NAC solution. Many IT organizations only construct policies to identify devices and assess their security posture against custom-defined rules based on user, location, device and host defense properties. However, next-gen NAC policies are capable of so much more. They also support application whitelisting and blacklisting; they can detect unsanctioned peripherals; and they can even detect high-bandwidth utilization of unsanctioned network ports.

Comply to connect

One way to close endpoint security gaps — particularly for (BYOD) devices not managed by the IT organization — is to configure your next-gen NAC solution is to apply strong NAC authentication and enforcement control that blocks or quarantines devices until they successfully pass all relevant compliance checks, otherwise known as a *comply to connect* approach.

By initially applying next-gen NAC policies in an audit-only *listen mode* (non-enforcement), organizations can gain situational awareness to see how their security program is progressing, identify gaps and exceptions, and allow a more appropriate level of enforcement that suits the severity or risk of the device security state.

Direct remediation

When endpoint devices are flagged for non-compliance with your next-gen NAC policies, they should be remediated as quickly as possible to prevent them from being exploited by potential cyberthreats. Today's next-gen NAC solutions have moved beyond self-remediation capabilities alone. Although you may certainly elect to have users install missing patches or AV signatures themselves, most organizations prefer to leverage the direct remediation capabilities of their next-gen NAC appliances.

With direct remediation, most policy violations can be attempted to be resolved without human intervention — at least for managed devices where IT possesses administrative credentials. Patches can be installed, AV signatures can be updated, security defenses can be enabled, and more. However, as I discuss in the next section, some organizations prefer their next-gen NAC to send remediation requests to third-party platforms.

Automating Third-Party Remediation

NAC technology has rapidly evolved over the past decade. What once was viewed as a simple "on/off" switch for connecting authenticated network devices has evolved into a "network control platform" connecting NAC to dozens of third-party security solutions.

In Chapter 2, I briefly discussed ways that next-gen NAC can *receive* requests from third-party products to quarantine hosts. In this section, I discuss three ways that NAC can *send* requests to third-party products to help remediate endpoint risk.

Vulnerability management

As I discussed in the "Minding Endpoint Exposures" section earlier in this chapter, next-gen NAC is an excellent tool for identifying host vulnerabilities, as defined in a policy, in between periodic active scans. However, full-featured vulnerability management (VM) platforms — such as those from Qualys, Rapid7, and Tenable — are better equipped to uncover vulnerabilities and security misconfigurations.

Leading next-gen NAC solutions can be configured to send vulnerability scanning requests to third-party VM platforms. This helps VM platforms evaluate hosts that were missed during prior scans and/or have never connected to the network before. Also, VM systems can send vulnerability details to next-gen NAC platforms to enhance NAC intelligence.

Patch management

Once endpoint vulnerabilities have been identified, patching them is another way that next-gen NAC solutions can help. Some organizations simply let their next-gen NAC appliances distribute patches from operating system and application vendors. Others prefer to leverage their existing patch management systems to deploy patches so all patching records can be maintained in one central location.

Next-gen NAC solutions can trigger an update from leading patch management solutions, such as IBM, Lumension, and Microsoft WSUS (Windows Server Update Service) and SCCM (System Center Configuration Manager).

Endpoint protection management

In the event your next-gen NAC appliance discovers a managed device without the company's standard endpoint protection suite installed, the appliance can be configured to send a request to the endpoint protection management system — say, McAfee ePO — to initiate installation of that missing agent. Any other agent-based security product, such as endpoint encryption, can also be reviewed to ensure the agent is installed, active, and current.

Financial services firm invests in next-gen NAC to improve endpoint visibility and control

A large, U.S.-based Fortune 500 financial services institution sought to fortify its enterprise security strategy and improve its ability to meet internal and external regulatory compliance requirements across a vastly distributed and complex global network. The company wanted greater visibility of all devices attempting to access network resources, to address potential rogue device threats, and to ensure authorized devices complied with corporate security standards. In particular, the company needed to assure that systems were patched, encryption-enabled, and maintained with up-to-date host-based security defenses.

The company's CISO directed his team to evaluate three leading next-gen NAC solutions. Two selection criteria were particularly important to this organization — enterprise-class scalability and the ability to integrate with key components of the company's existing IT infrastructure. After evaluating multiple next-gen NAC solutions head-to-head, the company selected CounterACT from ForeScout Technologies (www.forescout.com).

ForeScout CounterACT was easy to install, helping the company meet its objectives within the first few weeks. Furthermore, the company was able to execute a tiered mobile security strategy, comprised of guest management, network-based control, and mobile device management (MDM) integration.

The company deployed CounterACT to centrally manage and monitor more than 200,000 endpoints at more than 100 locations. As is the case with most organizations of this size, CounterACT provided visibility into more devices than the company had originally identified. The company is now confident that virtually all network devices and connections are accounted for. In fact, within the first nine months, the company went from 80 percent endpoint compliance to maintaining greater than 99 percent endpoint compliance – while leveraging bi-directional integration with its endpoint protection platform, SIEM, and systems management products.

Chapter 4

Regulating Access and Enabling BYOD

In this chapter

- Explore the second of four primary use cases for next-gen NAC
- Learn how next-gen NAC regulates access for three core types of users — employees, contractors, and guests
- Understand why next-gen NAC is a critical component of enterprise BYOD implementations

In Chapter 3, I discussed how next-gen NAC provides unprecedented endpoint visibility through sophisticated active and passive discovery and inspection techniques. I also explained how it can close endpoint security gaps by remediating system vulnerabilities and security misconfigurations directly or through third-party security technologies.

In this chapter, I build upon these concepts by describing how next-gen NAC policies can be granularly customized by user role and device type and detailing why next-gen NAC is a "must have" component of any sensible BYOD initiative.

Regulating Access by Role

Today's next-gen NAC solutions enable administrators to construct granular network access policies by user role. Role-based policies are generally constructed based on three types of users — employees, guests, and contractors.

In conjunction with user role, additional policy attributes include device type, acceptable use, location, and risk properties.

Employees

Employees are identified by next-gen NAC appliances following successful login to the organization's directory — usually Active Directory or other LDAP-based directory — although RADIUS, TACACS, and 802.1X authentication mechanisms are commonly supported. The better the directory has been maintained, the easier it will be to manage role-specific NAC policies.

If desired, organizations may construct two sets of employee policies — one when employees are connecting with managed devices and another when they are connecting with personally owned (unmanaged) devices. Devices can be identified by a variety of attributes, such as MAC address, and then checked against the next-gen NAC policy to determine if it is a managed corporate device or an unmanaged guest device. In the event an employee connects with a personal/unmanaged device, the policy could be less stringent if only allowing Internet access, or if the device was a smartphone or tablet, the policy could require it to be enrolled in an MDM product.

Of course, the scope of access to network resources varies by an employee's role in the organization. As a best practice, access should be limited to network segments containing resources necessary for the employee to do his or her job, and by appropriate need to utilize sensitive data.

Guests

At the other end of the user role spectrum are guests. Organizations typically bypass full inspection of guest devices and often restrict guests to Internet access (by moving the guest's connection to a separate WLAN or VLAN), sometimes upon completion of an optional online registration form (see "Guest management" section in Chapter 2). Guest registrations can be automatically approved or the request can be routed to one or more individuals in your organization for approval.

