IDC
Analyze the Future

# WHITE PAPER

## Endpoint Security: Proactive Solutions for Networkwide Platforms

Sponsored by: ESET

Andrew J. Hanson Brian E. Burke
Gerry Pintal

February 2009

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

## IDC OPINION

The past few years have witnessed several highly publicized cases of security breaches at major corporations. These high-profile incidents have emphasized the need to protect and control sensitive corporate information within the enterprise environment. As more data resides at the endpoint, administrators are being forced to defend a new architecture that has critical corporate resources dispersed around the globe. Fortifying the network perimeter, essentially placing sensitive data in a locked vault with towering walls, is no longer sufficient for enterprise security. The focus of many security solutions is rapidly moving away from a network-centric perspective and concentrating on the endpoints. Additionally, the threat landscape is evolving at an exponential rate that cannot be addressed by traditional security solutions.

Highlights of this white paper include:

- Proactive, heuristic scanning is increasingly necessary to protect endpoints from previously unknown dangers as the threat landscape develops at an alarming rate.

- Heuristic scanning is the first line of defense for the endpoint but should be complemented by integrated traditional security features.

- A growing number of antimalware applications necessary to protect endpoints will require an integrated and centralized management console.

- Security solutions must function as business enablers by improving system performance and not disrupting the user experience.

## IN THIS WHITE PAPER

This white paper examines the looming threat horizon that is forcing companies to reexamine their endpoint security functions and discusses ESET's solution for integrated security management that is built around its advanced heuristic technology. The threat landscape facing businesses has evolved significantly, and corporations are looking for security products that can protect against known threats and prepare for future attackers in a simple-to-use architecture.

# METHODOLOGY

IDC developed this white paper using existing market forecasts and direct, in-depth primary research. To gain insight into the needs of businesses and how such needs are being met by ESET's security portfolio, IDC conducted interviews with IT executives at companies of various sizes in several industry sectors. Additionally, IDC met with representatives from ESET to review their goals and tactics. This white paper reflects all of these research perspectives.

# SITUATION OVERVIEW

The nature of corporate IT security changed dramatically in the past decade. The expansion of the Internet has created an explosion of new technologies, services, and capabilities available to businesses via the Web. The cost of reaching an unlimited base of customers globally has all but disappeared. At the same time, business executives are finding that the Internet offers the prospect of lowering capital expenditures by providing access to remote workers, both locally and internationally.

This dramatic shift in network architecture has IT administrators scrambling to secure endpoints. In many cases, the obvious solution would be to restrict user privileges on a device, but this approach is ruled out because Internet connectivity and the necessary plug-ins associated with it are part of today's everyday operations. To restrict the user's ability to modify his or her system would inhibit daily tasks and flood IT departments with unrelenting demands for program approvals and system adjustments, resulting in what IDC refers to as "message fatigue": when users and administrators alike grow weary of constant warning messages commandeering their screen and begin simply clicking through them as opposed to reading the critical information being displayed.

