eScan™
Enterprise Security

eScan
Elite for Business

Advanced Protection against Ransomware Threats

eScan Elite for Business is a comprehensive antivirus and Information Security Solution that allows you to manage risk and protect your critical infrastructure efficiently. Moreover, the new eScan Management Console (EMC) module includes a Secure Web Interface that facilitates dynamic security management of the server and endpoints in a business network. It is an excellent combination of advanced and futuristic technologies that provides protection to your Windows based devices and endpoints in the business network.

eScan *Elite* for Business

eScan™ Enterprise Security

Why eScan Elite for Business?

Digital Defence

• Outbreak Prevention

Outbreak Prevention will allow the administrator to deploy outbreak prevention policies during an outbreak that restricts access to network resources from selected computer groups for a defined period of time. The outbreak prevention policies will be enforced on all the selected computers or groups. Incorrect configuration of these policy settings can cause major problems with the computers.

• Privacy Control

This will allow you to schedule an auto erase of your cache, ActiveX, cookies, plugins, and history. You can also secure delete your files and folders where no traces of deletion could be found.

Uniform Management

• 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 such as deployment status, protection status, as well as protection 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 as well as software resources installed on all the endpoints connected to the network.

eScan *Elite* for Business

eScan™ Enterprise Security

Key Features (eScan Server, Windows):

Client Live Updater

With the help of eScan's Client Live Updater, events related to eScan & security status of all endpoints are captured and recorded / logged and can be monitored in real-time. Also, the events can be filtered to retrieve exact required information to closely monitor security level on all managed endpoints on a real-time basis, thus ensuring total security on all managed endpoints. It also facilitates export of the reports in Excel format that can further be used for audit compliance.

Session Activity Report

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

Outbreak Prevention

This feature will allow the administrator to deploy outbreak prevention policies during an outbreak that restricts access to network resources from selected computer groups for a defined period of time. The outbreak prevention policies will be enforced on all the selected endpoints or groups. Incorrect configuration of these policy settings can cause major problems with the computers

Print Activity

eScan comprises of Print Activity module that efficiently monitors & 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.

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.

Zero-Day Protection

Along with heuristic analysis and behavior-based anomaly detection, eScan additionally employs deep learning, a technique of machine learning, to identify and block zero-day threats in real time. The deep learning-based proactive threat detection engine blocks the fileless attacks, exploit attempts, and advanced malware at the endpoint level, ensuring an adaptive security mechanism.

eScan
Elite for Business

eScan™
Enterprise Security

Key Features (eScan Server, Windows):

Update Agent

In a large organization the Administrator can create computer groups for better management and distribution of Policies and Updates. Using eScan they can install Update agent on anymanaged endpoint (where eScan Client is already installed). This update Agent will take the signature updates and policies and distribute the same to other managed computers in the group. The Update agent will alternatively query eScan Update servers on internet for getting updates whenever there is a connectivity problem between the update agent and eScan Total Security Server.

Endpoint Security (with Device Control & Application Control)

This module protects your computer or endpoints from data thefts & security threats through USB or FireWire® based portable devices. It comes with an Application control feature, which helps you block unwanted applications from running on your computer. In addition, this feature provides you with a comprehensive reporting feature that helps you determine which applications & portable devices are allowed or blocked by eScan.

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 behaviour 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.

Windows OS Patch Reports

eScan's Patch Management Module auto-updates Windows OS security patch from Cloud or from EMC Console, on PC's those are part of DMZ/Air-Gapped Networks. The module also reports patching availability for Critical Apps like Adobe, Java, etc.

Policy Criteria

The administrator can specify policy criteria and deploy it to endpoints automatically if it complies with the pre – defined criteria in the management console. The Administrator will select Policy Criteria based on which the policies will be deployed.

eScan
Elite for Business

eScan™
Enterprise Security

Key Features (eScan Endpoint)

File Anti-Virus

This scans all the existing files & folders for any infection. It will allow you to report / disinfect / quarantine / delete objects.

Web Protection

This will allow you to define the sites that you do not want to allow access to. You can define the site names you want to block, do a time based access restriction.

Mail Anti-Virus

This allows you to analyze all the incoming mails. This analyses the mails by breaking it into three sections the header, subject and the body.

Privacy Control

This allows you to schedule an auto erase of your cache, ActiveX, cookies, plugins, & history. You can also securely delete your files & folders where no traces of deletion could be found.

Firewall

This helps you in putting up a restriction to incoming and outgoing traffic and hacking. You can define the IP range, permitted applications, trusted MAC addresses and local IP addresses.

Anti-Spam

This prevents you from receiving spam mails by checking the content of outgoing and incoming mails, quarantines advertisement mails.

Other Important Features

Customized Client Setup

eScan allows you to create customized client setup with pre-defined Policy Template. This allows you to implement group policies to the endpoints automatically when eScan Client is installed on the endpoint manually. The major benefit of this feature is that even if the endpoint is not connected to the eScan server, the Policy template will be deployed on to the endpoint while customized eScan Client is installed on the endpoint.

Auto Grouping

The administrator can define the settings to automatically add clients under desired sub groups. The administrator 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.

Active Directory Synchronization

With the help of Active Directory synchronization, the administrator can synchronize eScan Centralized Console groups with Active Directory containers. New computers and containers discovered in Active Directory are copied into eScan Centralized Console automatically and the notification of the same can be sent to the system administrator. Administrator can also choose to Auto Install or Protect discovered Windows workstations automatically.

Advanced Persistent Threat (APT)

Integrated protection from malware that lurks on malicious websites Integrated real-time detection and prevention of zero-day threats and advanced persistent threat (APT) attacks for Windows applications.

eScan™

Enterprise Security

MicroWorld Software Services Pvt. Ltd.
CIN No.: U72200MH2000PTC127055
Tel.: +91 22 6772 2900
email: sales@escanav.com

www.escanav.com

An ISO 27001 Certified Company

Toll Free No.: 1800 267 2900

Awards

Partnerships

Comprehensive Protection for
SOHO • BUSINESS • CORPORATE • ENTERPRISE