Guest devices are distinguished from managed devices through the following mechanisms:

- ☑ Device did not successfully authenticate to directory

- ☑ Device's MAC address not on a known whitelist
- ☑ Device not running specific security application or agent that is standard on managed devices

Once a guest's registration has been approved, the next-gen NAC appliance can verify identity by sending a one-time verification code to the guest's email address or mobile phone number provided during registration. Many next-gen NAC solutions can pre-approve guests by using a built-in database or external directory.

Contractors

Contractors are a "hybrid" between employees and guests. Their devices are usually unmanaged like those of guests, but like employees, they often require access to specific IP ranges or systems within the production network.

When a contractor attempts to access the network from an internal network segment, a pre-designed captive portal screen can prompt the contractor to grant permission to the next-gen NAC system to conduct a security inspection of the device. At that point, the device can be assessed for certain vulnerabilities and the presence of specific required endpoint security defenses — depending on the policy attributes set for contractors. This allows the organization to align contractor devices to the same security standards as employee devices.

If the contractor refuses to grant permission for the NAC platform to conduct a security scan, their network connection can be moved to the guest network to obtain Internet-only access. Contractors can also be defined in a policy that references directory services, where by NAC can fortify login records and restrictions to network resources.

When contractors require network access for extended periods of time, better next-gen NAC solutions enable them to install client software so the system can more directly monitor their compliance with endpoint policies. The agent can be set as non-persistent to immediately dissolve at reboot or to dissolve at the end of the contract period. During the time the client software is active, the contractor's device can be managed by the agent and monitored according to policy.

Enabling BYOD

Implementation of BYOD policies by IT is both a blessing and a curse. On one hand, permitting employees to connect to network resources from personally owned computers, tablets, and smartphones adds to their productivity and job satisfaction. On the other hand, without controls to enforce policy, BYOD dramatically increases security risks.

Given the widespread use of personal and mobile devices at work, a BYOD policy is a necessity for any enterprise. As such, adoption of BYOD policies for companies with greater than 500 employees is projected to increase from 31 percent in 2014 to 77 percent in 2016, according to CyberEdge Group's 2014 Cyberthreat Defense Report. That report also found that 84 percent of respondents are using or plan to use NAC for mobile security.

Let's now discuss how enterprises leverage next-gen NAC to monitor and enforce BYOD policies.

Enforcing BYOD policies

The flexibility of NAC policies to accommodate device, identity, and enforcement attributes allows NAC to be applied across the entire BYOD adoption spectrum, from restricting personal devices to embracing their use. The following are typical options for enforcing BYOD policies:

- ☑ **Restrict** — deny access to unmanaged and/or personal endpoint devices
- ☑ **Sanction** – restrict access of specific users to Internet and other limited resources through a captive portal; enforce modest security requirements as necessary; and enable remediation of non-compliant systems
- ☑ **Allow** — enable broader access based on device type, location, time of day, and user role by applying network-based policy utilizing NAC device inspection and agent technologies, recording access, and requiring broader security settings
- ☑ **Embrace** – Enable all personal and mobile device use; record access; enhance by enrolling devices in additional host-based controls such as those provided by next-gen NAC and MDM; and enforce policy

Beyond dissolvable agents for desktops, some leading next-gen NAC providers offer mobile device security applications that can provide additional controls for smartphones and tablets, such as jailbreak detection, certificates, device configuration, password strength, application whitelisting and blacklisting, remote lock and wipe, and encryption.

Integrating with mobile device management

MDM systems are commonly used by enterprises to centrally administer mobile devices and their applications, to provision applications, to segregate and protect data, and to enforce policies concerning user, device, applications, and data for smartphones and tablets. However, in the context of BYOD, MDM has two limitations — it can only manage devices that have already been enrolled and it lacks network visibility and access control.

Better next-gen NAC solutions resolve these limitations by detecting mobile devices as they connect, whether they have the MDM agent installed or not, and restricting network access based on discovered properties. In the case where an approved device is missing the MDM agent, NAC solutions can also redirect users to an MDM enrollment screen.

Once devices are enrolled within the MDM system, the next-gen NAC solution can obtain their properties directly from the MDM system and share them with the NAC solution in order to provide administrators with a unified view of all network devices. Furthermore, NAC can enforce policy by triggering the MDM system to conduct a profile check of each MDM-managed device when accessing network resources. Should the device fail MDM security policy, the next-gen NAC solution can restrict or remove its network access, which is generally more acceptable than wiping or locking the device.

Global tech manufacturer assembles next-gen NAC solution to support its BYOD initiatives

A large, global technology manufacturer used a basic NAC platform as part of its defense-in-depth model and to support its corporate-wide BYOD strategy. Within 18 months following deployment, the company recognized several deficiencies with regard to scalability, operational disruption, management overhead, and overall cost.

In particular, the company's entry-level NAC platform enforced rigid compliance policies, which frequently caused disruptions in employee productivity. Also, it was not easily managed, requiring significant network re-architecting and upgrades, and would not fully integrate into the company's heterogeneous computing environment. The company's commitment to rolling out a highly anticipated BYOD policy remained unfulfilled.

Having learned of the compelling value that next-generation NAC brings, the company began evaluating replacement NAC platforms. After careful consideration, the company selected CounterACT from ForeScout Technologies (www.forescout.com).

Today, the company has deployed CounterACT appliances in more than 80 offices across three continents. The ForeScout next-gen NAC system is now protecting more than 65,000 users and more than 230,000 devices worldwide.

The CounterACT Enterprise Manager and distributed appliances are dynamically managing a broad range of NAC policies while integrating with a variety of endpoint protection and configuration management systems. By incorporating both NAC and MDM controls, the company has enforced different acceptable use policies for tablet and smartphone users, depending if the device is corporate-issued or personally owned.

As a result, the company has cut endpoint security violations by more than 50 percent and has dramatically reduced remediation costs. Best of all, the company was finally able to deliver on its BYOD promise while minimizing incremental security risks.

Chapter 5

Mitigating Advanced Threats

In this chapter

- Explore the third of four primary use cases for next-gen NAC
- Review today's advanced threat landscape to understand why traditional signature-based defenses are not enough
- Learn how next-gen NAC can help mitigate advanced threats

Hardly a day goes by without news of a major data breach. Despite spending billions on defenses, enterprises are constantly being impacted by advanced threats. But why? And what we can do to better manage the risk?

In this chapter, I review the advanced threat landscape and describe why traditional defenses are not enough to address the velocity and sophistication of modern cyberattacks. Then I discuss how next-gen NAC can dramatically improve an organization's attack surface and ability to mitigate advanced threats.

Today's Advanced Threat Landscape

Cyberthreats are constantly evolving and more sophisticated than ever. Today's hacktivist and cybercriminal communities are organized, skilled, well funded, and highly motivated. And in most cases, their attacks are targeted with a very specific objective in mind.