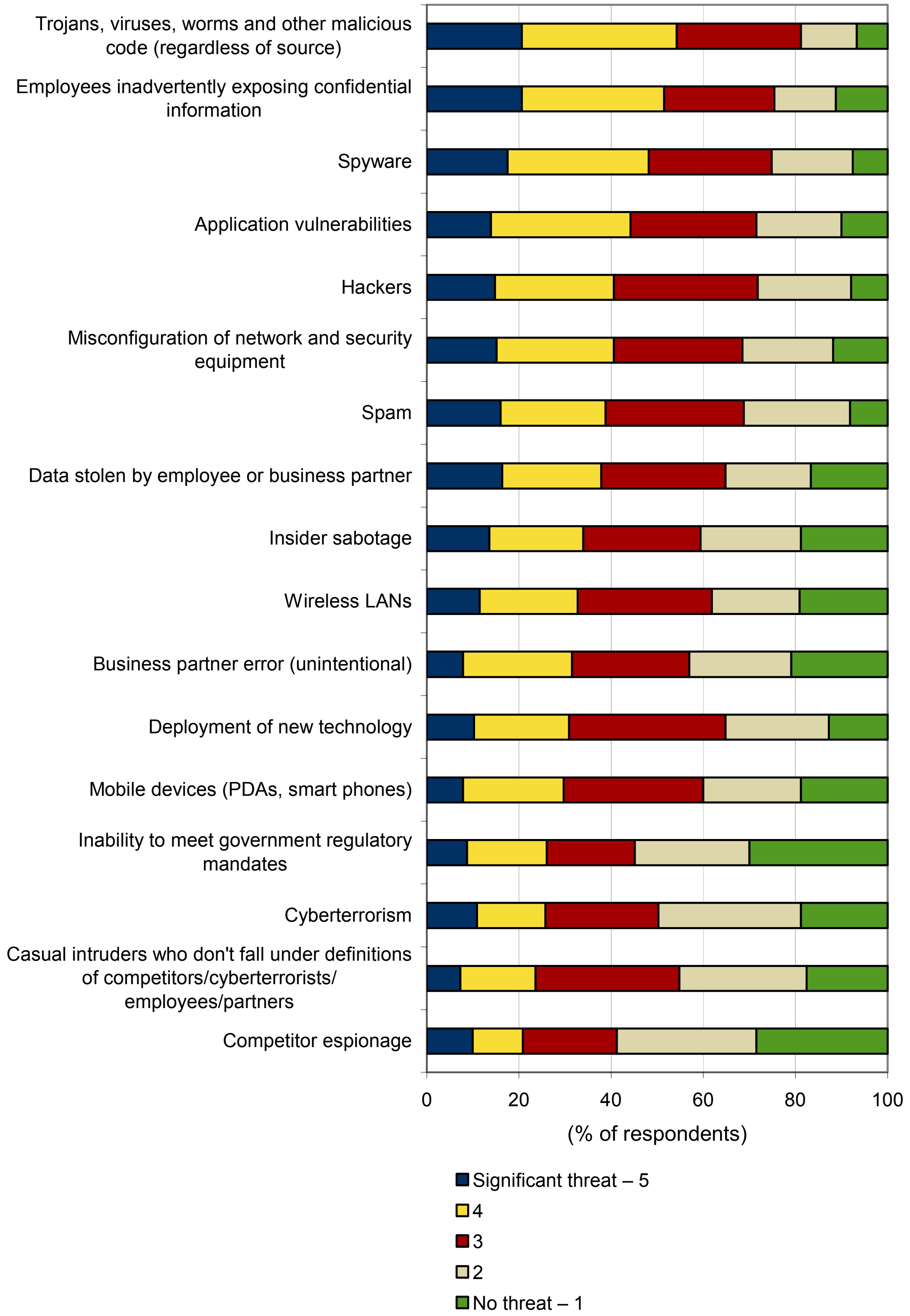
## The New Threat Landscape

In the not too distant past, security administrators' greatest fear was that a virus, worm, or other form of malware would penetrate the firewall and crash the system. Whether for prestige, revenge, sheer challenge, or merely to wreak havoc on the Internet, hackers could cost businesses millions of dollars in lost revenue while the network was offline. The attackers could be considered gifted misfits or troublemakers who were looking for attention or the simple pleasure of interrupting progress and business processes. They were glorified by movies such as *Hackers* and *The Matrix* trilogy. They obtained prestige with public exploits, allegedly fighting the establishment behind made-up "handles" such as Dark Avenger, v00d00, and ne0h.

In IDC's 2008 *Enterprise Security Survey*, malicious code bumped employee exposure as the number 1 threat to the enterprise network, reclaiming its traditional position as the premier threat (see Figure 1).

