CCT MARK IA CLAIMS DOCUMENT (ICD)

Netintelligence Limited

Ni Enterprise Manager
Version 5

VENDOR DETAILS
Netintelligence Limited
Lister Pavilion Kelvin Campus, West of Scotland Science Park, Glasgow, G20 0SP United Kingdom
Telephone Number: +44 (0) 870 050 0121
Vendor Website: www.netintelligence.com
Vendor Contact Email: info@netintelligence.com

CERTIFICATE DETAILS	
CCT Mark Certificate Number	2007/10/0031
CCT Mark Award Expires on	29 October 2009
ICD Issue Date	30 October 2007

1 Introduction

1.1 Background

This document outlines the IA claims made by Netintelligence in regard to the suitability of Ni Enterprise Manager V5., for use by the UK Public Sector for the protection of endpoints (laptops/desktops), and the enforcement of security & user acceptance policies (UAPs) across physical network and geographical boundaries.

Objectives

1.1.1 The objectives of this ICD are to provide:

Details of the product including functionality and operation

The framework for the CSIA Claims Tested Mark scheme including the claims for the product

An independent validation of any marketing claims made by the vendor in relation to the features/attributes of the product

1.2 Purpose of Document

1.1.2 This document is the ICD for Ni Enterprise Manager

1.1.3 This ICD is the baseline document for the CCT Mark claims testing process of Ni Enterprise Manager

1.3 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains the introductory material.
- Section 2 contains the description of functionality of Ni Enterprise Manager and all the information related to the security of the product
- Section 3 details the security claims that are being made by the Vendor

2 Product/Service Description

2.1 Product/Service Identification

Product Name: Ni Enterprise Manager

Version: V5. Platforms: XP Professional, Windows Vista Business Edition

2.2 Security Solution Overview.

As the working world becomes more mobile, so organisations are realising that their perimeter defences and point solutions are no longer adequate. Ni Enterprise Manager utilises the one common component that connects every worker today and the one thing that every organisation defends itself against – the internet.

Ni Enterprise Manager has embraced the internet and has used its ubiquitous properties to provide a ready-made virtual world wide network that offers

organisations a central deployment, administration and reporting platform for the delivery of unified threat protection direct to the endpoint.

In this respect, Ni Enterprise Manager combines both conventional security product and security service elements to provide a feature-rich solution for securing employees' endpoint laptops or desktop PCs regardless of their location or connectivity.

The product element consists of a client application, which is easily installed on each endpoint. With an additional component, this client can combine the core functionality of anti virus/spyware, web filtering, IM and P2P control with asset and usage management reporting. (The product also provides for a firewall although this is not the subject of any claims herein).

The Ni Enterprise Manager service element consists of a secured website from which the client application may be deployed, policies may be implemented and reports (which are generated by the client component over a secure connection) may be viewed.

Policies can be set by Individual user, machine, group, domain or organisation level. Policies that may be set within the Ni Enterprise Manager security solution include

- To allow or deny access to certain individual web sites or category group of sites such as Adult content.
- To warn when accessing certain individual web sites or category groups.
- To only allow access to a particular site or group of web sites and prevent access to any web site not contained within the specified acceptable web sites.
- To prevent or allow the use of adult keywords in search engines
- To prevent or allow the operation of instant messenger applications
- To prevent or allow the operation of peer to peer applications
- To prevent or allow the operation of binary newsgroups
- To prevent or allow the operation of the computer

A policy can only be considered completed once a time period governing its times of operation is assigned. Time periods can be set in 30 minutes slots using the 24 hour clock, by day, by week. In addition to the creation of policies to govern the end point usage, Ni Enterprise Manager also enables organisations to set policy on who they deem appropriate to access the data contained within the secure control centre. Policy can be set which provides:

- Master (Administrator) rights and Deployment Rights
- Policy Setting rights and Report/data viewing rights

- Dual Sign In rights (2 individual sign ins are required to access and view reports)

Ni Enterprise Manager offers a truly unique ‘plug and play’ web based internet security service.

2.2.1 Security Architecture

The Ni Enterprise Manager security architecture comprises a client (the product element) residing on the target endpoints which provides protection and data collection services along with a web based hosted service known as the Netintelligence Security Center, which provides the interface for setting and managing policies and viewing reports.

The Ni Enterprise Manager provides a default policy, which may be modified by nominated policy administrators within the company whose endpoints are protected, to ensure a best-fit policy for the individual corporate network for which they are responsible

2.2.2 Hardware requirements

Not applicable

2.2.3 Software requirements

Please refer to Claim Number Ni13 in section 3 for details

2.3 Usage assumptions

2.3.1 Assets

The following assets are to be protected by the deployment of Ni Enterprise Manager.

