



WHITE PAPER

THE CASE FOR AGENT-BASED NAC SOLUTIONS

Written by:

Eirik Iverson
Blue Ridge Networks



EXECUTIVE SUMMARY—ESTABLISH CONTROLS AT THE ENDPOINT ITSELF

Endpoints are essential to enterprise success. Endpoints must enable their end-users to be productive at anytime from anywhere communicating with anything that adds value. This exposes them outside the enterprise fortress where they can be targeted, making endpoints part of the edge of today’s virtual enterprise perimeter.

Therefore, the enterprise must achieve greater controls where these risks lie, at the endpoint itself, at all times, in all situations, and at all places, when within the enterprise and when off-enterprise. IT organizations can achieve greater operational economies, regulatory compliance, IT governance, and security without sacrificing end-user productivity by centrally managing a robust endpoint client software agent within the endpoint.

Today’s enterprise needs these greater endpoint controls because it operates in a fiercely demanding landscape where its data and information are its most critical assets. Security experts estimate that roughly 90% of sensitive data/information is in an unstructured form, and that much of it resides within emails and Microsoft Office documents on endpoints. A relatively new underworld of organized crime realizes billions of dollars in profits annually by surreptitiously acquiring enterprise information assets. In some cases, they can even profit by hindering the enterprise’s ability to operate.

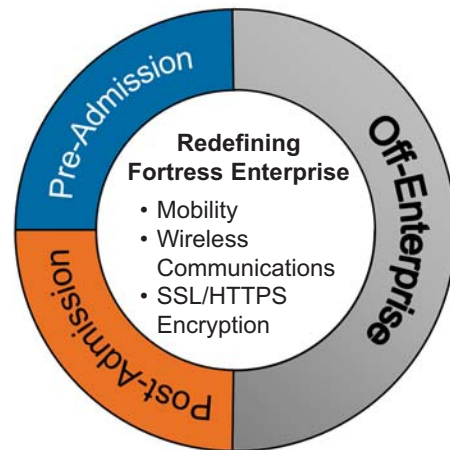
The enterprise endpoint increasingly represents the best target of opportunity to acquire information assets on it or to use it as a platform to reach other assets within the enterprise fortress. The information security industry responded to the underworld’s threat, in part, with the birth of network admission control (NAC).

But, its definition continues to evolve as the scope of the challenge is better understood and as outside forces alter the landscape with regulatory mandates from governments, industry associations, insurance companies, and the courts because of the harm to ordinary citizens from the underworld’s success. In parallel, organizations seeing operational benefits from first generation NAC implementations are looking at expanding endpoint policy enforcement beyond NAC and regulatory compliance to overall IT governance.

ENDPOINTS FORM THE EDGE OF TODAY’S VIRTUAL ENTERPRISE PERIMETER

Mobility, wireless communications, and the increasing use of SSL/HTTPS within the enterprise require that security controls no longer reside on appliances alone but be deployed on the endpoints themselves.

Approximately 40% to 50% of enterprise endpoints are mobile. End-users take them home and on the road where they operate outside the protections of perimeter defenses. When these endpoints return, they might bear crimeware seeking enterprise information.



The original NAC concept was focused on reducing risks to critical, intranet resources (i.e., maximizing uptime) from returning endpoints by admitting only those with a healthy posture. This pre-admission posture assessment blocks endpoints that are non-compliant with security policies designed to prevent malware infection. Among other things, such policies typically require that endpoints operate up-to-date anti-virus, anti-spyware, and personal firewall client software and that they have implemented the latest security patches to the operating system and select applications. However, a pre-admission posture check assesses the state of the endpoint at the moment, not for the last month, for example. Furthermore, pre-admission posture assessment-only implementations impose productivity penalties as end-user must await conclusion of a scan. This particularly impacts sales personnel that frequently need to get on and off the enterprise quickly.

This part-time policy enforcement means that endpoints can operate in a non-compliant or vulnerable manner at

all other times. Sophisticated malware infestations using rootkit technology can be practically invisible to all mainstream means for detection. Consequently, it is essential that endpoint security policies be enforced continuously to minimize the chances of malware establishing a beachhead.

