

WHITE PAPER

Addressing Endpoint Security Visibility and Management

Sponsored by: Promisec

Dan Yachin

November 2008

IDC OPINION

Endpoint security plays an increasingly important role in protecting against external and internal threats and in addressing regulatory requirements. With more endpoints being mobile, and thus out of the direct control of the enterprise, and as many of today's attacks are targeted at the endpoint, relevant security is constantly evolving to address an expanding range of threats.

As endpoint security environments are becoming more complex, challenges such as obtaining continuous visibility into all endpoints are becoming more apparent and prominent, as is tackling complexity issues. Along with the need to reduce the total cost of ownership of endpoint security management, these concerns are pushing organizations to seek alternatives to traditional approaches.

The consolidation of security solutions into endpoint security suites, and the 'outsourcing' of endpoint security functionalities to managed security service providers (MSSPs) are examples of this trend. Another emerging option for organizations to address challenges related to endpoint security management is clientless solutions, which can provide such benefits as reducing support and maintenance costs and minimizing network overheads and the impact of endpoint performance.

METHODOLOGY

IDC has developed this white paper using a combination of existing market forecasts and direct in-depth primary research. To gain insight into endpoint security visibility and management issues and to learn how Promisec INNERspace can help organizations address common endpoint security management challenges, IDC interviewed the company team on the issues of technology, product offerings, competitive landscape, and go-to-market strategy.

IN THIS WHITE PAPER

This IDC white paper addresses the need to obtain continuous visibility into corporate endpoints while simplifying endpoint security management. It discusses growing awareness toward the insider threat and the role that endpoint security solutions should play in mitigating it while analyzing common difficulties in effectively dealing with the insider threat using traditional endpoint security approaches.

SITUATION OVERVIEW

Introduction

After years of focusing efforts on keeping their boundaries safe behind firewalls, organizations have to deal with an expanding perimeter that blurs their boundaries. With Internet, mobile, and wireless connectivity, corporate internal networks become increasingly accessible to remote workers and external users via an increasing number and variety of devices. As a result, the convenient separation between trusted insiders and distrusted outsiders is no longer reliable.

A significant challenge for IT is securely keeping pace with the proliferation and use of existing and new endpoint devices, including personal digital assistants (PDAs), iPods, printers, and copiers. Many newly introduced IP devices that seek access to the network are unmanaged or unmanageable by IT and clearly represent added exposure to the network's overall security posture.

Enterprise networks have been giving local corporate users near-instantaneous access to internal and external digital information while providing secure remote network access for Secure Sockets Layer (SSL)/VPN and wireless access points. As the bandwidth, stability, and availability of corporate networks increases, they also become the conduit for supporting digital voice (VoIP) and video data streams.

As the proliferation of IP endpoint types continues, enterprise IT staffs are recognizing the significant increase in security vulnerabilities and threat vectors created by their deployment. At the same time, issues at the forefront for enterprise IT and security professionals continue to include network availability, network performance, network health, internal and external breach threats, malware, policy enforcement, and private and confidential information leakage.

Adding to this complex mix of technical challenges, federal, local, and international regulations now mandate that enterprises establish comprehensive policy enforcement mechanisms, significantly raising the risk stakes for enterprise management and IT.

