NAP Enhanced to Secure Endpoints On and Off the Enterprise

EdgeGuard tested successfully for NAP interoperability at InterOp 2008

INTEROP® LABS

Written by:

Eirik Iverson
Blue Ridge Networks

BLUE RIDGE NETWORKS

Introduction

On any given day an end-user with a PC performing seemingly innocuous activities may unleash a practically undetectable malware infestation that might steal sensitive information, spread itself to others, or attack mission critical servers from a presumably trustworthy machine. Any organization where PC end-users may do one or more of the following activities must take mitigating actions against a daunting array of risks: process emails, render web pages filled with content from multiple sites, interact with an enterprise server, use a public wireless connection, communicate via an instant messenger, transfer files, play audio/video content, insert a USB thumb drive, install software not vetted, and read/write a variety of Microsoft Office documents.

EdgeGuard Enhances NAP

- *Enforces policy off-enterprise*
- *Policy Extensions*
- *Automates remediation*
- *Quarantines non-compliant off-enterprise PCs*
- *Stops malware that eludes traditional defenses*
- *Plugs data leaks*

Nothing perfectly defends such an endpoint that voluntarily admits untrustworthy data into it. However, IT personnel know that a PC with optimized client security software and hardened configuration settings is far less likely to harm the enterprise than a machine without. So organizations are increasingly determined to not only authenticate an end-user that wishes to connect with the enterprise network but also to assess the endpoint's posture before admitting it. This applies to local/fixed hosts as well as remote or mobile ones. Non-compliant hosts can be quarantined until corrective actions are completed. This act of compartmentalization can protect the enterprise from widespread harms.

Microsoft has added functionality to its new Windows Server 2008, Windows Vista, and Windows XP SP3 to facilitate compartmentlization. Microsoft calls this Microsoft Network Access Protection (NAP). Far more important than its perimeter control function, NAP is a framework that enables other vendors to seamlessly extend this functionality to address information security issues holistically.

The endpoint risk management suite from Blue Ridge Networks called EdgeGuard™ greatly enhances the value of NAP. It adds more comprehensive posture assessment and automatic remediation, extends policy enforcement and audit to off-enterprise endpoints continuously, enforces IT policies even when users operate with administrative privileges, and defends computers from malware attacks that traditional defenses miss.

One Compromised PC Poses Serious Risks to Entire Enterprise

Enterprise organizations possess much information that an underworld of organized crime considers worth stealing. These professional hackers are targeting organizations and attacking them where they are most vulnerable, which changes. The hackers had been focused on enterprise servers. However, far more server vulnerabilities can be exploited from the same local area network than from the Internet. For this and other reasons, hackers have targeted end-user PCs, or endpoints, to use as launching platforms to attack servers from within. Consequently, enterprises grew concerned about reducing the exposure of their mission critical servers to potentially compromised PCs.

Compromised PCs attack enterprise servers from within, so at-risk PCs should be quarantined from enterprise assets

However, the hackers found an awful lot of valuable information on these PCs too. Typical end-users within typical organizations load vast amounts of sensitive information into endpoints. Hackers also acquire end-user credentials, both personal and corporate.

Client PCs can be far more exposed to threats than servers. Mobile endpoints venture outside the perimeter of enterprise defenses. They often use untrusted networks such as wireless or hotel broadband. Client PCs are also more difficult to secure because they are considerably more diverse than server machines in terms of software applications and configuration settings. The SANS TOP 20 report on enterprise risks from November 2007 starkly warns IT organizations that the vulnerable software applications and configuration settings of their endpoints are being aggressively targeted. (http://www.sans.org/top20/2007/top20.pdf)

Today's malware can be undetectable, prevention is critical

Hackers exploit programming mistakes in client applications or operating system components to gain control of them. After hijacking one, the hacker then attempts to infest the entire endpoint in a persistent manner. They increasingly use rootkit enhanced malware to operate undetected indefinitely because they fool traditional client security tools.

With one endpoint infected, the hackers seek to

- systematically steal information from that endpoint
- compromise other endpoints similarly
- compromise mission critical servers, or at least eavesdrop on all communications with them.

If there doesn't appear to be anything of further value to steal, the compromised endpoint might be made into a botnet node. A botnet is a network of centrally controlled computers that perform various malicious activities (e.g., distributed denial of service attacks, spam distribution, targeted malware attacks, etc.) without the knowledge of the computers' owners.

Malware Infestation Prevention and Anti-Proliferation are Essential

IT organizations must focus on practical preventative measures and compartmentalization to avoid malware outbreaks that steal sensitive data and disrupt productive operations. Compartmentalization serves not only to contain outbreaks when practical preventative measures fail but can also serve to ensure that endpoints that do not adhere to these preventative measures are denied access to desired services until compliance is restored. Generally a non-compliant device should be quarantined such that it can be served by remediation resources and cannot access mission critical servers.