Zero-day and targeted attacks

Hackers use malware to exploit vulnerable operating systems and applications. Most vulnerabilities are disclosed by software vendors upon the release of corresponding patches. Hackers occasionally discover vulnerabilities on their own and create *zero-day threats* to *exploit* them. They're called zero-day threats because the vulnerabilities are exploited before day one of patch availability.

Regardless of whether malware exploits a *zero-day vulnerability* or a known but non-remediated vulnerability, the result is the same. Since cybercriminals can customize malware using popular exploit kits, traditional signature-based defenses (IPS and AV) can be ineffective. Even perimeter-based defenses with *sandboxing* and port monitoring technology often miss an initial attack. Typically breaches occur months before detection and well before damage is discovered.

Land and expand realities

Cybercriminals recognize that it's easier and ultimately more efficient to compromise vulnerable endpoints than to directly target servers and databases of interest. Companies often fall behind in patching efforts, have inactive host defenses, and lack BYOD controls — creating a broad attack surface. Attackers are also leveraging social engineering tactics, such as *spear phishing* and *waterholing*, to trick unsuspecting users into sharing access credentials or downloading malware-infected files. Once a system is breached, hackers and malware seek to exploit other less secure systems as part of a "land and expand" strategy.

All it takes is interaction with one malicious email attachment, application, hyperlink, system request, or one rogue wireless device. Once an endpoint is compromised, the malware typically "phones home" to a command-and-control (CnC) server to receive further instructions. The next step often results in the subversive installation of remote access Trojan (RAT) software, which gives the cybercriminal full control over the endpoint and enables him (or her) to expand laterally onto other vulnerable systems until he finds his ultimate target.

Once he's obtained valid admin credentials for that target, probably through keylogger software, it's game over. Sensitive data is inconspicuously exfiltrated or encrypted and held for ransom, or systems are overloaded or used to conduct botnet attacks.

Mitigating Advanced Threats

Given the sophistication of today's cyberthreats, a defense-in-depth approach is best to tackle advanced threats from different perspectives. Since vulnerable endpoints are the easiest targets of most attack campaigns, next-gen NAC is a critical component of any threat mitigation strategy. It helps mitigate advanced threats in three highly effective ways, as described in the following sections.

Reducing the attack surface

Next-gen NAC can reduce your network's attack surface by identifying non-compliant and unknown systems and performing any or all of the following functions:

- ☑ Alerting you to compliance violations
- ☑ Keeping non-compliant, vulnerable endpoints off your network
- ☑ Remediating vulnerabilities and security misconfigurations directly or via third-party systems
- ☑ Ensuring that host defenses are installed, up-to-date, properly configured, and enabled

NAC is particularly effective at addressing security gaps introduced by transient network devices. Improving the security posture of these devices decreases your network's attack surface and thus reduces overall security risks.

Monitoring for suspicious network behavior

Once an endpoint has been compromised as part of a *targeted threat* campaign, the next step for the attacker is to spread laterally, such as running port scans to assemble a list of hosts and operating systems, or exfiltrating data via a communication port.

Leading next-gen NAC solutions provide endpoint monitoring capabilities to look for unusual network behavior, such as the use of non-standard communications ports and/or abnormally high bandwidth utilization. Better next-gen NAC solutions also incorporate virtual honeypot technology that serve system and application decoys to capture unauthorized network reconnaissance. Based on NAC policy, a malware-infected host that attempts to communicate with these virtual decoys or exhibits suspicious activity (e.g., non-standard port use) can invoke NAC defenses such as record, alert, or quarantine.

Integrating with your security infrastructure

Next-gen NAC works with a myriad of third-party products to share intelligence, enhance context, and contain threats.

- ☑ **Share intelligence** –NAC can dynamically share endpoint configuration and security details with other tools and receive data from these tools.
- ☑ **Enhance context** – Data exchange adds to the overall properties that can be applied to the rules engine of other tools, enhancing policies and actions.
- ☑ **Triggering mitigation** – Next-gen NAC can be configured to quarantine or remediate endpoints based on requests and data from external systems.

Specifically, next-gen NAC works with NGFW, web filtering, and advanced threat detection tools as follows:

- ☑ **Providing context** – Many security systems often lack complete details on device identity and configuration and security state. NAC can be configured to exchange this information.
- ☑ **Eliminating the threat** – Unless the security system is inline and has active defenses, an attack and data exfiltration may continue following a security alert. Security systems can inform NAC to directly isolate the host or specific port – preserving evidence and containing the threat.

Chapter 6

Aiding Compliance with Continuous Monitoring and Mitigation

In this chapter

- Explore support for compliance processes, the fourth and final primary use case for next-gen NAC
- Understand the principles of continuous monitoring and mitigation
- Learn how next-gen NAC helps organizations support security management, compliance, and auditing processes

Achieving and sustaining compliance, whether with internal IT governance policies or external industry- or government-imposed regulations, is a requisite for any sizeable IT security organization. Fortunately, next-gen NAC enables organizations to tick off not only the usual compliance check boxes associated with basic NAC capabilities, but several more specifications by interoperating with existing security defenses. By doing so, IT organizations can achieve what industry pundits are now calling *continuous monitoring and mitigation*, or CMM.

In this chapter, I describe how next-gen NAC capabilities align with common compliance framework controls. We will examine the guiding principles of CMM and then explore how next-gen NAC interoperability — as part of a CMM framework — helps organizations more easily support compliance mandates.

Effectuating IT GRC

The principles of IT governance, risk, and compliance (GRC) are to document policies and to employ processes and control specifications that enable IT to adhere to these policies. Most IT organizations face multiple sets of industry- and/or government-imposed compliance specifications, in addition to internal audit requirements. To optimize resources, reduce policy violations, and minimize risks, organizations should employ security tools that support multiple control mechanisms simultaneously.

Mapping next-gen NAC to common compliance controls

There are a variety of GRC-related frameworks such as ISO-27001, FISMA, PCI DSS and the CSC20. Beyond conventional access controls, the ability of next-gen NAC to provide real-time visibility, host-based configuration and defense verification, network enforcement, and endpoint remediation maps to a broad range of common technical controls within these frameworks, including:

- ☑ **Maintain inventory** – Manage known, authorized, and rogue devices and software
- ☑ **System integrity** – Manage and maintain secure system configurations and patching
- ☑ **Vulnerability assessment** – Periodically scan for and remediate vulnerabilities
- ☑ **Anti-malware** – Employ and maintain host-based anti-malware defenses
- ☑ **Secure wireless** – Secure the configuration of wireless access points and wireless network
- ☑ **Data protection** – Utilize encryption and access control methods to ensure authorized access to sensitive data. Monitor for unauthorized data exfiltration. Ensure backup and recovery services are active
- ☑ **Access control** – Ensure appropriate access to network resources, including administrative privileges

- ☑ **Network defenses** – Secure and maintain properly configured network devices
- ☑ **Perimeter defenses** – Maintain appropriately configured network perimeter defenses
- ☑ **Audit logs** – Ensure the capture, monitoring, and storage of audit logs

Integrating NAC with SIEM and GRC platforms

SIEM and log management tools are commonly used for compliance monitoring and reporting purposes. As described earlier, next-gen NAC offers the means to dynamically exchange data with external systems, such as SIEM and other GRC platforms. NAC can share policy violations and access events, but also real-time asset details that enhance the operational coverage of these platforms.