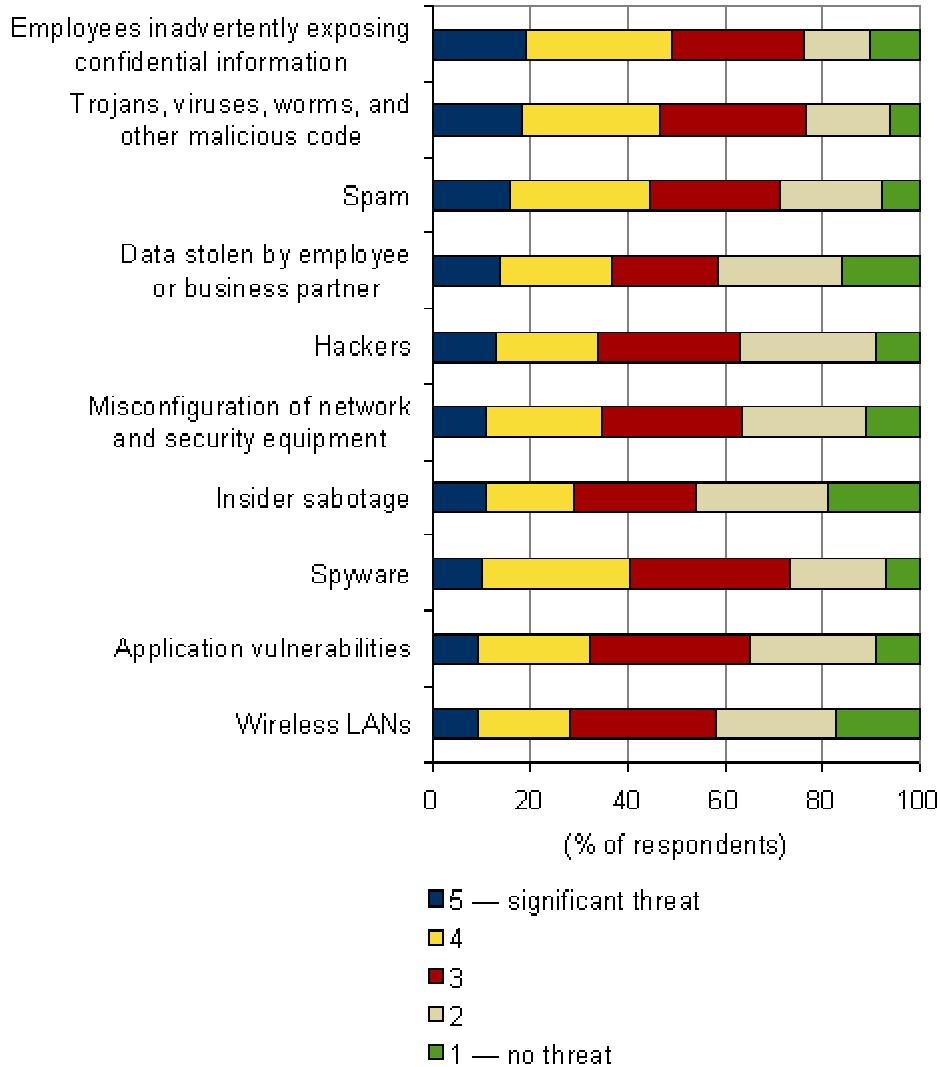
The Rise of the Insider Threat

The realization that most attacks are coming from inside the network leads to growing awareness of the insider threat, which endpoint security solutions can have a key roll in addressing. As an indication of this trend, for the first time in the eight years IDC has done its annual security survey, trojans, viruses, and other types of malicious code have been dethroned from the top spot of threats to enterprise security. The exposure of confidential information is now the single greatest threat to enterprise security. Moreover, insider threats (employees inadvertently exposing confidential information, data stolen by employees or business partners, and insider sabotage) now account for 3 of top 10 threats to enterprise security, as shown in Figure 1.

In fact, in addition to the abovementioned 'classic' insider threats, even traditional external threats such as viruses and other malware, spyware, and hacking can be considered closely related to insider threats, as many of today's attacks are designed to exploit endpoint vulnerabilities to launch targeted attacks, steal information, etc.

FIGURE 1

Top 10 Threats to Enterprise Security



Source: IDC, 2007

To mitigate insider threats in recent years, organizations have been expanding their endpoint security beyond personal firewall, antivirus, host-based intrusion detection, and other traditional solutions to include encryption, device control, host-based data leak prevention, security configuration management, network access control (NAC), and other protocols.

