



Automated Clientless Endpoint Management (CEM)

Executive Summary

Imagine if you could monitor all of your endpoints 24/7 and instantly know about any potential threat or non-compliance issue. You could view in-depth and accurate data about the event, analyze it and remediate it without the user ever knowing.

The solution would deploy in minutes and provide unprecedented control with no impact on the network. And, it could never be disabled or tampered with by users.

Hundreds of companies and organizations have transformed their IT security management capabilities. Hundreds of CISOs have eliminated serious threats to their corporate network infrastructures and increased productivity.

Protecting Investments in Endpoint Security

There is a growing need for reliable endpoint validation. Threats continue to increase and network infrastructures become more sophisticated and complex. Organizations need to know that their security investments are doing the job they were designed to do.

Today, wireless and mobile storage devices, popular P2P programs and social media sites have become fixtures at the office. But they have created easy targets for attackers. Hackers have funneled millions from corporate bank accounts, stolen sensitive consumer data and sold company secrets to competitors.

The response has been increased corporate vigilance. Companies invest millions in the latest enterprise security products. The IT security market has seen dramatic growth. But are popular endpoint security products getting the job done? How well are the investments being protected?

Most organizations lack the visibility they need to protect their investments. They rely on a partial view that misses hidden threats or problems with AV or other security agents.

Promisec compliments and safeguards investments in 3rd party security agents and leverages existing resources to optimize the network.

It takes years to nurture a solid trust among customers, partners and the general public. Effective technology is essential to securing that trust. IT security managers need powerful management capabilities and the visibility to see the whole picture.

Promisec CEM Technology

Promisec Clientless Endpoint Management (CEM) gives organizations a comprehensive view of all corporate endpoints. In minutes, Promisec CEM can be installed on any PC or laptop, enabling unprecedented control from a single management console. IT security managers can continuously monitor and validate (in real-time) the network's operational status with no client-side software installed at user workstations. Because Promisec is clientless, the solution provides the most accurate and reliable data in the industry.

Security at the Endpoint Level

Promisec focuses on the endpoint level, eliminating the problem of non-compliance. The solution provides fast in-depth inspection reports along with remediation tools to stop unknown threats. Promisec's reports identify a whole range of risks that can expose the network to attack: missing agents, file sharing, USB devices, dual connectivity, and more. Promisec then stops unauthorized processes and services and reverses any unauthorized changes to the registry, giving a CISO time to properly address a security breach.

Agent-based security management solutions cannot ensure comprehensive visibility. These solutions are inherently vulnerable to tampering and need periodic updates that are prone to error and neglect. They also place a heavy burden on network resources.

Promisec's lightweight clientless architecture cannot be disabled or tampered with by users and does not require updates at the endpoints.

Managing 3rd Party Security Agents

Promisec compliments and safeguards investments in 3rd party security agents and leverages existing resources to optimize the network. If one anti-virus, anti-spyware or firewall agent in a network of tens of thousands of endpoints is not updated or uninstalled, an immediate alert is sent and the problem can be addressed. This happens without disrupting the user or the user interfering with the fix.

IT Infrastructure Optimization

Promisec optimizes the network, validating up-to-date versions of corporate approved applications. Promisec defines the correct version's registry value and inspects for that value. The entire process is automated and fast, alleviating yet another administrative task.

Promisec Study Uncovers Threats Missed at the Gateway

A 2009 Promisec study of 100,000 endpoints across 25 organizations of various sizes in a variety of industries found that:

- ▶ 100% of organizations have security and compliance threats in 10-30% of the endpoints
- ▶ Increase in all types of threats from previous year
- ▶ 23% of endpoints were missing third-party agents
- ▶ 20% of endpoints had unauthorized peer-to-peer applications
- ▶ 15% of endpoints did not have the latest Microsoft service packs or hotfixes
- ▶ Dual connectivity, hacking software and unmanaged workstations were found in 2-3% of endpoints. These are serious threats, despite the low numbers
- ▶ Total USB device use went up dramatically, unauthorized USB or PDA use at 13%

Visibility

Despite the increasing complexities of IT, total transparency is attainable. However, the difficulties of managing and securing vast global networks leave many organizations with only limited visibility, missing critical issues.