Preventative measures for PCs must be enforced continuously, on and off the enterprise network

Practical preventative measures include

- ensuring that client security software is installed, up to date, currently running, and has been running as scheduled (e.g., periodic full scans by anti-virus agent, disc encryption engaged at all times, etc.)

- restricting applications that are typically targeted by hackers from modifying critical areas
- disabling promiscuous or risky configuration settings
- implementing operating system and client software patches
- preventing undesirable (e.g,. peer-to-peer, networked games, etc.) or vulnerable software from running
- blocking executables from launching from removable media (e.g., thumb drive) or network drives
- deploying workarounds for vulnerable software

All PCs are at-risk, fixed and mobile

Many information security periodicals have mistakenly focused almost exclusively on conducting posture assessments on laptop computers returning to the enterprise. Most of them have appended the need to conduct post-admission assessments as well to ensure that endpoints continue to employ practical preventative measures after joining the LAN. Unfortunately, they are missing two obvious points. First, all endpoints must be compliant with preventative measures policies. The endpoint in a cubicle is interacting with the world and hence it is exposed to threats too. It can become compromised and serve as a launching point into the enterprise. So, all endpoints must implement preventative measures to access the LAN. Second, pre-admission and post-admission posture assessments equate to part-time enforcement; full-time compliance is mandatory because malware infestations can be undetectable. In short, preventative measures must be implemented on all endpoints, on and off the enterprise network, continuously. Endpoints that do not should be quarantined.

Isolate Guest PCs from Enterprise Assets

Enterprise IT personnel can seldom force guests to alter their endpoints. Fortunately, most contingent workers (e.g., contractors, partners, etc.) usually require Internet access only.

NAP limits enterprise access to authorized guest machines with preventative measures implemented

However, some guest machines must access server resources within the enterprise. Some organizations can afford to deploy mirrored servers (i.e., servers that host the same content as the servers that enterprise employees access) to compartmentalize the guest machines. This approach does nothing to reduce the risks that sensitive information may be stolen from these guest machines because it does not ensure that practical preventative measures are implemented. This leaves a difficult question. How does an enterprise perform a non-invasive yet substantial posture assessment of guest machines and offer automatic remediation of non-compliance?

Microsoft Network Access Protection Quarantines At-Risk PCs

Microsoft NAP leverages existing network infrastructure and open standards to isolate non-compliant endpoints from critical assets in the enterprise.

Its operation is simple. When an endpoint from organization A attempts to

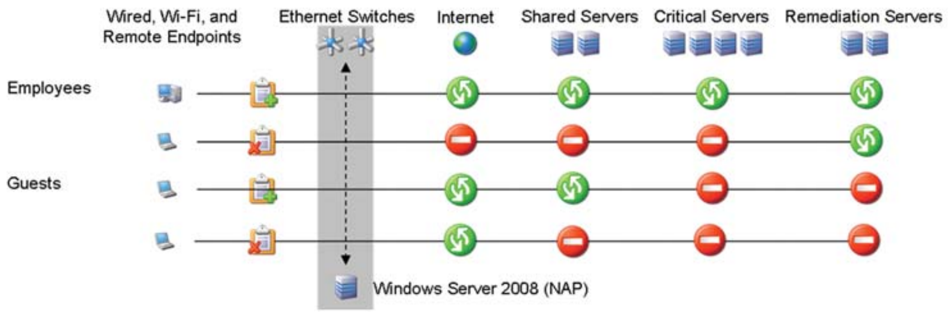

Figure 1: Microsoft NAP ensures that unauthorized and non-compliant hosts are properly compartmentalized from enterprise assets.

NAP scales well. Microsoft's deployment for over 120,000 PCs worldwide is served by 4 Windows Server 2008 hosts

connect to a NAP regulated LAN of organization B, the local Ethernet switch in organization B's LAN relays the admission request from the client PC to Windows Server 2008. A series of messages are exchanged via the Ethernet switch between the client PC and Windows Server 2008 that assess the policy compliance of the client PC. Organization B can either grant the endpoint full, partial (i.e., quarantine), or no admission according to what from these health check messages. If this laptop lacked the client component to interact with NAP, the Ethernet switch would place the client PC in a limited access subnet or VLAN by default, which typically allows guest Internet access.

