



How to Ensure Compliance in an Organization –The case for Clientless Endpoint Management (CEM)

Executive Summary

The biggest and most confounding challenge to enforcing corporate and regulatory compliance in any organization lies at the endpoints. As corporate computer networks grow larger and more complex in a global distributed environment, corporations struggle to implement compliance standards across the board on all remote workstations.

How well compliance standards are kept can have a dramatic impact on the success or failure of any organization. A company that is able to enforce strict corporate policies and adhere to all the latest regulatory requirements will protect vital information assets, keeping customer and partner confidence high, maintaining a strong brand in the market, and safeguarding trade secrets that form the backbone of its business.

Protecting information from diverse threats is the core principal surrounding information security. Corporations must protect the confidentiality, integrity and availability of sensitive information vital to the security of their businesses, customers and partners to ensure business continuity, minimize damages and maximize results.

Endpoint management is a necessity for any corporate IT security arsenal, but standard agent-based solutions are inherently ill-equipped to guarantee total compliance enforcement on all endpoints and servers. Because they require a client on the endpoints, the risk of malfunction or foul play is always present. The agent responsible for making sure all endpoint components are installed, updated and operational cannot be 100% reliable at all times.

In addition, agent-based endpoint management places a tremendous burden on network resources and consumes huge swaths of bandwidth in both the installation and implementation stages. Non-compliance at the endpoint level can place a huge strain on IT security personnel who have to address issues at physical workstations because the endpoint management tool failed to identify the problem.

Business interruptions are unavoidable if workers have to stop what they are doing while their workstation is being tended to. Ideally, corporations should be able to control the management of their internal networks remotely with the visibility to identify any and all threats to the endpoints and with the intelligence, speed and accuracy to keep the network and business running smoothly.

Promisec Clientless Endpoint Management (CEM) for Achieving Compliance Standards

In order to maintain a compliant environment, a set of policies, procedures and baselines must be defined and enforced for network users regarding the introduction of new equipment and software into the network. Promisec's clientless solutions provide the necessary tools to inspect your entire network of endpoints and servers and produce a full audit report of what is running or installed on each machine.

From this easy-to-read report, you can quickly identify any unnecessary or unwanted software and any rogue processes, start-up commands or misconfigured services. The report also shows any hidden risks on network endpoints such as storage devices, dual connectivity, shared folders, broken group policies, etc.

The next step in establishing a compliant network is to clean up the unwanted objects revealed in the initial audit and to use the necessary objects from the report to set up your baseline for each group of machines. Once a baseline is set it is very easy to maintain and enforce regulatory or policy compliance with Promisec's built-in right-click remote remediation. Promisec's right-click remediation allows administrators to fix problems remotely as soon as they appear, saving time by not having to physically visit problematic endpoints and minimizing PC downtime.

Ensuring Compliance at the Endpoint Level

One of the most foreboding tasks CIOs & CISOs face is maintaining compliance at the endpoints. Users often ignore procedures and notices to install updates that might interfere with their work and use a variety of unauthorized software, peripheral devices and freeware at their workstations.

Such misconduct dramatically increases the risk of exposing invaluable corporate data and causes enormous and costly damage.

Organizations must rely on a combination of innovative technological solutions and a strong, reliable infrastructure to keep critical corporate data and all machines in compliance.

Promisec eliminates such threats letting you manage your entire internal network 24/7 and ensure 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 level.

With Promisec, you can ensure that every endpoint deployed on the network will comply with the anti-virus, firewall, and 3rd party policies established by your organization, regardless of the chosen vendor. This assurance is guaranteed because Promisec is able to show you a complete picture of all network endpoints without relying on a client to work.

Promisec's clientless nature also gives you lightweight solutions with unparalleled speed, accuracy and comprehensive visibility on unlimited endpoints and servers in a globally distributed environment – in contrast with heavy less efficient agent-based solutions that have limited visibility and accuracy, take up large amounts of network bandwidth and are slow to install.

Flexible, Adaptable, Cost Effective

Promisec can also leverage existing customer technology to remediate deviations and bring the business into alignment with policy and regulations, making Promisec clientless solutions the most cost effective endpoint management products on the market today.

Corporate & Regulatory Compliance

The Challenge of Comprehensive Compliance & Threat Prevention

The inefficiencies and complexities of endpoint management are well known, but IT often lacks the manpower, budget or resources to address every potential threat on every endpoint in the network. Despite concerted efforts to establish a sound security policy, IT teams are still hit hard with security incidents due to a lack of visibility and control.

