



# **The Essential Elements of Comprehensive Endpoint Security**



# The Essential Elements of Comprehensive Endpoint Security

## Contents

Introduction .....	4
Endpoint security challenges .....	4
An ideal endpoint security solution .....	7
An ideal solution in the making .....	13

## Introduction

For today's computing environments, there is little question that endpoint security is a required component of an overall enterprise security strategy.<sup>1</sup> On one hand, various trends fostering user mobility ensure that many endpoints will frequently be exposed directly to the Internet. On the other hand, even when they are operating on the LAN, endpoints are still being exposed to numerous threats, both from other internal sources as well as from external sources that are all too often demonstrating the ability to penetrate or otherwise circumvent an enterprise's perimeter defenses.

It is not surprising, however, that establishing a comprehensive endpoint security solution is a complicated undertaking. A number of factors, such as accounting for unmanaged nodes, increase the scope of the challenge. In addition, selecting and stitching together an appropriate set of countermeasures often depends on navigating a complex and proliferating landscape of applicable point products.

Accordingly, the intent of this paper is to clarify the various aspects of the endpoint security problem and to identify the functional requirements of a comprehensive endpoint security solution.

## Endpoint security challenges

The primary challenges pertaining to establishing a comprehensive endpoint security solution can be categorized, for the most part, in terms of the closely related attributes of scope and effectiveness.

### Scope

Underestimating the scope of endpoint security responsibilities is a common issue that leads to diminished effectiveness, as well as the creation of a patchwork of multiple, potentially independent, "solutions" over time. There are two particular aspects of scope that are commonly overlooked, that is, at least initially. Fortunately, both can be clarified by closely considering what it is specifically that requires protection.

Ultimately the goal within any domain of information security is to ensure the confidentiality, integrity, and availability of the information that an organization considers to be sensitive or valuable. Furthermore, it is important to realize that this goal applies regardless of where the associated information resides at any given moment.

<sup>1</sup> For the purposes of this paper, endpoint refers to user computing stations such as laptops and desktops. However, it should be noted that many of the solution criteria and associated conclusions apply equally to personal computing devices (e.g., PDAs) and servers.

## The Essential Elements of Comprehensive Endpoint Security

Keeping these fundamental concepts in mind, the first overlooked aspect with regard to scope is that security must be provided not just for managed endpoints, but also for ones that are unmanaged. These are endpoints that are beyond your organization's sphere of administrative control, primarily because they are owned by other parties (e.g., employees, business partners, customers, or even the general public).

The case for managed endpoints needing to be secured is relatively clear. They typically have access to a broad range of information and, in many cases, are explicitly allowed to retain large portions of it (e.g., in the form of various types of documents). Of course, not all managed endpoints and their users will have the same rights and permissions when it comes to accessing and storing information. However, this just means that they will not all require the same set of countermeasures. This does, in fact, have implications in terms of the flexibility that an ideal solution must exhibit, but it almost certainly does not eliminate the need to secure the endpoint, at least to some extent.

In contrast, unmanaged endpoints generally have considerably less access to information and are typically not expected to retain it. However, once again, just because the scope and duration of access is reduced does not eliminate the fact that the associated information is being put at risk. Indeed, it could surreptitiously be stored, or for that matter, it could be intercepted or stolen as a consequence of the unmanaged endpoint having been compromised by some sort of malware. That said, what will necessarily be different with unmanaged endpoints is the type of countermeasures that can be invoked. As will be discussed shortly, not having control of the endpoint does impose some significant limitations in terms of what can be done and how it can be accomplished (e.g., not being able to dictate which types of security controls are persistently installed on the endpoint).

