



# WHITE PAPER

## **Developing a Collaborative Endpoint Security Solution: Why perimeter security is not enough...**

*By Mark Edmead*

## TABLE OF CONTENTS

### **Developing a Collaborative Endpoint Security Solution: Why perimeter security is not enough...**

Overview .....	3
What is Endpoint Security? .....	4
The Business Need for Security .....	5
Business Assets Are At Risk.....	5
The Threats Are Increasing.....	6
Technology Best Practices.....	7
Strong Security Policy .....	8
Hardware and Software Inventory.....	8
Scan Ports and Services.....	8
Patch Management.....	8
Security Management.....	9
Conclusion .....	9
About the Author .....	10
Corporate Background .....	11

## Overview

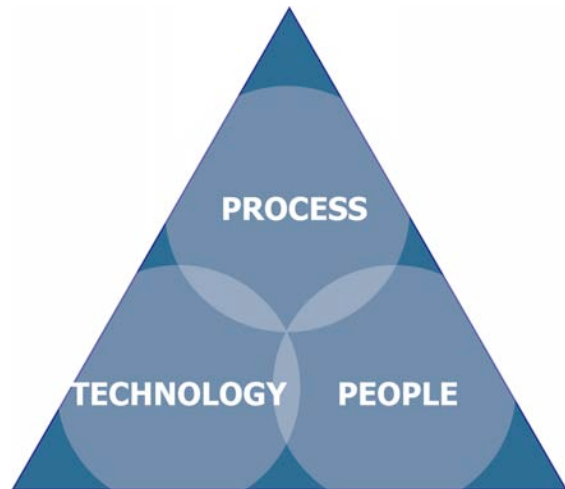
The classic definition of information security states that the goal is to protect information from possible breaches in confidentiality, integrity, or availability. Attacks come from many different places. Exposure to threats is all around us. Increased connectivity to the Internet results in more threats. These threats, combined with the vulnerabilities and weaknesses of our systems, result in a potential risk to the infrastructure.

Information security is not a standalone process. Security is not a separate entity, but should be considered as a critical element of your business operations. More importantly, information security is more than just a product you install on your network. Technology is an important aspect of security, but two other areas also require consideration. Security is comprised of technology, processes, and people. Each element is a critical point of the information security triangle. A change in one of these areas affects the other two. For instance, if a company applies new technology, such as a wireless LAN, they need to consider how the introduction of this new technology affects the processes (business or technology) involved and the people using (or operating) the technology. What this means is that an effective security approach goes beyond just applying technology. An effective security infrastructure addresses not only the technology, but also the process affected and the people involved in the use (or management) of the technology. People manage technology devices and security configurations; this is where many security problems reside. Unfortunately, people are the weakest link when it comes to information security.

