ENJOY SAFER TECHNOLOGY®

MULTILAYERED SECURITY:

ESET'S PROACTIVE DEFENSE AGAINST MODERN MALWARE

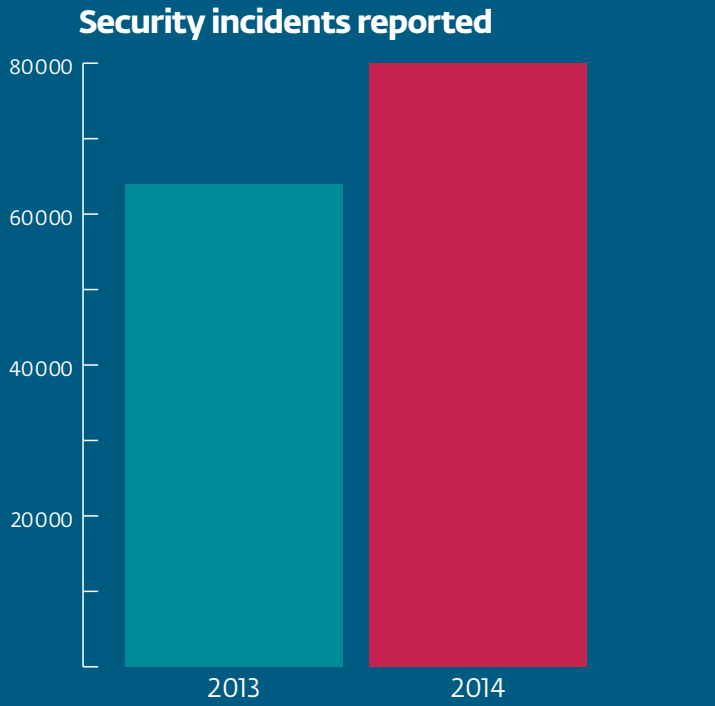
Multilayered Security: ESET's Proactive Defense Against Modern Malware

By Phil Herold, ESET staff writer.

According to the 2015 Verizon Data Breach Investigations Report, there were nearly 80,000 security incidents reported during 2014—a 25% increase over the previous year. It's a better time than ever to take a serious look at implementing or upgrading your antivirus and endpoint security solutions.

While the ability to detect viruses and other malware is obviously important, there are other practical issues to consider—especially in the areas of usability and IT automation. These are not so obvious, unless and until you have gained some real-world experience with security solutions.

That's when you realize that the practical issues we cover in this brief have a huge impact on you and your organization. The better your solution handles them, the happier your users will become, the less time you'll spend managing security, and the lower the cost-of-ownership on your solution will be.



Source: Data Breach Investigations Report—Verizon, 2015

1. Detection Rates

Let's start with the obvious: the ability to detect viruses and other malware. Several independent testing firms including AV-Comparatives and Virus Bulletin regularly test antivirus products for their detection capabilities.

ESET solutions have consistently achieved detection rates equal to or better than competitive antivirus products in these tests, year in and year out. Most notably, ESET holds the industry record for the most VB100 awards from Virus Bulletin, the longest consecutive string of those awards, and has never missed an "In the Wild" virus since testing began.

2. False Positives

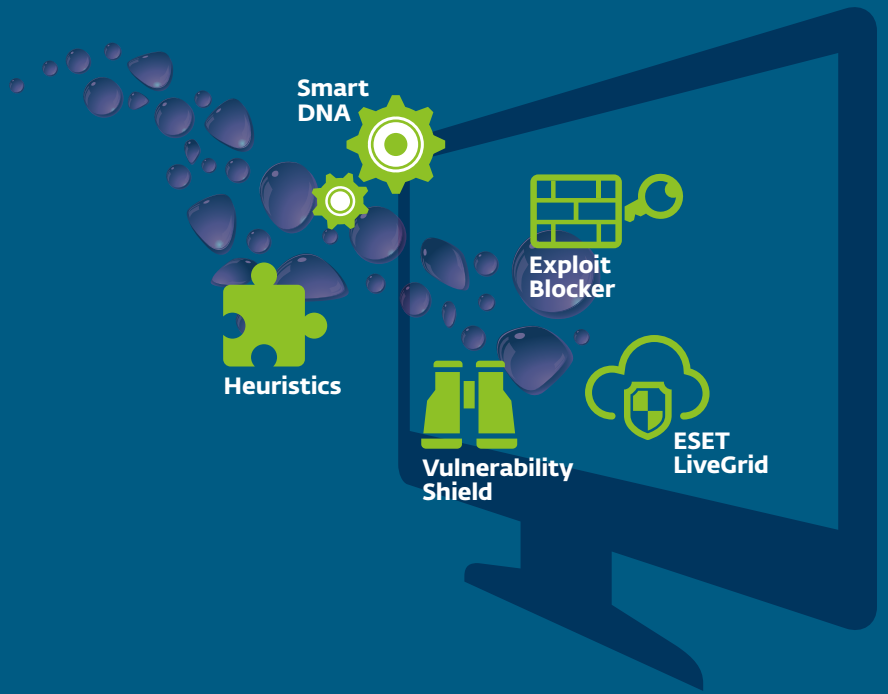
On the other hand, an antivirus solution that misidentifies a benign file as malware can cause problems, too. If high detection rates come at the expense of being over-protective and generating a high number of false positives, you waste valuable resources chasing down problems that don't exist. According to the Ponemon Institute, IT organizations spend an average of $1.2 million a year in wasted time responding to erroneous malware alerts. Even worse, antivirus software occasionally disables popular software or essential system files, triggering downtime and lost productivity for employees.