The second aspect of scope is perhaps a little more subtle, but it nonetheless represents a valid concern. Specifically, endpoint security should be considered to include the need to keep an endpoint from becoming a threat vector in its own right. In other words, the network and its computing and information resources need to be protected from endpoints that may be infected. Clearly, it could be argued that this falls under the domain of network or data center security. However, it should be expected that the node itself will increasingly play an important role. For example, promising network admission and access control countermeasures will be far more effective when they can take advantage of a client-based agent that is capable of performing an in-depth audit of an endpoint's security posture and configuration. As a result, to be considered comprehensive, endpoint security should also entail being a good citizen (i.e., participant) when it comes to supporting critical cross-domain security measures.

### Effectiveness

The next category of challenges has to do with the diminishing effectiveness of those countermeasures that have historically been used to achieve endpoint security. The biggest issue in this regard is the influence of a rapidly evolving threat landscape. A shift in hacker motivation (from notoriety to profit) and the accessibility of exploit development frameworks, among other factors, have caused a number of significant changes.

First, the increased determination and ease with which new threats are being built has not only sparked a dramatic rise in overall threat volume, but it has also precipitously reduced the timeframe required for threat development. As a result, the window of time between when a new vulnerability is disclosed and when a specific threat targeting that vulnerability is launched has been irrevocably reduced. In fact, in the first half of 2005, the average duration for this window was only six days.<sup>2</sup> The implication is that patch management, while still an important countermeasure for providing protection in the long run, is far from sufficient in the short run. Indeed, assuming a given patch is even available in time, which is highly unlikely,<sup>3</sup> the window of opportunity in which to assess and implement it is simply too short for most organizations.

Yet another challenge stems from the lightning-fast propagation times of today's threats. For example, in 2003 Slammer achieved an infection doubling rate of 8.5 seconds en route to infecting 90% of all susceptible hosts within 10 minutes. This challenge is subsequently compounded by the sheer volume of new threats and the rapid-fire release of associated variants. The problem with this situation is that, with increasing frequency, reactive countermeasures, such as those based solely on detecting signatures of known threats, cannot be updated quickly enough to provide protection during the early phases of new, or in other words unknown, attacks.

Finally, it is also the case that new threats are more elusive. Blended threats are becoming the norm rather than the exception, and attention is increasingly being focused on application- and system-oriented weaknesses as opposed to network-layer vulnerabilities. Consequently, another common client-based countermeasure, the personal firewall, is also struggling to keep up.

The point of all of this is that in order to be considered comprehensive, an endpoint security solution must address the changes in the threat landscape. This means that reactive and other less effective countermeasures must be supplemented with ones that are more proactive, as well as ones that are capable of stopping attacks against higher-layer services.

<sup>2</sup> Source: Symantec Internet Security Threat Report, Trends of January 05–June 05, Volume VIII, published September 2005.

<sup>3</sup> The source cited in the second footnote also indicates that, during the timeframe analyzed, patches were being released on average 54 days after disclosure of an associated vulnerability.

### **An ideal endpoint security solution**

Summarizing the previous section yields the conclusion that an ideal, or comprehensive, endpoint security solution is one that provides protection of and from both managed and unmanaged hosts, against both known and unknown attacks. To better understand what this means in terms of detailed requirements, it is helpful to separately discuss the specific countermeasures that are needed to secure managed endpoints and those that are needed to secure unmanaged endpoints. Subsequently, it is also necessary to consider operational characteristics that apply, in general, to both cases.

### **Securing managed endpoints**

An advantage with managed endpoints is that because they are within an organization's administrative control, persistent agents can be used to implement necessary countermeasures. This is significant because, as discussed previously, managed endpoints generally have more extensive rights when it comes to accessing and storing sensitive information. This in turn implies the need for more robust and comprehensive security measures which, in fact, can often only be achieved as a result of the greater capabilities available to fully installed, always-on agent software.

In any event, it should be clear based on the identified challenges that to fully meet the security needs of managed endpoints, a solution will need to address each of the following countermeasures.

