



INNERspace

Executive Summary

Managing vast and distributed global networks of endpoints is a complex and monumental task that is essential to the long term health & viability of any corporation. Endpoint user misconduct, whether inadvertent or malicious, or overlooked technical errors can cause significant and costly damage to corporate networks.

One of the greatest challenges facing every private sector and governmental organization today is the question of how to improve their overall IT and security posture in a climate of minimal resources.

To successfully manage the corporate internal network, IT administrators, CIOs & CISOs must be able to see and understand everything that is happening on the endpoints & servers at all times. Disabled anti-virus clients or other vital endpoint components that have been tampered with or are non-operational can easily go undetected leaving the network exposed and vulnerable to attack.

Without the visibility of an effective endpoint management system, it is virtually impossible to get a clear picture of all endpoint activity and be able to strictly enforce compliance policies. A dramatic increase in the use of risky and unauthorized storage & wireless Internet devices has further complicated corporations' network management initiatives to foil and prevent internal security threats.

Corporations value the trust they place in their workers and must find the most effective approach to protecting & managing the internal network

Monitoring and controlling entire global networks of endpoints and servers with Promisec is quick and easy. There is no client installed on inspected endpoints, and therefore no conflicts with endpoint software components.

without having to depend on employee diligence to maintain endpoint compliance. The best way to accomplish this objective, and with minimal resources and network impact is to employ a powerful and comprehensive endpoint management tool that is also lightweight to secure & optimize the internal network.

How is this possible?

Without any clients (not even dissolvable agents) installed on the endpoints, Promisec solutions bring visibility, speed, accuracy and efficiency to the network offering unparalleled operational performance in terms of risk and compliance management, IT implementation, and an organization's security posture. Promisec provides a complete and in-depth picture of your network infrastructure and its entire endpoint landscape quickly and reliably.

Promisec INNERspace™ Overview

Historically, managing endpoints requires installing a client on every workstation in the network, a time-consuming and cumbersome task and, at best, an unreliable endpoint management solution. Promisec's unique clientless technology overcomes this problem by offering the first clientless endpoint management solution to address a broad scope of internal threats.

Promisec INNERspace is a software solution that offers robust and reliable endpoint management for Compliance, Inventory, Security Monitoring & Alerting, Remediation, and Power Management for all of your endpoints in a distributed environment. With Promisec INNERspace, you get fully automated control and management capabilities for multiple networks (companies) from a single console at the Network Operations Center (NOC) so you can centrally monitor and manage the optimization & security of all endpoints and servers.

The Challenge of Ever More Complex IT Infrastructures

Today's IT and Security workforce has never been more educated, qualified and certified to face the infrastructural challenges of the coming decade. The most demanding challenge will be the amount of work and time required for gathering the most accurate data to make the right decisions in a timely manner.

Promisec INNERspace addresses this challenge head-on providing the most relevant, easy-to-understand and accurate information to the right people at the right time, improving operational efficiency at unprecedented levels across the IT and security infrastructures.

Unlike other products, Promisec offers tremendous versatility to deal with a broad scope of endpoint security and management issues. INNERspace is simple, intuitive, easy-to-use, quick to implement, and adaptable to unique environments. Our clientless technology and intuitive interface can be used to create tailored inspections to meet the specific needs of various departments within an organization, which allows for multiple simultaneous revenue streams for realizing ROI.

INNERspace's numerous features & benefits simplify IT security and tackle the most confounding challenges faced by large enterprises in today's complex environment.

Efficient Remediation. Increased Productivity.

Promisec INNERspace provides easy right-click (manual) or automatic remote remediation, with no PC downtime, letting you remotely re-enable disabled anti-virus clients and other services, eliminate unauthorized processes and start-up commands, repair & maintain registry settings, and uninstall unauthorized applications. INNERspace will also alert administrators about urgent issues and generate exception reports, enforcing policy compliance and tracking events.

Once all deviations from the security policy are detected, INNERspace completely removes suspected Trojan residual components or any other type of malware that may have infected the network.