Most organizations understand the importance to their core business of maintaining compliance and have even deployed solutions to address compliance issues. But most solutions on the market today fail to provide sufficient protection and management guarantees needed to tackle threats caused by a dramatic rise in Internet usage and rapid advancements in consumer technologies.

The right technology should ensure the success of your corporate compliance program and ultimately increase the profitability of your business. Corporate IT has the capability and obligation to become a business enabler, and Promisec's Clientless Endpoint Management software solutions are designed specifically with this objective in mind.

Corporate Policy Compliance

Corporate policy compliance may be seen as somewhat easier to define than regulatory compliance because it is dictated inside a company and not by external bodies. Each organization decides for itself what employees can and cannot do based on the security risks involved.

Promisec's unique technology lets you follow a standard image that each department has installed on its endpoints making setting a policy baseline relatively easy. For example, users may be prohibited from disabling security clients, installing certain risky or non-work related applications and connecting to unsecured networks.

The challenge, however, is in the validation and enforcement phases. It's one thing to establish a strict baseline policy for employees to follow, but it's an entirely trickier and more complicated task to make sure that your corporate policies are being followed and compliance is maintained 100%.

At the same time, while you are enforcing a policy of strict compliance, you must also allow for simultaneous flexibility. During the enforcement process, Promisec gives you the flexibility to remediate issues on a case-by-case basis accounting for users who might be blocked from installing a new and legitimate application only because it hasn't yet been defined as a part of your organization's compliance policy.

Promisec Clientless Endpoint Management solutions make defining and enforcing a baseline easy with no rule bases to follow, no complex scripts to write and most importantly, no clients installed on any of the machines protected.

Regulatory Compliance (PCI-DSS, HIPPA, SOX, ISO 27001-2)

Regulatory compliance is more challenging and complex for corporations because of the multitude of regulations such as PCI-DSS, HIPPA, SOX & ISO 27001-2 that are imposed according to a company's location, industry, and countries with which it conducts business. In order to fully comprehend the complicated demands of some regulations, organizations must employ specialists and consultants and produce special documentation to assist with proper regulation deployment procedures.

Promisec CEM features make it easy for your organization to follow complex compliance standards and practices. More importantly, Promisec solutions facilitate sustainable compliance to ensure the policies and best practices designed to protect your assets are always available and in effect, not just for your quarterly or annual audits.

Promisec Compliance features include:

- ▶ **Management of anti-virus clients, personal firewall & HIPS** - a 24/7 capability to identify 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 of seven monitors used to build a customized baseline list of approved applications, devices, services, administrators, toolbars, known hotfixes, 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/CIS** - compliance with standards & measurements established by the National Institute of Standards & Technology and the Center for Internet Security.
- ▶ **GPO Validation** - to make sure the Group Policy settings on all endpoints and servers within an organization are aligned with your desired policy.

Three-Pronged Approach to Building a Baseline

Promisec CEM uses white list monitors, an exhaustive black list database of potential threats and a user-defined module that work in unison to address any and all known & unknown threats. With the most accurate and comprehensive solution on the market, Promisec's unique and patented approach lets administrators use predefined or customized settings to build a baseline of authorized applications, processes, services, start-up commands and toolbars according to the specific needs of the organization

and industry compliance standards and regulations.

Promisec will identify (24/7) any deviation from your compliance policy and fix problems without you having to leave your management console and without consuming valuable bandwidth and personnel resources, leaving virtually no impact on network performance and freeing up IT staff for other important tasks.

A strong security policy sets the tone for a company's security environment and lets employees know what is expected of them. Policies should be reviewed at planned intervals, and as significant changes occur, the continuing suitability, adequacy, and effectiveness of the policy should be adapted and maintained. After a proper review of the policy, there should be updates to reflect any changes.

With Promisec's solution, you can define and enforce enterprise-wide or location-specific security and I.T. policies and track events. Promisec also detects forbidden applications and services (including Trojan Horses) that are hidden but aren't actually running, and verifies that unnecessary or unsecured services or protocols are not enabled.

Getting the Stamp of Approval from NIST & CIS

NIST and CIS offer important compliance guidelines that help organizations manage and protect valuable information assets all over the world and maintain the trust, loyalty and confidence of customers, partners and investors. Many companies struggle to understand numerous and complex regulations and what they mean from a business perspective. Promisec's lightweight software solutions make following compliance standards established by NIST and CIS easy.