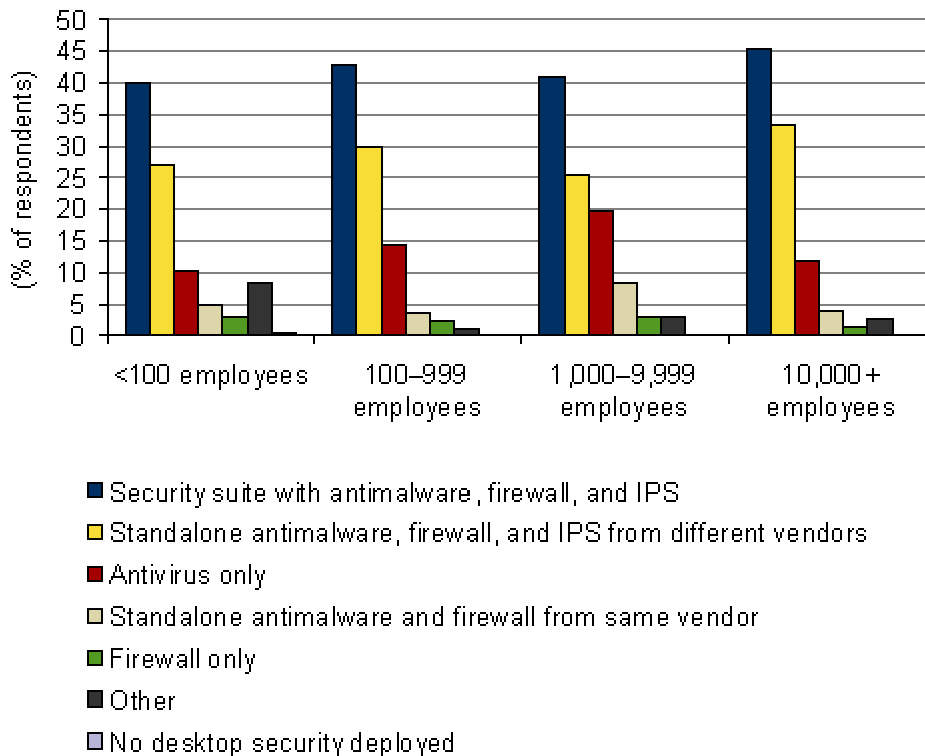
In addition, to effectively use and orchestrate multiple endpoint security products, there is a growing understanding that the cornerstone of any endpoint security framework is an overall policy that enforces both regulatory compliance and organization-specific security requirements.

By implementing this endpoint security model, organizations can significantly improve their ability to deal with insider threats. However, due to the common lack of sufficient correlation between different point products and difficulty in ensuring that all products are constantly updated and adhere to a centralized corporate security policy, endpoint security is often compromised.

In recent years, several market trends have emerged to address this problem. For example, an integrated endpoint security suite that combines desktop antivirus, antispysware, firewall, and host intrusion prevention solutions is now gaining popularity as an alternative to multiple standalone products. IDC's 2007 Security Survey provided evidence of this – 40% or more of all enterprises stated they had adopted endpoint security suites. However, as seen in Figure 2, many organizations are still using standalone solutions from different vendors.

FIGURE 2

Enterprise Use of Endpoint Security Suites by Company Size



Source: IDC, 2008

In addition, organizations are increasingly looking to adopt NAC solutions that provide them with centralized platforms through which they can inspect devices that log onto corporate networks for current versions of antivirus, firewall, and other security products and settings and through which they can ensure network access is only granted to compliant and trusted endpoint devices. Many NAC solutions also ensure that devices which do not adhere to policies are quarantined, and some solutions

ensure non-compliant devices receive required updates and configuration changes before they can re-access the network.

Endpoint Security Challenges

Despite the growing adoption of endpoint security suites and NAC solutions, organizations are still facing some significant challenges in managing their endpoint security environments. For the most part, these challenges revolve around manageability issues and insider threat protection.

Endpoint Security Management Pains

The need for endpoint security suites stems from the fact that installing and managing multiple agents on all endpoints often results in an increased burden on IT resources, technical support issues, network and desktop performance degradation, over complexity, and other issues. While endpoint security suites offer improved manageability, there are various issues that most currently available suites do not adequately address.

For example, as seen in Figure 2, while antimalware, firewall, and IPS are commonly integrated into endpoint security suites, organizations often adopt additional security solutions in order to effectively protect against insider threats, including Data Leak Prevention (DLP), application control, device control, encryption, and security configuration management. In addition, organizations are commonly using asset management solutions that can be used to detect all applications and executables installed on network PCs.

As many of these additional solutions require the deployment of additional agents, manageability remains an issue. Furthermore, as each of these solutions is aimed at a different problem, there is a need to correlate them to comprehensively protect against the vast variety of insider and endpoint security threats. This challenge is for the most part untapped, which may compromise a given organization's ability to effectively identify and protect against emerging threats (let alone in real-time) or to define and enforce a centralized policy across all endpoints.