## FIGURE 1

Top Threats to the Enterprise



Source: IDC's *Enterprise Security Survey*, 2008

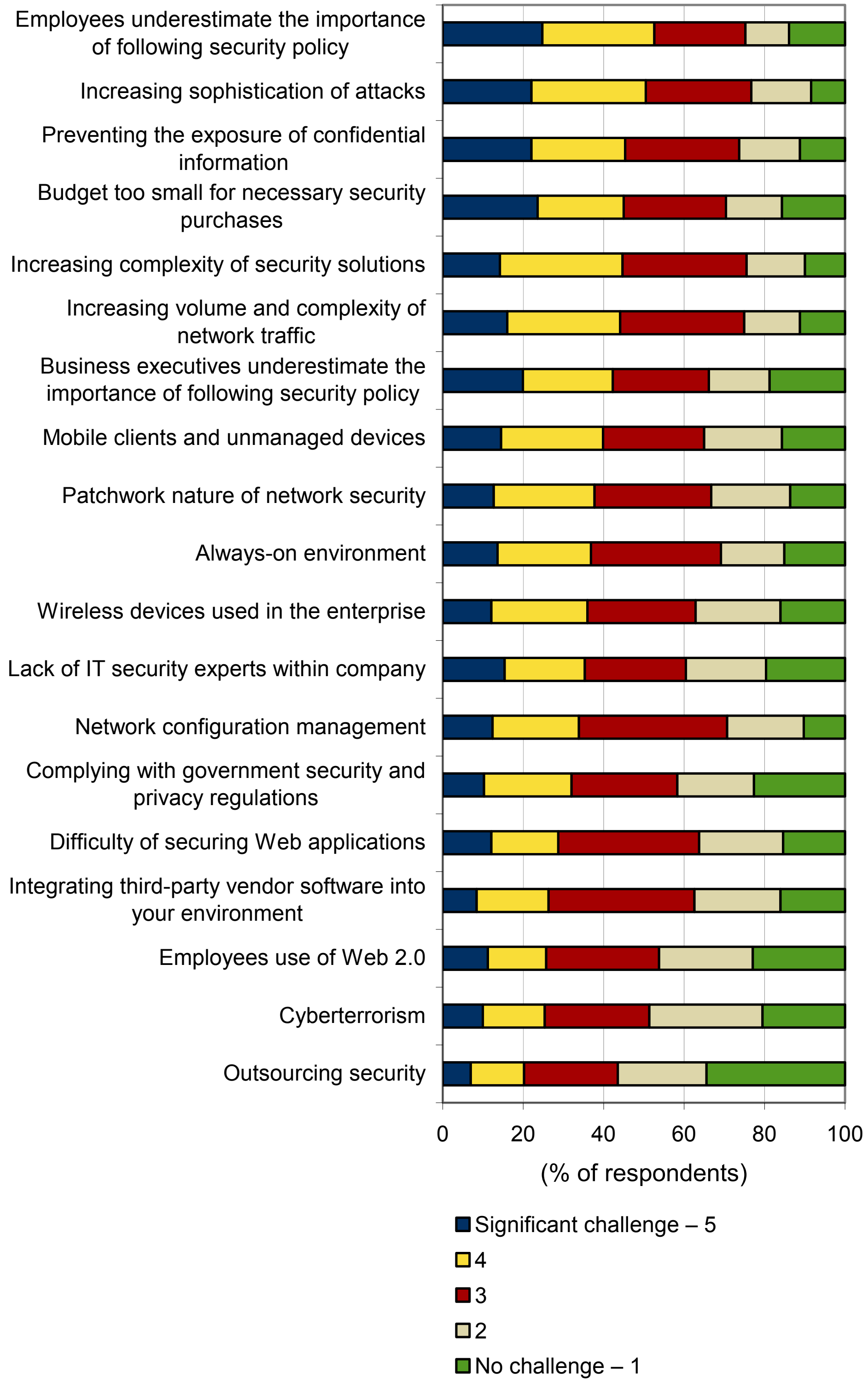
The complexity of threats and the complexity of security solutions have traditionally gone hand in hand as security vendors developed new solutions to address specific threats. However, the exponential growth of threat models demands a new protection architecture. The sprawl of point products and single-function security solutions has reached a level where it could actually be detrimental to corporate security. IT administrators are quickly being overwhelmed not only by the number of threats they face but also by the burden of managing and integrating a network built with an assortment of technologies, platforms, and vendors. This situation is getting worse as the threat environment develops at an astonishing pace.

