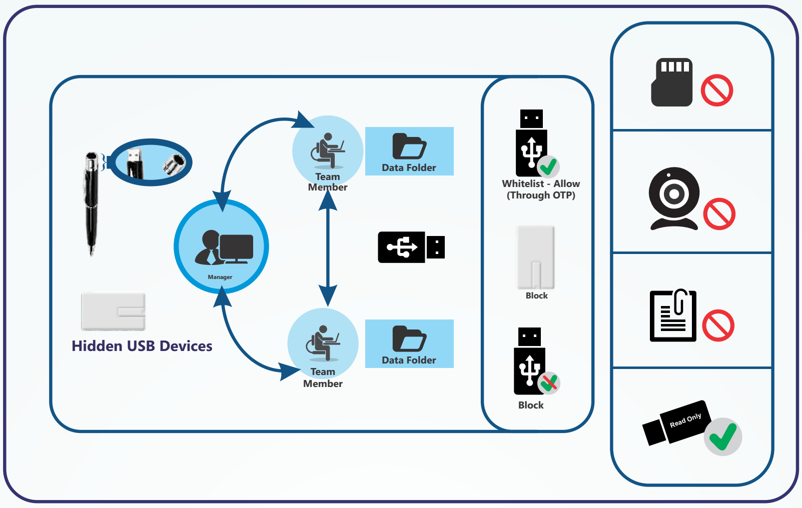
eScan Enterprise DLP (Data Leak Prevention)

eScan Enterprise DLP (Data Leak Prevention) security solution is a set of strategies, technologies, and techniques that ensure end users do not transmit critical or sensitive data outside an organization. Whether transmission of data is through message, email, file transfers, or some other way, information can end up in unauthorized locations, leading to compliance issues.

As an Enterprise Solution, DLP detects potential data breaches/data exfiltration attempts and prevents 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 employs business rules to enforce regulatory compliance 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 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.

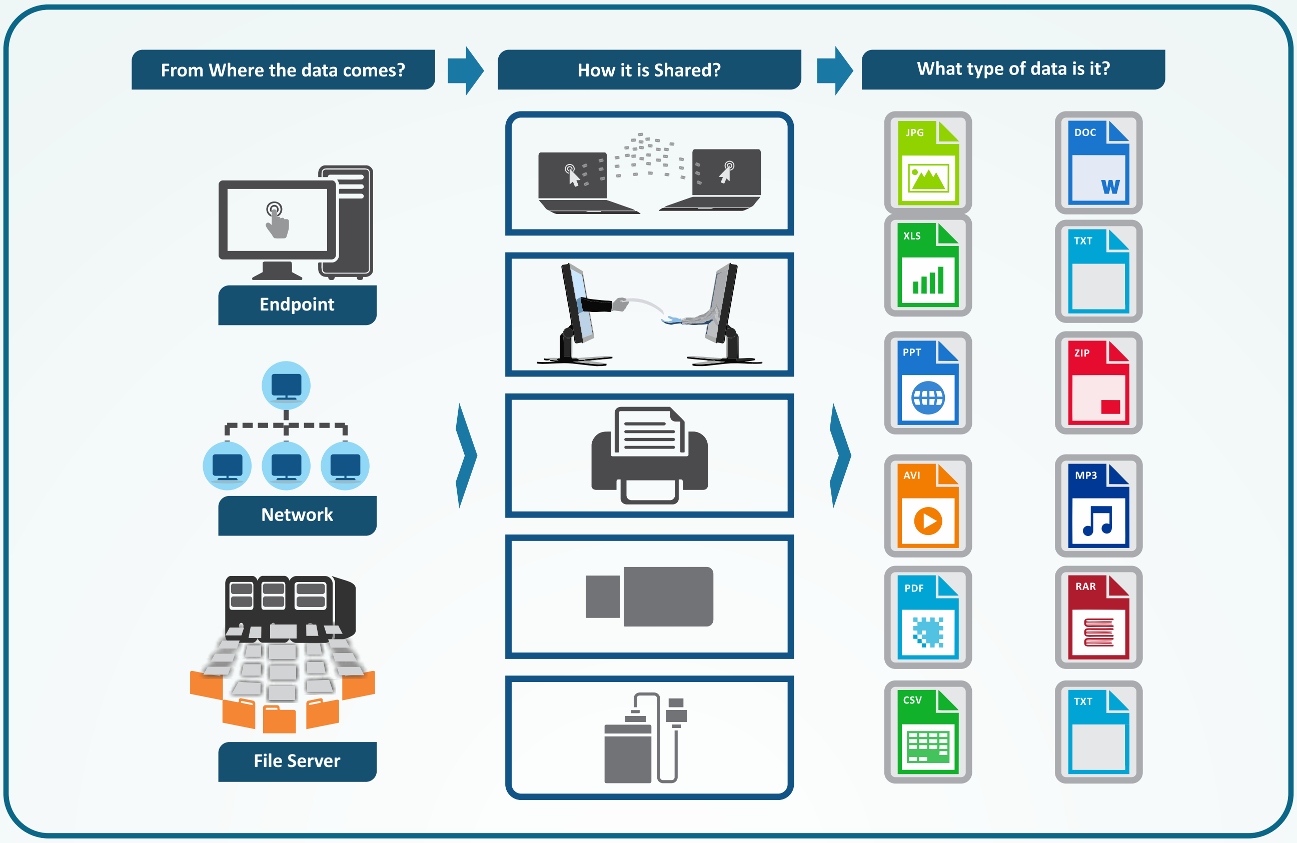
Many times, access to the USB port is misused and data pilferage becomes a common occurrence causing potential damage to the organization as intellectual property falls into wrong hands. A sub-feature in eScan Enterprise DLP's Device Control enables to send notifications to the administrator of the web-console, 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.