Wireless communications in the office likewise exposes endpoints. Inadequate Wi-Fi security effectively left the drawbridge open to TJX's enterprise fortress. Hackers can spoof IP addresses and Ethernet MACs, bypassing fixed security appliances entirely and sending malware directly to participating Wi-Fi endpoints. The enterprise Wi-Fi access points can be spoofed also, effectively making endpoints off-enterprise.

Even when endpoints fall within the domain of fixed perimeter defenses, their ability to detect malware infestations post-admission are increasingly circumvented by end-users employing legitimate applications that encrypt their communications. Even without encryption, sophisticated malware is embedding its communications within legitimate endpoint transmissions. For example, malware transmissions may hide within outbound instant messenger traffic.

Endpoint controls must reside on the endpoint to enforce policies when off-enterprise, using wireless communications, and/or to serve as a tripwire within the endpoint to detect malware indicators despite malware usage of encryption or steganography.

CONTINUOUS, PREVENTION-FOCUSED ENDPOINT POLICY ENFORCEMENT IS REQUIRED

| Continuity of Policy Enforcement | | | |
|----------------------------------|---|----------------|----------------|
| Off-Enterprise | Pre-Admission | Post-Admission | Off-Enterprise |
| | NAC Appliance | | |
| | Combined NAC Intrusion Prevention Appliance (s) | | |
| Full-time NAC Agent | | | |

Off-enterprise, only a persistent client agent can enforce endpoint security policies continuously: pre-admission, post-admission, and off-enterprise. NAC appliances only enforce policies when the endpoint is logically connected to the enterprise. Agents can enforce policies for mobile endpoints when they are off-enterprise, physically or

wirelessly, reducing the risk of their returning compromised. Sophisticated policy enforcement agents can even prevent malware from hijacking legitimate endpoint communications or sending out encrypted transmissions.

CONTINUOUS AGENT-BASED ENFORCEMENT MINIMIZES END-USER INCONVENIENCE

Pre-admission offerings scan a host for policy compliance when an end-user attempts to gain intranet admission for the endpoint. These scans can be very inconvenient for end-users. The more extensive the rule set from the policies the longer the compliance scan delays the end-user. A policy enforcement agent that continuously enforces compliance completely eliminates admission delays.

NAC'S SCOPE BROADENING: MORE DEMANDING POLICY ENFORCEMENT

Several drivers are expanding the scope of NAC into a more general-purpose endpoint policy enforcement paradigm. Governments and industry associations are mandating regulations that the enterprise must adhere to or face significant financial penalties as well as to validate with credible audit reports.

Information security personnel are expanding the scope of policies to include endpoint hardening rules that further narrow the exposure of endpoints by regulating configuration settings. Similarly, they are specifying application control policies that block execution of unauthorized applications and services on endpoints. IT operations personnel, considering the life-cycle perspective of managing endpoints, are seeking controls that enhance IT governance in general. Industry pundits predict that NAC agents will become an essential, integral element of endpoint life-cycle management.

Most market research firms report the following business drivers influencing NAC implementation decisions:

- Safeguard information assets
- Keep critical servers running
- Reduce endpoint IT operations costs
- Comply with regulatory requirements

Relatively new drivers are adding to regulatory compliance mandates including

- Demands from customers and business partners
- Business licensing requirements
- Insurance requirements.

The greater breadth and depth of policies and controls regarding endpoints demands agent-based systems to ensure continuous enforcement without the inconvenient admission delays of pre-admission offerings made worse with a larger rule set to enforce.

AGENTS PROVIDE THE MOST BREADTH AND DEPTH IN POLICY ENFORCEMENT



Posture assessment requires read privileges on the endpoint in question. A truly clientless solution does so via an external entity with administrator credentials sending remote function calls (RFC) into the endpoint. Such systems can only scan for compliance criteria supported by an RFC, which are limited. Some of these systems nudge

beyond this limitation by drawing inferences, sometimes yielding false positives.

Dissolvable agents that employ Javascript can do a little more, and those that use ActiveX can do even more. However, ActiveX was not designed for this purpose and hence it too is limited. Dissolvable agents can do their most when the end-user operates the endpoint in administrator mode, but this adds risk.