ESET solutions use multiple procedures to determine more precisely whether a file is legitimate or not, lowering the possibility of a false positive. These include advanced heuristics, Smart DNA signatures, and LiveGrid, which checks a file's reputation against a whitelist/blacklist drawn from data collected all over the world. The published results from the independent testing companies confirm ESET's ability to achieve superior detection rates with the fewest false positives.

3. Reliance on signatures

Antivirus signatures look for telltale patterns within files to identify them as malicious, and are a long-established method for detecting malware. Unfortunately, malware creators have become adept at cranking out slight variants so the malware looks just different enough to evade signature detection; in fact the 2015 Verizon Data Breach Investigations Report found that 70-90% of malware samples had signatures unique to the reporting organization.

ESET solutions use a multilayered approach that augments signature-based detection with other methods, so they can catch ever-mutating and increasingly sophisticated malware.



- Smart DNA signatures go beyond simple pattern-matching by detecting malware variants spawned from the same code, so each signature can detect literally thousands of malware variants
- Heuristics use emulation that allows suspicious code to execute in a protected manner, detecting malicious intent while blocking an infection
- Exploit Blocker fortifies applications that are commonly exploited by examining their processes, looking for suspicious activities and blocking them immediately
- Vulnerability Shield protects at the network level by detecting malicious behaviors that take advantage of vulnerabilities in network protocols
- ESET LiveGrid® detects emerging threats based on file and URL reputation; it gathers information on newly discovered suspicious activity detected by ESET scanners all over the world, stores it in the cloud, and uses this information to proactively protect other ESET users.

4. **Social engineering defenses**

Social engineering attacks misrepresent their intent to users, for example through phishing schemes that trick them into visiting infected websites that plant malware on their machines. The 2015 Verizon Data Breach Investigations Report calculated that by sending out just 10 emails, a criminal has a 90% chance of hooking at least one victim. This is another avenue of infection that is outside the realm of traditional antivirus protection.

ESET solutions incorporate an anti-phishing URL blocker the protects your users against fake websites that masquerade as legitimate ones and attempt to acquire passwords, banking data and other information. It draws from a database of fraudulent websites that reflects continuous invention of new methods for detecting phishing sites, and blocks them. IT managers can use the out-of-the-box, predefined web-blocking categories to limit access to various types of sites to enforce your organization's Internet-use policy; they can also create their own rules to block individual sites or create custom lists and categories.

5. **Botnet Protection**

Intrusions and data breaches often take weeks or months to discover, because advanced malware is so good at hiding. Deeply encrypted malware can lie dormant, then come to life as part of a "botnet" of infected machines and signal its new "owner" that it's ready for business.

ESET solutions protect against these advanced threats with an Advanced Memory Scanner. It monitors suspicious processes, and scans them after they've decrypted their payloads and reside in the memory. In addition, Botnet Protection inspects network traffic for known malicious patterns, checks them against a blacklist of Internet sites known to harbor botnet command-and-control servers, and blocks the communication.

6. **System performance**

Antivirus solutions that over-consume system memory, hog disk space and demand too much processor time slow down the rest of the system. It's a difference that users notice and that can seriously impact their productivity, especially if you're trying to stretch your dollars by extending the life of older equipment. If you're running virtualized systems, bursts of scanning activity that draw high resource use can contribute to AV storms that slow the entire environment to a crawl.