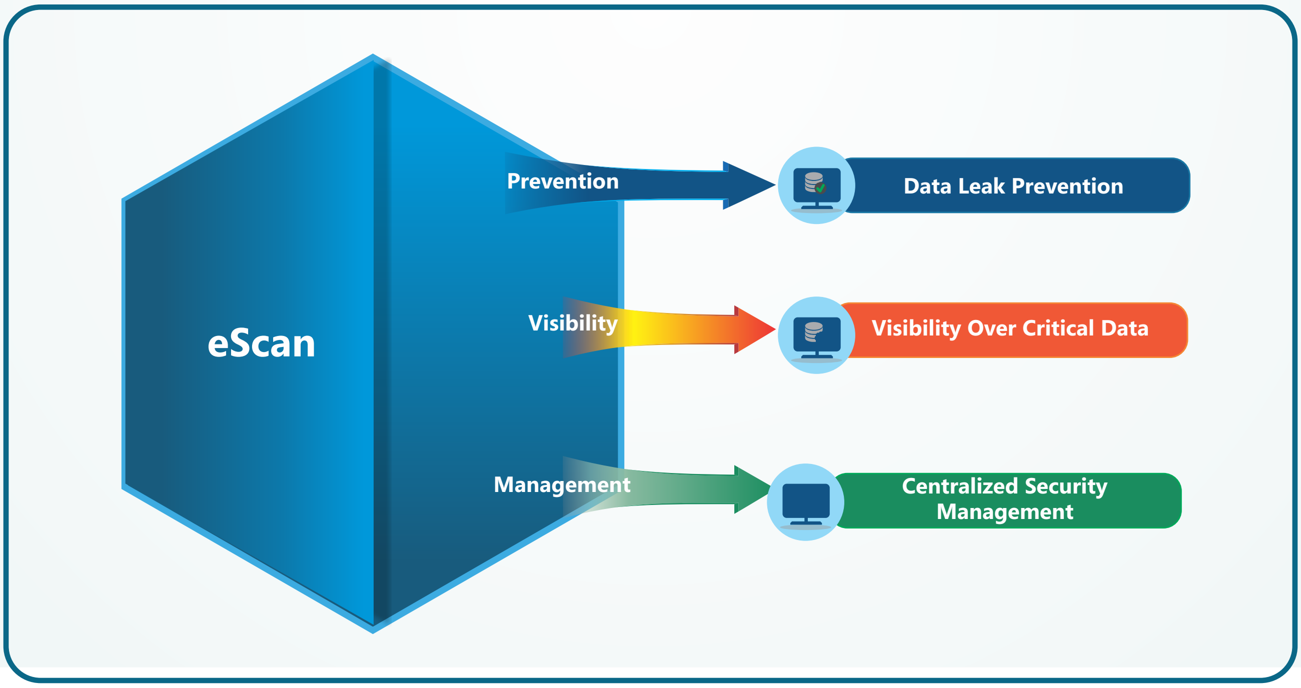
eScan Enterprise DLP's password protection feature restricts user access from violating a security policy deployed in a network. For example, assuming the administrator has deployed a security policy to block all USB devices, but someone wants to access it for a genuine purpose, for example – making a sales presentation residing on a USB pen drive. How would an administrator give the user access without violating the current security policy? OTP is the answer for the same. By generating eScan Enterprise DLP One Time Password (OTP) for a specified period of time, for that specific client computer, to disable the module without violating existing policy.