Another indication of the difficulty in effectively managing complex endpoint security environments can be seen in the growing adoption of managed services in this area. According to IDC research, endpoint security is the second-largest managed security services spending category (after managed firewall services) in the United States. The move toward managed security services is mainly driven by security complexity, regulatory compliance, and total cost of ownership (TCO), as well as the difficulty for security teams to keep up with the growing sophistication of threats. As these factors are highly relevant for endpoint security, the adoption of managed services in this segment is likely to grow in the coming years.

Gaining Visibility in Relation to Insider Threats

As the network perimeter becomes increasingly open to outside access, tracking the activities of authorized users is becoming as important as preventing unauthorized access. In addition, it is necessary to define different access and usage rules for authorized users depending on their locations. In other words, visibility must be obtained for each and every endpoint – not only when something accesses the network (as handled by NAC systems), but also during the entire time it is connected to the network – and adherence to corporate security policies must be enforced.

Although simple in concept, obtaining this visibility is a challenge due to various factors, including the following:

- ☒ **Increasing Usage of Unauthorized Applications:** Enterprise users typically download and install a significant number of applications that are unlicensed, non-business related, vulnerable, or malicious, such as P2P applications, Instant Messaging, VoIP, games, and media players. In addition to network and system performance issues that are caused by the size and massive bandwidth consumption of some of these applications, they also pose security risks, as they may contain malicious code or open unexpected shared folders inside and outside of the network, among others.

- ☒ **Unmanaged Devices:** As mentioned above, corporate internal networks can be accessed through a growing number and variety of mobile and wireless devices, as well as remote laptops and desktops. In many cases, employees are using their personal devices to access a corporate network. In addition, there is a growing concern over non-employees (partners, customers, contractors, etc.) that have access to accounts managed by the organization, although IT does not generally own or have control over the device, operating system, application, network connection, attachment of storage device, or user behavior. As a result, these unmanaged devices may serve as transfer agents for viruses and other malware as they log into corporate networks. In addition, employees using different mobile storage devices (e.g. external hard drives, memory sticks, cameras, and phones) that connect via USB, Infrared, and Bluetooth are raising concerns such as intentional or inadvertent data leakage and theft or misuse of sensitive information.

- ☒ **The Growing Sophistication of Attacks:** Modern malware is designed to evade traditional security methods by targeting the growing window of exposure – the time between the release of attacks based on a certain vulnerability and the time needed for enterprises to deploy a patch.

- ☒ **The Dynamic Nature of Enterprise IT Environments:** IT departments in large organizations often struggle to keep pace with frequent changes related to the installation, update, reconfiguration, and security applied to a growing amount of hardware and software. This is especially true of signature-based security solutions, which require frequent updates against new threats. As a result, the potential for vulnerabilities due to misconfigurations is constantly on the rise.

Beyond these main factors, insider threats may stem from other/different sources. For example, disgruntled employees may use their privileges to disable security systems or make registry changes, thus opening the door to various attacks. Power users and technical staff may also create vulnerabilities by failing to configure network or security settings appropriately, and technical faults may prevent endpoints from receiving critical security updates and patches.

To address these endpoint security gaps, monitoring solutions have emerged over the last few years. For the most part, these solutions combine different functionalities that are commonly included in solutions such as vulnerability management and security event management. In addition, some security monitoring solutions include compliance monitoring in a single platform, thus enabling comprehensive detection of vulnerabilities, security events, compliance violations, and misconfigurations.

The Case for Clientless Endpoint Security Management

While security monitoring solutions offer clear benefits in terms of obtaining endpoint visibility and monitoring user activities, they have inherent weaknesses that may undermine some of their advantages. For example, many solutions in this area rely on clients to accurately keep track and report on endpoint status or to monitor and prevent unauthorized user activities (installing unauthorized applications, running unauthorized services, using unauthorized devices, etc.).

On the other hand, being client-based, these solutions involve the abovementioned necessity to allow clients access to all the endpoints – installing such solutions and keeping them updated with upgrades and patches – as well as the necessity to continuously support end users. In addition, a client-based architecture often results in increased network overhead due to the communication traffic between clients and the central server, as well as increasing the load on the endpoint itself.