---

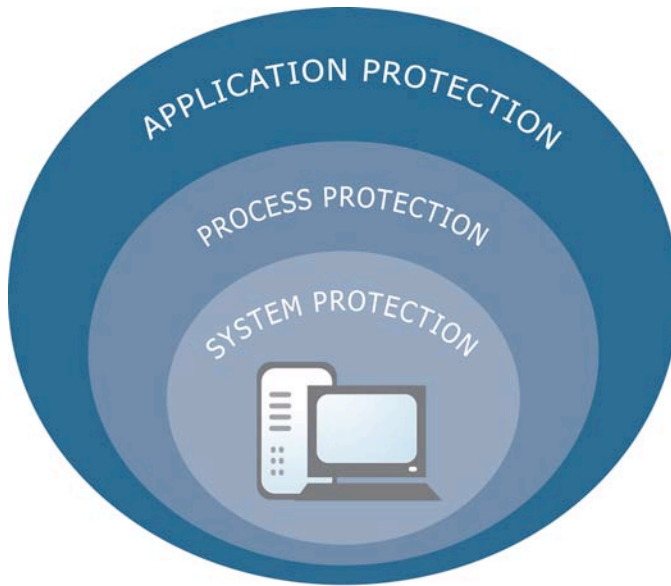
### THE SECURITY TRIAD

Information security can be implemented in a number of different ways. The main focus of information security is to protect an asset from a breach in confidentiality, integrity, or availability. Confidentiality means that the information or the asset remains available only to the authorized individual or process. Integrity refers to making sure that there are no unauthorized changes to the asset either by authorized or unauthorized individuals. Availability means that the information or asset is available when needed. Diagram 2 shows the typical representation of the "layered" or "ring" security architecture model. The outside ring provides the perimeter security. It is possible to have multiple rings that protect the inner layer. The inner layer represents the information or asset we wish to protect.



## DEFENSE IN DEPTH SECURITY

---



Some people like to think of security as a hard candy with a soft filling. That is, hard security on the outside and soft security on the inside. The old way of thinking is that all that was required to implement a secure environment was a hard outside. That would prevent all attacks to the inner circle. This approach does not consider one important factor. It addresses only potential attacks from an external source and not a potential attack from an internal source.

Implementing effective security architecture requires more than just a hard shell to protect from external attacks. Information security goes beyond addressing just technology. A collaborative approach to end-point security should include systems management tasks such as configuration and patch management. In the past, when the focus was on perimeter security,

companies believed coordination between their security and systems management organizations was unnecessary. However, with the new focus on end-point security, coordination between security and systems management organizations is critical to ensure effective security solution.

---

### What is Endpoint Security?

Perhaps we should answer the question: What is an endpoint? The term endpoint has been used in a number of different ways. For this whitepaper, an endpoint is an individual computer system or device that acts as a network client. Some common endpoints are desktops, laptops, application servers on the network, and personal digital assistants (PDAs).

Endpoint security includes all of the measures (with respect to process, technology, and people) taken to implement security concerning endpoints. These measures include determining the risk required to protect endpoints to protecting the network from the endpoints themselves. Endpoint security also includes the management and administration of these security measures, including risk management and reporting.

The term "host security" usually refers to a host system that includes configuration management, virus protection, host intrusion detection/protection, and some firewall capabilities. However, this system is only effective if it is configured correctly. This host security configuration might be able

**"An endpoint is an individual computer system or device that acts as a network client."**

to provide some reasonable protection from the outside layers, but will fail when facing attacks from areas invisible to the outer network security layers, such as attacks from "inside" the network.

## The Business Need for Security

The old school of thought is that perimeter security was enough to protect your network. All of your valuable information was contained inside the network, so perimeter security was all you need for protection. This works in theory, but reality is a different story. A company's sensitive and valuable information does not always remain inside the company. People are the weakest link when it comes to information security. Employees and contractors, with access to the internal network, copy information from inside the network onto laptops. They can take that information out of the protective shell of perimeter defenses. In recent months, many companies have lost valuable information residing on laptops.

The technology landscape is changing dramatically and constantly. New threats emerge on a regular basis. These threats exploit the inherent weaknesses or vulnerabilities. The typical perimeter security devices, such as firewalls, routers and perhaps a network intrusion detection system (NIDS) provide some good security protection against attacks. The challenge however, is that this type of security architecture only works when these devices can inspect and sanitize the network traffic BEFORE it enters the internal network. However, network-based security solutions cannot detect, let alone prevent, attacks they cannot see.

The other challenge facing management is to decide how much security is enough? If you don't enable enough security, the chances of unauthorized use increases. And if we implement too much security, authorized users will have to do more in order to get access (i.e. long and complex passwords, multi-factor authentication). The goal is to have just enough security to allow authorized users reasonable, easy access to the resources while having enough security so that unauthorized users are denied access. If, for instance, you institute a password policy with complex passwords (e.g. 14 character passwords, changes every 15 days, complex passwords), many users will probably start writing down the passwords on a post-it note and stick it to the bottom of their keyboard. This, of course, defeats the whole purpose of having passwords.