eScan
Enterprise DLP

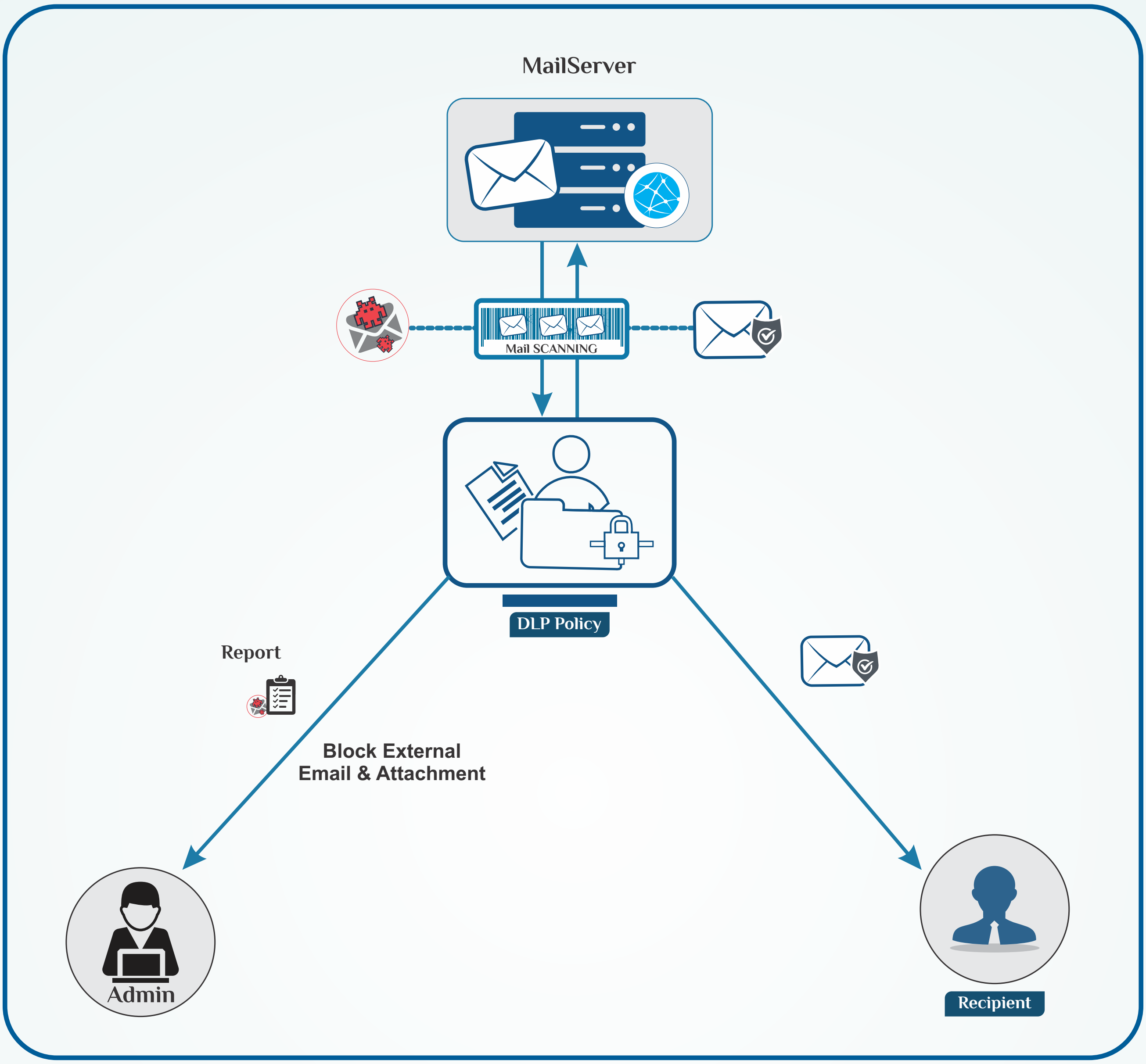
eScan™ Enterprise Security

Key Highlights




eScan
Prevention
Visibility
Management
Data Leak Prevention
Visibility Over Critical Data
Centralized Security Management