Today, the threats and the attackers behind them have evolved to be much more dangerous to enterprise security. They are profit driven, highly organized, and discreet. As the capabilities and features available on the Internet continue to evolve, cyberspace criminals are also improving their techniques, knowledge, and organization. There is a black market of Internet security developing in which standard market values are assigned to various types of sensitive data, such as Social Security numbers, credit card numbers, access codes, and so on. A crashed network hurts the company's bottom line, but to have an endpoint that contains sensitive data infiltrated without the administrator's knowledge can bolster an assailant's bank account and harm the company's customers. Attackers are now searching for specific information and are attempting to acquire it without alerting endpoint users and security administrators. As has always been the case, an attacked company can expect a significant financial loss at a minimum. With the new nature of threats, the consequences likely will be more severe and possibly irreversible, including loss of intellectual capital, bad press, damage to the brand name, loss of customer confidence, and finally, civil or criminal penalties resulting from failing compliance requirements.

Furthermore, attackers are becoming more skilled at techniques used to violate endpoint security. Combining a variety of threat profiles and exponentially increasing the number of variants to each malware algorithm, attackers are finding ways around targeted security solutions. IDC expects that threats to the endpoint will only increase in number and variety. Users must be prepared to protect against a combination of zero-day attacks, viruses, trojans, worms, botnet attacks, rootkits, adware, spam, and social engineering attacks. IDC's 2008 *Enterprise Security Survey* found that the sophistication of attacks will be the second greatest challenge to security administrators in the near future (see Figure 2).

## FIGURE 2

Top Security Challenges in the Next 12 Months



Source: IDC's *Enterprise Security Survey*, 2008

### *Limitations of Signature Scanning*

Signature scanning was previously capable, for the most part, of restraining major malware outbreaks. Obviously, this does not imply that all damage was averted, but earlier generations of both networks and threats limited the ability of threats to proliferate rapidly among various endpoints. When a new virus was recognized, infected machines or networks, which were disturbingly similar to sacrificial offerings to the religion of IT security, were quarantined, security vendors would analyze the virus' properties, and a signature file-update was released to customers. Security vendors cooperated to share the new virus signatures in order to roll out the solution as quickly as possible to contain the outbreak and protect users.

Once a virus signature has been identified and the patch rolled out, signature scanning is highly effective at preventing that specific virus. Nonetheless, this process is no longer sufficient to respond to the overwhelming number, variety, and speed of today's attacks. Vendors' ability to analyze and generate signatures is under stress, and signature databases are also growing unwieldy. This affects vendors' ability to distribute signature updates and the speed of the signature matching approach. Some vendors have turned to in-the-cloud antivirus to alleviate this pain. To effectively protect endpoints in today's threat landscape, security vendors must concoct a "crystal ball" of antivirus to provide the foresight that surpasses signature-scanning technologies.

### *Benefits of Heuristic Scanning*

Proactive scanning tools can complement traditional antivirus products that scan for known threats. Many security vendors are delivering new security products that scan files and network activity for threatlike behavior in order to recognize unknown threats before their execution. Known as heuristic scanning, this technology goes beyond recognizing threatening code, packet sequences, or file types to examine the conduct of programs running in the endpoint. Signature scanning asks, "Does this match a specific pattern known to exist in a previously identified threat?" However, heuristics asks, "Does the action being requested fit the expected, safe behavior, or is it looking to deviate from accepted actions?" Possible threats that deviate can be quarantined for further examination or cleaning.

### *Challenges of Heuristic Scanning*

In theory, proactive scanning is a strong addition to endpoint security platforms, but in practice, it is difficult to perfect. The effectiveness of behavior-based protection is, to some extent, dependent on the policy settings established by system administrators. It is a delicate balancing act: Policies that are too strict will prohibit necessary plug-ins, inhibit user experience, and overstimulate users and administrators with warning messages; however, policies that are too lenient, in extreme cases, would be analogous to removing the program altogether. In addition, heuristic scanning, by definition, uses behavior recognition technologies to compare misbehaving activities with the normal operation of similar file types. Therefore, this presents a learning period during which many false positives can slow device performance, preventing heuristics solutions from relying solely on behavioral analysis.

