

# I D C   E X E C U T I V E   B R I E F

## The Rising Concerns Over Endpoint Security

---

*March 2008*

Adapted from: *EndPoint Security Issues*, an IDC Presentation by Christian A. Christiansen

Sponsored by Novell

---

### Introduction

A generation ago, it was fairly simple to maintain system security: users worked at terminals under the direct control of the MIS department. Now, that's ancient history. Today's IT organization is charged with providing the most open, transparent, and multi-faceted computing environment possible for its many and varied users. Some may work only within the offices of the enterprise campus, but most are mobile using laptops in the office and remote connecting to the enterprise network via VPN or over the Internet. Users are increasingly using wireless mobile devices, from smart phones to POS devices, in a variety of work situations. Many use USB thumb drives to move work between machines and locations.

Each of these is an endpoint, and each represents a threat to the integrity of the IT environment. The cost of securing endpoints is rising, due to the ever-increasing diversity of devices that IT must support, as well as the rise in a variety of malicious threats and attacks. Corporate information assets are exposed, but moreover, these threats put the enterprise at risk of being out of compliance with regulations and laws such as GLBA, PCI, HIPAA, and SOX.

Endpoint security (EPS) is central to the many security problems IT has to deal with in order to sustain healthy systems and stable configurations. Unfortunately, the threat vector continues to change constantly and rapidly, and thus IT must adjust its responses accordingly. Recently, IT threat management has taken a new tack, focusing on data protection and wireless control. For these and many other reasons, IT departments are looking for a simplified solution to their many-faceted security problems, one that provides a single install and the ability to efficiently manage the various point tools.

A comprehensive and integrated security technologies solution is not only practical, but it can contribute to reducing total cost of ownership (TCO) by simplifying the management of diverse security solutions. This Executive Brief examines the benefits of an integrated endpoint security technologies solution.

## The Increasing Importance of Endpoint Security

Enhancing access to the enterprise information system, like the Chinese term *wei ji*, presents both an opportunity and a danger. The IT people must be astute risk managers to deal with today's network environment. Among the greatest risks are the following:

- There are now more laptops than desktops in the enterprise environment; their ubiquity poses the highest mobility threat because of data leakage issues. Laptops can contain sensitive information such as intellectual property or customer records that potentially violate privacy and compliance rules.
- Mobile access and wireless access are the greatest security concerns among IT managers today.
- More and more critical corporate information is stored locally, on both machines and portable storage devices, exceeding server-stored data and creating the potential for unnecessary exposure to risk.
- Wireless connectivity is quickly outpacing wired networks, posing the danger of criminal hackers capturing data transfers in mid-air.
- Smart phones are becoming handheld Wi-Fi computers, and the data stored on their flash discs can easily be copied or stolen.

Increased risk and exposure is pervasive. There has been a sea change in the threat landscape in recent years, such as the following:

- Threats that were once "noisy" and highly visible are now silent and often go unnoticed.
- Threats that were once indiscriminate are now highly targeted by professional criminals.
- Threats from "kiddie scripters," or novices, are more prevalent due to the fact that the tools with which to launch destructive attacks are easily available on the Internet.
- Threats from inadvertent downloading and exposure of sensitive information because employees simply don't know any better.

In the past, threats had names and were publicized, leading to more focused remediation, but today's attacks are overwhelmingly varied and are often zero-day threats. Large corporations are experiencing huge losses of both proprietary and public information. For example, customer personal data and credit card information for over 100

million people was lost or stolen in the U.S. just in 2007. In another instance, last year the UK government lost personal data for 15 million citizens being transmitted.

Remediation, which was once simple and technical — just remove the intruder — is now far more complex and may require the use of computer forensics to investigate and determine the source or cause. An IDC survey reports unauthorized intrusion and external net access was listed as IT's top priority for 2008, yet security budgets remain flat.

The bottom line is this: Point security and network access control are inadequate to deal with the scope and gravity of today's threats. Mobility and Wi-Fi jeopardize corporate data, but users demand ever more mobility and ease of access. In the process of trying to give users what they want and still protect corporate assets, IT becomes a sitting duck.