Attachment Monitoring/Control



File Attachment Block

The DLP Attachment Block feature enables granular control over attachment flows within your organization. Attachments can be blocked or allowed based on their file extensions, ensuring security by restricting potentially harmful file types. Trusted domains and sub-domains can be excluded from these restrictions, allowing seamless communication with pre-approved entities. A dedicated report template provides detailed insights into blocked and allowed attachment activities via email.

Attachment Monitoring

eScan DLP offers advanced attachment monitoring, enabling administrators to track and analyze email attachments with or without files. Monitoring based on file extensions ensures enhanced security by identifying and controlling specific attachment types

Email Monitoring

The Email Monitoring feature empowers administrators to oversee email communication comprehensively. It tracks emails with or without attachments, identifying their sources, destinations, and file types to ensure compliance and prevent data leaks.

Attachment Report

This feature delivers a robust reporting module that identifies which attachments are allowed or blocked by eScan Enterprise DLP. It provides real-time alerts to administrators about shared or uploaded attachments, including details such as file source, file extension, attachment type, and destination, ensuring transparency and proactive decision-making.

Data Classification and Discovery

Data Classification

eScan Enterprise DLP utilizes Sensitivity Labels for data classification, enabling organizations to categorize information by sensitivity and importance. This ensures appropriate security measures are applied, enabling swift responses to potential data leaks and enhancing overall data protection.

Data Discovery

Identify the location of sensitive or critical data across the organization's infrastructure, including databases, file servers, and cloud storage. eScan Enterprise DLP scans the network to detect and report on confidential information stored on endpoints, enabling informed decisions to mitigate data breach risks.

Sensitivity Labels and Content Control

Content-Aware Controls (Content DLP)

This advanced feature empowers administrators to monitor and control the flow of confidential information from endpoints, ensuring compliance with regulatory requirements such as DPDP, GDPR and more. Sensitive data, commonly referred to as Personally Identifiable Information (PII), is automatically identified and categorized for protection. The categories of sensitive information include:-

- **Aadhar Card Number**
- **Driving License Number**
- **Passport Number**
- **PAN Card Number**
- **Credit Card Numbers (RUPAY, VISA, Amex, MasterCard, etc.)**
- **International Bank Account Numbers (IBAN)**

Note: Personally Identifiable Information (PII), are constantly updated base on the regulatory/regional requirement.

Multi-Channel Filtering

eScan Enterprise DLP applies filtering for PII across multiple communication and data transfer channels, providing a comprehensive security solution. The monitored and controlled channels include:

- **External Storage Devices:** USB drives, CDs/DVDs, Bluetooth devices
- **Network Communication:** Email, file transfers, and other data transmissions
- **Recipient Domain Whitelisting:** Allows data sharing only with pre-approved trusted domains to prevent unauthorized dissemination

This robust functionality ensures that sensitive information is securely managed, preventing unauthorized sharing or leakage across endpoints, communication channels, and devices

Printer Control DLP

eScan Enterprise DLP manages and monitors the printing activity of sensitive documents, ensuring that only authorized users can print specific types of data on designated printers. Printer Control policies define which documents can be printed and by whom, based on predefined rules. In the event of unauthorized printing activity, the DLP system logs the incident, notifies the user about potential risks, and can block the print job immediately.

Furthermore, potential data breaches trigger alerts that are sent to administrators for timely intervention. This module also allows administrators to completely or selectively block access to network printers, providing fine-grained control over printing operations and enhancing data security across the organization.

Watermarking of Printed Documents

eScan Enterprise DLP enables the use of watermarks on printed documents to enhance data security and traceability. By default, the watermark is set to Confidential, but users have the flexibility to customize it with their own strings and variables. This includes adding information such as the IP address, hostname of the machine, username of the logged-in user, and other relevant data. Customizable watermarking ensures that sensitive documents are uniquely identifiable, helping prevent unauthorized distribution and enabling traceability in case of data leaks, while reinforcing compliance with organizational security policies.

