eScan Business DLP (Data Leak Prevention)

eScan Business Data Leak Prevention (DLP) is a data security solution built on a comprehensive set of strategies, technologies, and techniques designed to monitor sensitive or critical data outside the organization. Regardless of the transmission method, be it messaging, email, file transfers, or other channels, the data can potentially end up in unauthorized hands, leading to compliance and regulatory concerns.

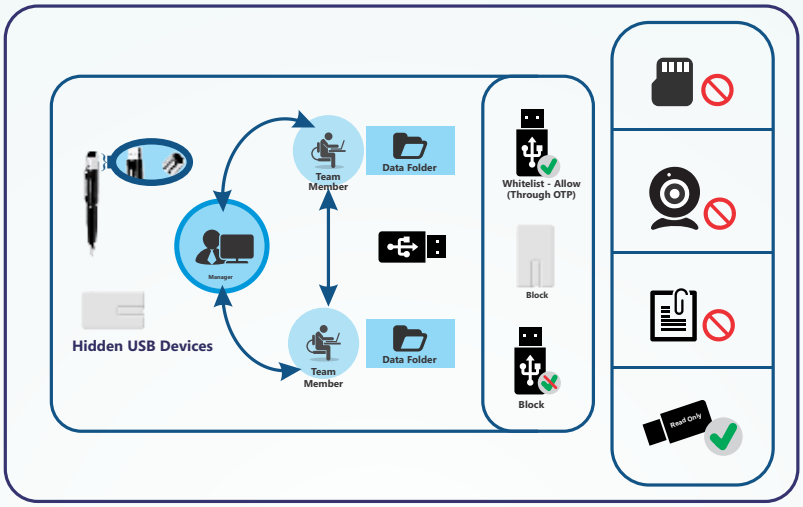
As a DLP solution, it detects and monitors potential data breaches or exfiltration attempts by continuously monitoring and detecting sensitive data when it is in use (through endpoint actions), in motion (across network traffic), and at rest (within data storage). An effective DLP solution applies data security rules to enforce regulatory compliance, support data classification, and secure confidential information. With its advanced capabilities, it safeguards against data exfiltration attempts, tracks access to sensitive data, detects potential leaks, and provides 360-degree visibility into the usage of confidential files, ensuring protection for critical business data.

eScan Business DLP

eScan Enterprise Security

Why eScan Business DLP?

eScan Business 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 Business Grade Centralized Management Console that allows you to deploy the solution on endpoints connected to your network. eScan Business DLP also provides protection on mail gateways to prevent leakage of critical data through email.



eScan Business 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.