### ***Personal firewall***

The value of personal firewall technology is derived from the fact that it is a positive-model countermeasure. As such, it will allow only traffic that is explicitly allowed by its policy, while denying everything else. This approach reduces an endpoint's surface area for attacks by blindly thwarting a wide variety of both known and unknown threats. Its effectiveness is limited, however, by the lack of granularity with which its policies can be set. Specifically, by operating primarily at the network layer, it cannot stop application-layer attacks that are conveyed over protocols and connections that are allowed by its rule base.

## The Essential Elements of Comprehensive Endpoint Security

### ***Application control***

The advantage of application control, also a positive-model countermeasure, is that it picks up where network-focused personal firewall technology leaves off. In particular, it supplies the missing granularity needed to refine the definition of traffic that is explicitly allowed, thereby further reducing the flow of unnecessary traffic and any exploit code that it might contain. Advanced implementations will also include the capability to perform integrity checks on an endpoint's applications and their components (e.g., DLLs). This feature can signal the potential compromise of an endpoint, while also providing a measure of threat containment by barring any corrupted components from operating.

### ***Host integrity checking***

This too is essentially a positive-model countermeasure. Host integrity checking involves auditing an endpoint to ensure the presence of various attributes. Typically these attributes will be associated with the security posture of the endpoint and will include items such as registry settings that correspond with specific patches, the date on an antivirus signature file, and the presence and version of the antivirus software itself. This capability is useful in its own right for helping to ensure that the endpoint is always well defended against any threats that it may encounter. However, this capability also doubles as a means to help protect the corporate network from endpoints that are weakly protected and therefore have potentially been compromised. Fulfilling this latter role, though, requires that the associated agent also be compatible with the widest possible range of network admission/control solutions. Another ideal feature for this countermeasure would be the ability, when the endpoint is found to be out of compliance, to accomplish remediation, either via self-contained capabilities or integration with external resources.

Despite their powerful defensive capabilities, all positive-model countermeasures are eventually limited by their granularity, not to mention the patience of organizations to exhaustively define "that which is allowed." Thus, it is essential that a comprehensive endpoint security solution also incorporate a full complement of negative-model countermeasures. The distinction is that the next five safeguards operate on the basis of identifying and mitigating those items that are either known or suspected to be "bad."

## The Essential Elements of Comprehensive Endpoint Security

### ***Patch management***

At first pass it may not seem appropriate to classify this as a negative-model countermeasure. However, patch management is fundamentally about identifying and eradicating weaknesses in software code. And while these are not inherently “bad,” they do indisputably enable bad things (i.e., threats) to be effective. Indeed, without any such code-flaw vulnerabilities, there would be considerably less cause for concern. Regardless of its actual classification, however, the point is that patch management is in fact a countermeasure that is applicable to endpoints, and therefore, it is included here for the sake of completeness.

### ***Network intrusion protection (host-based)***

Similar to a personal firewall, this countermeasure is concerned with network-layer communications and processes and the threats that operate against them (e.g., network-based worms). Basic implementations are signature-based and are, therefore, only effective against known attacks. Providing protection against unknown network-layer attacks will depend on incorporating further, advanced mechanisms. Chief among these is the use of vulnerability-based signatures. This involves predicting the characteristics of threats on the basis of the characteristics of the vulnerability they will be seeking to exploit. In other words, once a new vulnerability is disclosed, researchers develop and encourage deployment of signatures that anticipate the nature of yet-to-be-created threats. Another example of an advanced mechanism that could be included is protocol anomaly detection.

### ***Antivirus***

This is a well-known and highly deployed countermeasure. While it is limited due to its predominantly reactive nature, it nonetheless completes another piece of the puzzle by focusing on known attacks that are application- (and file-) based. That said, it should also be acknowledged that more modern implementations are increasingly incorporating positive-model elements, such as anomaly or heuristic-based threat detection. Advanced antivirus products should also incorporate antispware capabilities, thereby providing protection against nuisance adware as well as more serious threats such as keylogger Trojans.