Image DLP (OCR)

Image DLP uses OCR technology to extract and monitor text from image files, protecting sensitive information in scanned documents such as IDs, financial cards, and other confidential materials.

Sensitivity Labels

Sensitivity labels classify data into categories like Normal, Internal, and Confidential, ensuring appropriate security controls are applied. This enables organizations to regulate file accessibility and sharing, mitigating risks of data breaches and enhancing data security compliance.

Shadow Copy of Files Allowed to be Uploaded

The eScan Enterprise DLP feature provides a robust mechanism for creating shadow copies of files transferred over web services, email, and online storage platforms such as Google Drive, OneDrive, Dropbox, and others. When files are transferred, shadow copies can be automatically created based on criteria such as recipient, sender name, and attachment size. This ensures comprehensive monitoring of data being shared or stored, enabling administrators to track sensitive file movements and detect potential data leakage.

These shadow copies act as an additional layer of security, providing visibility into file transfers that might otherwise go unnoticed, enhancing overall data protection efforts.

Workspace Applications

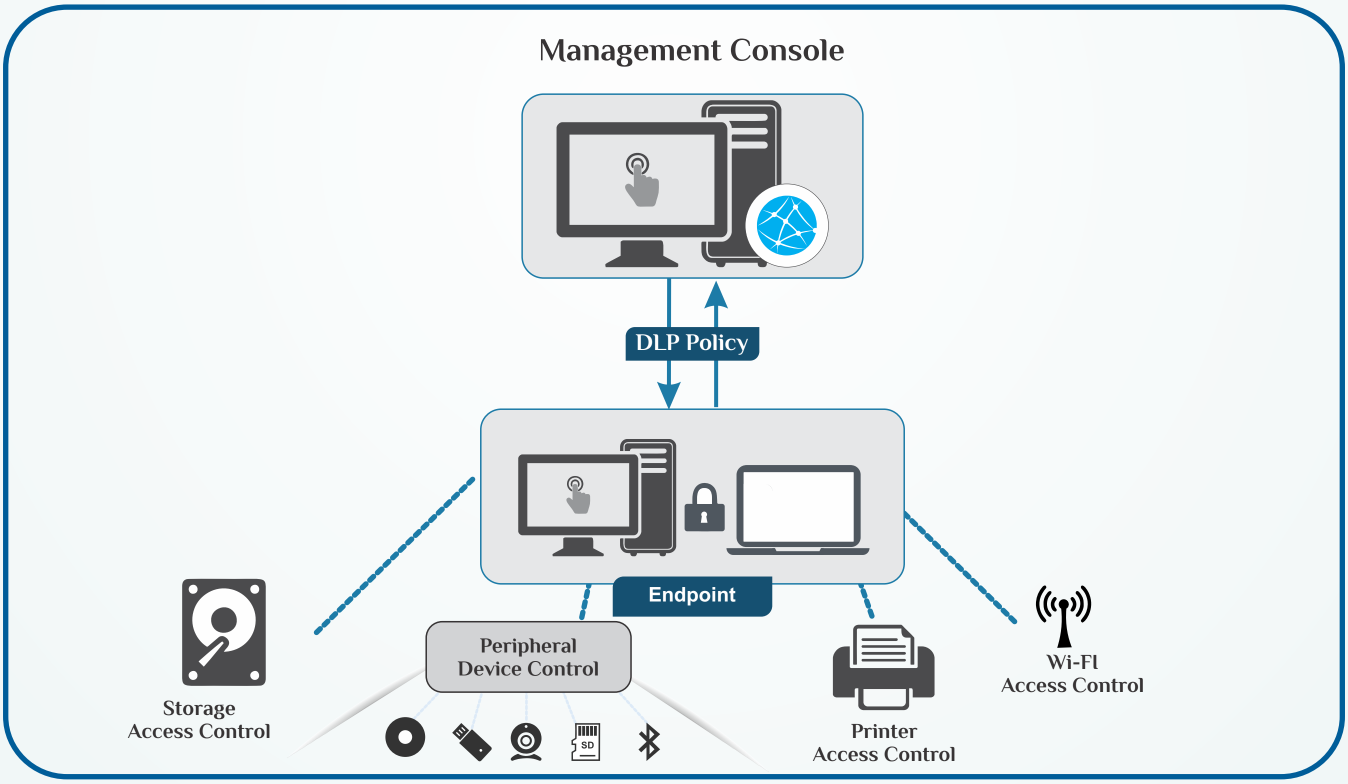
eScan Enterprise DLP enhances data security by enforcing domain-specific or account-specific restrictions across various platforms, ensuring employees can only access cloud-hosted services with corporate credentials.