Another risk area is the use of peer-to-peer (P2P) file sharing. The use of P2P has become more prolific; not only because of the convenience, but also because of the increased deployment of broadband. There are numerous security risks inherent in P2P clients such as Morpheus, KaZaA, and others. P2P's main feature, enabling direct communication between peers, offers the greatest security risk. Information can cross security measures such as firewalls. The use of P2P can result in insecure configurations and covert user-initiated connections to external networks.

Technology in itself is not bad. But implementing technology without considering the security ramifications increases risk. We want employees to be productive. Technology helps increase productivity. Take wireless LAN, for instance. The ability to have a WLAN allows users to access public Wi-Fi networks on the road. Wi-Fi connections are available at airports, coffee shops, bookstores, and hotels. But using an unsecured Wi-Fi connection could lead to a breach in confidentiality and integrity. Wi-Fi connections, even with WEP enabled, are inherently insecure. Would it be wise to have your employees transmitting sensitive corporate information over the Internet using an unsecured Wi-Fi connection? And what if these laptops become infected with a virus, worm, or other malware and are connected to the office network?

## Business Assets at Risk

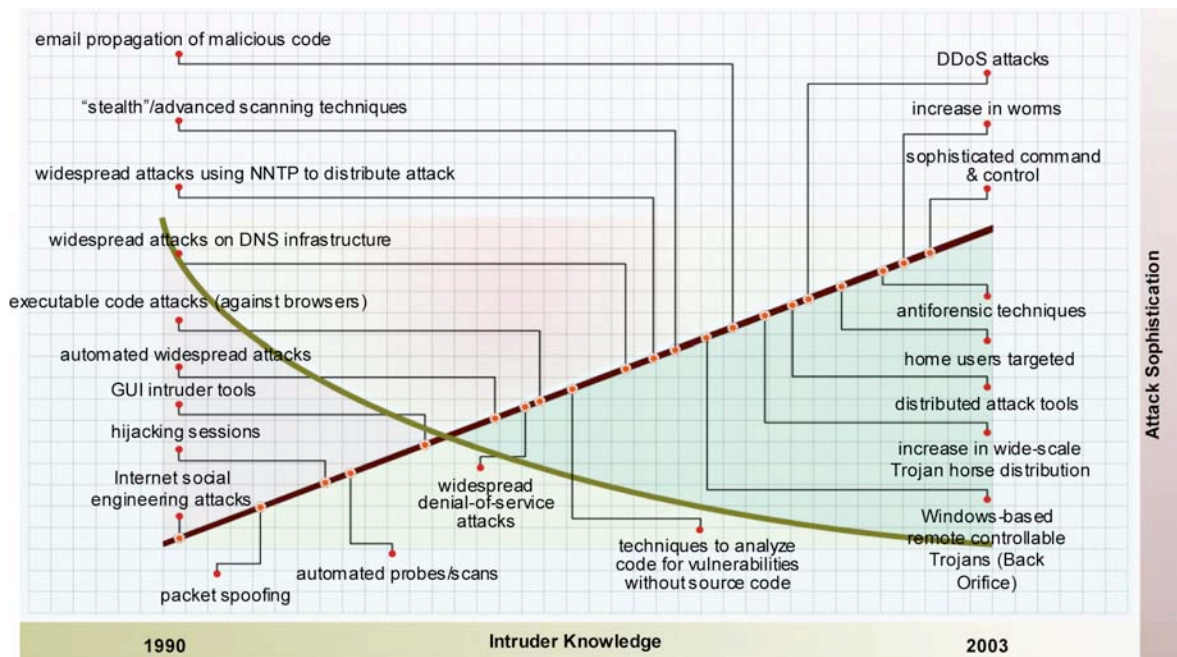
What exactly are we protecting? What business assets are at risk? Business asset risks can be divided into two groups: direct losses and indirect losses. Theft and productivity loss are two examples of direct losses. The theft could be of actual money, trade secrets, digital assets, computer resources, or consumer information. Productivity loss examples include recovery expenses and corruption of data. Examples of indirect losses include loss of potential sales, loss of competitive advantage, or negative brand impact. And in recent years, the big focus is on legal

exposure. This could mean failure to meet regulatory compliance laws (i.e. Sarbanes-Oxley, HIPAA, GLBA, SB-1386).

