

Reaching Comprehensive Endpoint Security  
Through Content-Based HIPS



## *Introduction*

Organizations are extending remote access privileges to an increasing share of its workforce. In support of this trend, the issuance of laptops with access into the business network and to Internet-based resources when workers are remote has become a standard practice. However, what is not so standard is how to effectively address the elevated challenges organizations inherit when their employees with these mobile devices exit the business network and, as a consequence, lose the blanket of insulation existing network-deployed and corporately-managed defenses and controls provide (e.g., firewalls, intrusion detection and prevention systems, gateway-based anti-virus, and Web address and content filters).

These challenges include:

- **Continuously protecting valuable business assets.** These assets include: (1) sensitive and confidential data stored on, processed through, or accessed by these mobile devices, (2) the business network, its operation can be compromised from infected mobile devices bypassing perimeter defense through internal re-connections or through an unfiltered remote connection, and (3) business reputation.
- **Ensuring productivity-supporting mobile devices operate reliably and are used appropriately.** Meaning, the mobile devices are free of or rendered harmless from infections that could interfere with the operation of legitimate business operations and that users exercise good judgment in the use of these devices.

Addressing these challenges requires extending network-deployed defenses and controls out to the endpoints. Consequently, the inescapable dilemma faced by organizations is how to assemble and effectively manage an optimal mix of endpoint security technologies to address these multi-faceted challenges.

## *Current State and Challenges of Endpoint Security*

For most organizations, endpoint security is not a new concept. Deployment of certain endpoint security technologies (i.e., security software deployed on users' devices) such as personal firewall and anti-virus are nearing saturation and other security technologies such as anti-spyware and Host Intrusion Prevention System (HIPS) has been on the rise. Representative data points on the growing pervasiveness of endpoint security are:

- **96% of organizations use anti-virus software** (Source: 2005 CSI/FBI Computer Crime Security Survey)
- **From that same survey, firewalls are equally pervasive, 97% of organizations use firewalls.** Intrusion Detection Systems (IDS) are also widely in use, 72% of the surveyed organizations use IDS. Not specified in the survey results is whether these survey statistics are inclusive of both in-network (network or server-based defenses) and endpoint deployments. Even so, personal firewalls (endpoint deployments) are highly prevalent, at least from the perspective of availability. For example, Microsoft's Windows XP operating system includes a personal firewall. IDS deployed at the endpoint may not be as prevalent as personal firewall and anti-virus. Nevertheless, we believe, like personal firewalls and anti-virus software, the use

of IDS (detection) and its counterpart IPS (prevention) at the endpoints has the potential to become as prevalent as organizations seek to strengthen the protection of their Internet-connected mobile devices.

- **Market research firm Frost & Sullivan determined worldwide business spending on personal firewall, host intrusion prevention systems, and anti-virus endpoint security technologies reached \$2.5 billion in 2005.**

Clearly, a portion of the rise in endpoint security is a growing recognition that mobile endpoints must be better protected. A second recognition also exists that additional investments in different types of endpoint security is necessary. Case in point, survey results confirm that anti-virus software is widely deployed, but the same surveyed organizations also have consistently identified that virus attacks are the most common type of attack in each of the past six years with over 75% of the 2005 respondents reporting a virus attack (Source: CSI/FBI Computer Crime and Security Survey). In other words, despite the investments in anti-virus, virus-based attacks continue.

Adding new layers of protection at the endpoint introduces its own set of concerns. The reason for concern is understandable; as more and different security technologies are deployed, the cost of security increases in terms of: (1) administrative overhead, (2) subscription fees, and (3) potential user inconvenience (a drain on productivity). Consequently, departments responsible for security and laptop support need to be pragmatic in their approach to endpoint security. Otherwise, the real potential exists that the spending on endpoint security technologies and associated costs will exceed the expected improvement in protection. For this reason, we believe that organizations will likely follow a best of breed approach in assembling layered or comprehensive security at their endpoints. With this best of breed approach, organizations will consider the following solution attributes: effectiveness of each security technology (e.g., personal firewall, anti-virus, anti-spam, phishing protection, and host intrusion prevention system), administrative ease, user transparency, and cross-vendor interoperability.

It is the purpose of this paper to outline a framework for endpoint security that balances the need for improved protection and control at the endpoint versus total cost. We will address this framework in two steps: (1) outlining the range of capabilities that should be present in a comprehensive endpoint security solution, and (2) the best of breed attributes these solutions should exhibit.

### *Comprehensive Endpoint Security Objectives*

In our definition of a comprehensive endpoint security solution, we believe the following objectives should be present.

1. **Protect information** – Establish strong safeguards around sensitive information and prevent data leakage.
2. **Prevent risky user activities, operation of unauthorized applications, and harmful network communications** – Establish and enforce policies to drive compliance and control the environment.