Clientless Architecture. Minimal Network Impact.

The only software required on managed networks is a Promisec INNERspace Sentry, installed on a single Microsoft machine on each managed network. The Sentry monitors the network and forwards reports and alerts to the NOC, where administrators can review the reports and address any problems remotely without having to physically leave the NOC to access PCs, or even pick up the phone.

A single Promisec INNERspace Sentry monitors all of a managed network's endpoints in minutes (1,000 machines in less than 10 min) for Compliance, Inventory and Power Management, sending alerts for any policy deviation or other unauthorized activity and hidden threats without overloading the network or the PCs being inspected.

Rapid Deployment. More Effective Security. Less Overhead.

INNERspace's clientless inspections allow Promisec to deploy in minutes (not the usual days or weeks) while avoiding costly testing and configuration changes normally needed to ensure that other software on the network will still work. Without stretching tight IT budgets, Promisec's technology enables more effective enforcement of security policies, preventing loss of mission-critical information.

Unprecedented Network Control, Optimization & Performance

Promisec INNERspace gives you unprecedented 24/7 clientless control of your endpoints, enabling maximum performance, productivity and uninterrupted business continuity. INNERspace complements and optimizes your existing security and IT controls to ensure and enhance their performance making sure that:

- ▶ Anti-virus is working properly throughout your entire infrastructure
- ▶ Patch Management is performing well and is reaching all endpoints
- ▶ Encryption agents are installed and running in the right places
- ▶ Group Policy (GPO) definitions are aligned with your expectations
- ▶ Inventory and package solutions are deployed and doing their jobs properly
- ▶ Any other 3rd party solution you might have in your infrastructure is operational.

Result: you get a solution that never stops working to provide the most robust IT security control available.

INNERspace Technology (Based on a Patented Algorithm)

Promisec's entire approach is unique. We understand that the endpoints are the weakest link from the standpoint of management and security in every IT environment. While clients are necessary for AV, PFW, HIPS, anti-spyware, etc., other vital network functions must be handled in a clientless manner because adding other agents or legacy technologies is heavy or assumptive. INNERspace's unique clientless technology distinguishes itself from other vendors who use legacy technologies to extend into the endpoint.

From the design stage, Promisec targeted the managing of endpoints and servers by using a number of methods to identify, retrieve, analyze and present required information.

- ▶ **Identification** - a number of APIs are used to know exactly where and what to look for and between which APIs to correlate information for optimal accuracy.
- ▶ **Retrieval** - algorithms indicate exactly what data to retrieve based on a user's query.
- ▶ **Analysis** - the algorithms know exactly what to inspect for, where to inspect for it and in what order, according to a function chosen by the user,
- ▶ **Results** - INNERspace provides detailed information based on the user's requests. Other clientless vendors only give finite "Yes" or "No" answers.

This entire process is performed in 4-8 seconds per PC entirely on the endpoints without data flowing back and forth between the inspection engine and the database and without impacting the network bandwidth or overloading PCs.

INNERspace Inspection Methodology

Promisec INNERspace inspections offer a unique comprehensive three-pronged approach to managing the security and optimization of your

internal network. The Black List, White List Monitors & User-Defined tools work together in unison to address any and all known & unknown threats with the most accurate, efficient & comprehensive solution available.

Black List: An exhaustive list of potential threats to endpoints that Promisec's research team updates on a monthly basis. INNERspace uses the black list to identify potentially harmful applications (P2P & other file sharing, IM, remote control, etc.), removable storage & network devices (dual connectivity, network cards, Wi-Fi, Bluetooth, modems).

White List Monitors (Define your company's policy compliance): Your company's pre-configured baseline for approved applications, processes, start-up commands, services, IE toolbars, etc. The white list is made up of 7 monitors used to set baselines allowing you to identify and remediate any new component that has been introduced or any essential component that has been removed or disabled. The baseline can be retrieved easily from an approved "image" or by using Promisec's discovery feature. This feature enables you to determine baselines for every business unit, OS, etc, by giving the statistics of every item that exists in your network.

