

Writer	Mike Lee (mwoong@unet.kr)
Date	Apr 9, 2008

UNETsystem Announce Network Access Protection Support for Linux

Seoul, S. Korea, Apr 9, 2008 – UNETsystem Inc. – the leader in Network Access Control and Network Behavior Analysis in Korea, today announced Anyclick for NAP Linux version that brings Linux based terminals to Microsoft Network Access Protection platform technology as they announced last year.

Microsoft NAP supports Windows XP with Service Pack 3, Window Vista, and with Anyclick for NAP, now Linux. In most corporate networks, single operating system based networks do not exist. Heterogeneous networks make administration complicated for network and system administrators from a management and security policy point of view. Companies that have a plan to implement Microsoft NAP should consider Anyclick for NAP as an initial setup.

Anyclick for NAP is a plug-in for extending the security health check capability and interoperability with third-party endpoint security solutions in Microsoft NAP platform. It enables more granular network access control in enterprise-wide NAP implementation that includes heterogeneous network terminals such as Windows, Linux and Mac OS X. Mac version is scheduled to be released in Q3, 2008.

Anyclick for NAP can Quarantine users that try to open specific ports used by worms, sending a warning message to the terminals that they do not have required software or run prohibited program such as P2P, enforcing application patch, and more health check functions are supported by Anyclick for NAP. All those actions are based on file size, installed program, process monitoring, registry keys, and components in INI files etc. More importantly, as it support Windows Management Instrumentation (WMI) that used in managements of configuration, status, and operational aspects in hardware and software of Windows - Web-Based Enterprise Management (WBEM) is used in Linux and Mac OS X -, administrators can use the managed objects as NAP policy objects. Using over than 7,000 managed objects, administrators can setup hundreds of policy sets. If you use this feature, terminals using mass storage devices such as external HDDs and CD writers, and/or unauthorized wireless network adapters would be quarantined from the corporate network. UNETsystem also have a plan to provide EC APIs to other third-party vendors to support fast development of other EC methods in Linux and Mac environment.

“We are pleased UNETsystem is helping to extend Network Access Protection infrastructure” said Manlio Vecchiet, Microsoft’s group product manager, security and access product marketing. “UNETsystem’s new products are a welcome addition to the Network Access Protection ecosystem.”

Microsoft proprietary Network Access Protection (NAP) is a new platform and solution that controls access to network resources based on a client computer’s identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of

Writer	Mike Lee (mwoong@UNET.kr)
Date	Apr 9, 2008

network access.

Visit this website to get more information: www.unet.kr/nap

The names of actual companies and products mentioned herein may be the trademarks of their registered owners.

About UNETsystem

UNETsystem Inc, the leader in ubiquitous network security in Korea, provides varieties of security solutions including 802.1X wireless LAN security, Network Access Control, Public Key Infrastructure, and Network Behavior Analysis solutions. Managed Security and Security Outsourcing services are also a major business area. UNETsystem, established in 2003 and located in Seoul, has nine patented and patent-pending technologies about Network Access Control and Network Behavior Analysis. UNETsystem is providing security services for many customers including government agencies, public organizations, financial institutions, telecommunications, logistics, IT companies, cooperatives and business partners.