- Client IT Systems - down to end point level
- Client information
- Client Reputation & reduced risk of legal liability
- Employee/end user exposure to inappropriate materials

2.3.2 Threat scenario

The following threats are countered by Netintelligence:

- Software changes to standard endpoint build
- Presence of unlicensed or unauthorised software
- Presence of ‘over licensed’ software
- Presence & use of Peer 2 Peer applications
- Presence and use of Instant Messaging applications
- Visits to inappropriate and non authorised web sites
- ‘Cyberslacking’

- A known virus is not detected
- A new virus is not detected
- A known piece of malware is not detected
- A new piece of malware is not detected
- Attempts to access the endpoint remotely by non authorised personnel
- Use of company asset outside of authorised hours
- Applying security policy across disparate & unconnected networks
- Effective enforcement of existing Policy across all endpoints regardless of connection, time or location
- Use of company asset for non official operation
- Use of the USB ports

2.3.2.1 Expected operational environment

Ni Enterprise Manager offers a full web based deployment, administration and reporting platform, which can be controlled centrally and managed remotely. No additional hardware or system integration is required. Organisations simply deploy a light client to each end point. Once installed, the client will manage both the activities of the user and will deliver unified threat protect at the same time. When connected to the internet, the client automatically receives new policies, updates and anti virus/spyware signatures without the need for any user intervention. The organisation receives real time user activity back from the clients - providing constant monitoring and a 'whole world' view regardless of the end point's location, connectivity or time.

2.3.2.2 Organisational security policies

Ni Enterprise Manager enforces or supports the following organisational security policies:

- All end user data is encrypted in transfer
- Only users who have been authorised will have access to end user data
- Ni Enterprise Manager can not be circumvented, disabled or removed from an end point unless the user has full Admin Rights
- All end user actions are reported upon
- The client will continue to function, using the last profile received, should the organisation lose communications with the central administration servers
- Ni Enterprise Manager will provide authorised individuals with a secure web based administration tool to effectively manage and control all endpoints remotely and centrally
- Security Policies can be set at individual, group or machine level

2.3.2.3 Security requirements on the environment

The successful deployment and operation of Ni Enterprise Manager will require the organisation to:

- Draft and execute a detailed AUP (Acceptable Use Policy) to be accepted and signed by every end point user where Ni Enterprise Manager has been deployed
- Ensure that at least 2 competent employees have been trained on implementing, operating and administering Ni Enterprise Manager as Full Rights Administrators
- Ensure that the designated Administrators are neither careless negligent nor willfully harmful and will operate Ni Enterprise Manager as prescribed by the Vendor

3 Security Claims for the IA Product or IA Service

3.1 Claims Statements

Unique Reference	Claims Statements
Ni1	Following installation all machine details needed for identification and subscribed users will automatically appear in the Ni Enterprise Manager Control Centre(a secure web site accessed via the web)
Ni2	Following installation access to the Ni Enterprise Manager Control Centre will be limited to authorised administrators using a secure login via SSL
Ni3	Following installation, the Policy Administrator can apply individual policies by machine, by group or by individual via the Ni Enterprise Manager Control Centre, once set the end users will not be able to circumvent the policies applied to them provided the end user does not have the rights to stop the service.
Ni4	The administrator can change and administer policy, deploy clients, and view and monitor reports from any internet connected PC via the Ni Enterprise Manager Control Centre
Ni5	The Clients once connected will check for new policy updates every 10 minutes and will send data back to the central databases at not more than 10 minute intervals. The clients will check for new policy updates either on first connection or within 2 minutes of release by Ni Enterprise Manager. New Anti Virus signatures will be checked for every 3 hours.
Ni6	The clients will operate and enforce policy regardless of the physical location, connectivity method or time of day that an end point connects to the internet