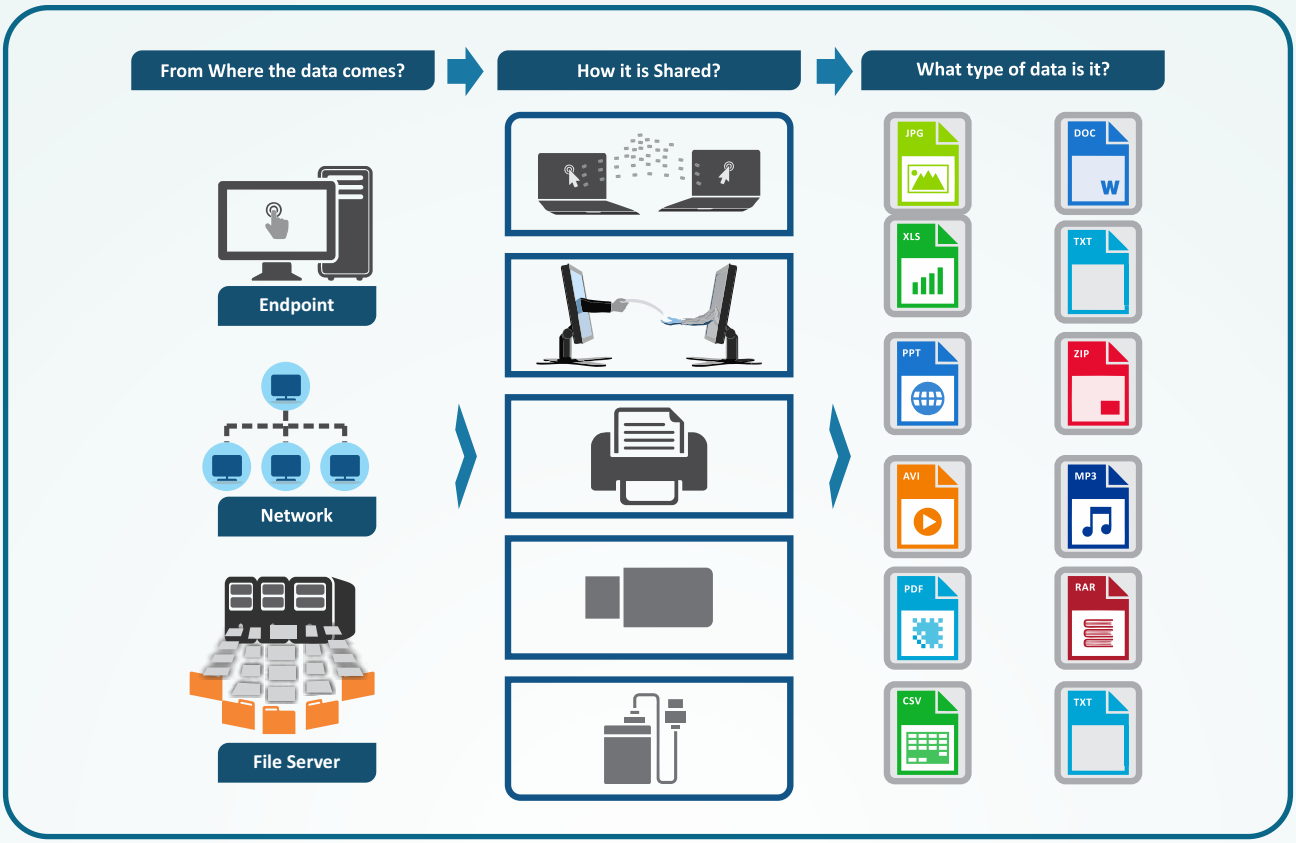
Many times, access to the USB port is misused and data pilferage becomes a common occurrence causing potential damage to the organization as intellectual property falls into wrong hands. A sub-feature in eScan Business DLP's Device Control enables to send notifications to the administrator of the web-console,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

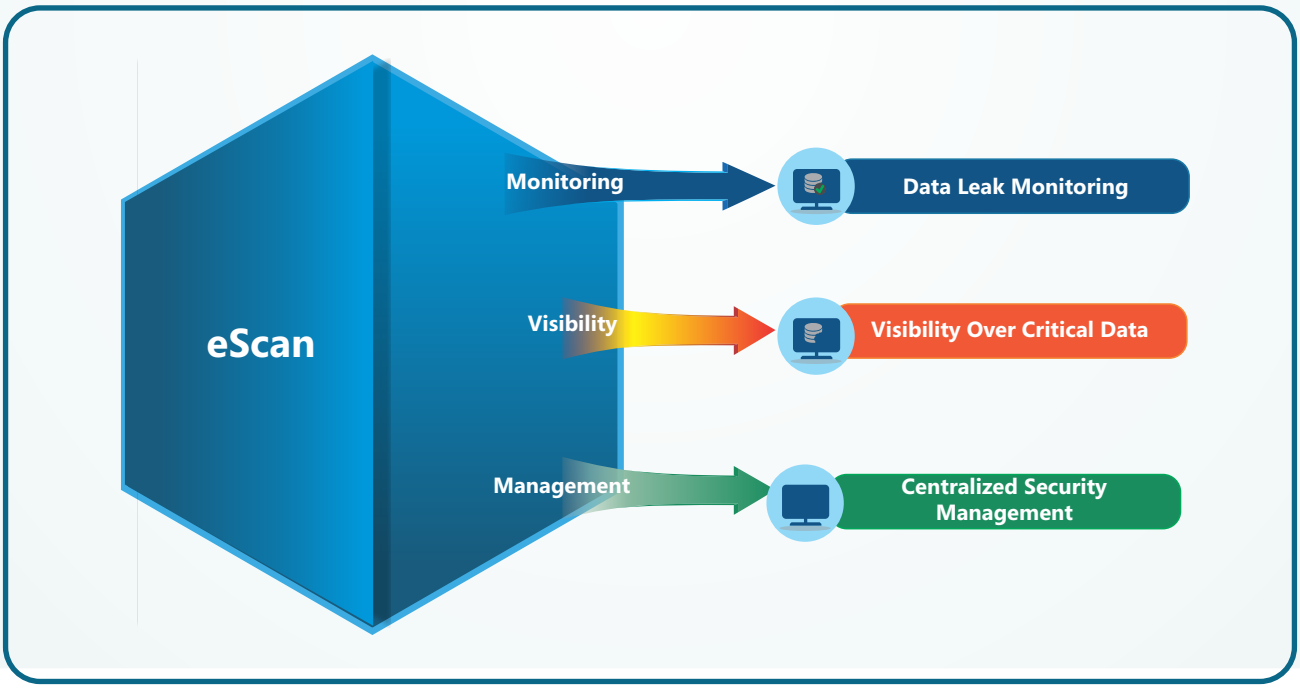
eScan Business DLP's password protection feature restricts user access from violating a security policy deployed in a network. For example, assuming the administrator has deployed a security policy to block all USB devices, but someone wants to access it for a genuine purpose, for example – making a 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 Business 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 Business DLP

