

Napera Networks Messaging and FAQ 2008

What is Napera Networks?	Napera Networks is a network security company focused on delivering cost-effective and high-performing products and online services to small and medium-sized enterprises.
What does Napera do?	Napera delivers the power of network access control to small and medium sized enterprises.
	Napera's switch-based appliance allows organizations to centrally manage Windows Security Center enabled computers utilizing Microsoft NAP (Network Access Protection) architecture.
	Napera helps IT staff take back control of the computers and users accessing the network while maintaining optimal network performance and user productivity.
What is the Napera solution?	Napera offers a line of integrated network access control products and Web services designed for small and medium sized enterprises that allows only healthy computers and authorized users to access the network.
	Napera provides a unified solution that ensures computers are healthy and up-to-date, identity is enforced and network access is controlled, based on security policies.
	Napera's network access control portfolio includes the Napera N24 and N24S appliance series and the MyNapera.com online management service for logging, reporting and alerts.
How does the solution work?	Napera solutions make it easy to control the computers and users accessing your network, so you can confidently allow wireless networking, guest access, and worker mobility while keeping your network safe and secure.
	Napera NAC appliances and online management services make sure only healthy computers access the network by: <ul style="list-style-type: none"> • Identifying every computer and IP address on the network • Providing real-time visibility into the health state of every computer • Enforcing the identity of users and computers before allowing access • Enforcing health standards and security policies before allowing access • Stopping the spread of malware or other threats across the network • Assigning non-compliant computers into quarantine or remediation • Controlling guest access to the Internet or pre-assigned printers
So what does this mean?	Napera is the only company delivering network access control solutions that are purpose-built for the SME but with enterprise-class performance and security.
	Companies need Napera because of today's mobile computing environment, where laptops move in and out of the network and users don't always keep their systems up to date or protected.
	Security and management solutions alone are not enough to keep your networks safe, because unhealthy, non-compliant computers are still able to access your network.
	Napera has solved the challenge around complexity, high cost and length of deployment, with solutions that are affordable and easy to deploy and manage and give IT professionals immediate control of all computers accessing the network.

Napera Networks Messaging and FAQ 2008

<p>What is the Napera N24?</p>	<p>A switch based appliance allowing organizations to centrally manage Windows Security Center enabled computers utilizing NAP (Network Access Protection) architecture.</p>
	<p>The Napera N24 includes an integrated Web-based service that provides reporting, logging, and alerting services.</p>
	<p>The Napera N24 keeps your network protected from unknown threats and malicious users by enforcing and controlling computer health, user identity, and network access.</p>
<p>How is Napera positioned in the NAC market?</p>	<p>Napera’s products and services are designed for small and medium-sized enterprises and bring the full power of network access control combined with ease of use and management, plug-and-play appliance functionality, online management services, and affordability.</p>
	<p>1. Designed for SME</p> <ul style="list-style-type: none"> • Single solution for guest access, employees on site and remote, identity and health enforcement • Easy to use and manage • Affordable: appliance and service initial investment of under \$4k • Interoperable: works with all wireless and wired networks, anti-malware solutions, Windows and Macintosh computers, and leverages Microsoft NAP. <p>2. Plug & Play Appliance</p> <ul style="list-style-type: none"> • Deploys like a switch • Configures in ten minutes • Easily expandable - scaling as the business requirements increase • Pre-configured policies for computer health standards • No desktop agents required <p>3. Software as a Service</p> <ul style="list-style-type: none"> • My Napera.com management service • Fast and easy logging, reporting, and alerting • Remote management • No local servers needed
	<p>Napera has the 4 C’s of network access control:</p> <ol style="list-style-type: none"> 1. Confirm user and computer Identity 2. Check computer health 3. Control access 4. Continue monitoring
<p>Who is the ideal Napera customer?</p>	<p><i>The Napera customer:</i></p> <ul style="list-style-type: none"> • A small to medium sized enterprise from 10 -999 users • With Limited IT resources, typically consisting of a small team of IT generalists. • With a Windows-based environment

Napera Networks Messaging and FAQ 2008

Customer Benefits	<p>Increased Security and Control:</p> <ul style="list-style-type: none">• Makes sure only healthy computers access network• Controls guest access to printers and the Internet• Clear visibility into security state of all computers on network• Remediation assistance for non-compliant computers <p>Ease of Use:</p> <ul style="list-style-type: none">• Works like a switch• Easy to deploy and manage: 10 minute deployment• Integrated Web service for ease of management and reporting• No Windows agents to install <p>Cost Effectiveness:</p> <ul style="list-style-type: none">• Affordable hardware and services• Leverages existing investments in security products• Leverages Microsoft NAP agent• Does not require Windows Server 2008 or infrastructure investments
Who needs Napera?	<p><i>You need Napera if you:</i></p> <ul style="list-style-type: none">• Have laptop computers that travel beyond the office walls• Want to stop security threats before they jeopardize the network• Want to know the identity and security state of every computer on your network• Need to control network access from wireless access points• Need to provide secure guest Internet or printer access
Why do customers need Napera NOW?	<p>Unhealthy computers are on your network</p> <ul style="list-style-type: none">• Laptops are moving in and out of the network and guests are accessing your network, potentially bringing unknown malware and threats onto your network.• Napera provides visibility of the state of network connected computers enabling administrators to monitor and set relevant policies that ensures <i>users adhere to your company security policies.</i> <p>Guests need controlled access to the Internet and printers</p> <ul style="list-style-type: none">• You can allow guests, partners, customers and other third parties Internet or local printing access in a controlled way when they are on your network <i>without compromising the safety of your network.</i> <p>Endpoint security solutions alone are not enough</p> <ul style="list-style-type: none">• Napera makes sure your anti-virus, spyware and other endpoint protection products are enabled and updated and that your users are following security policies.