Microsoft NAP works with existing enterprise Ethernet switches and client-side health checks (i.e., posture assessment) components included in all Windows XP SP3 and Windows Vista operating systems. NAP posture assessments do not require ActiveX to be enabled or for PC's to operate with administrative privileges the first time they enter a NAP network. With all of the intelligence located in the client components and Windows Server 2008, most organizations will not have to upgrade their Ethernet switches as may be the case with other infrastructure-based admission control frameworks. This admission control system accommodates managed and unmanaged PCs regardless of whether they are configured as workstation, domain, or another organization's domain.

NAP works with existing Ethernet switches to regulate enterprise admission of PCs

Microsoft NAP performs basic health checks on endpoints that logically touch the enterprise network. It does not enforce policies on endpoints off the enterprise. Fortunately, NAP is extensible so that other tools can seamlessly expand the breadth and depth of endpoint policies for client PCs on and off the enterprise network.

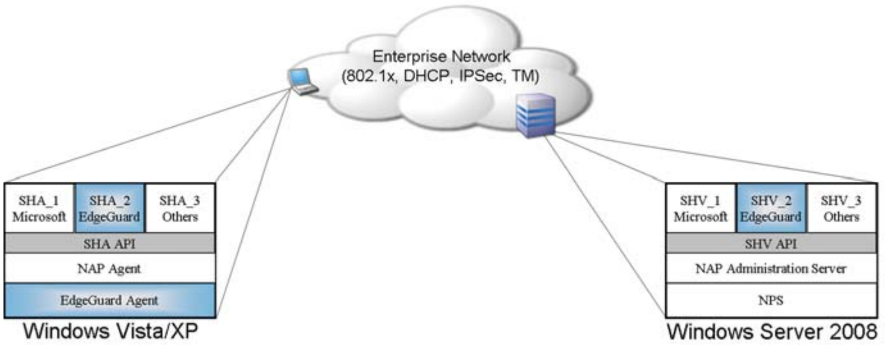

Figure 2: EdgeGuard seamlessly integrates into the Microsoft NAP framework, adding considerable policy breadth and more.

EdgeGuard Adds Controls for Off-enterprise Endpoints

Enforce endpoint policies anywhere, anytime.

Today's sophisticated malware can evade detection by the tools that administrators typically use. Consequently, practical preventative measures must be in place continuously, not just when a PC connects with the enterprise. Enterprise endpoints are most at risk of infection when they are off the enterprise network where they are on their own. Their defenses must be maximized.

EdgeGuard can monitor and enforce such endpoint policies on and off the enterprise at all times. It can automatically remedy most non-compliance issues such as re-enabling a personal firewall or triggering an anti-virus signature update. For non-compliance issues that require something from a vendor specific resource, an anti-virus agent requires a software update for example, EdgeGuard can either remind the end-user that action must be taken or it can impose a smart quarantine on the endpoint that limits network activity until compliance is achieved.

The smart quarantine can be enforced wherever the endpoint is located. It either limits network communications to/from remediation resources only or it can block communications entirely. This can prevent a non-compliant endpoint, which is by definition a vulnerable one, from becoming infected with undetectable malware.

EdgeGuard scales to organizations of all sizes and locations

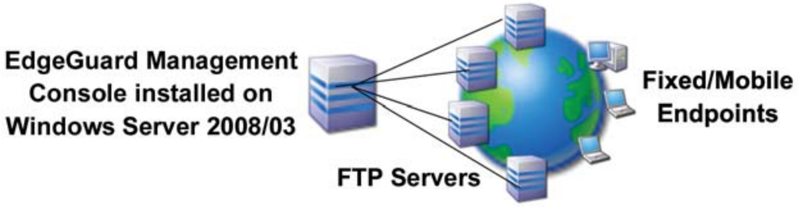
EdgeGuard Management Console installed on Windows Server 2008/03
FTP Servers
Fixed/Mobile Endpoints

Figure 3: Generic FTP servers exchange policy/logs in near real-time between IT and endpoints everywhere. All is encrypted and digitally signed to ensure privacy and accountability.

EdgeGuard Expands Scope of NAP Endpoint Policies

EdgeGuard allows a NAP enabled network to base endpoint admission on many additional criteria, see table below. Furthermore, EdgeGuard extends these policies off the enterprise and can vary them per situation (e.g., location). Situation based awareness means that policy might, for example, allow computer games when off enterprise but block them otherwise.

