eScan Enterprise DLP - Cloud

eScan Enterprise DLP (Data Leak Prevention) – Cloud is a security solution that consists a set of strategies, technologies, and techniques that ensure end users do not transmit critical or sensitive data outside an organization's cloud infrastructure. Whether transmission of data is through message, email, file transfer, or some other way, information may end up in unauthorized locations intentionally or unintentionally. This may attract compliance issues, which can be eliminated by eScan Enterprise DLP.

As an Enterprise Solution, DLP needs to detect potential data breaches/data exfiltration attempts and prevent the same by monitoring, detecting and blocking sensitive data while in use (Endpoint actions), in motion (Network Traffic), and at rest (Data Storage). An effective DLP solution also needs to employ business rules to enforce regulatory compliance, classification and secure confidential information. With its advanced features, it gives protection against exfiltration attempts, monitors sensitive data access and/or leak, and permits 360 degree all round visibility of confidential file usage and protection of data tagged as critical by a user.

Why eScan Enterprise DLP?

eScan Enterprise DLP – Cloud is equipped with a wide range of advanced features and technologies to protect data in motion or data at rest & these features assist you in tracking, monitoring and protecting critical data within your network. These features can be configured as per your requirements through a comprehensive & Secure Enterprise Grade Centralized Management Console that allows you to deploy the solution on endpoints connected to your network. eScan Enterprise DLP also provides protection on mail gateways to prevent leakage of critical data through email.

eScan Enterprise DLP's advanced Device Control feature helps in monitoring USB devices that are connected to Windows or Mac endpoints in the network. On Windows endpoints, administrators can allow or block access to USB devices such as Webcams, CD-ROMs, Composite devices, Smart-Phones, Bluetooth devices, SD Cards or Imaging devices. Unauthorized access to external devices can be blocked using password protection, thus preventing data leakage through USB devices.

A sub-feature in eScan Enterprise DLP's Device Control enables to send notifications to the administrator of the web-console, when any data on the client system's hard disk is copied to the USB. Device Control, ensures that data theft is completely eradicated leaving no scope for misuse of confidential data.

Key Features

Attachment & Content Control

• File Attachment Block

The DLP Attachment block feature lets you control attachment flow within your organization. You can block/allow all attachments that a user tries to send through specific pre-defined processes. You can exclude specific domains/sub-domains that you trust, from being blocked even if they are sent though the blocked processes mentioned above. A separate report template is available to receive detailed information through email.

• Attachment Report

This feature provides you with a comprehensive reporting feature that lets you determine which attachments are allowed or blocked by eScan Enterprise DLP. It also gives alert to the administrator about attachments being shared/uploaded, source of the file-attachment and the destination.

Key Features

Attachment & Content Control

• Content-Aware Control

This superlative feature enables the administrator to monitor & control the confidential information which can be sent outside of the endpoint. The sensitive information, also termed as PII, which many a times are controlled by government regulations like GDPR, can be broadly categorized as below (new categories are constantly added & can be customized as per customer/country requirements):

- Aadhar Card number
- Driving License number
- Passport Number
- PAN Card Number
- Voter ID Number
- Credit Card Numbers (RUPAY, VISA, Amex, MasterCard, Diners Club, Maestro, etc)
- International Bank Account Numbers (IBAN)

eScan Enterprise DLP filtering for above PII can be applied for various channels like:

- External Storage Devices (USB, CD/DVD, Bluetooth)
- Printers
- Network Communication

• Corporate Cloud-based Email, Storage, Communication Access

There are several other ways that employees using Corporate Gmail, O365, Slack, WebEx, Dropbox, etc., for business reasons, put the company's data at risk. To avoid any possible leak, eScan Enterprise DLP provides functionality to block personal account access to Cloud-hosted services. This feature ensures that team members can only access the services using their corporate login credentials and not their personal credentials. Following Hosted Services are supported:

- Office365 or O365 (Hosted Outlook)
- Corporate Gmail
- Slack
- WebEx
- DropBox
- Teams

Key Features

Attachment & Content Control

• Email Report

Email is one of the omnipresent business communication tools that permits attachments, links, and sharing of corporate details with coworkers and customers. eScan Enterprise DLP email report provides the administrator with fine details about the recipient, attachment types, size of the email and many more. The administrator can monitor and control the leak of data through emails.

• Shadow Copy of files allowed to be uploaded

This eScan Enterprise DLP feature provides copies of files which are transferred over web, email & online storage (Google Drive, OneDrive, Dropbox, etc.) With any activity of files being transferred, Shadow copies of these files can be created on the basis of recipients, sender-name and attachment size, which ensures effective monitoring of data being shared or stored.

Device Control

• Printer Access Control

eScan Enterprise DLP manages the printing activity of sensitive documents. Printer Access Control options can define which data can be printed on specific printers and by whom. One advantage of this technical solution is that in the event of unauthorized activity, the DLP system logs the incident, notifies the user about the risks, and can also block the print. Potential breaches trigger alerts which are then delivered to the administrator. This module also allows the admin to completely or selectively block network printers.