eScan®
Enterprise Security

Key Highlights

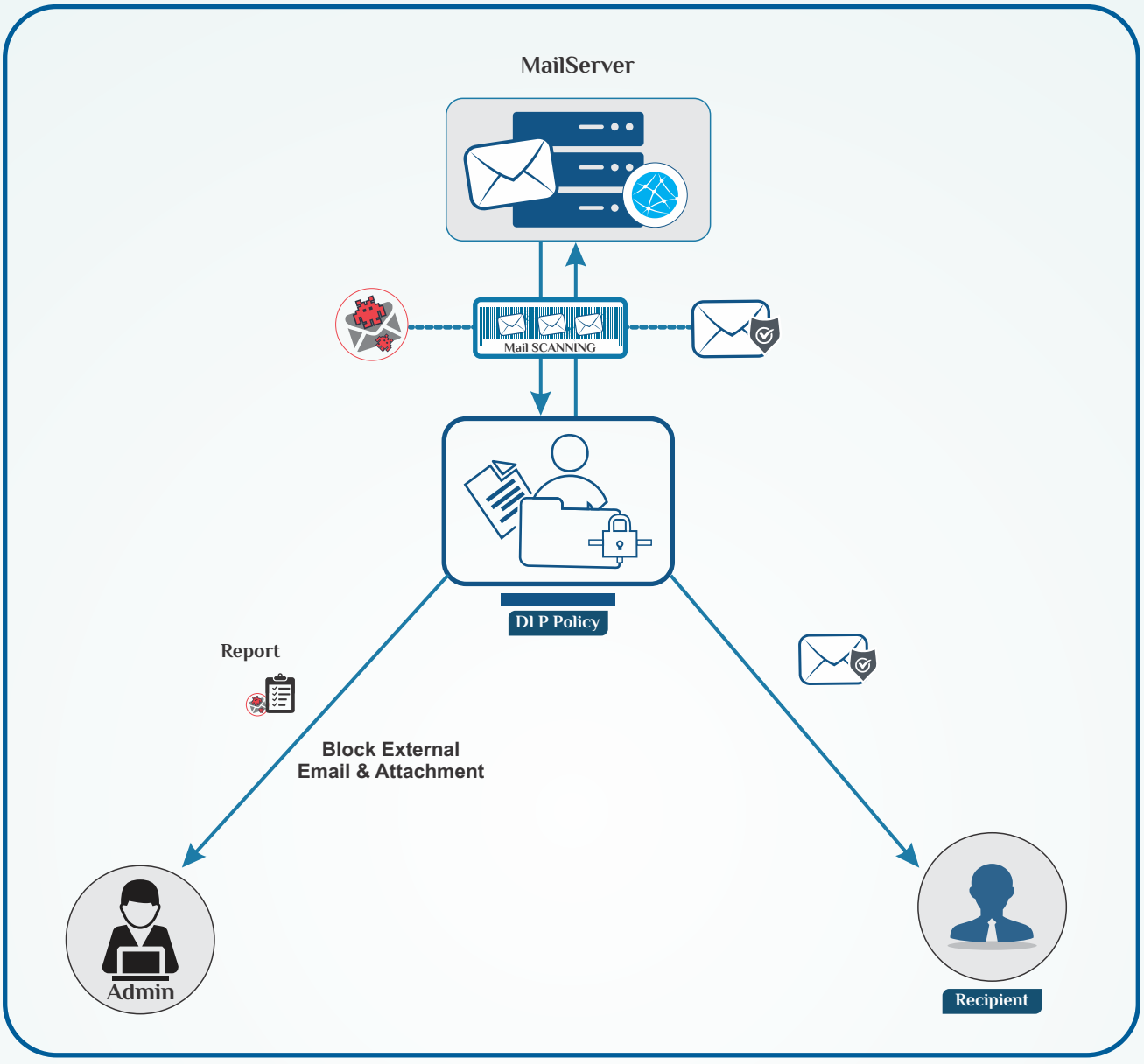




eScan Business DLP

eScan Enterprise Security

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 subdomains 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.

NOTE: File attachment blocking can be achieved on Windows endpoints.

eScan Business DLP

eScan Enterprise Security

Attachment Monitoring

eScan DLP offers advanced attachment monitoring for Windows, endpoints, enabling administrators to track and analyze emails with attachments.

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 Business 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, Discovery

Data Classification

eScan Business 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.

DLP Database Discovery

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

DLP Discovery Scan

This is the policy that can be defined to locate and manage sensitive data across the network. It scans and generates a detailed report (on a scheduled basis) of your sensitive data present in the Windows endpoints. This helps you take informed decisions regarding the same and ultimately mitigate risks associated with data breaches.

eScan Business DLP

eScan Enterprise Security

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, but are not limited to:

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

Content Monitoring: The monitoring of sensitive content is available on Windows endpoints.

Multi-Channel Filtering

eScan Business 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 Business DLP gives organizations full control over the printing of sensitive documents, ensuring that only authorized users can print specific data on designated printers. With customizable printer control policies, you can define who can print what, based on predefined rules.

If an unauthorized print attempt occurs, the system logs the incident, alerts the user to potential risks, and can immediately block the job. Administrators receive instant notifications of potential data breaches, enabling rapid intervention. Plus, with the ability to selectively or fully restrict printer access, this module delivers precise, granular control over printing activities safeguarding sensitive information and strengthening data security across the organization.

eScan Business DLP

eScan Enterprise Security

Watermarking of Printed Documents

eScan Business 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.

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.

Password-Protected File Inspection

eScan DLP solution decrypts the file, scans for sensitive content, and applies appropriate security measures based on findings to block.

Workspace Access Management (Tenant Control)

eScan Business 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 on Windows machines.
- **Microsoft 365:** Implements Tenant ID restrictions to ensure access is limited to corporate Microsoft accounts.
- **File Sharing Services:** Controls access to platforms like Dropbox ensuring sensitive files are handled securely.

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

Remote Access Software

Organizations rely on remote access software for technical support, system configuration, and application installation. The Remote Access Software feature enforces essential restrictions to prevent unauthorized activities. It blocks VPN clients to maintain web filtering, restricts SafeMode booting during remote sessions, prevents access to Android's Development mode, and allows only corporate AnyDesk accounts.

Control Sync Settings

eScan Business DLP Control Sync Settings in a corporate network is crucial for data security, network performance, and regulatory compliance. It prevents unauthorized data sharing, protects user privacy, and optimizes network resources. Administrators can enhance security by disabling sync for apps, browsers, passwords, and credentials; blocking file storage on OneDrive, limiting access to QR code sharing in Chrome and Edge; and limiting YouTube access. Moreover, admins have full control over the browser extensions that users might add in their web browsers for various purposes. For more precise control, the extension whitelisting option is also made available.