### ***Host intrusion protection***

This countermeasure is complementary to antivirus in that it provides protection against unknown attacks that operate at the system and application levels. The techniques for accomplishing this inevitably vary from one product to the next, but in general involve preventing application and operating system behaviors that are either known a priori to be bad (e.g., an unauthorized application trying to modify the registry) or that are dynamically determined to be bad via pre-execution analysis. Overall this can be a very powerful countermeasure, even though avoiding excessive false positives requires most implementations to either: (a) conduct periodic profiling of “normal” system behavior, or (b) provide protection for a somewhat smaller subset of attacks (i.e., only those which exhibit behaviors that correlate to actual attacks nearly 100% of the time).

### ***Buffer-overflow protection***

Also referred to as memory protection, this countermeasure is intended to prevent known and unknown attacks that attempt to exploit buffer overflow vulnerabilities. It is based on monitoring system memory for the occurrence of a buffer overflow and then stopping the executable code (i.e., payload) that has been injected into the system. However, because the buffer overflow itself is not prevented, a (relatively minor) denial-of-service attack may still occur as corruption of the system’s memory may require one or more processes—or the entire system—to be restarted. Typically, buffer-overflow protection will not be a stand-alone countermeasure. Instead, it is usually included as a feature of another product, such as host intrusion protection.

### ***File/disk encryption***

All too often encryption of stored data is a neglected part of an endpoint security strategy. In general, it cannot prevent an attack, and in many cases, ironically, it will not even prevent access to sensitive information (e.g., when an attacker assumes the rights of an endpoint’s user). However, file and disk encryption is indisputably effective, particularly for laptops, in the event that the endpoint is physically stolen. In any event, in this age of regulatory compliance and heightened sensitivity for data privacy, it is a countermeasure that is increasingly getting attention. This is particularly true for any endpoints that are deemed “critical” based on the nature (and quantity) of the information they store.

### **Securing unmanaged endpoints**

The challenge with unmanaged nodes is that they do in fact have access to sensitive information; do in fact pose a threat to your computing environment; but are not, in fact, under your organization's control. The primary implication is that using persistent agents with extensive protective capabilities is generally not an option for securing them. Instead, any protective measures that are used must be ephemeral. They cannot impose any changes or restrictions on the endpoint beyond the duration of a specific application session or its connection to a protected network. Due to its transitory nature, this type of protection is often referred to as being "on-demand."

Scenarios where such on-demand protection would be applicable include onsite guest access, customer access to e-commerce applications, partner extranet access, and employee access from public kiosks or home computers. Significantly, not only would this protect the interests of the organization, but it would also enable the organization to extend a value-added service to its customers. For example, with such on-demand protection capabilities, a financial institution or credit reporting agency could assure customers that data downloaded from its site is indeed safe from interception.

It should also be noted that a consequence of needing to be ephemeral is that available countermeasures tend to be dependent upon browser technology. This is true at a minimum for delivery of the associated security code and, in many cases, also represents the scope of the countermeasure's applicability (i.e., only for Web-accessible services and applications). Fortunately, this should not be a significant limitation since the majority of access by unmanaged nodes is indeed conducted via a Web browser, or is at least readily adaptable to this approach.

In any event, not only should a comprehensive endpoint security solution support unmanaged nodes, but in doing so it should also provide, at a minimum, the following set of associated countermeasures.

### ***On-demand host integrity checking***

This is completely analogous to the previously discussed host integrity checking countermeasure. The only exception is that the scope of audit capabilities may be somewhat reduced as a result of the ephemeral agent not having the same system-level rights as a permanently installed agent.

### ***On-demand cache cleaning***

This countermeasure is responsible for removing information remnants from browser- and even application-specific caches upon completion of an access session.

### ***On-demand malicious code protection***

This countermeasure involves identifying keylogger Trojans and other malicious code that may reside on an endpoint, potentially even despite the presence of an antivirus package. This is typically accomplished via behavioral analysis techniques. Also, since removal of malware is not usually possible in an on-demand scenario, the response will be limited to (optionally) blocking access from the infected endpoint.