EdgeGuard Policy Extensions	Benefit
Render applications “unstartable”	Prevent usage of risky software
Render applications “unstoppable”	Ensure that monitoring or security software runs
Location aware application control	Start/stop applications that must or must not run in specific locations (e.g., prevent instant messenger while on enterprise allow when off)
Block executables launch from USB devices	Prevent malware infestations from untrustworthy sources
Block all write operations to all USB devices	Prevent sensitive data leaks
Assess or enforce configuration settings	Disable promiscuous settings that pose risks to enterprise (e.g., auto-run from peripherals, automatic wireless features, Internet Explorer settings, etc.)
Implement workarounds to hosts everywhere	Push out temporary fixes to software vulnerabilities until vendor patches are available
Smart Quarantine	Reduce exposure of non-compliant (i.e., vulnerable) off-enterprise PCs to potential threats
File Lock	Render application preference files unalterable to control their settings
Block Malware Infestations	Stops what anti-virus/spyware misses

EdgeGuard adds an administrator "Panic Button" to temporarily block enterprise access to all PCs in emergencies

EdgeGuard Policies Supersede End-user Administrative Privileges

EdgeGuard does not make deploying end-users with administrative privileges a “best practice”. Instead, EdgeGuard greatly diminishes the risks. First, EdgeGuard ensures that the practical preventative policies defined by IT personnel cannot be circumvented by end-users with administrative privileges. This means that configuration settings and application usage can be monitored and controlled. Second, EdgeGuard prevents hackers from using applications with administrative privilegeswith administrative privileges to install malware into the endpoint.

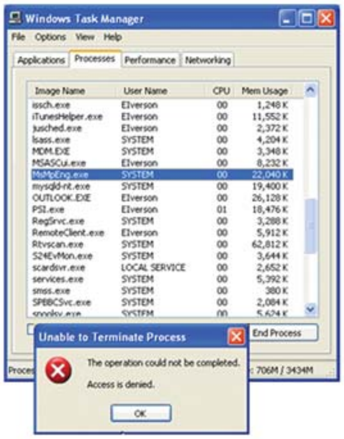

Image Name	User Name	CPU	Mem Usage
issch.exe	Elverson	00	1,248 K
iTunesHelper.exe	Elverson	00	11,552 K
jusched.exe	Elverson	00	2,372 K
lsass.exe	SYSTEM	00	4,204 K
MDM.EXE	SYSTEM	00	3,348 K
MSASCui.exe	Elverson	00	8,232 K
MsMpEng.exe	SYSTEM	00	22,040 K
mysqld-nt.exe	SYSTEM	00	19,400 K
OUTLOOK.EXE	Elverson	00	26,128 K
PSI.exe	Elverson	01	18,476 K
RegSrvc.exe	SYSTEM	00	3,288 K
RemoteClient.exe	Elverson	00	5,912 K
Rtvscan.exe	SYSTEM	00	62,812 K
S24EvMon.exe	SYSTEM	00	3,644 K
scardsvr.exe	LOCAL SERVICE	00	2,652 K
services.exe	SYSTEM	00	5,392 K
smss.exe	SYSTEM	00	380 K
SPBBCSvc.exe	SYSTEM	00	2,084 K
spoolsv.exe	SYSTEM	00	5,624 K

The operation could not be completed.

Access is denied.

Proces

: 706M / 3434M

Figure 5: User with administrative privileges could not terminate security tool

Monitor and control PCs operated by users with administrative privileges

Combining EdgeGuard and NAP Reduces Enterprise Risks

Microsoft NAP adds security policy compliance checks to the network logins for both enterprise and guest PCs. Non-enterprise and/or non-compliant PCs can be compartmentalized. Endpoints without a known, legitimate need to access mission critical servers, such as a visitor, may be limited to Internet access. Non-compliant hosts may be segregated into remediation zones. This limits the spread of malware and the exposure of mission critical enterprise assets without the cost and shortcomings of dedicated NAC appliances.

EdgeGuard expands the breadth and depth of security policies that can be monitored, assessed, enforced, and automatically remediated on enterprise endpoints. It even does so when end-users operate PCs with administrative privileges. Deploying more practical preventative endpoint policies reduces the probability of security breaches. Extending such policies to endpoints off the enterprise for continuous monitoring and enforcement reduces security risks even more. EdgeGuard yet further reduces enterprise risks by defending endpoints against attacks from unknown malware that evades traditional defenses.

About Blue Ridge Networks

Blue Ridge Networks is a respected and leading provider of unparalleled security solutions for government and private industry. The company's products have a proven ability to exploit the advantages of the internet and are relied upon by hundreds of large enterprises. Blue Ridge solutions represent high standards of security strength as tested and certified by independent organizations. The company's products have earned: FIPS 140-2, Common Criteria, Joint Interoperability Test Command (JITC), ARMY TIC, and Department of Defense SPOCK certifications. Additionally, they comply with important HIPAA, HSPD-12, and PCI regulations. Information about the company's products and managed services can be found by visiting www.blueridgenetworks.com.