User-Defined: Allows you to customize your own set of objects & policies beyond the black list & white list monitors based on your organization's unique needs and requirements.

Inspect for the absence or presence of specific:

- ▶ **Services** - their status and start mode
- ▶ **Applications**
- ▶ **Processes**
- ▶ **Registry settings**
- ▶ **Files** - or all files with a given extension
- ▶ **Hotfixes** - Microsoft hotfixes (i.e. Security patch Q76572) based on the host's OS version

Promisec INNERspace CEM: Enterprise Solutions for Globally Distributed Networks

Compliance

One of the most foreboding tasks CIOs & CISOs face is maintaining compliance at the end-user level. Users often do not install updates that might interfere with their work and use a variety of unauthorized software, peripheral devices and freeware at their workstations. Promisec INNERspace's fully automated 24/7 remote internal network management ensures that all endpoints are installed with the latest updates and service packs, all clients (agents) are up-to-date and operational and no unauthorized changes are made at the endpoint.

With our clientless technology we can ensure that every endpoint deployed on the network will comply with the anti-virus, firewall, and 3rd party policies established by the organization, regardless of the vendor they choose.

Promisec INNERspace can also leverage existing customer technology to remediate deviations and bring the business into alignment with policy, making Promisec the most cost effective solution on the market today.

Compliance features include:

- ▶ **Management of anti-virus clients, personal firewall & HIPS** - a pre-defined list of the most common anti-virus products in the market to know (24/7) exactly where an AV client is not installed, not running or out-of-date; a common problem often identified upon Proof of Concepts (PoC) where many organizations' endpoints fail a compliance check 10-30% of the time, often despite false positive health reports from their AV Console.
- ▶ **Management of additional 3rd party agents** - a User-Defined Module to define and validate a critical "service" or "process" (whether it exists or does not exist) in the network.
- ▶ **Service Packs** - choose your required service pack for every windows machine or business unit and know (24/7) exactly where there are machines whose service packs are not compliant.

- ▶ **Hotfixes** - choose your required hotfixes for every windows machine or business unit and know (24/7) exactly where there are machines whose hotfixes are not compliant.
- ▶ **Change Configuration Management** (White list) – customized baseline list of approved applications, services and start-up commands from an approved image to identify any new application introduced to the network or any deviation from configured approved services.
- ▶ **Customized list of unauthorized devices and connections** – to make sure no back door is opened to the network by dual Wi-Fi connectivity, 3G modems, memory sticks, etc. In some cases, when memory sticks are prohibited, you can see who is using them.
- ▶ **NIST\GPO** – INNERspace complies with standards & measurements established by the National Institute of Standards & Technology.

Inventory

Promisec INNERspace provides you with a complete list of all hardware and software on each endpoint. The inventory report includes a count of invalid registered software licenses and applications.

This service improves your network visibility and keeps you up-to-date with:

- ▶ **Software compliance** – the User-Defined Module lets you to define a specific application name, how many applications you own and their precise location.
- ▶ **Software inventory** – quickly sweep the network and get a complete list of application inventory.
- ▶ **Hardware inventory** – quickly sweep the network and get a complete list of the hardware inventory.

Security Monitoring & Alerting

Monitor your endpoints and servers (24/7) and receive real time alerts for any deviation or threat with minimal impact on network bandwidth.

INNERspace Monitoring & Alerting is based on a database of over 1,500 black list items and includes a customization module to allow for individual inspection criteria.