Device Control

Storage Access Control

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

Peripheral Device Control

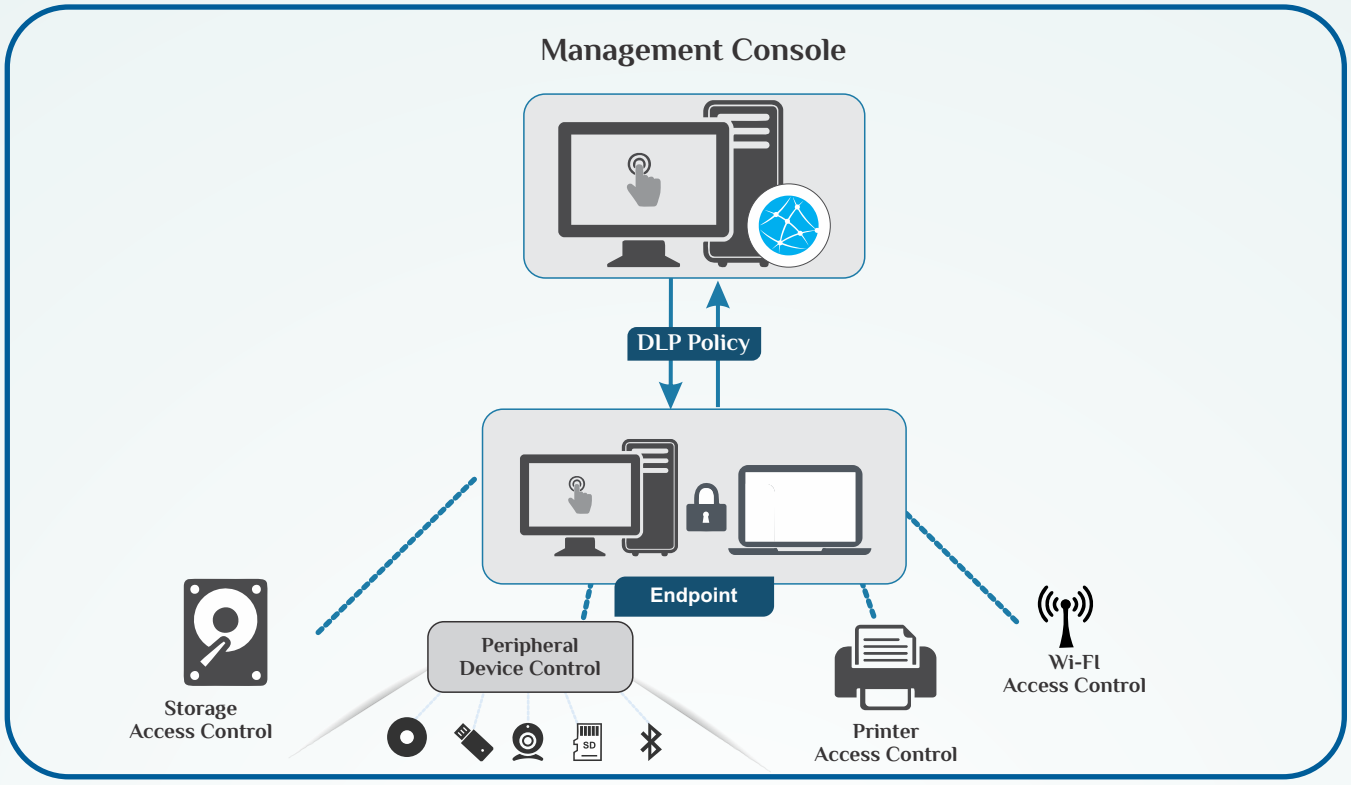
eScan Business DLP protects critical data from leaving your company through peripheral and removable devices, such as USB drives, Bluetooth devices, and recordable CDs and DVDs. Device control provides the option to monitor and control data transfers from all desktops and laptops, regardless of where 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).

eScan Business DLP

eScan Enterprise Security



User Entity Behaviour 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)

