eScan Corporate Edition (with Hybrid Network Support)

With information technology being the backbone of any business today, IT security is considered as a key part of business strategy by the organizations. Amidst constantly increasing threats in the cyber-security landscape, protection of valuable intellectual property and business data against theft/ misuse without interrupting business continuity is a critical issue.

The new eScan Corporate Edition with Hybrid Security Network strengthens the cyber-security capabilities of the businesses by providing multi-layered protection to the IT infrastructure from complex threats and secures critical business information effectively without constraining business growth. It is an excellent combination of advanced and futuristic technologies that provides protection to Windows, Mac and Linux-based endpoints in the network.

Key Features (eScan Server, Windows)

New Secure Web Interface with Summarized Dashboard
The new Secure Web Interface uses SSL technology to encrypt all communications.

eScan's summarized dashboard provides administrators the status of the managed endpoints in graphical format like deployment status, protection status and statistics.

Asset Management
eScan's Asset Management module provides the entire hardware configuration and list of software installed on endpoints. This helps administrators to keep track of all the hardware and software resources installed on all endpoints connected to the network.

Role Based Administration
Role based Administration through eScan Management Console enables the administrator to share the configuration and monitoring responsibilities of the organization among several administrators.

Client Live Updater
With the help of eScan's Client Live Updater, events related to eScan and security status of all endpoints are captured, recorded and can be monitored in real-time. Also, the events can be filtered to retrieve exact required information to closely watch security level on all managed endpoint on a real-time basis, thus ensuring total security on all managed endpoints.

Data Loss Prevention
eScan empowers enterprises to minimize the risk of data theft with its advanced features like Attachment Control and Device Control. Through Attachment control the admin can block/allow all attachments the user tries to send through specific processes as well as trusted websites that you define.

Session Activity Report
eScan Management Console monitors and logs the session activity of the managed computers. It will display a report of the endpoint start up / shut down / log on / log off / remote session connects/ disconnects. With this report the administrators can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

File Activity Report
eScan Management Console monitors and logs the file activity of the managed computers. It will display a report of the files created, copied, modified, and deleted. Select and filter the report based on any of the details captured. It also allows you to export the generated report in desired file formats such as PDF, Excel, or HTML.

Policy Templates
Policy deployment can be made easy through policy templates; this will allow the administrators to create policy templates and deploy it to the desired managed groups.

Auto Grouping
The administrators can define the settings to automatically

Other Highlights

- ▣ Centralized Management Console with Secure Web Interface for Windows, Mac and Linux
- ▣ Daily Updates of all Threats, Malwares & Virus definitions via eScan ESN Cloud Security
- ▣ Set advanced security policies
- ▣ On Demand Scanning
- ▣ Secure Web Interface
- ▣ License Management
- ▣ Import & Export of Settings
- ▣ Task deployment
- ▣ Outbreak Prevention (Improvised)
- ▣ Policy Templates (New)
- ▣ Update Agent (Improvised)
- ▣ Auto Grouping (New)
- ▣ Active Directory Synchronization (New)
- ▣ Message Broadcast (New)
- ▣ File Reputation Services
- ▣ Sophisticated File Blocking & Folder Protection
- ▣ Powerful Antimalware & Antispyware Protection based on Heuristic & Proactive Scanning
- ▣ Malicious Traffic Detection Mechanism and Host Intrusion Prevention (HIPS) within a Single Client Agent
- ▣ Endpoint Critical Patch Management through MAPP
- ▣ Auto Back-up and Restore of Critical System files
- ▣ Wizard to create a Linux-based Rescue USB to clean Rootkits & File infectors
- ▣ Inbuilt eScan Remote Support
- ▣ 24x7 FREE Online Technical Support through e-mail, Chat & Forums

add clients under desired sub groups. The administrators will have to Add Groups and also add client criteria under these groups based on host/host name with wild card / IP address / IP range.

Send Message
Send message will allow the system administrators to send an announcement or an alert message asking user to log off the system or contact the system administrator, this can be easily done using eScan console, without installing any third party software on the client system.

Update Agent
The administrator can add computers as Update Agents. This will reduce the traffic between the eScan Corporate Server and the client. Update Agent will take the signature updates & policies from eScan Corporate Server and distribute the same to other managed computers in the group. (Bandwidth is saved).

Print activity
eScan comprises of Print Activity module that efficiently monitors and logs printing tasks done by all the managed endpoints. It also provides a detailed report in PDF, Excel or HTML formats of all printing jobs done by managed endpoints through any printer connected to any computer locally or to the network.

PBAE
Proactive Behavioral Analysis Engine provides real time protection for organizations and users against Ransomware attacks. It monitors the activity of all processes and blocks the one whose behavior matches to a Ransomware.