Platform-Specific Restrictions

- **Google Workspace:** Enforces organization-based restrictions to block personal Google accounts while allowing access via corporate credentials.
- **Microsoft 365:** Implements Tenant ID restrictions to ensure access is limited to corporate Microsoft accounts.
- **Collaboration Tools:** Supports restrictions for third-party platforms like Slack, Webex, Zoom, and AutoDesk to prevent unauthorized logins.
- **File Sharing Services:** Controls access to platforms like Dropbox and WeTransfer, ensuring sensitive files are handled securely.
- **Code Repositories:** Enforces restrictions on platforms like Bitbucket to safeguard intellectual property.

By blocking personal account logins and ensuring access only through corporate credentials, eScan Enterprise DLP helps organizations comply with security policies and prevent data leaks.

Device Control



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.

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).

User Entity Behavior Analytics (UEBA) - Activity Monitoring

File Activity Monitoring (Local/Network/Storage Devices)

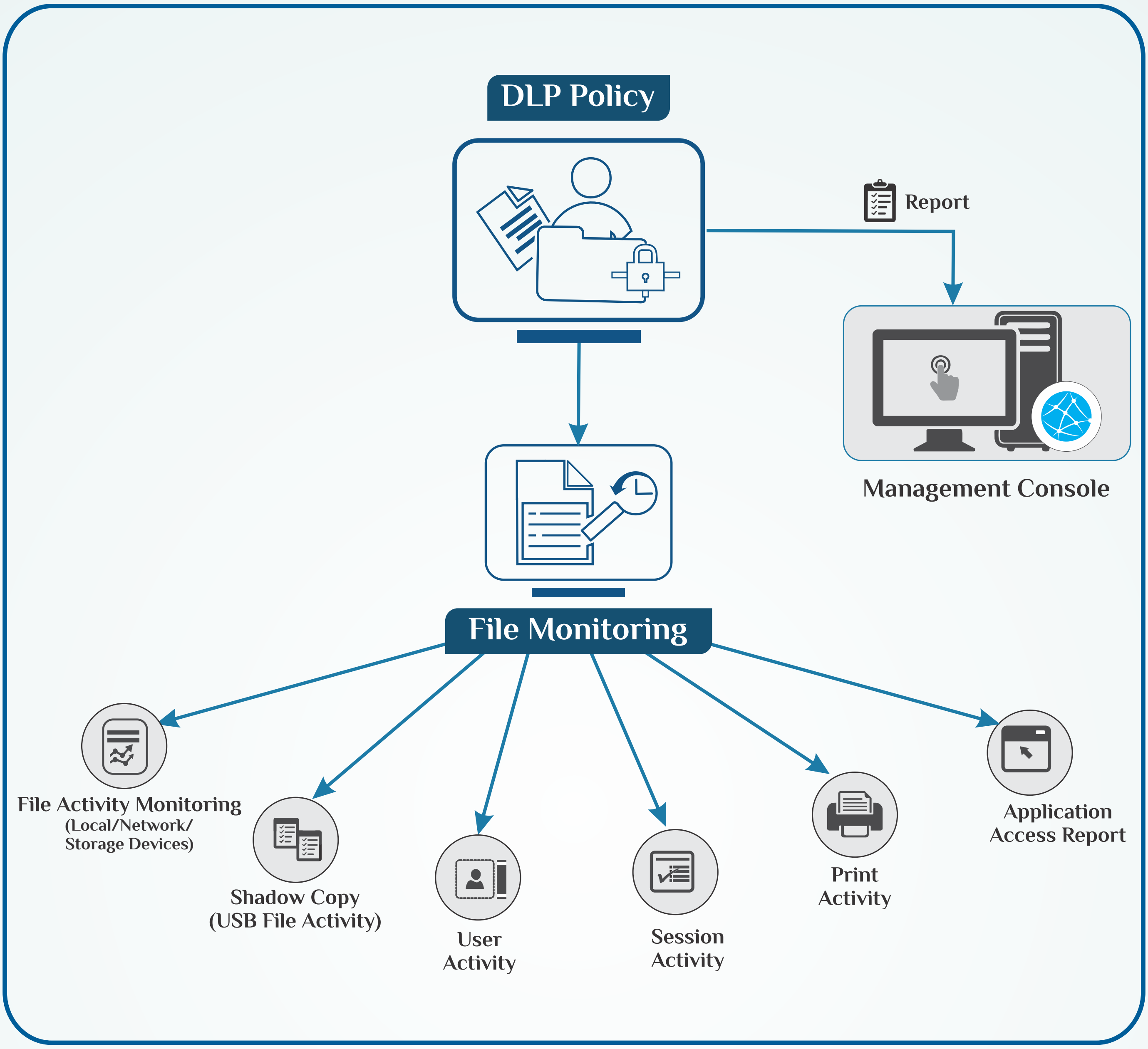
The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. Additionally, in case of misuse of any official files, the same can be tracked down to the user through the details captured in the report. The Administrator can select and filter the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

