

# Avenda / Microsoft NAP Agent Comparison

## Enhanced Health Checks



Avenda’s OnGuard solution leverages and extends the benefits gained from deploying Microsoft’s Network Access Protection (NAP) with clients running Microsoft, Apple and Linux operating systems. The Avenda solution provides incremental value that allows organizations to easily deploy NAP in heterogeneous operating system environments which takes advantage of NAP’s robust endpoint health policy architecture. Avenda’s solution also provides the ability to create fine-grained policies that deliver more than just verifying the existence of endpoint security applications.

The use of Avenda’s OnGuard solution also lets organizations use the policy server resources they have already deployed. All three functions of Windows Server® 2008 Network Policy Server (NPS); RADIUS server, RADIUS proxy, and NAP health policy server are leveraged across all access methods, wireless, wired and VPNs if desired. A secondary policy server is not required when using Avenda’s solution. Avenda’s eTIPS Identity-based policy server should be used when extending NAP health checks to Apple Mac OS X endpoints.

Security deployments that require NAP support for manageable endpoints (laptops, desktops, etc.) and unmanageable endpoints (smartphones, printers, etc) that belong to guests and other visitors can also use Avenda’s eTIPS Policy Server to support this business case as well.

### Extended NAP Capabilities

The attached comparison highlights the capabilities of Microsoft’s SHV with those of OnGuard. Both perform some basic checks, but more granular checks can be completed with the use of the Avenda solution.

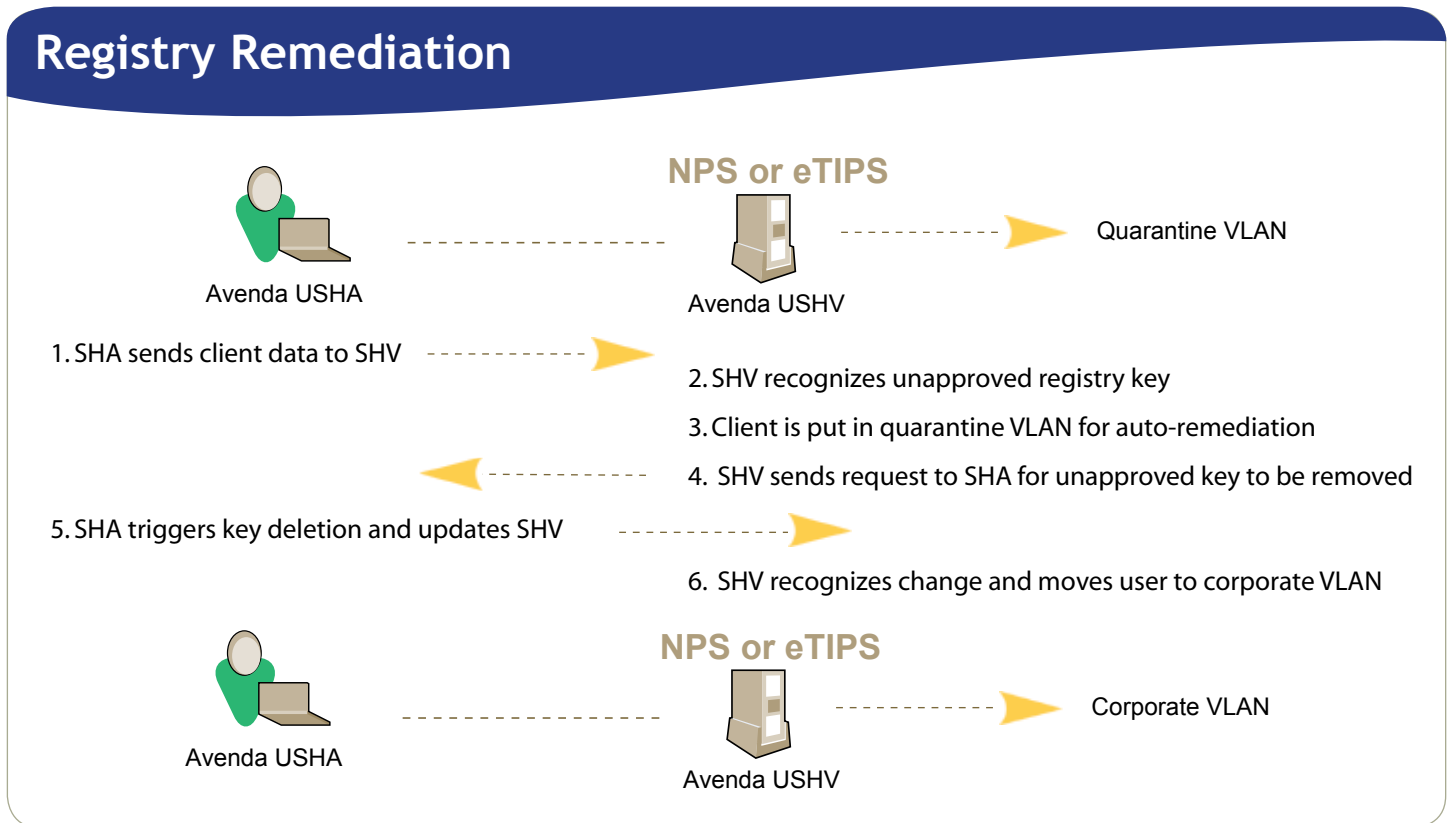
- Verifying if specific services or P2P applications are “running or stopped” is available with the OnGuard solution
- Auto-remediation or user initiated remediation can be used to satisfy security policies. For example, a registry check can be used to disallow unapproved applications. If a registry key for an instant message (IM) application that is not allowed is found, full network access is not given until remediation occurs.

Agent Comparison	
	MICROSOFT    AVENDA
<b>STANDARD CHECKS:</b>	
<b>FIREWALL</b>	Y            Y
<b>ANTI-VIRUS</b>	Y            Y
<b>ANTI-SPYWARE</b>	Y            Y
<b>AUTO UPDATES</b>	Y            Y
<b>AUTO-REMEDATION</b>	FW ONLY    Y
<b>SERVICES RUNNING</b>	Y
<b>REGISTRY CHECKS</b>	Y
<b>FIREWALL - LATEST VERSION</b>	Y
<b>A/V - VER, DAT &amp; ENGINE FILES</b>	Y
<b>A/S - VER, DAT &amp; ENGINE FILES</b>	Y
<b>A/V, A/S - LATEST VERSIONS</b>	Y
<b>PATCH MANAGEMENT</b>	Y
<b>PEER TO PEER APP DETECTION</b>	Y
<b>PROCESS CHECKS</b>	Y

## Patch Management

The Avenda OnGuard solution can also be used to ensure that clients/endpoints are also running approved patch management applications before gaining access to the network.

## Remediation Example - Unapproved Registry Key



## Conclusion

The Avenda OnGuard solution provide a growth path that extends the capabilities of Microsoft's NAP framework to securely protect your network from unauthorized users and endpoints. OnGuards standard and extended checks can be used with Microsoft NPS or with Avenda's eTIPS policy server. The choice is up to the customer. In order to support mixed operating system environments, and managed and unmanaged endpoint requirements, eTIPS is a simple addition to any existing NAP solution.



Avenda Systems, Inc.  
3255 Scott Blvd., Bldg. 2, Suite 102  
Santa Clara, California 95054  
408.748.0902 x123  
info@avendasys.com  
www.avendasys.com



## Next Steps

Build identity-based network security through user and endpoint trust using the NAP framework. Visit [www.avendasys.com](http://www.avendasys.com) for a free 30-day OnGuard trial or sales assistance.