National Institutes of Standards & Technology (NIST)

NIST is a non-regulatory federal agency within the U.S. Department of Commerce that provides important guidelines to help companies maintain sound corporate policy and adhere to regulatory compliance requirements. NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that

enhance economic security and the quality of life. NIST's work in promoting the economic stability of the marketplace assists a wide range of organizations in maintaining the integrity and security of their businesses.

The Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a not-for-profit organization that helps enterprises reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS provides enterprises with impartial third-party benchmarks and other resources for measuring information security status and making rational security investment decisions. These highly prescriptive benchmarks specify recommended settings for the configuration of data center elements to minimize the risk of a security breach.

Promisec will assure you a stamp of approval from both NIST and CIS and help keep your business run smoothly, efficiently and threat free.

Promisec Clientless Solutions for Compliance

Promisec offers software solutions that help you maintain all necessary corporate and regulatory compliance policies alerting you when unauthorized events take place. Promisec INNERspace and Promisec Spectator, two award-winning clientless endpoint management products from Promisec Inc., give you the monitoring and remediation capabilities you need for a successful compliance program while optimizing and streamlining your IT security operation.

With easy-to-read in-depth reports, Promisec provides a comprehensive solution with complete visibility ensuring that your business and employees are in line with government standards and corporate baselines.

How do Promisec Solutions Maintain Compliance?

With Promisec Clientless Endpoint Management products, you can:

- ▶ Set procedures and controls to regularly review your Information Security Management Systems (ISMS)
- ▶ Continuously monitor your network endpoints
- ▶ Follow your compliance status 24/7 via Web-based dashboard
- ▶ Verify that your security and policy requirements are being met
- ▶ Review risk assessments, detect security events using vital indicators to prevent security incidents
- ▶ Regularly review the effectiveness of your corporate policy based on your objectives
- ▶ Perform regular internal audits of your internal network
- ▶ Implement significant improvements to your best practices & improve your overall compliance posture
- ▶ Take appropriate corrective actions to address non-compliant events.

Promisec Clientless Endpoint Management solutions are installed at a single central location inside your network from which you can inspect all of your network's machines and enforce compliance policy without having to install any type of client on the endpoints.

Benefits of Compliance to Business

- ▶ Ensure business continuity & minimize business loss by protecting information from a wide range of threats
- ▶ Adhere to complex regulations directly and indirectly
- ▶ Provide measurement and independent evidence that industry best

practices are being followed

- ▶ Strengthen trust & confidence on the part of partners, customers & investors
- ▶ Gain a competitive edge by maintaining a strong reputation and brand
- ▶ Motivate management to demonstrate adherence to good security practice
- ▶ Reduce insurance premiums

Systematic Risk Assessments for Ensuring Compliance

Risk assessment plays an important role in the implementation of information security and is one of the requirements for regulatory compliance certification. Parties involved in the handling of personal information are legally required to prepare risk assessments and review such assessments on a regular basis.

When preparing a risk assessment, it is important to use a systematic method that ensures that another person performing the same risk assessment reaches the same conclusions. These conclusions are useful for guidance and to determine and prioritize the appropriate actions and controls.

As a part of a comprehensive feature set, Promisec products provide an efficient and reliable method for implementing systematic risk assessments. Promisec conducts regular and automated in-depth monitoring and reporting on all endpoints in each business unit to make sure your company meets all of its compliance requirements at any given time.

Risk Assessment results appear in an easy-to-read format at the NOC identifying the controls chosen for your environment. To assure that regulatory compliance is achieved, the report demonstrates how the selected controls relate to the respective risks they are supposed to eliminate.

Reports are presented to reflect relevant corporate and regulatory policy and as a clear documented confirmation of the state of an organization's

information security and compliance status. Promisec's reports enable you to easily produce detailed documentation to appropriate regulatory bodies when they request specific information on the security of your organization.

Regular Internal Audits – Making Life Easier

Internal audits are essential to maintaining a reliable compliance strategy identifying and appropriately addressing any policy failures.

Promisec can help you with the planning of your internal audits by:

- ▶ Scheduling your internal audits at planned intervals
- ▶ Clarifying the scope of each internal audit
- ▶ Specifying the audit's inspection criteria for each internal audit.

Promisec will perform regular internal audits at specified times for a specified group of users based on each group's inspection criteria and provides flexibility for what should and should not be reported taking into consideration the differences between each group.