Typically, to get a complete picture, the CIO or CISO must submit requests to people operating separate security mechanisms inside their respective divisions. Unfortunately, the data returned is usually incomplete, outdated or inaccurate. In short, the process is complicated and time consuming.

Promisec erases this process. An IT security manager can get the picture he/she needs on all endpoints in minutes. Promisec delivers critical information about all endpoint (and server) activity with no need for staff in remote locations. With comprehensive visibility, Promisec monitors and inspects every last endpoint (whether in Beijing, London or New York). The internal network is scanned continuously in less than six seconds per endpoint. Reports are delivered that are accurate and easy to understand.

The report provides complete real-time intelligence on all endpoint activity and any missing or non-operational component. Historical information is included about the use of unauthorized applications or devices, even when a PC was not attached to the network.

Endpoint Validation

Endpoint security tools must do their jobs. Security investments must be protected and company assets properly safeguarded. To ensure that these basic needs are met, IT security managers must consider three simple questions:

- ▶ Are all security tools fully deployed and can this be accurately verified?
- ▶ What percentage of the network is actually using the security tools?
- ▶ Are corporate compliance and government regulations being followed?

A 2009 Promisec study of 100,000 endpoints across 25 organizations of various sizes in a variety of industries found that:

- ▶ 100% of organizations have security and compliance threats in 10-30% of the endpoints
- ▶ Increase in all types of threats from previous year
- ▶ 23% of endpoints were missing third-party agents
- ▶ 20% of endpoints had unauthorized peer-to-peer applications
- ▶ 15% of endpoints did not have the latest Microsoft service packs or hotfixes

In an optimized environment IT becomes a profit enabler rather than a corporate burden.

Promisec's clientless solutions facilitate that environment with round-the-clock validation of all endpoints.

- ▶ Dual connectivity, hacking software and unmanaged workstations were found in 2-3% of endpoints. These are serious threats, despite the low numbers
- ▶ Total USB device use went up dramatically, but unauthorized USB or PDA use was at 13%

Companies can no longer manage internal security risks and compliance issues using heavy and intrusive legacy tools. Point based security and agent-based management solutions cannot sufficiently address the numerous and complex demands organizations of all sizes face today.

With efficient technology and the proper auditing controls in place, organizations can meet these demands. In an optimized environment IT becomes a profit enabler rather than a corporate burden. Promisec's clientless solutions facilitate that environment with round-the-clock validation of all endpoints. Promisec increases productivity, ensures corporate and regulatory compliance and maintains business continuity.

Validating 3rd Party Security Agents and Maintaining Compliance

Promisec provides a complete picture of its existing endpoint security posture. With pinpoint accuracy, Promisec can verify that all AVs, firewalls, anti-spyware, and other endpoint security components are deployed, functioning and compliant.

Many organizations do not recognize a threat until an attack occurs. Even one missing AV can expose the entire network. Promisec's clientless validation gives IT security managers a preventative tool to ensure that what should be working is working.

Core Benefits of Promisec Clientless Validation:

Comprehensive Endpoint Validation and Auditing

- ▶ Endpoint and server protection from architectural limitations in security tools
- ▶ Hackers trying to exploit those limitations
- ▶ Threats caused by user misconduct that violates compliance policies

Optimization for Network Efficiency and Increased Productivity

- ▶ Streamlining of IT security
- ▶ Dramatic increase in network performance
- ▶ Saving valuable time and money

IT security managers can “set and forget” or individually assess a problem before fixing it.

Either way, there is never any need for physical intervention between the Network Operations Center (NOC) and the endpoints.