TSPM
Terminal Services Protection Module by eScan not just detects the brute force attempts but also heuristically identifies suspicious IP Addresses / Hosts. It blocks any attempts to access the system.

eBackup
eScan allows you to take a backup of your files on a scheduled basis, and is stored in an encrypted and compressed file format. It takes backup of many data based extensions.

One-Time Password
Using One Time Password option, the administrator can enable or disable any eScan module on any Windows endpoint for a desired period of time. This helps to assign privileges to certain users without violating a security policy deployed in a network.

Key Features-eScan Endpoints

Enhanced Endpoint Security

Device Control
eScan's Advance Device Control features help in intelligent access controls & monitoring for Windows, Mac & Linux endpoints in the network. On Windows endpoints, administrators can control access of devices like CD-Roms, Composite devices, webcams, CDROMs, Composite devices, Bluetooth devices, SD Cards or Imaging device. This also adds a Data Loss Prevention function & avoidance of malware infection.

Data Theft Notification
The USB port may be misused and data pilferage becomes a common occurrence which may cause damage to the organizations intellectual property & reputation. eScan's Device Control allows sending notification on any data movement from endpoint to the USB device. Thus, helps in arresting Data Theft.

Application Control
eScan's effective Application Control module allows you to block/ whitelist and define time restrictions for allowing or blocking execution of applications on Windows endpoints. It helps in accessing only the whitelisted applications, while all other third-party applications are blocked.

Advanced Anti-Spam
eScan's Advance Anti-Spam Engine equipped with AI & ML capabilities helps to prevent incoming as well as outgoing spam emails. The real-time engine will identify & quarantine advertisement/campaign like emails.

Enhanced Two-way Firewall
The two-way Firewall with predefined rule sets will help you in putting up a restriction to incoming and outgoing traffic and hacking. It provides the facility to define the firewall settings as well as define the IP range, permitted applications, trusted MAC addresses and local IP addresses.

Privacy Control
Privacy control allows scheduling the auto erase of your cache, ActiveX, cookies, plugins, and history. It also helps to permanently delete files and folders without the fear of having them retrieved through the use of third-party applications, thus preventing misuse of data.

Advanced Web Protection
eScan comes with an advanced Web Protection feature that allows administrators to define the list of sites to block or whitelist on endpoints connected to the network where eScan is installed. For Windows endpoints eScan also provides the facility for time-based access restriction.

On Demand / Schedule Scanning
eScan engine allows you to perform an On-Demand / schedule scan of files/directories that you access or copy on to your endpoint. It allows you to select different files / folders or running process. Thus providing you with the best protection against cyber threats.

Minimum System Requirements

Windows
(Windows Server and Workstations)
Platforms Supported
Microsoft® Windows® 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1
(For 32-Bit and 64-Bit Editions)

For Server
- CPU - 2GHz Intel™ Core™ Duo processor or equivalent.
- Memory - 4 GB and above
- Disk Space (Free) – 8 GB and above

For Endpoints (Windows)
- CPU - 1.4 Ghz minimum(2.0 Ghz recommended) Intel Pentium or equivalent
- Memory - 1.0 GB and above
- Disk Space (Free) – 1 GB and above

eScan Console can be accessed by using below browsers:
- Internet Explorer 7 / 8 / 9 / 10
- Firefox 14 and above
- Google Chrome latest version

Linux
(Linux Endpoints)
Platforms Supported
RHEL 4 and above (32 and 64 bit)
CentOS 5.10 and above (32 and 64 bit)
SLES 10 SP3 and above (32 and 64 bit)
Debian 4.0 and above (32 and 64 bit)
openSuSe 10.1 and above (32 and 64 bit)
Fedora 5.0 and above (32 and 64 bit)
Ubuntu 6.06 and above (32 and 64 bit)

Hardware Requirements (Endpoints)
- CPU - Intel® Pentium or compatible or equivalent.
- Memory –1 GB and above
- Disk Space – 1 GB free hard drive space for installation of the application and storage of temporary files

Mac
(Mac Endpoints)
Platforms Supported
OS X Snow Leopard (10.6 or later)
OS X Lion (10.7 or later)
OS X Mountain Lion (10.8 or later)
OS X Mavericks (10.9 or later)
OS X Yosemite (10.10 or later)
OS X El Capitan (10.11 or later)
macOS Sierra (10.12 or later)
macOS High Sierra (10.13 or later)

Hardware Requirements (Endpoints)
- CPU - Intel based Macintosh
- Memory –1 GB and More recommended
- Disk Space – 1 GB and above