ESET solutions regularly receive top marks for performance from independent testing labs. In 2014, Passmark Software ran tests comparing ESET to other endpoint security products. ESET far outperformed the aggregate competition across the board in measures that included boot time, scan time and memory consumption.

7. **User alerts**

Antivirus software should simply do its job and stay out of the user's way. Those that issue excessive or unnecessary informational messages, alerts and warnings are an annoyance—especially when they require the user to clear the box to regain full use of the screen. It's especially annoying (and embarrassing) when a security alert pops up in the middle of a presentation in a roomful of business associates.

ESET solutions issue fewer alert messages in general. Moreover, IT managers can configure the software to minimize the number of alerts the user sees, or completely disable the user interface so the protection runs silently. In addition, an easy-to-configure setting automatically puts the security software into presentation/gamer mode when the system is running full screen. This mode suppresses all alerts and notifications, and restores them when the full-screen session ends.

8. **Usability and user impacts**

Slow-running or overly interruptive antivirus software can be not just a productivity drain, but also a security risk. Complicated or hard-to-use solutions encourage IT admins to configure them to decrease the complaints, compromising security in the process. Or, they lead users to circumvent or disable the security entirely. When companies that have antivirus software in place get hit with an infection, it often turns out that employees disabled the software.

ESET solutions allow IT managers to specify and lock settings against changes by end-users, preventing them from "tweaking" the system and compromising security. In addition, built-in self-defense technology prevents malicious software from corrupting or disabling the protection. Aside from these specific measures, ESET has also invested in global user research to ensure the usability and speed of our endpoint-security products. Our customer support team, based in the U.S., offers free help for employees who have questions. We can also provide onsite or online training on cybersecurity best practices.

9. Manual intervention

Antivirus that puts the burden on the user to initiate tasks, make decisions and actively manage the solution not only wastes time, it can also seriously jeopardize the system. If the user isn't clear on what to do, then makes a guess and guesses wrong, a malicious process can get the green light to wreak havoc on the system.

ESET solutions are largely or fully automated through an agent—a small application that executes tasks, collects logs, interprets and enforces policies and monitors the system. It communicates with and applies automation settings that are maintained by the web-based administration console.

10. Removal procedures

An antimalware solution should create less work, not more, for IT teams. However, the Ponemon Institute found that companies spend on average almost 600 hours each week on malware containment, devoting the most time to dealing with networks, applications and devices damaged or infected by malware.

ESET solutions deal with malicious files by silently quarantining and removing them automatically. ESET also has free downloadable tools for ridding systems of particularly resilient threats.

11. Ease of administration

You don't want an antivirus solution that monopolizes your day. If you have more than a handful of computers to protect, jumping from machine to machine manually configuring security solutions is a waste of time. The larger your environment, the more important centralized administration becomes.

ESET solutions include a web-based remote administration console that manages all aspects of configuring, managing and monitoring security at your endpoints from a single location. Their automated security management frees your time to focus on more important tasks.

- Active Directory synchronization frees you from having to create users and groups just for your security solution, and makes it easier if your organization assigns sets of policies to different roles
- Updates are automated and seamless
- Task management system lets you run reports, manage quarantined files, assign different privileges to users and enforce consistent security, with many daily tasks automated via policies and triggers
- Dynamic Groups allow you to specify conditions you are interested in monitoring; the software then dynamically creates a group pinpointing the endpoints needing attention
- Built-in AV Remover utility makes switching your endpoint security solution automated and painless by uninstalling all traces of old antivirus software and installing ESET

12. Cross-platform capabilities

While there are fewer threats targeting Mac®, Linux and Android®, they exist. Also, if you share files between platforms, any machine regardless of operating system can serve as a repository for malware transmitted via email, file shares and USB drives. Installing antimalware on all endpoints adds additional layers of security against cross-platform infections.

ESET solutions support Windows®, Mac, Linux and Android, and consistently apply the same scanning engine across all platforms. This means that a machine running MacOS can block and remove malware intended for Windows machines, stopping it before it can be transferred to the targeted systems and do actual harm. The remote administration console allows you to manage the security of all of these endpoints including computers, laptops, tablets and smartphones from a single console, including managing licenses, updates and configurations.

Now that you know the issues,
test-drive **ESET Endpoint Security**.

We invite you to take a **free business trial** and see for yourself how ESET handles all the issues and concerns that come with implementing **real-world** endpoint security.

www.eset.com/us/business/free-trial

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®