This, in turn, expands the scope of these platforms' compliance monitoring, reporting, and auditing capabilities. SIEM and GRC tools produce alerts and reports but do not offer active mitigation capabilities. Interfacing these solutions with next-gen NAC allows their controls to trigger NAC network enforcement and endpoint remediation capabilities.

Most NAC solutions work with SIEM and log management platforms by utilizing the syslog protocol and sending events whose message is constructed according to the *common event format* (CEF). Next-gen NAC goes beyond simple CEF data transfer, invoking other protocols through the use of SIEM and web service APIs. This provides SIEM platforms rich network and asset configuration intelligence that can be stored and cross-correlated with other SIEM data sources. The result is newfound contextual data that can dramatically improve forensic analysis processes and better equip security practitioners with the intelligence needed to make good decisions.

Beyond exporting network and asset intelligence to SIEM platforms, better next-gen NAC solutions can receive automated requests from SIEM systems to quarantine or remediate hosts identified as the source or target of a security issue.

By rapidly quarantining such hosts, IT can stop or contain potential security breaches before more data is exfiltrated or additional hosts are compromised.

Fortifying Compliance Specifications

Let's now review four common compliance mandates facing enterprises and government agencies today and understand how next-gen NAC helps IT organizations support them.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS version 3.0 is comprised of 12 high-level requirements and more than 200 sub-requirements that merchants must follow when processing credit card transactions. Table 6-1 depicts a small sampling of PCI DSS requirements addressed by next-gen NAC technology.

Req.	*Topic*
1.4	Ensuring presence of personal firewall software
2.2	Developing configuration hardening standards
5.2	Ensuring all anti-virus mechanisms are current
5.3	Ensuring anti-virus mechanisms are running
6.2	Verifying installation of security patches
6.4.1	Separating test and production environments
7.1	Limiting access to computing resources
7.2	Establishing an access control system
11.1	Detecting unauthorized wireless access points

Table 6-1: Sample PCI DSS requirements addressed

To learn more about PCI DSS, connect to: https://www.pcisecuritystandards.org/.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) requires that healthcare providers establish, record, and assess policy and technical controls to safeguard patient health information (PHI) for appropriate access and use. The Health Information Technology for Economic and Clinical Health (HITECH) Act extends to appropriate and secure PHI use, transmission, and exchange. Table 6-2 depicts a sampling of HIPAA requirements addressed by next-gen NAC.

Req.	*Topic*
§ 164.308(a)(1)	Security management process
§ 164.308(a)(4)	Information access management
§ 164.310(c)	Workstation security
§ 164.312(a)(2)(iv)	Encryption
§ 164.312(a)(1)	Access control
§ 164.312(e)(2)(ii)	Transmission security, encryption

Table 6-2: Sample HIPAA requirements addressed

Encryption is not only a required technical control to protect PHI when connecting to systems and applications, but it is also a safe harbor for breach disclosure as per The Security Rule within the HITECH ACT. NAC can be used a secondary control to ensure host-based encryption service use.

To learn more about HIPAA, connect to: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Critical Security Controls (CSC)

The Top 20 Critical Security Controls (CSC) – commonly called the Consensus Audit Guidelines or CAG – were first developed in 2008 by a consortium of federal government agencies and private parties in response to data losses experienced in the U.S. defense industry. Up until August 2013, the Top 20 CSCs were governed by the SANS Institute, but ongoing development and adoption of the controls are now

the responsibility of the Council on CyberSecurity (www.counciloncybersecurity.org).

The Top 20 CSCs (now at Version 5) are revised annually to offer a pragmatic control methodology to help organizations keep up with modern threats. The following controls are particularly relevant to NAC:

Section	*Topic*
CSC 1,2	Inventory
CSC 3	Secure configurations
CSC 4	Vulnerability assessment
CSC 5	Malware defenses
CSC 7	Wireless device control
CSC 11	Control network ports, protocols
CSC 13	Boundary defense
CSC 15	Controlled access

Table 6-3: Sample Top 20 CSCs addressed by NAC

To learn about the Top 20 CSCs, connect to: http://www.sans.org/critical-security-controls/.

Federal Information Security Management Act (FISMA)

FISMA was passed in 2002 to govern the management of information security among U.S. federal civilian agencies. FISMA requirements are detailed, in part, in a series of NIST Special Publications (SPs), including NIST SP 800-137, which defines continuous monitoring.

In short, continuous monitoring is the process and technology used to detect IT security compliance and risk issues in real time. Continuous monitoring, fueled by next-gen NAC, plays a pivotal role in all six steps of NIST's renowned Risk Management Framework, including:

- ☑ Categorizing information systems
- ☑ Selecting security controls
- ☑ Implementing security controls
- ☑ Assessing security controls
- ☑ Authorizing information systems
- ☑ Monitoring security controls

To download NIST SP 800-137 or other NIST publications, connect to http://csrc.nist.gov/publications/PubsSPs.html.

Achieving Continuous Monitoring and Mitigation

CMM is an extension of the aforementioned continuous monitoring concept developed by NIST. CMM embraces the notion of continuously monitoring your network, defenses, and vulnerabilities, but extends the concept by streamlining the discovery and mitigation of security gaps, misconfigurations, and host vulnerabilities.

This section describes the guiding principles of CMM, which, as you'll discover in the following section, are achievable by leveraging next-gen NAC interoperability.

Asset intelligence

When configured optimally, your next-gen NAC solution will provide you with more endpoint intelligence than you ever dreamt possible. You'll see everything — device types, operating systems, applications, virtual machines, security risks, network locations, and more — all in real time. You'll learn which systems are not adhering to configuration policy and you'll be able to identify rogue devices, unsanctioned applications, inactive host security defenses, and licensing gaps.

Endpoint vulnerability and compliance remediation

A foundational capability of CMM is automating vulnerability management and endpoint remediation. As described in Chapter 3, next-gen NAC can directly facilitate emergency patching, software installation, and fixing misconfigurations. However, many organizations prefer to leverage their existing system management and patch management solutions to remediate endpoint concerns.

Next-gen NAC can be used to send information to these platforms, such as endpoint protection suites or popular management applications, to invoke a vulnerability scan, update a patch, or install necessary software.

HBSS assurance and access control

CMM requires that *host-based security systems* (HBSS) be implemented and appropriate measures be taken to restrict access to network resources and sensitive data. Next-gen NAC can interface with popular HBSS suites to ensure that encryption, personal firewall, and anti-virus software is not only installed, but active and up-to-date. Next-gen NAC can also dynamically identify systems that are not meeting configuration policy as set forth by HBSS platforms. And clearly, next-gen NAC provides port-based and roles-based control of access to network resources.