Moreover, IT is tasked with improving security without incurring greater operating costs. IT works diligently to assure that its operations support best business practices. But moving forward, IT needs to reach a deeper accord with senior management to integrate its security practices with the existing best practices, assuring that regulatory compliance and intellectual property assets are protected and secure.

## **Understanding Endpoint Security Issues**

An "endpoint" is any computing device in use by a local, remote or mobile employee, business partner, or customer connected to the enterprise network. IDC defines endpoint security (EPS) as centrally managed client security. EPS protects the corporate environment from threats associated with unapproved remote access, inadequate security for mobile devices, and inadequate client security practices at the device, or endpoint. Individual access is controlled at the machine, application, or file level, across network resources in use.

IT must always be vigilant to ensure that corporate data and information resources are well protected, and that the corporation's security is sufficient to remain in regulatory compliance. As mentioned, IT is constantly confronted with new threats, such as the following:

- Bluesnarfing, using Bluetooth devices to capture data
- Podslurping, using an iPod to download large quantities of data
- Thumbsucking, using USB thumb drives to capture or transfer data without IT authorization
- Zero-day threats, ones so new that no solution exists

Monitoring the flow of sensitive information to laptops and storage devices, such as USB drives, must be part of the solution. The other

part is encrypting the information that employees need to carry with them and transmit.

## **Why Endpoint Security Matters**

In IT's assessment of the total enterprise computing environment, all devices must be considered endpoint devices. An EPS strategy must be implemented, backed up by a stringent, enforceable policy, to manage and protect those endpoint devices. When IT must account for the unknown, best practices must be established as policy; this becomes the baseline upon which enforcement is implemented.

Trusting users to do the right thing is like forest fire danger: it modulates for all kinds of environmental reasons. The honest, a rational user may, when trying to meet a deadline, copy sensitive files to a thumb drive. A laptop with corporate intellectual property may accidentally be left in an unlocked auto. When there are breaches or perceived threats of danger, IT is well advised to roll access back to the lowest or most secure privileges level.

There is no need to risk unnecessary exposure. For example, if there is no justifiable need for wireless connectivity, or if there is a perceived danger from bluesnarfing, disable it. If removable devices are being used for podslurping or thumbsucking and pose a perceived violation of regulatory compliance, disable USB ports.

The first line of defense used to be the firewall, but today EPS is. At first, individual EPS point solutions were installed to fight specific problems, for example:

- Anti-virus
- Anti-malware
- Anti-spyware
- Intrusion detection
- Behavior-blocking software
- Identity management and authentication

Yet each of these point solutions had to be managed, patched, and often reinstalled on the endpoint devices when a significant change occurred, such as an update or a change in regulations. As important as security is to the enterprise, this not only taxed IT resources, but also human and fiscal. In short order, managing all security threats from a single, integrated solution emerged as the more efficient and cost-effective solution.

Patches, for example, traditionally had been created ad hoc, often by a solutions provider that had previously done the work. Now there are integrated solutions for desktop management that keep

endpoints patched at the appropriate levels. Practically all successful attacks are based on known but unpatched vulnerabilities.

## **EPS is Mission-Critical**

Success in EPS depends on three key initiatives: endpoint user policy, perimeter management, and an integrated EPS security management solution.