• Wi-Fi Access Control

Wi-Fi access points come with a default SSID and password that must be updated, although default passwords are frequently kept in place. This makes it simple for an attacker to log in and take control over the router, configure settings or firmware, load malicious programs, or even change the DNS server to send all traffic to an attacker's IP address. Wi-Fi access control blocks or allows the specific Wi-Fi network to access your network based on a list of allowed Wi-Fi SSIDs (Whitelisted).

• Storage Access Control

Device Control protection in eScan Enterprise DLP prevents users, endpoints, or both from using unauthorized removable storage media. eScan Enterprise DLP prevents a user from copying an item or information to removable media or USB device. Storage access control blocks data from being written to removable drives that aren't protected.

• Peripheral Device Control

eScan Enterprise DLP protects critical data from leaving your company through peripheral and removable devices, such as USB drives, Bluetooth devices, and recordable CDs and DVDs. Device control provides the option to monitor and control data transfers from all desktops and laptops, regardless of where users and confidential data go, even when they are not linked to the corporate network.

Key Features

User Entity Behavior Analytics (UEBA) – Activity Monitoring

• File Activity Monitoring (Local, Network, Storage Devices)

The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. Additionally, in case of misuse of any official files, the same can be tracked down to the user through the details captured in the report. The Administrator can select and filter the report based on any of the details captured.

• Session Activity

This sub module monitors and logs session activities of managed computers. It displays a report of the Operation type, Date, Computer name, Group, IP address and event description. With this report, the administrator can trace the user Logon and Logoff activity, along with remote sessions that took place on all managed computers.

• User Activity

User Activity lets you monitor Print, Session, Application and File activities occurring on client computers. It also provides reports of the running applications. The Print Activity monitors and logs print commands sent by all computers. The Application Access Report gives a detailed view of all the applications accessed by computers which are part of Managed Computers. The File Activity Report displays a report of the files created, copied, modified, and deleted on managed computers.

• Print Activity

Print Activity lets you keep track of printers by adding them in a group and assigning it an alias name. The printers can be added or removed from this alias group. Print Activity monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer and/or Username. Furthermore, this module lets you export a detailed print activity report in XLS, PDF, and HTML formats. The generated log report consists of Print Date, Machine Name, IP Address, Username, Printer Name, Document Name, along with the number of Copies and Pages.

• Application Access Report

The Application Access Report module gives a detailed view of all the applications accessed by the endpoints which are part of Managed Computers. The log displays list of applications executed and the time duration for which the app was active. Options for Filtering or Exporting the log in desired formats are also present on the same interface. You will get the details of the computer name which accessed the app and duration.

• Shadow Copy (USB File Activity)

It is a technology that allows you to create a copy of files which a user copies to an external USB drive. This feature allows administrators to audit files those leave the endpoint.

Key Features

Access Control

• IM Blocking

Cyber thefts typically happen using file transfers or inadvertent messaging, bypassing traditional gateway security. Information Exfiltration activities are done by hackers by hijacking popular Browsers and IM Apps (such as Firefox, Skype, Opera) through known vulnerabilities such as buffer overflows or boundary-condition errors. eScan Enterprise DLP IM rules will only work if the processes utilized for file transfer are the ones you are specifying in your application list while creating the rule. The IM rule provides a blanket block on all attachment and file transfers through Instant Messenger applications.

• Sensitive File Protection

This feature will ensure that sensitive data cannot be accessed using any other application except the default application specified. Once a folder is classified as "Sensitive", its contents cannot be changed / deleted in any way. The files can be accessed using only the associated apps and any kind of editing is blocked to avoid data modification.

• Disable Print Screen

This will block any screen-shot and/or screen-grab process, like windows snipping tool, from capturing desktop screen image. This feature will ensure that users cannot capture sensitive information as an image and transfer it outside. Hence it is an important aspect of DLP.

• Disable (Copy / Paste / Drag / Drop)

For a device, once data is copied into the clipboard by any app, it can also be accessed from any other app. With Copy/Paste option disabled, a user is prohibited from copying any information to the clipboard.

• File and Folder Encryption

The DLP file and folder encryption protects sensitive and confidential data from unauthorized access and data leak. It provides an advanced level of password protection to your important files/folders.

• Application Control

Application Control feature lets you block unwanted applications from being executed on Endpoints. This helps the admin to control the execution of applications on endpoints. Also, eScan Enterprise DLP enforces the application control policy to provide continuous monitoring of systems to prevent security breaches, data leak, and outages.

• Network Access Control

eScan Enterprise DLP Network Access Control helps an organization to control access of shared network drives and folders. This feature provides a granular read-only or full access of individual shares, there by controlling confidential data access and modification.

eScan™

Enterprise Security

An ISO 27001 Certified Company **Toll Free No.: 1800 267 2900** **www.escanav.com**

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

Awards

Partnerships

Comprehensive Protection for

SOHO • BUSINESS • CORPORATE • ENTERPRISE