### *Scanning in the Cloud*

Recently, there has been a surge of activity by vendors to take the in-the-cloud or software-as-a-service (SaaS) approach to antivirus. By doing this, a number of potential benefits are thought to be possible. The endpoint client may lessen the demand on the CPU by analyzing new and unknown threats in a remote datacenter; it could allow a reduction in the size and frequency of virus signature database updates by deferring some decisions to be made in the cloud; and by taking a global view of the threat landscape, it may be possible to identify and curb the spread of certain malware quicker.

However, as with the in-the-cloud or SaaS approach to messaging security, there is a trade-off between offloading analysis and response latency. Furthermore, the dependency on always-on network connections, may not be possible for all users to satisfy; therefore, offline detection and cleaning of malware needs to remain robust. A hybrid approach that complements the quick response time of an endpoint antivirus solution with the global view and in-depth analysis of new and unknown threats in the cloud is likely to be embraced by most organizations.

### *Managing the Endpoint in a Dispersed Network*

It is clear that modern businesses need a wide range of security products to address a growing field of threats. The issues of managing, coordinating, and integrating multiple point products on the client device are increasing problems for security administrators, and they are compounded by the dissolving perimeter. For security applications to function properly and protect the device, they must be updated frequently with signature definitions, patches, and reconfigurations to address new vulnerabilities and threats. More advanced attacks, such as blended threats, demand that security products work in conjunction to stop a threat that would likely defeat a single line of defense.

Therefore, security customers, like customers in many technology markets, are looking to have more features baked into a smaller package that is easier to use. Consolidation is the catchphrase throughout the industry. Integrating security management will significantly reduce administrative and support costs for businesses. It not only will reduce the demands on IT personnel but also will ensure that security products are working cooperatively and efficiently to improve the productivity of users.

## BEST PRACTICES FOR ENDPOINT SECURITY

IDC's research has revealed that the following points are critical to effective and efficient endpoint security solutions:

- **Proactive security.** The threat landscape is evolving at a rate that cannot be contained by traditional signature-scanning security features. Security vendors must generate proactive security solutions that recognize the behavior of threats without relying on signature identification and analysis.

- **Performance.** Security solutions have the opportunity to shed the label of "necessary evil" and, in fact, be business enablers. Properly configured security systems should run transparently on the endpoint with minimal impact on the user experience and device performance. This will allow users to enjoy full protection without any effect on their routine actions. It is important that security vendors strive to reduce the system footprint consumed by their products.

- **Centralized management.** In the enterprise space, network administrators desire endpoint solutions that can be controlled by a limited IT staff from a centralized location. Signature, patch, policy, and configuration updates should be rolled out in networkwide deployments with minimal effort by the administrator.

- **Agile security.** Increasingly sophisticated threats and the targeted, profit-driven nature of attacks mean that any breach, no matter how small or short-lived, can result in major costs for the violated business. IT administrators are looking for security solutions that deploy quickly and easily and, most important, identify and respond to new threats as quickly as possible.

- **Integration.** It is clear that there is no simple solution for endpoint security. Complete protection requires several layers of security. For these layers to function cooperatively and efficiently, they must be integrated into a common platform.

## FUTURE OUTLOOK

In 2007, total worldwide revenue for endpoint security products reached approximately $5.6 billion, representing approximately 14% year-over-year growth. Preliminary IDC estimates suggest that 2008 revenue will grow by approximately 13% to $6.4 billion total worldwide and that over the next five years, the industry will see a compound annual growth rate of over 10%.