Features:

- ▶ **Black list** - Exhaustive database of threats updated monthly by Promisec with the latest risks. INNERspace will alert you (24/7) about who (inside the network) is using P2P applications like Kazaa, Edonkey, Bittorent, Limewire, etc., as well as Remote PC applications, such as LogMein, GoToMyPC, and more. INNERspace will also expose other security risks such as open shares, back doors (dual connectivity), unauthorized usage of memory sticks, synchronization devices (IPAQ, Palm, etc.), unauthorized files (video/music), and unauthorized local administrators.
- ▶ **Change Configuration Management** (White list) - baseline list of approved applications, services and startup commands from an approved image to identify any new application introduced to the network or any deviation from configured approved services.
- ▶ **User-Defined** (customized search criteria) - tailored inspections for the absence or presence of specific:
 - ▶ **Services** - their status and start mode
 - ▶ **Applications**
 - ▶ **Processes**
 - ▶ **Registry settings**
 - ▶ **Files** - or all files with a given extension
 - ▶ **Hotfixes** - Microsoft hotfixes (i.e. Security patch Q76572) based on the host's OS version

In-Depth Inspection

Promisec INNERspace contains a built-in "WMI Analyzer" feature that increases the user's flexibility to customize inspection criteria and gain the maximum benefit from using WMI (Windows Management Instrumentation) for specific queries.

Good for the Environment. Great for Your Bottom Line.

One of the most overlooked enterprise costs today is power consumption. Every enterprise uses PCs, monitors, printers and other peripherals, which are normally left on even when they are not in use - at night, weekends, holidays and even breaks during the work day.

Energy Star estimates that a company can save up to \$75 per PC annually if they employ an effective power management solution. The challenge for most organizations is to reduce power consumption without impacting performance.

Promisec offers simple, yet effective, power management solutions that directly address this challenge in a manner that eliminates the need for any software to be deployed on employee workstations.

With Promisec, you can – within hours:

- ▶ Define your specific power management policies
- ▶ Audit, deliver and enforce your policies on all endpoints in the organization in the very first sweep of your internal network
- ▶ Reduce Endpoint Power Consumption by up to 50%

WMI is a tool provided by Windows for writing scripts and automating administrative tasks on remote Windows based computers that can be quite complex and difficult to use. Promisec's WMI analyzer simplifies the whole process by providing an engine that allows you to simply write a question requesting certain types of data. The WMI analyzer converts your question into an appropriate script and retrieves the relevant data.

Power Management

One of the most definitive ways to gain immediate ROI and monetary value is by achieving real, quantifiable cost savings. Promisec's Power Management feature does exactly that. Promisec Power Management lets you measure your power consumption and savings potential by implementing and enforcing power management settings when machines are not in use – on breaks during the workday, at night, on weekends and holidays.