Since organizations operate in a communication environment where comprehensive control over user populations, user activities, applications in use, networks used, and device configurations cannot always be guaranteed, multiple sources of security risk are present. Notably, there is the risk that improper

and/or illegitimate communications can occur at multiple levels - user, application, and network – producing communication events that elevate the risk for the organization.

In the following two sections, we describe in greater detail the security mechanisms necessary to support these objectives. It is important to note that many of these mechanisms are not mutually exclusive; they can support both objectives.

### **Information Protection**

Stimulated by a rising tide in regulatory mandates and a steady stream of publicized identity theft, concern over the extensive clean-up activities that follow a breach of sensitive information, and the damage that information leakage can cause to competitiveness, enterprise interest in solutions that protect information in motion and at rest is climbing. There are several mechanisms that exist in this category, more than can be discussed in detail within this document. However, below are those we believe have or will garner the greatest attention.

- **Remote URL filtering** - Block backchannel, browser-based communication to known malicious websites. These websites secretly record user's keystrokes (e.g., usernames, passwords, and other personal identification information) through malicious code inserted at the endpoint. By preventing users from even visiting these sites from his/her mobile device, this particular risk of unintentional disclosure of confidential information is reduced.
- **Network and application access control** – With growing fervor, numerous solutions have been introduced into the market that support an organization's need to sharpen user and system access to networked resources. Through effective access control, the risk to sensitive information is lowered as the flow of sensitive information can become more restrictive and tightly controlled. Furthermore, greater depth in accounting of who accessed which information resources is also supported.
- **User Action Control** – Given the low cost, compact size, high capacity, and simplicity of use, removable storage mediums (e.g., flash drives and writable CDs) permit users to easily capture and then transport vast amounts of sensitive information outside the organization. Unless the organization has mechanisms to exert control over these user actions, the risk of this type of information leakage remains unaddressed.

### **Prevent Risky User Activities, Operation of Unauthorized Applications, and Harmful Network Communications**

Because complete control is not feasible or cannot be guaranteed and there is a variety of user, application, and network communications that are potentially harmful, no single mechanism will suffice, multiple mechanisms must operate in concert. The three mechanisms listed below are distinguished by the risky user activities, operation of unauthorized applications, and harmful network communications they are designed to prevent.

- **Prevent access to known or enabling sources of harmful code or content** – The intent of this mechanism is to prevent users from reaching Internet sites that have been identified as containing inappropriate content, having fraudulent intent (e.g., a phishing site) or are associated with malicious drive-by code (e.g., code that is automatically transferred from a website to the user's device when the website is visited). Web filtering supports this prevention mechanism.

- **Prevent harmful applications from operating** – The intent of this mechanism is to prevent the launching of unauthorized applications intentionally by the user or without the user’s knowledge. In support of this mechanism, user-tamperproof lists of unauthorized applications and programs (i.e., black list) and authorized applications (i.e., white list) are maintained and periodically updated on the user’s device. Operating in the background, this mechanism will compare each application launch to these two lists and initiate appropriate action such as blocking the launch of a black listed application.
- **Prevent suspicious network communications** – With the previous prevention mechanism, specific knowledge of web sites and applications is needed, which may not exist in totality. Therefore, this type of mechanism serves to prevent certain types of endpoint or externally initiated network communications that are potentially harmful. Controlling the opening and closing of network ports and authorization of communication protocols (e.g., FTP and Telnet) serves this mechanism and is completed through personal firewall policy settings and application communication policies.

### *Endpoint Security Solution Operational Attributes*

In the previous sections, security mechanisms that form a comprehensive endpoint security solution were described. In this section, the focus is on operational attributes; attributes that assist in managing the total cost of endpoint security as the number of endpoint security technologies and endpoints increases.

In this context, it is important to recognize that the full cost of endpoint security is not limited to software subscriptions but also includes the technical and administrative resources consumed in managing endpoint security and the inconvenience and disruption that may be encountered by the users of the endpoint devices. It is this holistic definition of endpoint security costs that is used in our listing of operational attributes.

- **Minimize the number of unique security software applications** – As the number of endpoint security applications increase, so too does the administrative oversight to install, configure, and update. Consolidation of two or more security functions into a single software application contributes to optimizing administrative oversight.
- **Always-on and user tamperproof** – For endpoint security to reach its maximum effectiveness, it must operate continuously. Any lapse results in an increase in security risk. If users are not systematically blocked from tampering with the state of the security applications (e.g., turn them off) or modifying their security settings, then the endpoint devices and the organization’s network become more susceptible to infection and disruption. Both of these consequences lead to additional administrative effort in responding to helpdesk calls and clean-up efforts.
- **Lightweight user involvement** – While maintaining strong and consistent security should be a goal for all employees, reliable user and, in many instances, administrator involvement in security-related tasks is impractical. The technical requirements of security are too complex and confusing for most users and, consequently, driving security management down to the user level in most instances guarantees that there will be security inconsistencies. Relevant examples of low-touch user involvement include the following:

- o Application installations, updates, and upgrades should occur in the background, transparent from users. In addition, the consumption of device processing capabilities and access bandwidth in completing these tasks should be kept to a minimum.
  - o The interaction between users and security applications should be limited and, when essential, highly intuitive in order to minimize users' feelings of uncertainty and anxiety by having a role in managing security applications that are operating on their devices.
- **Broad and reliable platform support** – Since every endpoint device represents a point of vulnerability and organizations need flexibility to choose the types of endpoint devices that best meet their business requirements, endpoint security applications need to be supportable on a broad range of endpoint platforms. Otherwise, the organization will sacrifice flexibility in selecting endpoint devices as they seek to strengthen endpoint security or vice versa.
  - **Integral to security information ecosystem** – Security is an information-intensive discipline and performs best when information is shared across security applications and functions. Following are security functions that would benefit through an integrated flow of information from endpoint security applications:
    - o Personal / Desktop Firewalls,
    - o Network Access Control,
    - o Network-based Intrusion Prevention,
    - o Patch Management and other Remediation Systems/Processes, and
    - o Security Event Management.
  - **Leverage existing endpoint security applications** – Since most organizations have some level of endpoint security applications already deployed, a valuable attribute of additional security applications is that they interoperate with existing applications in order that the organization gains synergistic benefits. In addition, as desktop software vendors such as Microsoft incorporate security technologies into its software packages (e.g., a personal firewall is included in Windows XP SP2), interoperability with these security functions conserves an organization's expenditures by avoiding separate investments.
  - **Scalable, centralized, and tiered administration** – As the number of endpoint devices increase, administrative effort should not be linear. Rather, economies of scale should be expected resulting in declining administrative effort per endpoint as the number of endpoints increase. Centralized and tiered administration contributes to economies of scale benefits.

## *Conclusion*

Endpoint security is complicated. For example, the rising tide of mobile devices marginalizes the protection of network perimeter defenses and greatly challenges administrative control. Reliance on users to follow best security practices is of limited assurance. Moreover, attackers are equally aware of these same vulnerabilities and continuously invent new ways to exploit them to their benefit.

Organizations are at a pivotal point in time to assess their current approach to endpoint security and determine what modifications are necessary to improve their security state and to become more prudent in their expenditures and security administration. To begin this process, we suggest that the organization first begin with a clear statement of their security objectives pertaining to endpoint security. We recommend the following:

1. Protect information, and
2. Prevent risky user activities, operation of unauthorized applications, and harmful network communications

The next step is to review the ever-growing number of security mechanisms available in the market today and determine which of these are needed. The conclusions that we believe will be reached are:

- The number of competing solutions is a bewildering mix and attempting to stitch together and effectively manage security solutions from multiple vendors will be a significant undertaking.
- Security mechanisms must have multiple levels of content awareness. Awareness of network level communication flows, while important, is an insufficient base to create a comprehensive approach to endpoint security. A comprehensive endpoint security solution must account for and have the means to address the potential of unauthorized applications, inappropriate and risky user activities, and the user-attractive but harmful locations on the Internet.

Websense® Client Policy Manager™ (CPM) is a new breed of endpoint security solutions that epitomizes both of those objectives and is comprehensive in its security technologies, offers multi-level content awareness, and is designed to be administrative-friendly.

*Michael Suby  
Program Director – Business Market Strategies  
Stratecast Partners (a Division of Frost & Sullivan)  
msuby@stratecast.com*

#### **About Stratecast Partners**

Stratecast Partners directly assists clients in achieving their objectives by providing critical, objective and accurate strategic insight, in a variety of forms, via an access-and-industry-expertise-based strategic intelligence solution. Stratecast provides communications industry insight superior to a management consultancy, yet priced like a market research firm. Stratecast Partners' product line includes: Monthly Analysis Services [Convergence Strategies & Network Architectures (CSNA), OSS Competitive Strategies (OSSCS), Network Professional Services Strategies (NPSS), Consumer Market Strategies (CMS), and Business Market Strategies (BMS)]. Weekly Analysis Service [Stratecast Partners Insight for Executives (SPIE)], Standalone Research, and Business Strategy Consulting,

#### **About Frost & Sullivan**

Frost & Sullivan, a global growth consulting company founded in 1961, partners with clients to create value through innovative growth strategies. The foundation of this partnership approach is our Growth Partnership Services platform, whereby we provide industry research, marketing strategies, consulting and training to our clients to help grow their business. A key benefit that Frost & Sullivan brings to its clients is a global perspective on a broad range of industries, markets, technologies, econometrics, and demographics. With a client list that includes Global 1000 companies, emerging companies, as well as the investment community, Frost & Sullivan has evolved into one of the premier growth consulting companies in the world.