IDC expects enterprise users to be harassed with a variety of multifaceted threats, including viruses, spyware, worms, trojans, rootkits, adware, spam, and other sophisticated social engineering attacks. As discussed earlier, threats will increasingly be more stealthy, targeted, malicious, and organized. With the disappearance of the network perimeter, protecting critical company information will translate to securing the endpoint with the most advanced antithreat solutions available. Businesses must secure sensitive data with a variety of security features, spearheaded by advanced proactive security solutions.

IDC expects that separate client antivirus, client antispyware, client firewall, and host intrusion prevention products will increasingly be incorporated into a single, integrated offering to provide a comprehensive endpoint security solution that can manage all of the tasks previously performed by the individual products. This can increase the ease of manageability, reduce the risk of incompatibility across security functions, and minimize the endpoint security memory footprint.

Centralized management for endpoint security is becoming increasingly critical to mitigating security risk by containing malware, eliminating botnet infections, reducing unwanted software such as file sharing, and preventing data loss — especially in Web 2.0 environments.

Endpoint management provides important business benefits too, including higher user productivity, lower IT costs from less client overhead, fewer support calls to the help desk, and lower desktop management costs by stabilizing the system image. Moreover, better endpoint management can improve corporate governance and regulatory compliance.

## Case Study: United Auto Credit Corporation

United Auto Credit Corporation (UACC) was founded in 1996 by Ray C. Thousand and currently has approximately 1,000 employees. It is a wholly owned subsidiary of United PanAm Financial Corporation. The company specializes in subprime auto financing. Headquartered in Irvine, California, UACC operates 130 locations in over 30 states throughout the United States, with heavy concentration on both coasts and in the Midwest. Through its network of branch offices, it works with auto dealers to provide financing to customers with limited or impaired credit who would be unable to acquire financing from traditional lenders. As a result, the company handles large quantities of personal and financial data. The threat of a viral outbreak is secondary to information protection and control at UACC.

### *Security Architecture*

To support numerous remote sites, UACC has employed a hub-and-spoke architecture. The company has a centralized datacenter at its headquarters, while remote offices have limited PCs and Wyse Winterms connected to a private network. IT administrators at UACC estimated that there are 30 servers and 150 PCs at the headquarters and that each branch office has approximately 3 PCs, totaling approximately 600 endpoints that must be managed by an IT department of 10 people, 6 of whom directly support products and users. The company has chosen to secure all sensitive data and applications at the central datacenter. However, UACC has deployed ESET antivirus solutions on every PC and server within the network.

### *Review of Transition to ESET*

Before implementing ESET, UACC used corporate antivirus solutions from another major security vendor. According to UACC sources, ESET was considered after a trade show in early 2007. UACC representatives attending the show decided to test the ESET antivirus solution on their PCs and a trial server for one month. The administrators "aggressively trialed" the solution by intentionally visiting malicious sites and found dramatic results: ESET not only protected their systems from new threats but also discovered malware that had evaded the previous antivirus solution.

Within two months of completing the trial period, UACC decided to employ the ESET antivirus software on all corporate endpoints. The full deployment took approximately one year to complete, but UACC explained that the installation time was due in large part to internal staffing constraints, which were resolved by hiring an outside third party.

As for ESET support, UACC did not find it necessary to purchase the priority service contract offered because the company has been very pleased with the basic support package included with all ESET products.

Since completing the deployment, the IT department at UACC has experienced significant improvement in its endpoint security solution, including fewer help desk calls as well as employees reporting improved system performance. Furthermore, UACC reported that the entire ESET solution cost approximately 20% less to deploy and maintain than its previous solution. The company has successfully reduced operating expenditures, improved system performance, and increased employee satisfaction by utilizing ESET NOD32® Antivirus on all corporate endpoints.

## The ESET Endpoint Security Solution

### *Company Overview*

ESET is a privately owned software company headquartered in Bratislava, Slovakia, with offices in major cities around the globe, including its worldwide distribution headquarters in San Diego, California. Since its founding in 1992, the company has developed threat protection software to combat the rapidly evolving nature of IT security threats. The company sells its solution in over 160 countries and maintains an extensive network of global partnerships.