Connecting the Dots From NAC to CMM

Next-gen NAC is a foundational CMM component that supports all five stages of the CMM lifecycle, as depicted in Figure 6-1. I'll now connect the NAC to CMM dots for you:

- ☑ **Continuous visibility –** I think you get the picture by now. Next-gen NAC generates rich, real-time endpoint and network intelligence.
- ☑ **Endpoint authentication and inspection** – Next-gen NAC monitors user and device authentication and assesses devices against built-in and custom-configured NAC compliance policies.
- ☑ **Information integration –** Next-gen NAC utilizes standard and third-party APIs to share network and asset intelligence with external systems.
- ☑ **Network enforcement –** Next-gen NAC can be configured to re-assign network access, limit port use and even quarantine non-compliant devices. Next-gen NAC can receive data and requests from third-party systems to invoke enforcement actions.
- ☑ **Endpoint remediation –** Next-gen NAC systems can directly remediate a wide variety of issues or forward remediation requests to third-party systems. As with enforcement, next-gen NAC can also receive data and requests from third-party systems to invoke remediation actions.

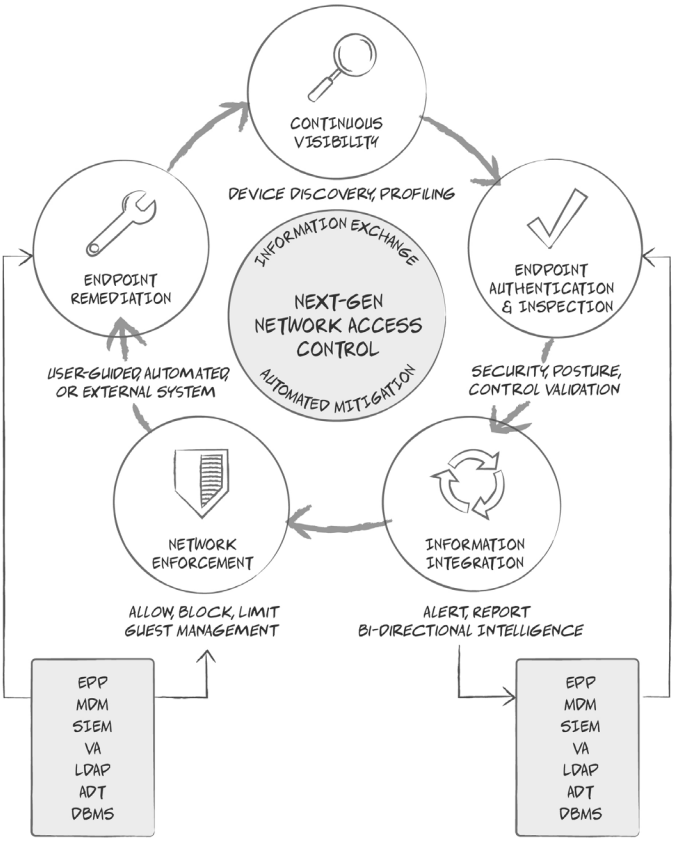

Figure 6-1: Continuous monitoring and mitigation life cycle

Now that we've covered all four primary next-gen NAC use cases, I hope you're ready to move onto the next step. The next chapter will describe what to look for, and what to avoid, when evaluating next-gen NAC solutions and will provide numerous tips and tricks for getting your next-gen NAC investment up and running.

Chapter 7

Getting Started

In this chapter

- Learn the fundamentals of scoping your next-gen NAC project and making architectural decisions
- Know what to look for, and what to avoid, when evaluating next-gen NAC solutions
- Understand everything that's involved with getting your next-gen NAC investment up, running, and optimized

Unlike single-purpose network security products — such as IPS, VPN, and AV— which can be relatively simple to deploy, NAC platforms can be deployed in many different ways to satisfy a variety of use cases. Careful thought should go into scoping, selecting, and deploying a next-gen NAC solution. This chapter will help you get started

Scoping the Project

Before you begin evaluating next-gen NAC offerings, it's important to scope out your project, determine the most pertinent and critical use cases, and identify the most beneficial results so you know exactly which functional requirements are crucial for your organization — today and in the near future.

Don't forget that next-gen NAC addresses many different use cases and offers a wealth of functionality. As with other IT investments, as you scope out the project with your colleagues, it's prudent to note which capabilities may be important in the future so you can select a next-gen NAC platform that can accommodate your anticipated needs.

Assembling the team

Like any IT project, planning is a pre-requisite for a successful NAC deployment. Along with designating an IT executive to help direct, manage, and track decisions, I recommend expanding the project scoping discussion to a broad audience including:

- ☑ Network infrastructure and security architects
- ☑ Desktop/systems management and help desk
- ☑ Network and security operations
- ☑ Risk and compliance personnel

Next-gen NAC is rightfully considered a network security platform. But if you only engage your network security colleagues in the project, you won't achieve optimal results.

Establishing use cases

Once the team is assembled to help scope and define the project, members should identify, rank, and document sets of required use cases, needed controls, processes, capabilities, infrastructure interfaces, and possible timeframes. The use case sets typically fall into the following categories:

- ☑ Achieving endpoint visibility and posture assessment
- ☑ Securing managed endpoints
- ☑ Regulating guest and contractor access
- ☑ Supporting BYOD initiatives
- ☑ Mitigating rogue devices and applications
- ☑ Remediating security violations and exposures
- ☑ Reducing malware and advanced threat risks
- ☑ Supporting regulatory compliance
- ☑ Fortifying other tools and controls
- ☑ Enabling port-based authentication and access control

Determining deployment coverage

Although it's possible to deploy next-gen NAC appliances across your network in short order, the larger and more distributed the environment, the more likely you will be successful by deploying in prioritized phases — by network location, segments or type, by use case, by business criticality, or according to resource constraints.

Designing the Architecture

Once the overall project is scoped, you'll need to make several architectural decisions that will influence your next-gen NAC selection process. This section describes key architectural decisions you and your team will need to make.

It's entirely probable these architectural decisions will change as your organization's security profile improves and as your infrastructure evolves to support new business requirements. A next-gen NAC solution can easily accommodate new devices, policies, and threats.

Centralized or decentralized

Organizations today vary in their network architecture. Some have hub-and-spoke type infrastructures and some have multiple remote locations connected via an MPLS cloud. Infrastructure services like Internet access, DHCP, DNS, and Active Directory can be centralized or distributed.

Furthermore, you may have main datacenters or remote disaster recovery sites to ensure business continuity. Placement of appliances in either a centralized or decentralized manner, along with high-availability options, are deployment decisions that should be considered in advance — ideally made with the assistance of qualified vendor or channel partner personnel that can guide you through additional deployment considerations.

Physical or virtual appliances

Most organizations select physical rackmount appliances because the software is pre-installed by the vendor, the operating system is hardened (optimized for security), and

the appliance is equipped with different high-speed network interfaces. However, many next-gen NAC vendors offer virtual appliances with equivalent capabilities. In some cases, such as a global deployment, a mixed appliance approach may be desired. Thus, be sure to select a vendor that can accommodate your preference.

Agent-based or agentless

Depending on the vendor, the NAC platform may or may not require agents. Some vendors, such as those that are 802.1X centric and offer purely pre-connect NAC, will require agents or supplicants on all managed endpoints — further examined in the next section.

With next-gen NAC, the vast majority of your devices will be monitored and evaluated without the addition of software agents. Although an agentless approach is faster to deploy and less costly to manage, there are situations that may call for a NAC agent.