### ***On-demand firewall***

This is similar to the previously discussed firewall countermeasure, with the exception that it typically involves far fewer connection control capabilities (e.g., the ability to prevent split tunneling) as a result of the ephemeral agent not operating with full system-level rights.

### ***On-demand secure virtual workspace***

This is a countermeasure that helps ensure against information leakage by creating an encrypted workspace on the endpoint. Typically the workspace and any associated information will be deleted upon completion of the session. However, advanced implementations will support optionally retaining it as a password-protected file.

### **Other practical matters**

Having a full set of protection capabilities for both managed and unmanaged nodes is certainly a necessary element of a comprehensive endpoint security solution. However, it is not sufficient. In particular, having to deploy all of the previously discussed countermeasures separately would be both cumbersome and costly. As a result, an ideal solution should also exhibit the following beneficial characteristics.

- All countermeasures for either population of endpoints (i.e., managed and unmanaged) should be available not necessarily as a single software agent, but at least as part of a unified agent architecture. What this means is that administrators should be able to select (and license) whichever countermeasures are deemed necessary for a given group of endpoints and then have those be deployed as a single, ideally integrated, package. Furthermore, it would be appropriate for this architecture to be extensible. In other words, as new countermeasures are developed, they can be made available in the same manner, as opposed to requiring entirely separate products to be implemented.
- All countermeasures should be administered via a single, centralized management system. Appropriate features include integrated policy development, both push and pull configuration update capabilities, role-based administration, monitoring and alerting, consolidated logging and reporting, and integration with corporate identity and policy stores.

### **An ideal solution in the making**

By this point it should be clear that the goal when it comes to endpoint security is to enable maximum protection with minimal total cost of ownership by consolidating the functionality of numerous point products into a single, comprehensive solution.

## The Essential Elements of Comprehensive Endpoint Security

It should also be clear that this is a goal that Symantec both understands and is actively working to achieve. Its acquisition of Sygate, in particular, serves to demonstrate this point. Sygate's technology and product portfolio complements and vastly enhances Symantec's existing products and services (see table).

### ***Symantec + Sygate = Endpoint Security Success***

Symantec	Sygate
Symantec AntiVirus™ Corporate Edition	Enterprise Protection (pFW, AC, NIP, HIP, BOP)
Critical System Protection (HIP, BOP)	On-Demand (comprehensive)
Client Security (pFW, NIP)	Network Access Control (with HIC)
Enterprise-class management	Enterprise-class management

Key: pFW = personal firewall; AC = application control; NIP = network intrusion protection;  
HIP = host intrusion protection; BOP = buffer-overflow protection; HIC = host integrity checking

In addition, Symantec's earlier acquisition of WholeSecurity should not be overlooked, as it further contributed to the breadth and depth of the on-demand security and malicious code protection capabilities that are now available in Symantec's portfolio.

Of course, what remains to be seen is tangible progress toward achieving a unified agent architecture and a single, integrated management system for all of these countermeasures. However, it would be logical to conclude that this is indeed the direction in which Symantec is headed. And, in any case, it should be evident that when it comes to endpoint security, Symantec will be a force that must be reckoned with, both now and in the future.

### **About the author**

Mark Bouchard, CISSP, is the founder of Missing Link Security Services, LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mr. Bouchard has assessed and projected the business and technology trends pertaining to a wide range of information security topics for nearly 10 years. He has established a reputation for thought leadership and is a sought-after speaker in the areas of security architecture, DMZ design, secure remote access, network security, and related technologies (e.g., firewalls, intrusion prevention systems, and virtual private networking).



## **About Symantec**

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit [www.symantec.com](http://www.symantec.com).

For additional information in the U.S. call toll-free 1 (800) 745-6054 or visit <http://ses.symantec.com/secureapps>.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, Symantec AntiVirus, Sygate and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. 02/06 10552718