Agent-based solutions bear none of these limits and do not require endpoints to operate in administrator mode. They also facilitate more comprehensive auto-remediation and compliance reporting.

SOME DISSOLVABLE CLIENTS NEVER GO AWAY

Some vendors extend the scope of their dissolvable clients by actually installing persistent client software via

ActiveX. The communications between the dissolvable and persistent agents of these offerings usually rely on ActiveX, which limits their ability to exchange information and causes reliability problems.

Such offerings should no longer be characterized as clientless because they truly alter the image of the endpoint. Any persistent client software can interfere with the proper operation of an endpoint. Software that reads and writes to all parts of an endpoint can create conflicts with other components. Consequently, best practice IT organizations regression test all client software prior to deployment, including the persistent agents installed by dissolvable agents.

**“EMBEDDED NAC”:
NAG, NAP, TNC, NEA**

There are several frameworks in development that integrate posture assessments with the network itself. Each element, such as an Ethernet switch, will enforce admission control over endpoints requesting intranet entry, blocking non-compliant hosts. Eventually, these frameworks will meld and facilitate interoperability among all vendor network elements within the intranet. Meanwhile, an agent-based solution can implement NAC capabilities today without impacting the network elements or topology. The agents can continue to fulfill the posture assessment role when the enterprise is ready to implement “embedded NAC”.

Agent-based systems should substantially enhance “embedded NAC” because it can provide more detailed posture assessments and enforce policies when endpoints are off-enterprise. Dedicated NAC appliances, however, can certainly continue to add the same value they do today but will eventually become redundant and unnecessary.

AGENTS OFFER NETWORK INFRASTRUCTURE AND PATH INDEPENDENCE

The Aberdeen Group reported that best in class organizations cited “integration with current network infrastructure” and “network infrastructure independent” were two of the ten most desired NAC features, second and sixth, respectively (“Endpoint Security Strategies Part I, The Network Access Control Benchmark”, November 2006) . Similarly, they found organizations cited failure to deliver these features as two of the most frequent reasons for rejecting a NAC solution.

Deployment of policy enforcement agent systems that use driver level personal firewall technology to quarantine non-compliant endpoints requires no network redesign or network infrastructure upgrades. Such solutions serve as an overlay, working within homogenous or heterogeneous network infrastructure environments. Without reliance on VLAN tagging, IT personnel need not define and propagate VLAN definitions to all network nodes. These agent solutions also spare them from re-designing their intranet such that an enforcement mechanism guards every path between endpoints and intranet servers. This can be particularly beneficial in highly distributed organizations with many different LANs comprising their intranet. Similarly, an agent using driver level NAC agent technology does not rely on the mistake-free implementation of IP subnets throughout the intranet to compartmentalize different assets. It is far more tolerant, flexible, and secure.

Infrastructure additions or upgrades do not require network administrators to confirm that all paths remain covered. Wherever endpoints are located, policy enforcement agents effectively virtualize the enterprise perimeter, simplifying operations immensely.

AGENTS SCALE GRACEFULLY WITH THE ENTERPRISE

Doubling the number of employees in an organization bears an incremental cost increase that is a fraction to that of an inline NAC appliance implementation. Enough inline appliances to handle the additional bandwidth must be added. Plus, high availability requires that at least two appliances reside on each path between end-users and intranet servers. Out-of-band NAC appliances scale more favorably than inline ones but they are still cost prohibitive compared with agent-based solutions, particularly for highly distributed organizations.

POLICY ENFORCEMENT AGENTS: NO HIDDEN SECURITY RISKS

Once installed on an endpoint along with other critical client security software, policy enforcement agents operate as a service. They do not require an end-user to operate their endpoint in administrator mode as do dissolvable agents (e.g., ActiveX, Javascript). Regardless of user mode, the persistent agent can read and write anywhere within the endpoint. This also applies to software updates for the agent. Dissolvable agents are dynamically installed, however. While they

may persist within a browser environment after installation, updates require administrator privileges. These applets only operate when the browser operates. So policy enforcement ends when the end-user shuts down the browser, or uses another one perhaps. Thus, dissolvable agents cannot be counted on for off-enterprise operations. Fortunately, within the enterprise, NAC appliances can quarantine an endpoint post-admission when the end-user shuts down the browser. That can, however, place the endpoint into harms way, a dirty VLAN.