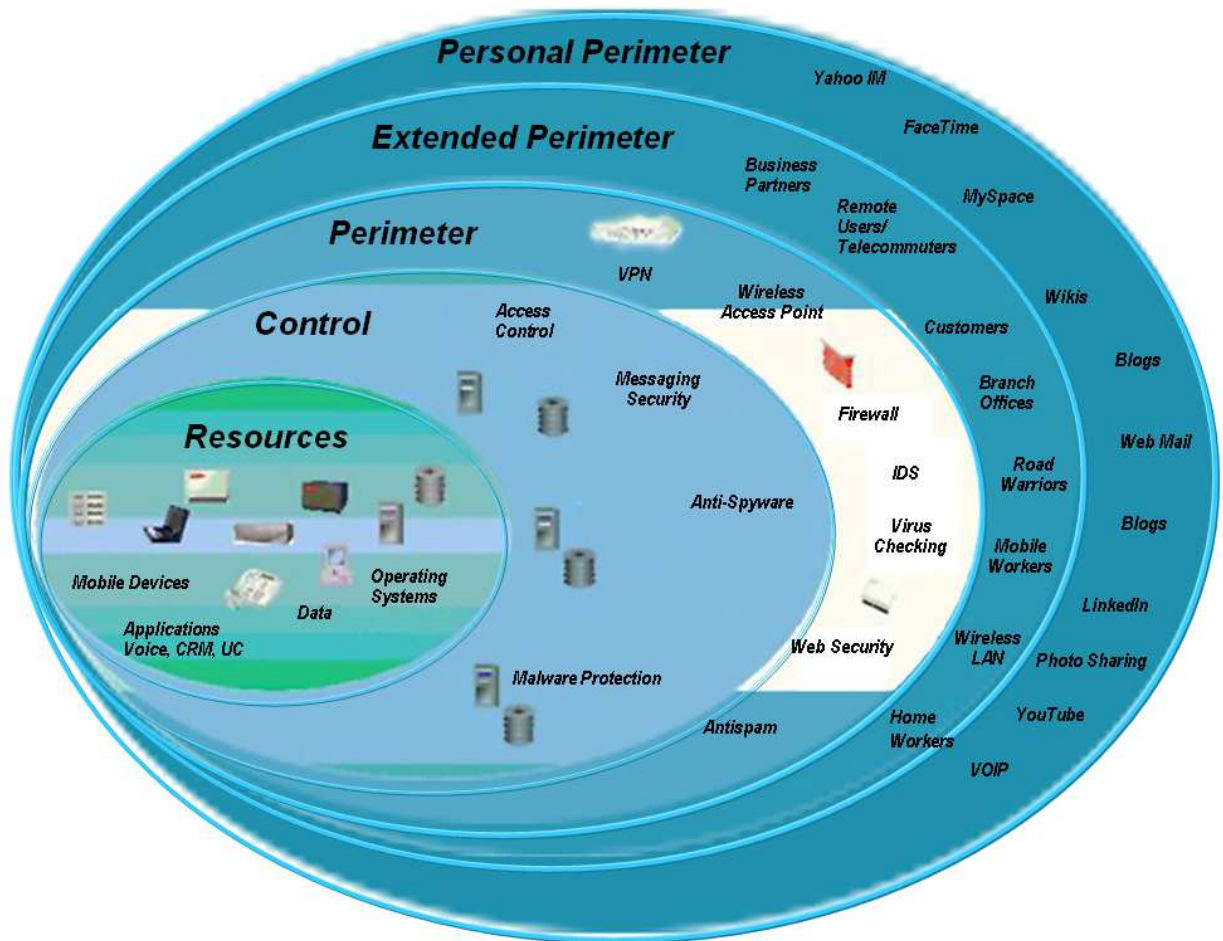
Endpoint user policy establishes what users can and cannot do without IT supervision or permissions. Some of this can be delivered as user documentation, although it should be backed up with policy-based enforcement. Some must be embedded in systems, e.g., user logons for identity-theft protection. Security incident/event management can be used as a way to correlate incident and events from endpoints and other parts of the network, and to provide a consolidated overview of pending security problems.

Perimeter management gives IT control over network extensions from endpoints (see Figure 1). This includes the following:

- Device setup and applications installation
- Access control and extant security software
- Perimeter to the Internet or external networking
- Extended perimeter to outside users, customers, and business partners
- Personal perimeter to an individual user's Internet resources

**Figure 1**

Perimeters Extend from Corporate Employees to Partners to Personal



Source: IDC, 2008

An integrated EPS management solution at the access perimeter gives IT the best perspective and highest degree of control over what goes in and out of the computing environment. It aids in placing enforcement procedures as closely as possible to the threat or vulnerability, thus ensuring the most responsive and highest level of protection.