## The Threats Are Increasing

The increasing number and variety of threats to endpoints has recently made endpoint security a "hot topic." Current threats to endpoint security include viruses, Trojans, worms, the use of endpoints as Distributed Denial of Service (DDoS) zombie hosts, and spyware. New threats and new types of threats emerge on a regular basis. Enterprises end up with extreme vulnerability to a bewildering array of threats that increase each day. Endpoints are where the typical enterprise conducts most of its business, and disruption to endpoints is a huge impact to enterprises in terms of cost and lost productivity. Since endpoints are now a primary target of these threats, enterprises are forced by necessity to confront endpoint security as a core business issue.

Our challenge is that the level of expertise required to execute an attack is decreasing. Figure 1, taken from a presentation on Internet User Security by Laurence Rogers of the Software Engineering Institute at Carnegie Mellon University, shows the attack sophistication versus the technical knowledge required by the intruder. As you can see, the knowledge required to operate these hacker tools is decreasing. This means that anyone, with just a little knowledge, can attempt to compromise systems.



©2005 Carnegie Mellon University (Lawrence R. Rogers, Author)  
 \*CERT® Training and Education Home Computer and Internet User Security

The business need for security is to protect both the network and data from a single, central location. This requires the ability to identify network devices and the software installed on each computer. This information can be used to assess vulnerabilities to known configuration and security issues. If the vulnerability is mitigated by installing a patch, it is important to have the ability to access, sort, prioritize and install these patches.

Many of today's exploits involve malicious software covertly installed onto unsuspecting machines. An effective endpoint security framework incorporates the detection and removal of all forms of spyware, adware, key-loggers, and other forms of malware. Other business needs include preventing unauthorized software from running on your system, restricting endpoint access to unknown ports, and reporting security status at any time.

## Technology Best Practices

It might be beneficial to think of security in terms of what a hacker does in order to gain access to your network. As we stated earlier, our goal is to protect ourselves from hacker attacks. So what does a hacker do in order to gain and compromise a system? The typical hacker attack phases are:

1. Footprinting
2. Scanning
3. Enumeration and vulnerability identification
4. Penetration
5. Privilege escalation
6. Evidence elimination
7. Staging the return

Footprinting and scanning are methods used by hackers to gather intelligence about your network. Information gathered includes IP addresses, machine locations and so on. Scanning is used to map out the network and identify specific information such as services running, open ports, protocols, and applications running on the machines. With this information, a hacker can then determine if there are any known vulnerabilities they can exploit. Once a vulnerability is exploited and the hacker gains access, they have the keys to the kingdom. They can possibly create new accounts; install Trojans, rootkits, and sniffers. This is why it is critical that you know what is on your network and more importantly, identify the potential weaknesses before the attackers do.

As security professionals, we need to learn how to counteract these attacks. Companies are well advised to incorporate the technology 'best practices' for security protection. The easiest way to think of this is to put it in terms of a process flow or security 'lifecycle.' A total enterprise security process is comprised of five (5) main processes. They are:

1. Issue a security policy
2. Design security defenses
3. Perform active monitoring
4. Perform intrusion testing
5. Security management

How does this translate into actions an IT administrator can take to protect their network? Let's address each one of the security processes:

## Strong Security Policy

The first step is to develop a security policy. A security policy is a formal statement that dictates how security will be implemented in the organization. A security policy should define the level of security and the roles and responsibilities of managers, administrators, and users. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities. Another policy example is a policy for the use of wireless LAN (Wi-Fi) in an organization. One of the great things about Wi-Fi is that you can go to your local computer store, purchase a Wi-Fi access point for less than \$100, connect it to the network, and have wireless access. The bad thing about Wi-Fi is that you can go to your local computer store, purchase a Wi-Fi access point for less than \$100, connect it to the network, and have wireless access. That is, it is so easy to add new technology to your network that if you don't consider the type of policy for the technology use, the organization is open to possible attacks. A security policy helps define acceptable use of the technology and enables everyone to understand the risks associated with using the technology.