Protecting Business Assets All the Time

- ▶ Validation of endpoint changes anytime, not just during standard maintenance periods (12am–3am) when many company endpoints are offline
- ▶ Continuous and automatic inspections and validation that prevent growing threats to critical infrastructure
- ▶ Real-time audits exposing threats while enforcing compliance and regulations

Clientless Remediation

Without endpoint management, remediation can be resource intensive, often requiring time consuming physical intervention to fix problems. Client-based endpoint management products let you configure automated policies for remediation from a central management console. But, these solutions are prone to inadvertent agent tampering, technical errors at the endpoint level and hacking.

Promisec erases these problems. With no client software installed on the endpoints, Promisec remediates efficiently without any risk of user tampering or hacking.

Promisec offers two options for remediation: automatic and remote (on-demand) remediation. IT security managers can “set and forget” or individually assess a problem before fixing it. Either way, there is never any need for physical intervention between the Network Operations Center (NOC) and the endpoints.

Promisec’s lightweight clientless architecture increases productivity by enabling the fastest most reliable remediation on the market.

Automatic Remediation

Promisec’s automatic remediation is implemented according to an administrator’s preset configurations prior to running an inspection. The administrator can configure actions to deal with specific events. Once these configurations are pre-set, no further action is required to remediate threats.

Remote “Right-Click” Remediation

Promisec’s right-click remediation allows security administrators to see and assess a problem before making remote changes. A problem can then be remediated with a simple right-click on a report.

Promisec Clientless Remediation capabilities include:

- ▶ Deploying missing agents

- ▶ Uninstalling applications
- ▶ Re-enabling “stopped” essential services
- ▶ Disabling unauthorized services
- ▶ Maintaining and enforcing power management settings
- ▶ Eliminating known harmful or resource depleting processes
- ▶ Resetting tampered with registry settings
- ▶ Hardening registry settings so that any change is automatically reversed
- ▶ Blocking specific peripheral devices e.g. removable media
- ▶ Removing new unknown processes and unwanted start-up commands
- ▶ Closing unauthorized shared folders

Three-Pronged Approach to Monitoring and Remediation

White List Monitors, Black List, User-Defined Module

Promisec CEM is a powerful auditing tool with a comprehensive approach to monitoring and remediation. Fast inspections are performed based on an organization’s specific corporate baseline requirements. With white list monitors, an exhaustive black list of threats, and a flexible user-defined module, Promisec inspections miss nothing.

- ▶ White list monitors: Baseline list of approved applications, services, processes, and startup commands from an approved image. Promisec white list monitors identify any new component introduced to the network or any deviation from approved and configured policies.
- ▶ Black list: Exhaustive database of threats updated monthly by Promisec with the latest risks. Promisec sends alerts (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, Teamviewer, and more. Other security risks include open file shares, dual connectivity, USB storage, synchronization devices (IPAQ, Palm, etc.), unauthorized video or music files, and unauthorized local administrative access.

- ▶ User-defined module (customized search criteria): Tailored inspections for the absence or presence of specific services, applications, processes, registry settings, files, hotfixes, Microsoft hotfixes (i.e. Security patch Q76572) based on the host's OS version.

Conclusion

Point-based perimeter security alone no longer protects the corporate network. The evolution of endpoint activity and the sophistication of today's threats have given rise to the need for comprehensive endpoint management. Vendors have responded. But, traditional agent-based models are inherently vulnerable to the same risks as the clients they manage.

Clientless Endpoint Management (CEM) technology erases this risk and provides organizations with unprecedented control and visibility. Promisec sees everything - down to the last endpoint - that is happening inside the network. Audit reports are delivered with a level of accuracy and speed that agent-based products simply cannot attain.

Promisec CEM has made security management and optimization simple and cost effective. As threats to the corporate network environment have grown, Promisec has empowered IT security managers with the most reliable and cost effective solution on the market.

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