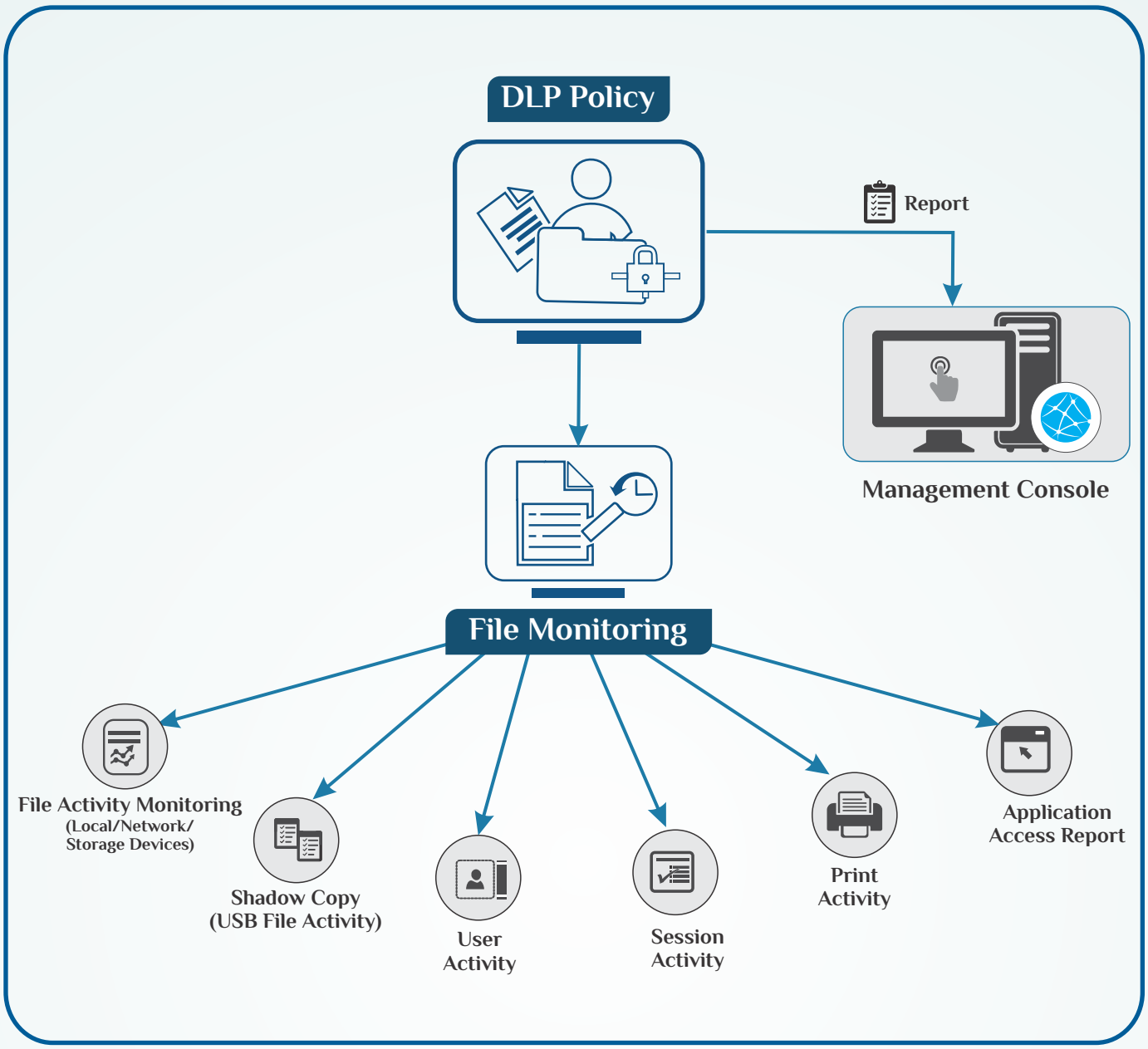
It is a technology that allows you to create a copy of files that a user copies to an external USB drive. This feature allows administrators to audit files that leave the endpoint.

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 that are part of Managed Computers. The File Activity Report displays a report of the files created, copied, modified, and deleted on managed computers.

eScan
Business DLP

eScan®
Enterprise Security



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 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, and document name, along with the number of copies and pages.

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's logon and logoff activity, along with remote sessions that took place on all managed computers.

Application Access Report

The Application Access Report module gives a detailed view of all the applications accessed by the endpoints that are part of Managed Computers. The log displays a 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 that accessed the app and the 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, and Opera) through known vulnerabilities such as buffer overflows or boundary-condition errors. eScan Business 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.