**"If you don't consider the type of policy for technology use, the organization is open to possible attacks."**

## Hardware and Software Inventory

Before we can design our security defenses, we need to fully understand what it is we are protecting. This is accomplished by obtaining a full hardware and software inventory of your network. This inventory shows you what's running on your network so you can more effectively identify all computers in your environment and formulate your overall endpoint security plan. This list will help identify which default installations provide weak security configurations. A hardware and software inventory will help identify new systems that might have connected to the network and determine if they pose a security threat due to unauthorized connections or insecure configuration. Take the Wi-Fi example again. An employee might have connected a Wi-Fi access point without permission. A hardware scan of the network would identify this "rogue" access point and give you the opportunity to disconnect the device from the network before it can be used to gain unauthorized access.

## Scan Ports and Services

The next step is to monitor (not just once, but continuously) what is going on in your network. By performing vulnerability scanning, you can identify known configuration and patch vulnerabilities that can be used to quickly find and remediate potential security threats. Vulnerability scanning involves scanning for unused or unnecessary ports and services. Many system default configurations have running services (such as Telnet or SNMP) that can pose a security threat. The same concept applies to open ports. Many systems have open ports that are not used. These ports could be used by attackers to gain access to the system. Intrusion testing (also known as penetration testing) is a more invasive form of determining the vulnerabilities of your network. This is where in addition to scanning for vulnerable ports and services; you actually try to exploit these weaknesses in order to gain unauthorized access.

## Patch Management

When vulnerabilities are found, in most cases it can be remediated by installing a patch. This vulnerability is why it is critical that all of the operating systems and applications are updated with the latest patches. Keeping your systems patched will help close vulnerabilities that can be exploited by hackers. Patch management is the process of controlling the deployment and

maintenance of your operating systems, applications, and network devices. It helps you to maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain the stability of your environment.

## **Security Management – Keeping your eye on the ball**

A very critical and often overlooked phase of the security process is security management. Enabling security is not a device you install one time with no other requirements. Security controls are only effective if you closely monitor the controls and respond in real-time to any indication that your system has been compromised. Security is a continuous business improvement effort. Because our environment changes (i.e. changes to process, technology, and people), what used to be a secure system before might not be a security system today. New threats are presenting themselves constantly and we need to be proactive rather than reactive when it comes to securing the network.

## **Conclusion**

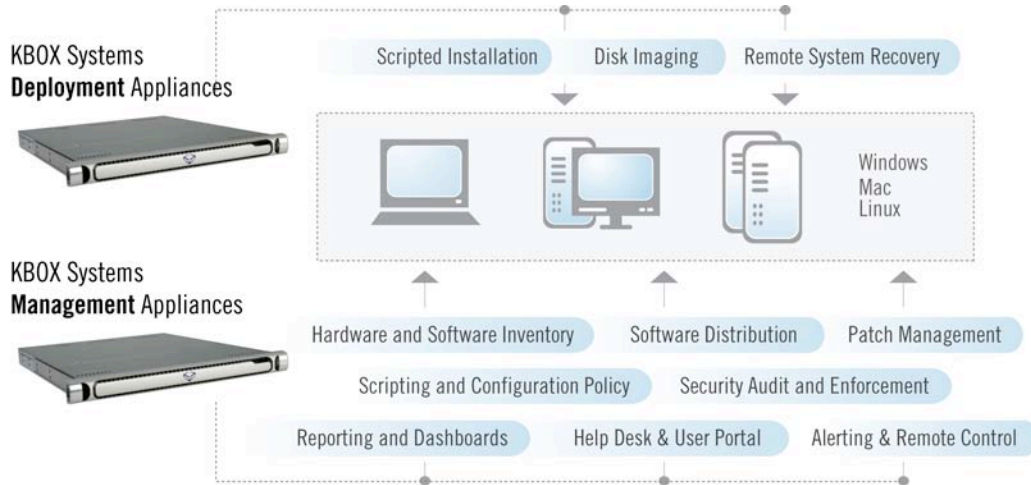
Maintaining network security is an on-going process. This means that our work is never quite done. Computer and network security is fundamental to doing business. Attacks on our network infrastructure make it harder to do business. Attacks cost money, have the potential to cause unbounded losses, and could result in bad publicity. Traditionally, computer and network security had been a “technology” issue. That is, use only technology (i.e. encryption, firewalls, IDSs, etc.) and the problem would be resolved. The myth was that only technology can counter the threats and that only technology can make us secure.

