Anti-Virus
& Content Security

eScan Security Network

Created on: 5th November, 2012
Document Version Number: ESN(14.0.0.1)

From
MicroWorld Technologies

eScan Security Network

With the growing amount of malware in-the-wild, we realized it would be practically impossible to secure our clients using the traditional approach of detecting and preventing new threats. Antivirus laboratories normally follow a set of procedures in dealing with new malware: The samples are received (a new virus, worm, Trojan...), analyzed by a Malware Analyst and a corresponding signature is created. This is then uploaded to the servers, allowing users to update their database signatures, thus protecting them against new viruses.

This model, which without any doubt had functioned adequately in the past, became useless when laboratories went from receiving few samples a day to an average of 65,000 and more. This would require a whole army of Malware Analysts working against the clock to process all the new samples of malware received.

By taking situations such as these into consideration, we at eScan have developed a technology called eScan Security Network (ESN). This technology can automatically analyze, classify, detect and quarantine 99.99% of new malware we receive every day at our labs, keeping our clients protected in real time. eScan Security Network is a state-of-the-art technology implemented in the latest versions of eScan SOHO products. When it comes to detecting new malware, ESN ensures a prompt response and an advanced level of detection that provides superior protection. eScan Security Network is not only capable of detecting and blocking unknown threats but can also locate and prevent zero-day threats and phishing attempts.

Current threats such as viruses, worms, Trojans & phishing have posed as major threats to the normal functioning of computers and to the information stored in them. These kinds of threats are constantly evolving, thus challenging the current security standards laid by security products. According to a general study done by security experts, more than 65,000 malware strains are being detected on a daily basis.

The Digital world requires a new embedded approach to ensure digital security. This approach has to combine the advantages and minimize the deficiencies of the traditional methods of combating malicious software and automatic updating of new real-life threats. This approach has been implemented in eScan Security Network.

eScan Security Network

The Basics of eScan Security Network

eScan Security Network includes several subsystems:

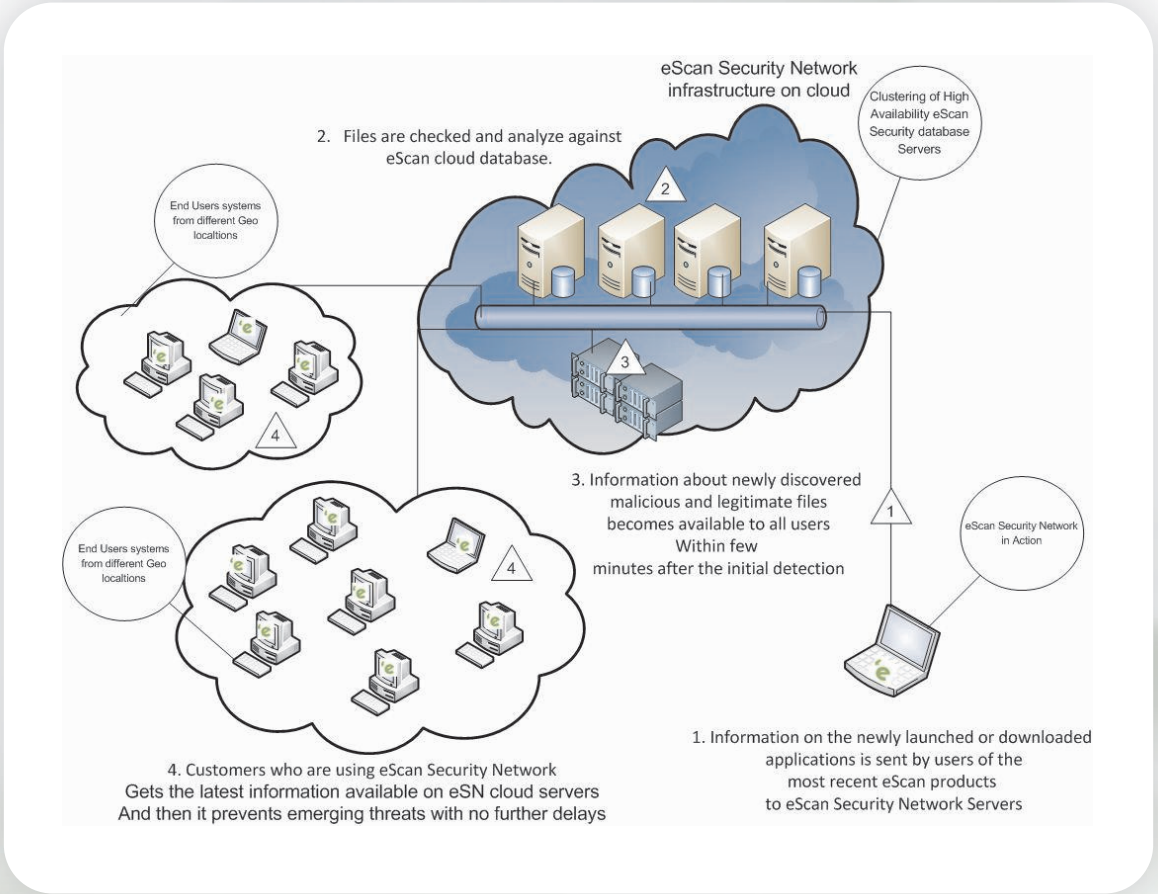
- Continuous global monitoring of real-life threats and immediate delivery of collected data to eScan host servers.
- Analysis of the collected data, creation of protection measures against new threats and the fast distribution of those measures to all connected users.
- ESN automatically collects information and sends the data to eScan labs. Information about suspicious files downloaded to and executed on computers is also collected, regardless of their source (websites, email attachments, peer-to-peer networks, etc).
- This is strictly done voluntarily and confidentially – the user of any one of eScan SOHO products has to agree to participate in the system. In any case, strict confidentiality is maintained and no personal information such as user names, passwords or any other personal details is collected.
- The decision on the safety of a program is made based on internal algorithms such as valid digital signature along with a number of other factors.
- As soon as a program is declared malicious or unsafe, the information becomes available to eScan product users even before the signature for that piece of malware is created and updated on their computers.

This way eScan clients receive prompt information about new and unknown threats minutes after the launch of a cyber-attack, compared to traditional signature database update which generally take a couple of hours to get created.

Flowchart of eScan Security Network

This flowchart describes the basic principles on how users of eScan products interact with eScan Security Network. This interaction includes 4 different phases:

- Information on the newly launched or downloaded applications is sent by users of the most recent eScan products to eScan Security Network Servers.
- The files are checked and added to the eScan database if they found to be malicious. Legitimate files are added to the “Whitelisting” database.
- Information about newly discovered malicious and legitimate files becomes available to all users of relevant eScan products minutes after the initial detection.
- Local database of application whitelisting is built and maintained for known applications.



eScan Security Network therefore makes use of a combination of heuristic and signature based malware detection

Cloud-Based Protection for Consumers

The latest versions of eScan products, namely eScan Internet Security v14, eScan Anti-Virus v14 and eScan Total Security v14, enjoy the full support from eScan's cloud based Security Network, better known as eScan Security Network. Apart from the common benefits of cloud protection, the new versions of SOHO products allow users to receive general statistics about eScan Security Network: Safe and unsafe data processed.

eScan Security Network identifies and blocks new threats before they become widespread and cause any significant damage to system. A proactive defense system is essential to ensure stable and uninterrupted operation of IT equipment and the business processes it supports.