Ni7	Netintelligence is able to block the use of Instant Messengers (MSN Messenger, Yahoo! Messenger, AIM/ICQ) and P2P applications (Limewire, BitTorrent)..
Ni8	The Netintelligence Central Security Databases are updated with the latest Netintelligence assessed threat url files on a daily basis. Updates to other signature databases such as Anti-virus are provided when they become available, however signature updates are regularly checked for by the endpoint client (see Claim Ni5)
Ni9	The client uses the last updated configuration and continues to operate to that configuration whether the endpoint is on or off line, provided no changes have been made to the system clock within BIOS & Windows
Ni10	The Ni Enterprise Manager Control Centre will provide reports on Hardware/software configurations, all web sites successfully blocked/visited, all instant messenger conversations, using the most common IM applications such as MSN, Yahoo!, AIM, ICQ and end point application usage
Ni11	Ni Enterprise Manager can deploy the Ni Enterprise Manager client (3.8MB approx. desktop based software application which provides the policy and reporting tools), Anti Virus client and firewall client (20.4MB approx.) centrally and remotely via the internet to any machine contained with the organisation's active directory and that is online.
Ni12	Ni Enterprise Manager does not require the need for any additional hardware to be installed to operate or for any additional configuration to be made, other than possible changes to Proxies or Firewalls, which would be undertaken by an organisation in their usual manner, to enable the clients to communicate, to an existing network infrastructure for it to operate.
Ni13	Ni Enterprise Manager can be deployed and operated on commonly deployed Windows Operating systems - XP Professional and Vista Business Edition
Ni14	The Ni Enterprise Manager Control Centre supports the latest versions of the most widely used internet browsers - Opera, Firefox, Mozilla, Internet Explorer, Netscape
Ni15	Ni Enterprise Manager will individually record data for every logged on user who interacts with an Ni Enterprise Manager protected end point
Ni16	Historic user data will be available to the administrator via the Ni Enterprise Manager Control Centre.
Ni17	The service shall provide Anti Virus & Anti Spyware protection to the Checkmark Certification Anti Virus Level 1 & Anti Spyware Desktop certification standard

Ni18	The service shall provide Content Filtration to the Web Content Filtration Checkmark certification standard
Ni 19	The product shall record the addition or removal of hardware devices requiring drivers from the end point's USB ports
Ni 20	The service provided by the Ni Enterprise Manager is available for 99.9% of the year.
Ni 21	Communications between the endpoint clients and the Netintelligence Security Center servers are encrypted with SSL.

3.2 Existing assurance certificates

Netintelligence has the following certifications:

- Checkmark Antivirus Level 1
- Checkmark Anti-Spyware desktop
- Checkmark Web Filtering Premium

For more information on Checkmark, please visit http://www.westcoastlabs.org

Annex A Glossary of Terms

Administrator	A nominated and designated employee tasked with the management, deployment and administration of the product on behalf of the organisation
Asset Management	Inventory tracking and record-keeping for all company hardware and software
AUP (acceptable User Policy)	A policy designed to limit the ways in which a computer or network can be used. Acceptable Use Policies usually include explicit statements about the required procedures, rights, and responsibilities of a technology user. Users are expected to acknowledge and agree to all AUP stipulations as a condition of system use, as should be certified on the AUP by the user's signature
Cyberslacking	using a company's Internet connection or computer during working hours for activities which are not work-related, such as shopping, playing games etc.
Firewall	A Firewall is a system which limits network access between two or more networks. Normally, a Firewall is deployed between a trusted, protected private network and an un-trusted public network e.g. the internet
Hardware	The physical equipment of a computer system, including the central processing unit, data-storage devices,

	terminals and printers
Instant Messaging	Instant Messaging is a form of electronic communication which involves immediate correspondence between two or more users who are all online simultaneously
Malware	Short for “Malicious software”; a generic term covering a range of software programs and types of programs designed to attack, degrade or prevent the intended use of an ICT or network
Peer 2 Peer	A peer-to-peer (or P2P) computer network is a network that relies on computing power at the edges (ends) of a connection rather than in the network itself. P2P networks are used for sharing content like audio, video, data or anything in digital format. P2P network can also mean grid computing.
Software	Computer programs, the instructions by which the machine operates, which includes both systems oriented programs (ie DOS) and applications programs (ie, word processing)
Spyware	Any application that may track a person's or organization's online and/or offline PC activity and is capable of locally saving or transmitting those findings to third parties, most often without their knowledge or consent.
SSL	The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission over the Internet
Virus	A dangerous computer program with the characteristic feature of being able to generate copies of itself, and thereby spreading. Additionally most computer viruses have a destructive payload that is activated under certain conditions.

Annex B Marketing Statement to be used

Desktop & Laptop user management & control gets the hosted service treatment, with Ni Enterprise Manager offering a simple way of enforcing endpoint policy regardless of the physical location of the users.

Ni Enterprise Manager is an ‘all in one’ software as a service solution that combines core physical security functionality of anti virus/spyware, firewall, web filtering, IM & P2P control, asset management, with comprehensive end point usage reporting.

Ni Enterprise Manager offers a truly unique 'plug and play' hosted managed service, enabling the central management and enforcement of usage policies across de-perimeterised networks and physical boundaries.