Essential to a comprehensive, integrated management solution is a top-down approach, starting at the endpoints rather than the network. Disparate technologies should not be kludged together. It makes far more sense to design an EPS architecture from the endpoint devices out to the network perimeters; this assures uninterrupted user productivity and protection for enterprise information assets. IDC defines this architecture broadly as "information protection and control," or IPC, which includes solutions that discover, protect, and control sensitive information. IPC is a

comprehensive solution that prevents sensitive customer data or company information from being distributed either within or outside the enterprise in violation of regulatory or company policies.

IPC includes the following technologies:

- **Data-in-motion IPC.** Data-in-motion IPC includes solutions that monitor, encrypt, filter, and block outbound content contained in email, instant messaging, peer to peer, file transfers, Web postings, and other types of messaging traffic.
- **Data-at-rest IPC.** Data-at-rest IPC includes solutions that discover, protect, and control information on desktops, laptops, file/storage servers, USB drives, and other types of data repositories.
- **Data-in-use IPC.** Data-in-use IPC includes solutions that protect and control information in use. These solutions are used to maintain the integrity of sensitive information such as contracts, term sheets, and other business-critical documents.

Key features to look for in an IPC include the following:

- Asset management
- Desktop computing support
- Device control, such as USB and Bluetooth storage devices
- Encryption as part of a data-leakage solution to lost data on stolen laptops
- Identity management
- Integrated audits
- Management tools with which to instantly see and understand everything occurring within the security perimeters
- Security Incident/Event Management that provides correlation for all the incidents at the endpoints, so threats can be detected early and dealt with quickly
- Patch control
- Policy implementation and oversight

### **Advantages of Integrated Solutions Over Point Products**

Today's security environment must address technological, regulatory, fiscal, and data integrity concerns.

Technical concerns include quickly eliminating incidents caused by viruses, malware, and spyware with a samurai sword stroke. In

addition, since the emphasis has shifted from the network interface, or firewall, to the endpoints, a more holistic view of security is essential to provide secure perimeters.

Regulatory concerns include protecting individuals' identities and customer information, as well as corporate information assets.

Fiscal concerns include avoiding loss from the incident, while not incurring additional loss due to regulatory fines and/or investigative and legal fees, as well as monitoring total cost of ownership (TCO) for the EPS solution.

Security and integrity of enterprise data concerns include not only maintaining data integrity in storage, but assuring that it's not corrupted by malicious hacker intrusions or through irresponsible alteration by users.

All these concerns can be addressed with a single-source solution, which would be difficult if not impossible using point solutions. Given management's reluctance to spend more on IT security, it becomes imperative to evaluate solutions based on TCO. In most cases, the single-vendor relationship that offers a unified solution from a single console will prove most cost-effective.

The EPS problem is a multi-headed, ever-changing Hydra — there is no single, perfect security solution and lopping off heads one at a time is inefficient and costly. It falls to IT to explore the advantages and cost-effectiveness of a single-source, integrated EPS solution. The best defense is a good offense. The place to begin any evaluation of EPS and enterprise-wide security is with a review of policy. While many IT organizations rely on monitoring and auditing to assure systems are secure, it is often too little, too late. A proactive policy with appropriate system shutdowns or lockouts is far more effective.

## **Conclusion: Reducing Threat Exposure**

Today's IT environment is increasingly vulnerable to threats and attacks, both from within and without. Every aspect of the IT environment, from the innocent user to the malign hacker, from the thumb drive on a laptop to the enterprise database on the mainframe, must be under constant security surveillance. The most vulnerable node in the enterprise network is the endpoint. EPS point products may have their uses, but in terms of efficiency, thoroughness, and cost-effectiveness, it may make more sense to consider an integrated EPS solution with multiple security layers, which has been proven to deliver the highest level of protection at the lowest TCO.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at [gms@idc.com](mailto:gms@idc.com) or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more information on IDC Executive Briefs. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services or [www.idc.com/gms](http://www.idc.com/gms) to learn more about IDC Go-to-Market Services.

Copyright 2008 IDC. Reproduction is forbidden unless authorized.