Persistent agent posture assessments do not require hashed administrator passwords to pass through untrustworthy networks, as do truly clientless NAC offerings. Hashed administrator passwords can be intercepted and cracked, which can completely compromise all endpoints that employ that same hashed administrator password. Compromised endpoints then become remote platforms for hackers to attack the enterprise from within.

MYTH: NAC APPLIANCE SYSTEMS ARE LESS SUSCEPTIBLE TO MALWARE THAN AGENTS

Appliances themselves are unlikely to be corrupted. They do not operate within a vacuum though. They rely on posture assessments that originate from the endpoint. Several security experts have demonstrated at Black Hat and other conferences just how the dissolvable applets or truly clientless posture assessments can be compromised. Posture assessments from dissolvable applets, RFC endpoint queries from an external inquisitor (i.e., "truly clientless posture assessments"), and persistent agents rely on the integrity of some software within the endpoint. Thus, they are all vulnerable to a potential compromise.

A persistent agent can feature numerous redundant integrity mechanisms, including hardware-based trust systems, to better resist malware as well as to detect a compromise, reporting this and then disabling all network drivers so neither it nor the malware can do harm to other enterprise assets. Dissolvable agents must be lightweight, however, bearing fewer, less sophisticated safeguards confined to the browser environment. Consequently, NAC appliance offerings are more vulnerable to malware than persistent policy enforcement agents.

AGENTS DELIVER BETTER TCO AND SECURITY

Today's enterprise has something that a new underworld of organized crime wants: information that translates into big money. The relatively weak underbelly of the enterprise is the endpoint. It not only contains valuable information itself but can serve as a proxy from which to strike from within. Case studies show that the enterprise can dramatically reduce malware outbreaks and hence operational costs by implementing a NAC solution that mitigates the risks to the endpoint. Yet, most offerings provide only part-time policy enforcement, leaving a large window of opportunity open when endpoints are off-enterprise.

Agent-based policy enforcement can implement more comprehensive policies without the scanning delays of other approaches that annoy end-users and disrupt their productivity. More comprehensive policies equate to a lower expected value of security breaches and lower operational costs from fewer help desk trouble tickets, automated regulatory compliance and reporting, and simplified IT governance. Agent-based enforcement is in fact more secure than appliance based enforcement. Greater security at less up front and operational cost translates into long term cost savings.

Client software agents become the dynamic edge of the virtual enterprise perimeter, saving IT operations costs from network infrastructure integration, redesign, and capital costs. They will continue to add value to the enterprise after "embedded NAC" matures because they represent the only practical means to enforce the broad and deep endpoint policy enforcement that the industry is beginning to realize is required. Agents also scale more economically than alternatives, growing and adapting to enterprise changes.

One legitimate criticism of agent-based systems remains, however. Any software on an endpoint can be compromised. So, how can an enterprise be assured that their agents would not be corrupted and turned against them. That answer lies in the use of hardware-based trust mechanisms featured in today's personal computers but seldom utilized. We will explain this in subsequent papers.

BLUE RIDGE/ SECURE EDGEGUARD™: ENDPOINT RISK MANAGEMENT

Deep Policy Enforcement

Unsurpassed Security

Control for Fixed and Mobile Endpoints.

EdgeGuard reduces operational costs from malware, hackers, and end-users. The solution offers deep policy enforcement, an asset for meeting urgent compliance mandates. With this advanced solution, enterprises can wield the combined power of individual endpoint protections in a single system. EdgeGuard employs TPM-fortified policy enforcement agents, allowing unsurpassed security at fixed and mobile endpoints to regain control of these resources that contain and work with enterprise information.

Any software on an endpoint can be compromised... the answer lies in the use of hardware-based trust mechanisms featured in today's personal computers but seldom utilized.

**Any software on an endpoint
can be compromised... the
answer lies in the use of
hardware-based trust
mechanisms featured in
today's personal computers
but seldom utilized.**