### *Company Strategy*

ESET recognizes that the Internet has generated avenues of communication that have contributed to the growth of the global economy and business of all sizes. To encourage this development, ESET is concentrating on securing the endpoint devices with which users access the Web. The company acknowledges that signature-based antimalware solutions are critical to enterprise security but are also lacking in foresight and proactive prevention. The company pioneers holistic security solutions that are built around advanced heuristic security and include traditional features, such as signature-based antivirus, antispyware, antispam, and so on. ESET emphasizes that these features should complement each other in a comprehensive solution with a common management console. ESET's proactive security is intended to analyze and interpret malware algorithms and behavior to stop unidentified threats before they can do damage. Instead of waiting for signature updates, ESET has generated heuristic technologies that recognize algorithms, not just bit sequences, to prevent a successful attack from a new threat. Using this approach, ESET has been able to avoid bloating its signature database, keeping its solution light and fast. ESET's ThreatSense.Net, a built-in global early warning system that users can opt into for anonymous participation, collects samples of potential malware detected by its advanced heuristics scanner for analysis by ESET's Threat Lab. As necessary, signatures for newly confirmed threats are generated and distributed to help stem the spread of new malware. Proactive security is being integrated as yet another layer of prevention in ESET's innovative approach to endpoint security.

### *ESET Product Architecture*

ESET Smart Security is a comprehensive security solution for home and business endpoints. Introduced at the end of 2007, Smart Security combines ESET's advanced ThreatSense heuristics and NOD32 Antivirus into a single, integrated engine along with antispam, antispyware, and firewall protection. The Business Edition includes Remote Administrator, a centralized management tool that facilitates networkwide updating without interrupting user experience. From the beginning, ESET designed the Smart Security endpoint solution to have a very small system footprint, offering comprehensive security without affecting system performance.

- ESET's ThreatSense is the core of the Smart Security solution and is discussed in detail in the ESET ThreatSense Engine: Advanced Heuristics section.

- ThreatSense.Net complements ESET's multilayer proactive protection by allowing users to submit anonymous samples for analysis by ESET Threat Lab. Unlike some in-the-cloud antivirus systems, ESET Smart Security does not rely on ThreatSense.Net to offload heuristics analysis; rather, it performs the analysis on the endpoint directly and uploads samples of interest, with the user's permission, for the purpose of stopping the spread of new threats worldwide.

- The graphical user interface (GUI) is available in Standard and Advanced modes. Standard offers preconfigured, ready-to-use protection settings, while Advanced allows for more granular tools and controls, such as log viewer and quarantine. The latter allows administrators to customize Smart Security for their unique environment but demands input on configuration settings.

- Smart Security's antivirus and antispyware features examine files, email, and Internet activity for malicious programs. When a threat is identified, the system has the ability to clean, quarantine, or delete to ensure system integrity.

- ESET Smart Security's firewall is available in three configuration options: Automatic, Interactive, and Policy. Automatic mode employs predefined rules to allow incoming and outgoing communications. Interactive mode goes one step beyond Automatic: When a case arises that is not covered by a predefined rule, the system will prompt the user to allow or refuse the connection. Over time, customized rule configurations will develop as a result of the user's past decisions. Finally, Policy mode allows the network administrator to deploy companywide connection policies via the Remote Administrator module. If a case arises that does not have an administrator-defined rule, the connection is automatically denied.

- The antispam feature uses Bayesian analysis, rule-based (heuristic) scanning, as well as a global threat database to scan all incoming email. Scanning is done in parallel (nonsequentially), and each email is given a rating from 0 (not spam) to 100 (known spam). Depending on the ranking, mail is delivered or sent to a designated "Junk" folder. Smart Security's antispam feature protects Microsoft Outlook, Microsoft Outlook Express, and Windows Mail products.

- ESET Remote Administrator and Mirror components, included in the Business Edition, offer centralized management across the entire network, minimizing cost, time, and resources required to deploy and maintain the ESET endpoint security solution.