For example, in situations where your company uses long-term contractors or has employees who connect their own devices to your internal network, you can enroll them as NAC-managed devices via the persistent or non-persistent agent to enable endpoint inspection and local enforcement actions.

Pre- or post-connect NAC

Most organizations prefer post-connect NAC over pre-connect NAC (both supported by next-gen NAC) because it is less invasive, easier and more flexible to manage, and preserves user experience when connecting to the network. Rather than being denied access until NAC-authenticated and assessed, users instantly connect to the network or a more restricted VLAN where the security posture of their device can be evaluated and different policy-based actions can take effect.

802.1X requires three components: a supplicant, an authenticator and an authentication server (note: it does not specify additional controls beyond authentication). The supplicant is often referred to the managed software on a device that offers credentials to the authenticator. The authenticator is a network device, such as a switch or wireless access point, which relays the credentials between the

supplicant and authentication server. The authentication server, usually a device running a RADIUS service, validates the credentials of the supplicant and informs the authenticator that device access is authorized.

Why describe 802.1X? 802.1X is a pre-connect NAC technology, but it is only tied to authentication transactions for access enforcement. The advantage is that it operates at Layer-2 and blocks network communications until device authentication. However, the disadvantage of 802.1X is that all network infrastructure components — clients and authentication — need to be current, configured correctly, and maintained. Any deviation may impact network and user operation.

To avoid this impact, enterprises need a unified infrastructure, a plan to manage non-802.1X supported devices, and a process to more effectively audit issues. 802.1X authentication is well suited to a homogeneous network environment and is easier to implement in wireless LANs than in wired LANs. Wireless LANs are predominantly used by newer devices with built-in supplicants, whereas wired LANs tend to have a larger variety of legacy endpoints that do not support supplicants.

So, do your homework. Your organization should review the host agent management, infrastructure, deployment and operational requirements and costs of pre-connect 802.1X NAC approaches to see if they meet your functional requirements, resource constraints, and budget.

Quarantine or monitor

Most organizations opt for an approach that initially monitors users, devices, and applications rather than take the extreme action of blocking or quarantining them, as the risk of lost productivity or an outage may be higher than the possible security exposure. As mentioned earlier in this chapter, this approach is best suited by a post-connect NAC configuration.

Most next-gen NAC solutions offer granular policies to allow you to selectively phase in network enforcement actions. But if you decide to quarantine non-compliant devices sooner rather than later, I recommend you wait until your next-gen NAC solution has been in production long enough for you to reduce the percentage of non-compliance for the various policies to a manageable amount.

That way, when you do turn enforcement on, you're minimizing the number of endpoints affected — and the number of end user calls to your help desk. Enforcement and remediation will also be dependent on the criticality of the device as an end user device has less impact than a mission critical server.

As you implement NAC policies, certain policies may require stronger mitigation actions than others. For example, with guest management, immediately enforcing a captive portal or HTTP hijack for registration and allowing Internet-only access from a guest network is a policy that should be immediately enforced. However, companies often give warnings or attempt self-remediation and NAC-based remediation for other policies, such as anti-virus, before blocking access.

Figure 7-1 illustrates how most organizations phase in next-gen NAC mitigation and remediation actions over time to minimize impact and preserve user experience.

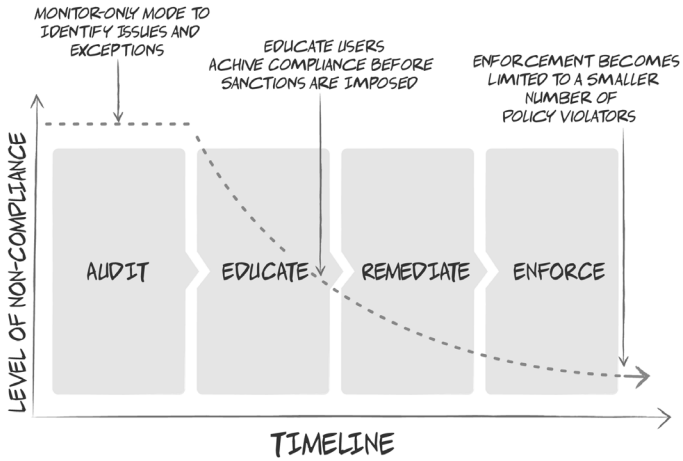

Figure 7-1: Evolution of typical next-gen NAC deployments

Most next-gen NAC products allow you to run policies in a non-enforcement mode first so you can assess how many and what type of endpoints would have been quarantined or remediated if that action feature had been activated.

Selection and Testing

Now that you've scoped the project, and have made key (at least) short-term architectural decisions, it's time to go shopping for your next-gen NAC solution. This section will help you refine your selection process and facilitate evaluation.

Selecting the right next-gen NAC solution

The following are attributes of leading next-gen NAC products. If you start with this list, you can't go wrong.

- ☑ Post-connect and/or pre-connect implementation
- ☑ Support for agentless deployments with the option of an agent under certain situations
- ☑ Guest registration interface and guest management
- ☑ Flexible policy engine (users, devices, time of day)
- ☑ Ease of use, rapid implementation, and convenient exception handling
- ☑ Customizable dashboards and reports
- ☑ Policy management, templates, and extensibility
- ☑ Comprehensive integration with popular network and security infrastructure components
- ☑ Breadth of network enforcement and remediation
- ☑ Advanced SIEM, VM, MDM, advanced threat detection, and system management interoperability
- ☑ Honeypot capability to detect advanced network threats
- ☑ Flexible licensing, appliance, and deployment options
- ☑ Customer support and professional service options

When evaluating competing solutions in a mature product category, check to see if Gartner has produced a "Magic Quadrant" report. If so, start with the "Leaders" as their feature sets and support infrastructure are generally more comprehensive.

Conducting a proof of concept

Before you sign on the dotted line, it's best to conduct a proof of concept (POC), usually a 30-day trial, to ensure the solution you've tentatively selected will truly meet your needs. I recommend installing and configuring the product on your own in an environment designed to recreate the production network as closely as possible in order to better ensure that you fully understand what is required to deploy the solution within your infrastructure and to identify potential incompatibilities.

During this phase, it's a good idea to bring your NAC project team into the different POCs for various products so they understand their upcoming roles and responsibilities during actual product deployment. Also, you may flush out products that aren't a good fit for your organization based upon feedback from members of your team. Conversely, the right product will become easily apparent if your team members find the product to offer low impact and high value.

Conduct your POC in a reduced implementation, non-production network or lab — preferably an environment that will be able to demonstrate operational coverage, your key use cases, and third-party integration. And if you want to test the product's enforcement and remediation capability, limit it to certain devices and users to minimize potential user disruption.

Implementing Your Solution

Once you've selected your ideal next-gen NAC platform, it's time to roll it out. The faster you can get your investment up and running, the quicker it will pay returns.

Depending on the scope of your project, the number and location of devices and network segments, extent of deployment, project time, and experience, I recommend you engage professional services employed by your vendor or channel partner to help roll out your solution — at least in the beginning. These consultants can apply field-proven best practices to ensure your deployment is optimized according to your needs. Consider allocating additional professional services to be used after the product has been deployed to help you transition from one deployment stage to the next.