A clientless security monitoring solution is likely to be less effective in preventing unauthorized activities, but it can address the abovementioned inherent weaknesses by offering the following benefits:

- Provides visibility into unmanaged endpoint devices without requiring the installation of an agent or ActiveX control download
- Reduces support and maintenance costs and thus total cost of ownership
- Can be rapidly deployed
- Reduces network overheads
- Does not compromise endpoint performance
- Places the monitoring mechanism out of reach of both individuals and sophisticated malware so it cannot be bypassed or neutralized

PROMISEC INNERSPACE CLIENTLESS ENDPOINT SECURITY MANAGEMENT

Promisec is a provider of clientless endpoint security management solutions that were designed to address manageability and insider threat issues surrounding endpoint security. Based on the company's Clientless Endpoint Security Management (CESM) technology, Promisec INNERspace centrally monitors and manages endpoints and servers and their security across all networks. The product operates by continuously keeping track of all endpoints and the different devices, processes, and applications installed on them and ensuring that there is no deviation from the corporate security policy.

At the core of the product is INNERspace Sentry, which inspects the servers and endpoints within the protected network, assesses risks and vulnerabilities, and enforces compliance to corporate policy and regulations (e.g. Sarbanes-Oxley, HIPAA, BASEL II, PCI and others). The Sentries enable continuous monitoring of applications, devices, processes, start-up commands, services, toolbars, network shares, suspicious files, and other items on each endpoint and identify deviations from corporate policies. In addition, INNERspace Sentry can identify missing,

disabled, or out-of-date third-party security agents. This way, the product can be used to protect against a wide range of insider threats, from traditional threats such as viruses and spyware to data theft and leakage from portable devices.

This auditing process utilizes a combination of blacklist and whitelist methods. The blacklist includes a regularly updated description of potential threats such as file sharing, IM and other P2P applications, remote control applications, removable storage devices, network devices (e.g. dual connectivity, network cards, WiFi, Bluetooth, and modems), and common irregular configurations. The whitelist consists of an organization-specific baseline of authorized usage configurations, including approved applications, processes, start-up commands, services, and toolbars.

In addition to auditing, INNERspace provides prevention and remediation capabilities, enabling users to block unauthorized devices, terminate processes, uninstall applications, enable and disable services, repair registry entries, and more. Alerts and exception reports can be used to notify administrators on security events, allowing them to automatically or manually remove suspicious components and malware and automatically reconfigure or repair specific services.

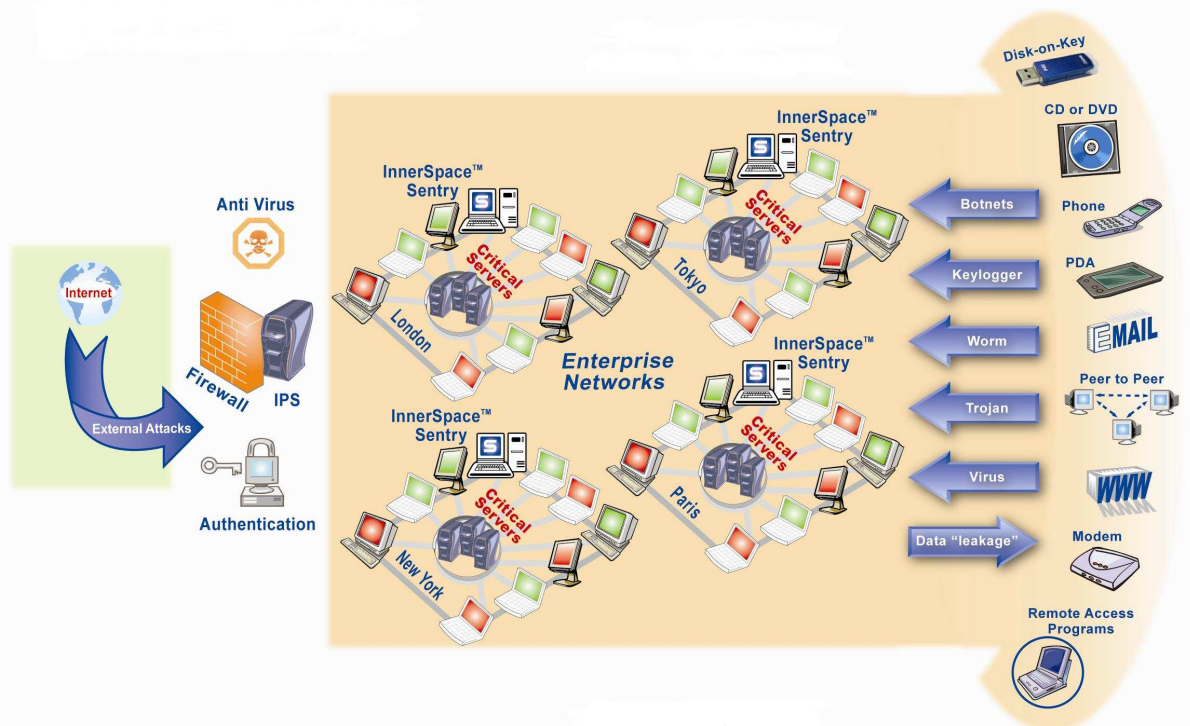
Promisec INNERspace also features INNERspace Server, a centralized console for handling all communication and management tasks; and INNERspace Analyzer, which receives the data gathered by the Sentries, analyzes it, and generates alerts based on predefined rules in accordance with corporate security policies.