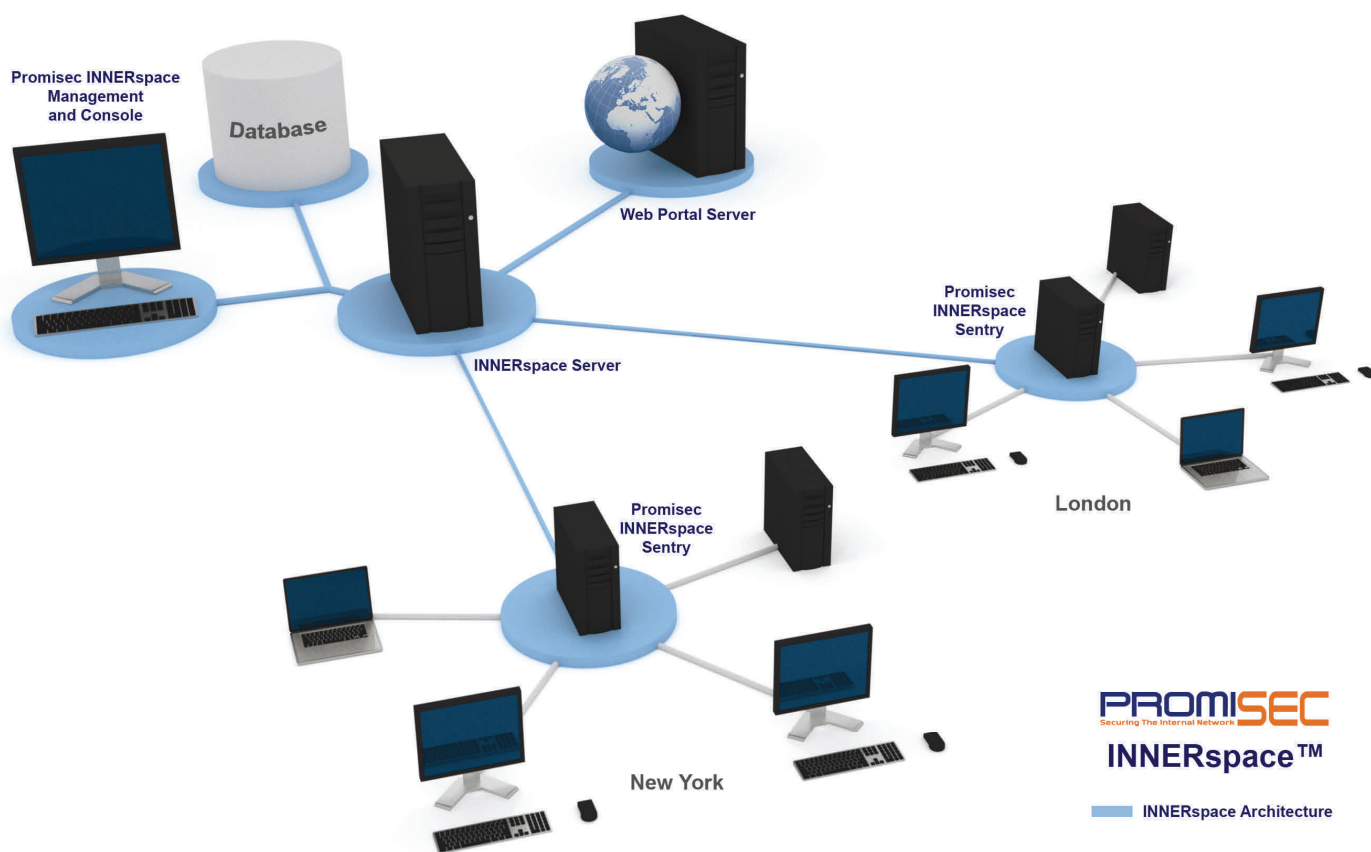
Experts suggest that an effective power management strategy can reduce endpoint power consumption by as much as 50%¹, saving up to \$75 per PC annually².

Features & Benefits:

- ▶ **Enforcement** - enforce pre-defined or customized power management policies.
- ▶ **Ease-of-use** - enjoy complete remote control of all endpoints in the internal network from Promisec's central management interface.
- ▶ **100% compliance** - you no longer have to rely on the diligence of employees to turn off PCs and monitors.
- ▶ **Enhanced control** - if changes are made to power settings, you can change them back easily, in line with original corporate approved policies.
- ▶ **Schedule to wake machines** - schedule wake up times i.e. making sure all machines are on and ready for patch Tuesday.

- ▶ **Immediate savings** - get immediate environmental and cost savings within hours of deployment.

INNERspace Infrastructure



Server-Side Components (implemented in the NOC):

- ▶ **Promisec INNERspace Server** - handles all communication and management. All communication between the server and the different components is encrypted.
- ▶ **Promisec INNERspace Analyzer** (*optional component*) - receives & analyzes inspection data collected by the Sentries, sends out alerts and stores the data in an internal database. INNERspace is compatible with MS SQL 2005.

User Interface Components:

- ▶ **Promisec INNERspace Management** - a dashboard for configuring and managing Promisec INNERspace configurations and services.
- ▶ **Promisec INNERspace Console** - an operations interface used to view alerts and create reporting.
- ▶ **Promisec INNERspace Portal** (*optional component*) - a graphical interface that allows you to view detailed inspection data and save the findings in various formats.

The Managed Network:

- ▶ **INNERspace Sentry** - uses Promisec Clientless Endpoint Management (CEM) technology to inspect all servers and hosts within its network.