Promisec offers automatic and remote right-click remediation to remove non-compliant elements and their causes by:

- ▶ Eliminating any component that is not part of the standard image for a machine
- ▶ Identifying any missing essential components needed for the security and correct operation of an endpoint
- ▶ Closing any unauthorized shared folders
- ▶ Sending alerts about any client missing the latest updates.

Promisec products continuously audit enterprise PCs and provide assessment logs for review and as evidence for forensic and in-depth analysis.

Addressing Internet Risk Inside the Corporate Network

Promisec's research team scours the Internet for new file sharing, instant messaging and other potentially dangerous applications that are generally prohibitive within a corporate environment. Such applications can introduce malicious code into the network and can cause serious violations of compliance laws and regulations governing the use of electronic communications inside corporate networks.

When properly approved and regulated as part of an organization's baseline, Web based applications can also be productive tools for certain work related tasks. Promisec enforces the use of approved electronic messaging products and other applications as part of an organization's IT policy.

Eliminating Threats to Business Continuity

Interruptions to business processes are often compliance related and can lead to even more severe consequences such as costly fines, network security breaches and a loss of confidence - on the part of customers and partners - in a company's capacity to safeguard valuable and sensitive information.

The first order of business of course must be to sell your staff on the importance of following compliance rules (corporate or regulatory policy) and the true long term benefits of compliance to the success and safety of the company. Furthermore, the often complex and costly nature of time and resources spent adapting your corporate environment to regulatory policies can be daunting but ultimately rewarding to the flow and financial stability of your business.

The good news is that with the right technology and approach, maintaining compliance can be simple, producing the results you need during regular audits and eliminating the risk of serious threats to your internal network.

Introducing Promisec Clientless Products

Promisec Spectator and Promisec INNERspace, based on Promisec's patented clientless technology, are feature-rich, highly scalable software solutions from Promisec Inc. that give you unprecedented security control and compliance, maximum productivity, network optimization, and seamless business continuity.

Promisec products ensure the availability of third-party security clients (anti-virus, anti-spyware, host-based IDS and/or IPS, etc.) and safeguards investments in gateway security solutions by eliminating back doors into your network.

Promisec enhances your network security without interfering in your existing security monitoring processes, has virtually zero impact on network performance, does not require any changes to endpoint hardware, data or applications and can be installed and operating within minutes. Monitoring begins immediately and initial reporting results are provided within minutes of installation.

Promisec solutions are simple and quick to deploy, can inspect thousands of endpoints in a matter of minutes and require no change to any network configurations or updates to its software at the endpoints since there is nothing installed on the endpoints.

Conclusion

Organizations must move away from reactive compliance and focus on proactive compliance to attain cost-effective information protection and control and maintain brand integrity, customer confidence and business continuity. To accomplish this goal, organizations must make complying with regulatory standards (PCI, HIPAA, SOX, ISO-27001, etc.) a top priority.

Benefits of a Strong Internal Policy

To achieve and even exceed minimum requirements, enterprises should adopt strong internal policies to gain an even higher level of assurance. The right internal policy procedure will help you perform automated checks and give you peace of mind in advance of auditing. A strong internal policy

should be designed for both successful regulatory compliance and as a benefit to your specific business, enabling you to report on a regular basis, monitor employees and discern behavior patterns to stop malicious and noncompliant actions before they occur.

Promisec solutions are designed to make maintaining complex regulatory compliance easy and cost efficient allowing you to show auditors a high level of security in your IT environment.

An April 2008 issue of Information Security Magazine gave Promisec an "A" on a "Policy Control" report card. Their verdict: "Promisec Spectator is a solid product for monitoring endpoint policy compliance, especially for organizations that do not wish to incur the overhead of installing, maintaining and running endpoint agents."

Fastest Inspections in the Industry

Promisec customized inspections are the fastest in the industry – thousands of endpoints in minutes – identifying any failure or deviation from compliance almost instantly with no complex script coding, negligible impact on your network and single installation out-of-the-box operation. Promisec products are "must-have" lightweight tools for IT security compliance managers enabling IT to become a business enabler.

Promisec Clientless Remediation Eliminates the Causes of Non-Compliance

Promisec's clientless solutions not only monitor the network 24/7 to immediately identify any compliance failure but also provide you with the tools necessary to remediate problems and eliminate the causes of non-compliance. Because Promisec operates from a single management console with no clients installed on the endpoints, you get the fastest most accurate and comprehensive intelligence without having to worry about the unpredictability of non-compliant end-user behavior.

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."