ESET backs all Smart Security products with a list of frequently asked questions (FAQs), online technical support, and the ESET NOD32 Antivirus Forum hosted by Wilders Security. These resources are available around the clock. Priority Service contracts are also available, providing a dedicated support phone number with priority response and service-level agreements that guarantee a response within 30 minutes. Finally, ESET and its partner network offer training and best-practice processes for customers.

### ESET ThreatSense Engine: Advanced Heuristics

ESET is pioneering the transition to integrated antithreat solutions on the endpoint that incorporate traditional antivirus features with proactive heuristic analysis to identify and stop previously unknown threats. Although proactive scanning is not intended as a replacement to traditional antivirus solutions, ESET has positioned its advanced heuristics ThreatSense engine at the heart of its antithreat architecture with traditional security features integrated to create a comprehensive endpoint solution. To simplify the integrated architecture, ESET has emphasized the need for centralized management.

Thus far, the content of this paper has divided antithreat solutions into two major categories: traditional antivirus and proactive heuristics. It is obviously unnecessary to clarify that most vendors have slight variations in their presentation in either or both of these approaches.

It is important to emphasize that ESET's advanced heuristics ThreatSense engine employs both passive and active heuristics. ESET's innovative antithreat solution distinguishes its heuristic antivirus solution from other heuristic engine approaches. ESET's ThreatSense approach includes the following:

- ESET's Passive Heuristics component, like traditional heuristic scanning technologies, examines the content of a program for potentially harmful instructions before the processor is allowed to execute the code. The passive scanning mechanism looks for algorithms, content, or programs that exhibit "bad" or "risky" behavior, indicating malicious activity.

- ESET's Active Heuristics technology takes the company's solution to a higher level of heuristic scanning. ESET's Active Heuristics component isolates suspect or questionable code in an emulation space that maintains the security of the overall system. Within this area, the code is executed and behavior and patterns are analyzed, and if they are found to be malicious, the code is discarded or quarantined. In essence, ESET's Active Heuristics executes and tests parts of the program in a quarantined section of the system. By decrypting or decompressing code in a safe zone, the "sandboxing" technique exposes it to other scanning capabilities and, consequently, reveals the full extent of potentially malicious activities that other solutions would not identify. ESET's sandboxing method runs in parallel with multiple other scanning solutions to provide an efficient architecture that increases the valid detection of new malware. Furthermore, the thorough analysis of malicious activity reinforces the complete removal of malicious code by ESET's heuristic cleaning capabilities.

Although many security vendors incorporate some type of heuristic analysis similar to ESET's Passive Heuristics component, the company's Active Heuristics addresses many of the shortcomings of previous heuristic solutions. Specifically, ESET's sandboxing technique comprehensively examines malicious code, allowing for resolution that goes beyond the limitations of "quarantine for antivirus or allow" functionality, as mentioned earlier.

#### *Proven Security*

ESET's antithreat technology has consistently proven itself in a variety of evaluations by third-party examiners that look at threat prevention and system performance. According to *Virus Bulletin*, ESET's ThreatSense technology has received 54 VB100 awards for threat detection from May 1998 to February 2009. At the same time, ESET Smart Security has proven to cause almost no degradation of performance, based on Performance Test from PassMark Software.

### Challenges to ESET Smart Security

ESET has approached the endpoint security market with a well-planned approach that offers multilayer security and centralized management. However, as mentioned earlier, security solutions are a balancing act that depends on policy configuration. Proactive technologies are not expected to be 100% effective in blocking unknown threats, and it is clear that traditional antimalware solutions are not 100% effective either. Multilayered technologies must be properly configured and managed by the network administrator.

## CONCLUSION

As the threat landscape develops at an astounding rate, security vendors are forced to revise their protection strategies and must eradicate the need for a "sacrificial" system in order to identify a new malware outbreak. ESET is pioneering the development of the endpoint security market that is built around advanced heuristic analysis to identify, analyze, and diagnose malware threats in a protected virtualized environment. In addition to the core ThreatSense technology, the company's Smart Security platform employs advanced heuristic analysis, which includes behavior-based quarantining, and traditional antithreat features to create a comprehensive endpoint security solution with centralized management.