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.

eScan
Enterprise DLP

eScan™ Enterprise Security



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.

Session Activity

This submodule 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.

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.

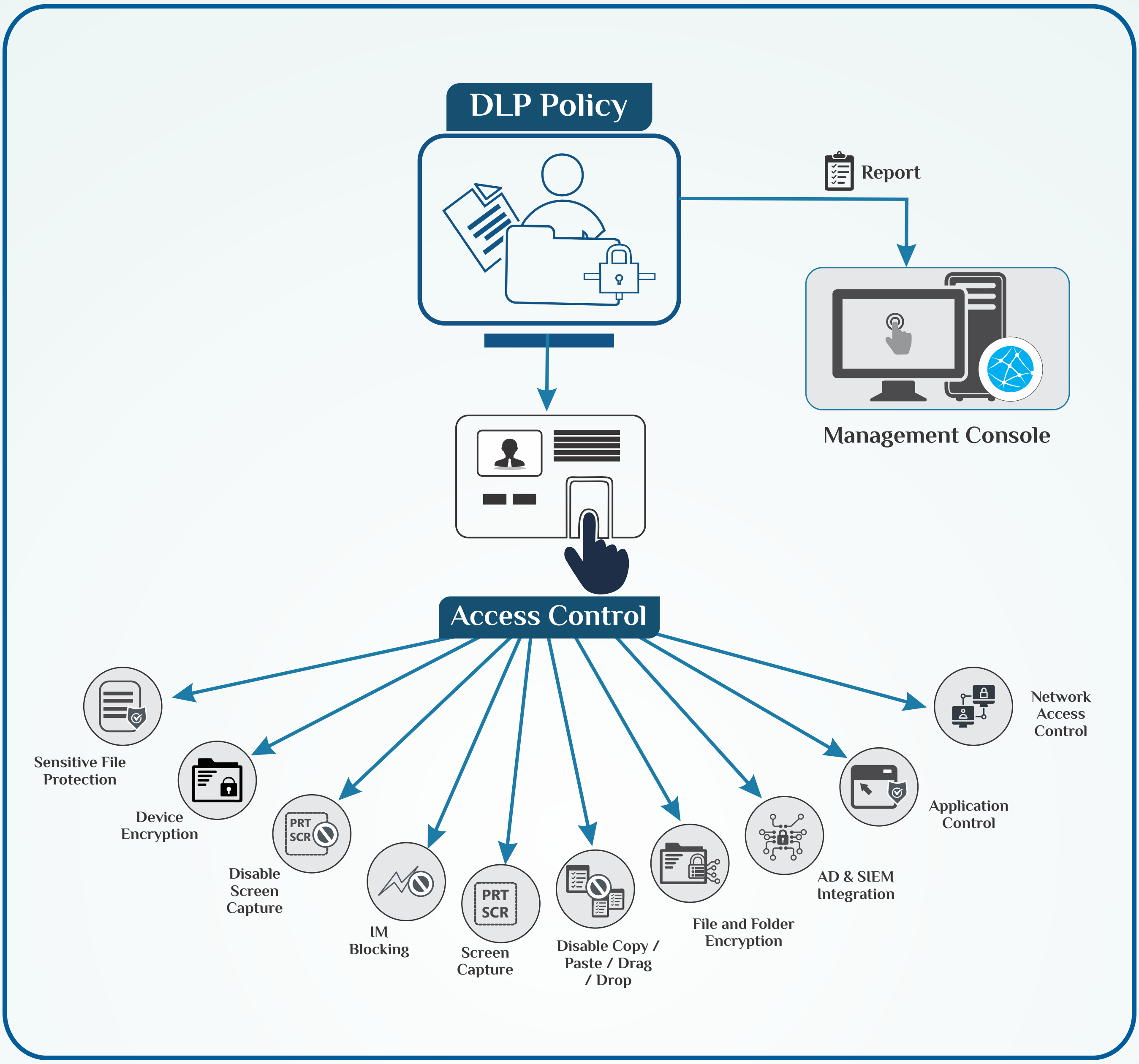
Access Control

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

Screen Capture

Screen Capturing makes it easier to take desktop screen-shots. As a business owner, it becomes crucial to be aware of the activities of employees, especially in the case of customer service or help-desk teams. Employees may work hard but to clearly understand their productivity, screen capturing gives you a detailed insight into the work being done.



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.

DLP's Data-Vault is encrypted using 256-bit Advanced Encryption Standard (AES) and HMAC-SHA 256-bit key. A password is required to access the vault. When a user accesses the data-vault, using the correct credentials, stored data will automatically be decrypted. Vice versa, after a user closes the vault, the data stored will automatically be encrypted

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.

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.

Removable Device Encryption

Removable Device Encryption is one of the security features that protects your data from unwanted access, in the event an external drive is misplaced or stolen. When you enable this function, the device is encrypted and all data stored on this device can be accessed only by trusted endpoints, which are part of eScan Enterprise DLP Managed Group. eScan Enterprise DLP Device Encryption allows you to manage Device Encryption on Windows endpoints through eScan Enterprise DLP Management Console.

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.

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.

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.

Logging and Reporting

Incident Response and Reporting

eScan Enterprise DLP provides comprehensive Incident Response and Reporting capabilities to manage and mitigate data loss risks:

- **Incident Handling:** Establish a defined process for responding to DLP incidents, including investigation, remediation, and escalation to compliance officers or regulators as required. This ensures prompt and effective action to minimize the impact of security breaches.
- **Reporting:** eScan Enterprise DLP maintains comprehensive logs and reports of DLP violations and actions taken, ensuring full traceability for compliance audits and regulatory requirements.