Napera Networks Messaging and FAQ 2008

<p>What are the key market drivers for Napera's NAC solutions?</p>	<p>Business Mobility</p> <ul style="list-style-type: none"> Employees are no longer desktop bound and mobile computers and teleworking are business norms, with laptops moving in and out of our network. This changes the way we must manage and secure our systems.
	<p>Wireless Networks</p> <ul style="list-style-type: none"> Just as our employees work from anywhere, wireless networks and hotspots are everywhere, making network and Internet access easier but also introducing new challenges. We need solutions that work seamlessly with wired and wireless networks and provide the same level of control.
	<p>Outsourcing & Collaboration</p> <ul style="list-style-type: none"> All companies, particularly SMEs, are using an increasing amount of outsourced workers and contractors and also need to collaborate with customers and partners. These third parties need secure and controlled access to printers, network resources or the Internet from your office.
	<p>Changing Threats</p> <ul style="list-style-type: none"> Today's security threats are more dangerous and financially motivated and have moved up the stack to applications and personal information. Ironically, the greatest threat to your network is your employees and their computers. We need to ensure employees adhere to security policies and computers are compliant before accessing the network.
<p>What is network access control? (NAC - generic)</p>	<p>Network Access Control or NAC is a network security concept and emerging market that aims to do exactly what the name implies - control access to a network.</p>
	<p>NAC typically includes both pre-admission endpoint security policy checks and post-admission controls over where users and computers can go on a network and what they can do.</p>
	<p>NAC solutions enable network infrastructure, such as routers, switches and firewalls to work together with back office servers and end user computing equipment to ensure the entire system is operating securely and the network is protected from attacks and other security threats.</p>
	<p>The overarching goals of NAC are:</p> <ul style="list-style-type: none"> Mitigation of threats The key value proposition of NAC solutions is the ability to prevent endpoints that lack antivirus, patches, or host intrusion prevention software from accessing the network and placing other computers at risk of cross-contamination in quarantine or remediation. Policy enforcement NAC solutions allow network administrators to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them in switches, routers, or network middleboxes. Identity and access management Where conventional IP networks enforce access policies in terms of only IP addresses, NAC environments attempt to do so based also on authenticated user identities.

Napera Networks Messaging and FAQ 2008

What is Cisco NAC?	<p>Cisco NAC stands for “Network Admission Control”.</p> <p>Network Admission Control (NAC) is available as an architecture-based framework solution built from an existing base of Cisco network technologies and existing deployments of security and management solutions from other manufacturers.</p> <p>Through the Network Admission Control Program for third-party vendor integration, Cisco shares technology features with the some 75 participants, who design and sell client and server applications as well as services that incorporate features compatible with the NAC infrastructure.</p> <p>In addition to the Cisco NAC architecture, Cisco provides NAC appliances.</p> <p>As with other NAC solutions, Cisco Network Admission Control allows only compliant and trusted endpoint devices, such as PCs, servers, and PDAs, onto the network and restricts the access of noncompliant devices.</p>
What is MS NAP?	<p>Microsoft Network Access Protection (NAP) is Microsoft’s version of NAC.</p> <p>NAP is a policy enforcement platform built into Windows XP SP3 and Vista and Windows Server 2008 that helps protect network assets by enforcing compliance with system health requirements.</p> <p>NAP enforces health requirements by monitoring and assessing the health of Windows-based computers when they attempt to connect to a network. Client computers that are not in compliance with the health policy can be provided with restricted network access until their configuration is updated and brought into compliance with policy.</p> <p>Microsoft NAP has a partner ecosystem of some 120 technology companies, including Napera, which enables greater interoperability and integration across products, platforms, and operating systems.</p>
Why can’t I just use MS NAP? Why do I need Napera, too?	<p>To implement Microsoft NAP, you need to deploy both the client and server components, as well as configuring 802.1x for network level enforcement.</p> <p>With Napera, companies can leverage the Microsoft Security Center and NAP agents in Windows XP SP3 and Vista and achieve the power of NAP without the cost or complexity of back-end server infrastructure.</p> <p>Napera makes Microsoft NAP easy, while adding further benefits around identity enforcement, guest Internet and printing access, and strong visibility and reporting on the health of all computers on the network.</p> <p>Napera functionality not found in Microsoft NAP, includes:</p> <ul style="list-style-type: none">• Web based dashboard showing real-time status of entire network• Web-based reporting, logging, and alerting• Network level enforcement without the need for a complex 802.1x deployment• Integration with Mac OS X computers• Real-time visibility into health state of all computers on the network