As we have seen, this traditional approach does not work. Computer and network security is getting worse. And while defensive technologies are getting better, so are the attack technologies. Combine this with the fact that our network environment is getting riskier: more users, more critical applications, and more dependency on the Internet.

The solution is to think of security as a process and take a proactive approach rather than a reactive approach. We need to fully understand our computing network and its vulnerabilities. We need to mitigate these vulnerabilities and closely monitor our systems to make sure we are secure as possible. We need to quickly respond to possible attacks and learn from these incidents. We need to continuously adapt to our environment and realize that if we don't, we will ultimately be vulnerable to attacks.

## The KACE for KBOX

KBOX™ appliances are comprehensive, secure and make it easy and affordable for IT professionals to deploy and manage networked computers. Utilizing an appliance-based architecture, KBOX appliances deliver a complete, pre-integrated bundle of operating environment and application software via a dedicated server appliance. KBOX appliances provide support for a wide range of laptop, desktop and server platforms including Windows, Macintosh and Linux.



### End-to-End Automation with the KBOX™ Appliance Family

KBOX provides exceptional performance, reliability, and scalability through a purpose-built comprehensive systems management solution that provides functionality ranging from HW/SW inventory to distribution, patch management, disk imaging and security.

## About the Author

Mark Edmead has over 25 years of experience in computer systems architecture, information security, and project management. Mark has extensive knowledge in IT and Application audits, IT Governance, including Sarbanes-Oxley compliance auditing. He understands all aspects of information security and protection including access controls, cryptography, security management practices, network and Internet security, computer security law and investigations, and physical security. Mark has consulted with Fortune 500 and Fortune 1000 companies in the areas of information systems, and Internet security. He has worked with many international firms, and has delivered security presentations in Japan, China, Singapore and Europe. He has taught advanced Windows security courses and presented technical papers on Windows performance and implementing information security solutions at numerous conferences worldwide. He currently teaches audit and IT security courses for the Institute of Internal Auditors (IIA) and Learning Tree International.

\*CERT, CERT Coordination Center and Carnegie Mellon are registered in the U.S. Patent and Trademark Office.



## Corporate Background

KACE™ is the leading systems management appliance company. The award-winning KBOX™ family of appliances delivers easy-to-use, comprehensive systems management capabilities. KACE customers usually install in one day and enjoy the lowest total cost compared to software alternatives.

KACE is headquartered in Mountain View California. To learn more about KACE and its product offerings, please visit <http://www.kace.com> or call **1-877-MGMT-DONE**.

## Corporate Headquarters

1616 North Shoreline  
Mountain View, California 94043  
(888) MGMT-DONE office for all inquiries  
(+1) (650) 316-1050 International  
(650) 649-1806 fax

## Email & Web

Sales and partnering: [info@kace.com](mailto:info@kace.com)  
Support: [support@kace.com](mailto:support@kace.com)  
Other Information: [info@kace.com](mailto:info@kace.com)  
On the Web: <http://www.kace.com>