Integrations

SIEM Integration

eScan Enterprise DLP seamlessly integrates with Security Information and Event Management (SIEM) systems, enabling centralized monitoring and real-time correlation of DLP events, enhancing threat detection and incident response across the enterprise.

Active Directory (AD) Integration

eScan Enterprise DLP provides seamless integration with Active Directory (AD), enabling efficient grouping and management of endpoints based on the organization's predefined structure. This integration allows for centralized policy enforcement and user access control, ensuring that DLP rules are applied consistently across all endpoints in accordance with the organizational hierarchy and security requirements.

CASB Integration

eScan Enterprise DLP integrates with Cloud Access Security Brokers (CASB), enabling visibility and control over cloud applications and data. This integration ensures consistent enforcement of security policies across cloud environments, preventing unauthorized access and data leaks while maintaining compliance with organizational and regulatory standards

eScan
Enterprise DLP

eScan™
Enterprise Security

Compliance and Data Visibility

Regulatory Compliance

eScan Enterprise DLP helps organizations comply with regulatory standards such as DPDP (Digital Personal Data Protection) by ensuring data protection policies are enforced, sensitive data is safeguarded, and compliance requirements for data handling, breach notifications, and audits are met.

Cloud Data Visibility

eScan Enterprise DLP provides comprehensive visibility into sensitive data stored and processed across cloud platforms, enabling organizations to monitor, manage, and secure their cloud-based information. This ensures full control over data access, movement, and sharing, reducing the risk of unauthorized exposure and enhancing compliance with security policies.

Key Highlights

- Secure eScan Management Console
- Set advanced security policies
- License Management
- Task deployment
- Policy Templates
- Policy Criteria
- Update Agent
- Auto Grouping
- Active Directory Synchronization
- Message Broadcast
- Session Activity
- Customize Setup
- Manage updates
- Real-Time Protection against Malware
- Sophisticated File Blocking & Folder Protection
- Powerful Heuristic Scanning for Proactive Protection
- Inbuilt eScan Remote Support
- 24x7 FREE Online Technical Support through e-mail, Chat & Forums

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