



CONSENTRY INTEGRATES LANSHIELD PRODUCT FAMILY WITH MICROSOFT NETWORK ACCESS PROTECTION

Combined solution delivers strong pre- and post-admission access control features to secure assets on the LAN

Milpitas, CA – February 7, 2007 – ConSentry Networks, a leading provider of secure LAN solutions, announced today it has worked with Microsoft to integrate its LANShield access control platforms with Microsoft Network Access Protection (NAP). The integration of ConSentry's network-based enforcement platform with Microsoft's admission control and endpoint posture check enables mutual customers to benefit from a comprehensive suite of access controls. As an initial public demonstration of this integration, ConSentry has been selected to showcase the product integration in the Microsoft Network Access Protection Partner Pavilion at the RSA show in San Francisco this week, in booth #2325.

The ConSentry LANShield platforms provide the full scope of LAN security features, including admission control, LAN visibility, identity-based control, and threat control. With the ConSentry platform, enterprises can define specific post-admission policies that control where users can go and what they can do on the network, based on their roles. These post-admission, network-based controls complement the admission controls in Microsoft Network Access Protection. The integration with Microsoft Network Access Protection allows enterprises to extend their access control policies to adjust access rights based on the health of the PC, as reported by the Microsoft Network Access Protection architecture.

Network Access Protection is a policy enforcement technology built into the Windows Vista and Windows Server (code-named "Longhorn") operating systems that allows customers to better protect network assets from unhealthy computers by enforcing compliance with network health policies. Microsoft Network Access Protection technology is publicly available with trial versions of Windows Vista and is available to select partners and customers with Beta 2 of the future version of Windows Server "Longhorn."

"Network Access Protection is focused on providing extensive admission control, compliance checking, and remediation help to ensure that only healthy PCs are able to access the LAN," said Mike Schutz, group product manager of Security and Access Products at Microsoft Corp. "Working with vendors such as ConSentry to gain complementary post-admission controls extends the value that Network Access Protection provides to our customers."

In addition to providing post-admission control, ConSentry can also provide authentication and posture check capabilities for platforms that cannot participate in Network Access Protection, such as non-Windows-based PCs, printers, or voice over IP (VoIP) phones.

"ConSentry and Microsoft's combined work in this space makes sense, as the integration complements each technology's strengths. In addition, this interoperability means organizations considering a Network Access Control deployment can move forward now, knowing that the investment will be protected if they also choose to implement Network Access Protection in the future," said Zeus Kerravala, vice president of security and

networking research at Yankee Group. "This partnership is one more example of ConSentry's progress in separating themselves from the NAC start-up pack."

With the interoperability of ConSentry's LANShield with Microsoft Network Access Protection, customers will see the benefits of both solutions:

- Customers can initiate NAC projects today that will interoperate with Network Access Protection in the future, using the ConSentry platform for network-based enforcement.
- Enterprises gain a complementary set of strong pre- and post-admission capabilities, without the need for any network changes or client software.
- ConSentry's LANShield Controller and LANShield Switch can automatically and dynamically learn the Statement of Health provided by the Network Access Protection infrastructure and adapt access policies based on that health check.
- ConSentry provides comprehensive access control for devices not covered by Network Access Protection, including non-Windows-based PCs, printers, VOIP phones, card readers, and unmanaged PCs used by contractors or guests.

"ConSentry is excited to be working with Microsoft to deliver the full scope of functionality enterprises need to secure their LANs," said Tom Barsi, CEO of ConSentry Networks. "Our customers are demanding that we interoperate with best-of-breed endpoint solutions. This integration with Microsoft Network Access Protection is the first step in our broader strategy of being the 'Switzerland' of endpoint interoperability."

For More Information

- [Building the Secure LAN](#)
- [LANShield Controller](#)
- [LANShield Switch](#)
- [InSight Command Center](#)

About ConSentry Networks

ConSentry Networks delivers Control without Compromise with its family of award-winning LANShield platforms - the LANShield(tm) Controller and LANShield Switch. ConSentry enables businesses to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry's LANShield platforms and InSight(tm) Command Center provide network admission control, visibility, identity-based control, and threat control. This combination of pre- and post-admission controls provides enterprises with a simple, proven, and affordable means of integrating security into their LAN infrastructure and controlling access to business resources and applications. Backed by blue-chip venture capital firms that include Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital, ConSentry is headquartered in Milpitas, California.

ConSentry Networks, the ConSentry Networks logo, LANShield, and Control without Compromise are trademarks of ConSentry Networks Inc., for use in the United States and other countries. All other product and company names herein may be trademarks of their respective holders.