Staging the rollout

Earlier in this chapter (see "Determining deployment coverage" section), I discussed the need to plan the rollout of your next-gen NAC deployment in phases, perhaps by covering key use case, locations, or business criticality first. Now that you've selected your next-gen NAC vendor and presumably acquired appropriate appliances, it's time to develop a deployment schedule that maps to your pre-determined phases.

Depending on your deployment and implementation phases, I recommend that you determine how many devices will need to be under management, by location and infrastructure, in each phase so that you procure the correct number and type of next-gen NAC appliances and management components.

Installing components

With your schedule in place, it's time to begin installing your next-gen NAC appliances. If you decide to utilize a SPAN or mirrored port to analyze traffic as part of your next-gen NAC deployment, you may consider installing aggregation TAPs — which are nowadays called network packet brokers — to aggregate applicable traffic from multiple switches into one shared next-gen NAC appliance. This alleviates concerns related to port density or oversubscribing the interfaces on your next-gen NAC appliance.

Some NAC solutions may require network re-architecting, deploying in-line devices, integrating with different network services and tools, and/or upgrading certain network infrastructure components. Be sure you know the deployment dependencies before you embark on any NAC journey.

Integrating with your network and security infrastructure

With your next-gen NAC management console and appliances in place and the basic appliance configuration completed, the next step is configuring your solution to interface with your existing network and security infrastructure. In particular, the common security systems your next-gen NAC interoperates with include: directory services, VPN, SIEM, endpoint protection management, systems management, VM, MDM, and

advanced threat detection. Next-gen NAC also can interface with other systems using open, standard protocols.

Integrating with third-party systems is not especially complicated if you're prepared. Determining the interface points and obtaining access credentials in advance will save you and your team considerable time, effort, and headaches.

Constructing policies

The policies you construct should support the use cases you selected during the project scoping phase. Most next-gen NAC solutions have a broad range of built-in and extensible policy templates to help you get started.

There are many factors to consider when constructing next-gen NAC policies, including:

- ☑ Users roles and groups
- ☑ Acceptable endpoint devices
- ☑ Endpoint security violations
- ☑ Time of day (optional)
- ☑ Remediation options
- ☑ Quarantine options
- ☑ Network segmentation

Test, test, and then re-test

Before activating next-gen NAC policies across your general user base, I strongly recommend building in a test period so your IT team, and perhaps a handful of production users, can put your next-gen NAC solution through its paces.

Setting your NAC policies to monitor-only mode will allow you and your team to identify gaps, issues, exceptions, and areas to improve.

Grab as many different devices in as many different security states as possible (such as missing critical patches, having outdated AV signatures, not registered with your MDM solution) and verify that what the user sees is exactly what you were

expecting them to see. Once you've gained an additional level of comfort, it's time to move your next-gen NAC appliances into production mode.

Transitioning into Production

The time has finally come to push your next-gen NAC appliances into production. This section describes tasks you'll need to consider.

Widening your policies

Assuming you took my earlier advice by configuring "test" policies that only affect a select group of users during your testing phase, it's time to widen those policies to include your general user population. Thankfully, most next-gen NAC offerings work well with Active Directory, LDAP, and other directories, so assigning policies to groups of users should be a snap.

Gaining endpoint visibility

The first thing that new next-gen NAC administrators notice is the rich network and endpoint intelligence obtained. Three revelations that are common among new next-gen NAC administrators include:

- ☑ the actual number of devices on your network is materially larger than what you had anticipated
- ☑ the large number of unknown devices on your network is more than expected
- ☑ the actual number of non-compliance devices on your network is materially larger than what you thought

You'll be amazed at the quantity and variety of endpoint devices connecting to your network. Use this intelligence to your advantage by sharing it with your SIEM platform and granting access to your help desk and security incident response teams to be able to view this information. Having greater context for root cause analysis, investigation, and security alerts is empowering.

Monitoring and reporting

With your next-gen NAC solution in production, it's time to construct dashboards for users based on their role in the organization. Dashboards should be configured to make it easy to monitor for endpoint compliance violations.

Also, reports should be configured to satisfy the needs of both IT managers and internal and external compliance auditors. Before creating reports from scratch, consider using the templates provided by your vendor. Your solution will likely have most of the report templates you need. Work with your NAC project team to determine what reports should be run on what schedule and delivered to which groups or employees.

Extending Controls

It's never too early to plan for the future. Here are some things you should consider in the months and years following your initial next-gen NAC rollout.

Phasing enforcement

As I mentioned on more than one occasion in this book, very few organizations start out "enforcing" their next-gen NAC policies by quarantining non-compliant devices. Rather, they capture violations and exposures and alert IT staff and/or users to security concerns, or they remediate non-compliant devices directly or through third-party security systems. However, once your next-gen NAC system has been in production for a while, you may wish to consider phasing in stronger policy enforcement and automated remediation functions to enhance your company's security posture.

Expanding use cases

Earlier in this chapter, I provided a list of use cases — many of which have been discussed in this book. Organizations that chose not to implement all of these use cases on day one will certainly refine use cases and revisit additional use cases. For example, if you didn't configure your next-gen NAC appliances to detect suspicious network behavior or to trigger remediation through your systems management platform, you may choose to do so now. After all, you've already paid for this functionality, so why not take full advantage?

Advancing integrations

One of the biggest advantages of next-gen NAC solutions over their legacy predecessors is the ability to integrate with your security infrastructure in so many ways. If there are integrations that you did not take advantage of on day one — such as registering mobile devices into your MDM system — you may want to revisit such integrations in the future.

Performing health checks

Like any critical security application, your next-gen NAC product needs to be updated to address the ever-changing security landscape. As your needs and your environment evolve, so should your next-gen NAC system. Keep your NAC project team engaged in regular assessments of the project and invest in professional services with a qualified and experienced vendor or channel partner to keep your investment fine-tuned and current.

In Conclusion

Given ever-growing network complexity, accessibility demands, and threat landscape, next-gen NAC provides a useful, powerful, and extensible means to gain real-time visibility and automated control over devices connecting to and on your network. By way of expanding usability, functionality, and interoperability, NAC will surely evolve as the de facto foundation for network control, both on the enterprise network and in the cloud.

So now that you have a knack for NAC, roll up your sleeves and get busy!