How Promisec INNERspace Works

INNERspace **Management** manages the Sentries via the **Server module** providing user-defined customization for all configuration types (policies), ascribing configured policies to a Sentry and monitoring whether the Sentry is operational. INNERspace Management also offers the option of generating the configuration file from a predefined template or by adding individual inspection types to hosts.

INNERspace **Sentry** sends reports to the INNERspace **Server module** that forwards them directly to the INNERspace **Analyzer**.

INNERspace **Analyzer** collects the results from all incoming logs and audit reports, categorizes them accordingly, attaches a degree of severity to each group of results, flags alerts as required and stores the audited information in the INNERspace **Database**.

INNERspace **Console** - a separate interface that IT and Security administrators can use to view reports from specific Sentries assigned to a particular Console. Log entries in the Console window are color-coded according to their level of severity.

INNERspace **Portal** - a separate interface that “C” level can use to view the condition of their IT and security infrastructure in a dashboard.

Integration with Third Party Solutions

Promisec INNERspace can integrate easily with 3rd party management solutions: loggers, event correlation & management, vulnerability management, ticketing systems, etc. offering the flexibility of not having one more console to view.

INNERspace Main Features:

- ▶ Secure endpoint management platform
- ▶ Comprehensive visibility and control
- ▶ Full HWSW Inventory list
- ▶ Corporate & regulatory Compliance enforcement
- ▶ Monitoring & Remediation (right-click, semi-automatic, automatic)
- ▶ User-defined customization
- ▶ Power Management enforcement: audit current settings, clientless monitoring & enforcement, not dependant on wake-on-LAN (WoL)
- ▶ Simple integration with existing systems
- ▶ Multiple, simultaneous inspections
- ▶ Secure administrator access

INNERspace Main Benefits:

- ▶ Unprecedented visibility
- ▶ Monitoring and alerting to any changes on endpoints
- ▶ Fast Inspections: 4-8 seconds/PC
- ▶ Deploys in minutes
- ▶ Endpoint validation
- ▶ Endpoint optimization
- ▶ Accuracy of deliverables
- ▶ Reports with in-depth intelligence, not just "yes" or "no" answers
- ▶ Fast ROI

Promisec INNERspace Competitive Advantages:

- ▶ Easy, flexible and cheap to deploy
- ▶ Zero impact on business processes
- ▶ Unprecedented internal network security for enterprises
- ▶ Efficient use of human and network resources
- ▶ Rapid deployment and affordable maintenance
- ▶ Comprehensive auditing
- ▶ Unlimited scalability from a single central location

References

¹ Gartner Research, Publication Date: 31 August 2007, ID Number: G00150422

² ENERGY STAR Website: General Technical Overview of Power Management

http://www.energystar.gov/index.cfm?c=power_mgt.pr_power_management

About Promisec®

Promisec, Inc. provides clientless endpoint management (CEM) software solutions that give corporate IT administrators unprecedented visibility, speed and control over internal network endpoints, in-depth real-time intelligence to identify threats, and the tools to neutralize them. The company's products, Promisec Spectator® and Promisec INNERspace™, are used by a wide range of SMBs and Global 2000 organizations. With 24/7 or on-demand clientless monitoring, compliance and remediation, Promisec protects against business disruption caused by internal network threats while optimizing IT operations and enabling organizations to confidently place trust in their most important assets - their people. Founded in 2004, Promisec's headquarters are located in Israel with offices in New York and Paris.

For More Information

USA

Promisec USA

Promisec

55 Broad Street, Suite 20C

New York, NY 10004

Tel: +1 (212) 743-9916

Fax: +1 (212) 889-3213

Email: sales@promisec.com

Internet: www.promisec.com

Copyright© Promisec 2009. All Rights Reserved.
All technical specifications are subject to change.



2009 Red Herring 100 Award Winner
honoring Promisec as "one of the top
100 most promising tech companies."



PROMISEC
Securing The Internal Network