The product provides security administrators with a dashboard (INNERspace Management), which enables the configuration, management, and deployment of the Sentries, the definition of controls and privileges for users, and the execution of remediation activities. Furthermore, a centralized console enables administrators to view alerts, drill down into monitored endpoints, remove unauthorized applications, stop processes, and modify settings.

In addition to direct and indirect sales through channel partners, Promisec has recently launched its Clientless Service Provider Program (CLSPP), which enables managed service providers (MSPs) to offer Promisec solutions as a managed endpoint security service. The company has several OEM partnerships with notable IT vendors, including Aladdin, which uses CESM in its eSafe Spyware Neutralizer. Promisec also has a technology partnership with CA to integrate CESM technology into CA's Audit solution.

FIGURE 3

Promisec INNERspace



Source: IDC, 2008

CHALLENGES AND OPPORTUNITIES

By addressing traditional endpoint security management challenges, Promisec INNERspace can capitalize on market demand for new approaches to continuous endpoint visibility while tackling complexity issues. Based on a clientless architecture, the product can be used as either an alternative for existing endpoint monitoring solutions or as a complementary solution for client-based endpoint security products.

In addition to providing traditional software solutions, Promisec should continue developing its MSP offering. In light of the growing competition in this area, service providers are increasingly looking to expand their ranges of services. INNERspace can therefore serve as a platform for MSPs to deliver endpoint security services without imposing significant overheads on their computing and network resources or on their clients' infrastructures.

In the longer term, Promisec should consider expanding INNERspace into additional security and IT management areas, such as asset management and change and configuration management. Although involving a shift from Promisec's current focus, the trend today is clearly toward combining security and IT management functionalities.

More specifically, the emergence of IT governance, risk, and compliance (IT GRC) solutions, which are driven by IT risk management concerns combined with business process-intensive regulations (e.g. SOX and HIPAA) and industry-specific initiatives (e.g. PCI DSS compliance), represents the convergence of system and network management, storage management, and information and perimeter security. To date, most IT GRC solutions are focused on specific functional areas, such as compliance policy documentation and regulation mapping, the auditing and testing of change, the separation of duties, identity management, and broader IT security and vulnerability-related issues. IDC has identified an opportunity to create a feedback loop between GRC solutions that focus primarily on the business and financial health of organizations and enterprise IT GRC and between enterprise IT GRC solutions and lower-level change management-centric and security-centric testing, auditing, and reporting applications. Promisec may benefit from this opportunity by expanding INNERspace's capacities to tackle these issues.

CONCLUSION

The growing complexity of security environments in general, and endpoint security environments in particular, is creating significant management challenges for organizations. At the same time, growing awareness of insider threats and their potential impact on a company's business, along with regulatory compliance pressures and other factors, is pushing organizations to recognize the importance of endpoint security. As a result, organizations have been increasingly looking for new approaches to ease the administrative burden and address common challenges involved in implementing and managing comprehensive endpoint security, as well as a means of enforcing corporate security policy across all endpoints.

Promisec INNERspace can tap into this trend by addressing endpoint security visibility and management challenges. Based on a clientless architecture, the product provides continuous monitoring of all endpoints, including unmanaged endpoint devices, without compromising network and endpoint performance.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.