Glossary

802.1X: The IEEE standard that provides a mechanism to authenticate devices or users before network resources are provisioned. Used in pre-connect NAC. (*See pre-connect NAC.*)

acceptable use policy: A set of rules and/or guidelines typically established by a company's IT department that restrict ways in which computers, applications, data, and network resources may be used.

advanced persistent threat (APT): A sophisticated, targeted cyberthreat campaign that initially exploits a system vulnerability (usually on a user device) to gain network access to compromise systems and confidential data. Also known as a targeted threat. (See *targeted threat.*)

attack surface: The sum of all exploitable security misconfigurations, violations, and unpatched system and application vulnerabilities that exist within hosts and network infrastructure devices on a given network.

bring-your-own-device (BYOD): A policy of denying, allowing, or promoting employees to bring personally owned mobile devices to the workplace and granting those devices network access to company applications and data.

captive portal: A pre-connect NAC technique that quarantines an endpoint device on a separate VLAN and then displays a special web page to authenticate the user and/or device before granting network access. (See *pre-connect NAC* and *comply to connect.*)

comply to connect: An alternative term for pre-connect NAC mode of operation. (See *pre-connect NAC.*)

continuous monitoring and mitigation: An IT security strategy that leverages the exchange of network and security intelligence to continuously monitor hosts for security exposures and mitigates them directly or through automated interaction with third-party systems.

defense-in-depth strategy: An information assurance concept in which multiple defense layers (security controls) provide redundancy in case one defense layer fails.

exploit: (*noun*) Specially crafted malware that exposes a security vulnerability or security misconfiguration to compromise a vulnerable system. (*verb*) The act of malware taking advantage of a security weaknesses in order to compromise a vulnerable system. (See *vulnerability*.)

guest management: A next-gen NAC capability that extends guest networking by incorporating guest registration, authorization, and monitoring capabilities. (See *guest networking* and *guest registration*.)

guest networking: A basic NAC capability that monitors the security posture of guest devices as they connect to the network and restricts guest access to network resources.

guest registration: An option pertaining to guest management that transitions guest devices to a captive portal where they are prompted to log in or register for access. (See *guest management* and *captive portal*.)

host-based security system (HBSS): A security agent, application, or service on a host, such as a personal firewall, anti-virus, IPS, and encryption.

hardened: An expression used to describe the process of securing a host or network infrastructure device by reducing its attack surface. (See *attack surface*.)

listen mode: A mode of next-gen NAC operation that merely records data and alerts IT to user-defined security issues and endpoint compliance violations rather than enforcing compliance by quarantining and/or remediating non-compliant hosts.

malware: Malicious software developed by cybercriminals to exploit host vulnerabilities and/or security misconfigurations to gain unauthorized system access.

network access control (NAC): A method of bolstering network and endpoint security by monitoring and/or restricting the availability of network resources to devices that comply with a pre-defined security policy.

next-generation NAC: An enterprise-class, highly scalable, agentless NAC solution deployed in hardware and virtual appliance form factors. Key capabilities include: pre- and post-connect NAC modes of operation; flexible policy management; endpoint visibility and compliance, direct and third-party remediation; and guest management. Commonly deployed as part of a continuous monitoring and mitigation strategy. (See *pre-connect NAC*, *post-connect NAC*, *guest management*, and *continuous monitoring and mitigation*.)

out-of-band: A NAC deployment method where the NAC device inspects network traffic mirrored from network TAPs and/or network switch SPAN ports – negating single point of failure and network latency risks. Opposite of inline.

patch: A vendor-supplied software update to correct one or more vulnerabilities in an operating system or application. (See *patch management*.)

patch management: A category of network security technology responsible for remotely deploying software patches to vulnerable hosts and maintaining records of patched systems. (See *patch*.)

phishing: A cyberthreat designed to acquire personal information and/or deliver malware by transmitting seemingly innocuous emails, which appear to be sent from a legitimate entity for a legitimate purpose, to large numbers of individuals. (See *malware* and *spear phishing*.)

post-connect NAC: A common mode of NAC operation that adopts an "innocent until proven guilty" approach by assessing endpoint devices for compliance with NAC policies moments after they connect to the network.

pre-connect NAC: A less-common mode of NAC operation that enforces a "guilty until proven innocent" approach to granting network access by quarantining devices on a separate VLAN until the user has properly authenticated and the device has been deemed compliant with NAC policies. (See *comply to connect*.)

sandboxing: Sophisticated network security technology designed to evaluate suspicious files in the safety of a (usually Windows-based) virtual machine (or sandbox) by attempting to detonate potential malware that bypasses traditional signature-based defenses.

security misconfiguration: An improperly configured host or network infrastructure device security setting that, if uncorrected, could lead to an unauthorized breach.

spear phishing: A form of phishing directed at small numbers of hand-selected individuals within an organization to initiate a targeted threat against that organization. (See *targeted threat* and *phishing.)*

targeted threat: An alternative term for advanced persistent threat, or APT. (See *advanced persistent threat*.)

vulnerability: An exploitable weakness (computer bug) in a host's operating system or application that can be leveraged by a cybercriminal in an effort to compromise that host. (See *exploit* and *vulnerability management*.)

vulnerability management: A category of network security technology designed to remotely identify unpatched system vulnerabilities through active and sometimes passive vulnerability scanning techniques. Also known as vulnerability assessment. (See *vulnerability*.)

waterholing: An emerging cyberthreat technique that leverages malware to compromise a website likely to be frequented by a particular target group, rather than attacking the target group directly.

zero-day threat: A cyberthreat that exploits an unknown (or unreported) operating system or application vulnerability before the associated software vendor has distributed a patch. (See *exploit*, *vulnerability,* and *patch*.)

zero-day vulnerability: An expression used to describe an operating system or application vulnerability that can be exploited by cybercriminals prior to corresponding patch availability. (See *vulnerability* and *patch*.)

forescout.com

If Muhammad Ali were a Network Security Solution He'd be ForeScout CounterACT™

Lightning quick. Knock-out punch.

Access and device diversity, dynamic exposures and advanced threats. No problem. Just as Muhammad Ali was a boxing game-changer, ForeScout has changed the game of network security. Leveraging our ControlFabric™ technology, ForeScout delivers the continuous monitoring and mitigation necessary to enable business agility without compromising defenses. Be a game changer. Check us out at forescout.com/gamechanger.

Complete Network Visibility and Control. Any Device. Anywhere.

ForeScout
BE A GAME CHANGER

Discover how next-gen NAC dramatically reduces endpoint security risks while enabling BYOD initiatives, mitigating advanced threats, and supporting continuous compliance.

Over the past decade, network access control (NAC) has matured into a powerful security platform advancing BYOD (bring your own device), threat management, and continuous monitoring and mitigation programs. Today, next-gen NAC delivers unprecedented network visibility, flexible policies, automated endpoint compliance, and limitless integration possibilities. If you think you know NAC, think again.

- Fundamentals of network access control — understand how NAC works, how it has evolved, and how organizations leverage it
- Exploring next-gen NAC technology — explore key capabilities of next-gen NAC solutions
- Achieving endpoint visibility and security — achieve extensive network visibility and close endpoint security gaps
- Regulating access and enabling BYOD — regulate access for employees, guests, and contractors and secure BYOD devices
- Mitigating advanced threats — mitigate advanced threats that bypass traditional defenses
- Aiding compliance with continuous monitoring and mitigation — fortify compliance with PCI, HIPAA, CSC, FISMA and more

About the Author

Steve Piper is an information security author, consultant, analyst, and speaker with more than 20 years of IT experience. He has authored numerous award-winning books on cyber-security, networking, and Big Data. Steve holds a CISSP security certification from ISC2 and BS and MBA degrees from George Mason University. Follow Steve on Twitter at @StevePiper or learn more at www.stevepiper.com.

CYBEREDGE PRESS

Not for resale

ISBN 978-0-9888233-4-1

9 780988 823341