File and Folder Encryption (Data eVault)

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

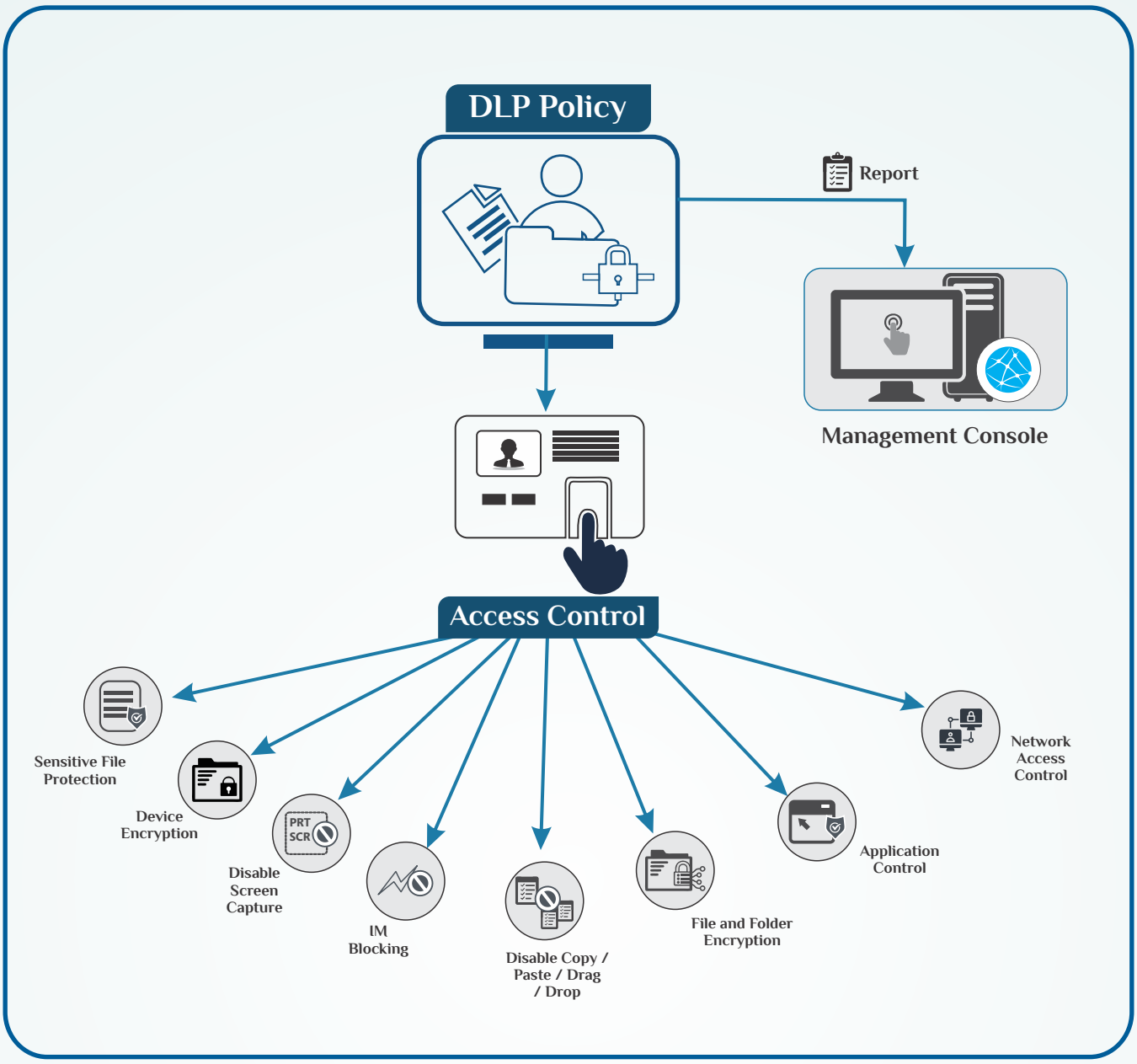
DLP's Data-Vault is encrypted using 256-bit Advanced Encryption Standard (AES) and HMAC-SHA 256-bit key. A password is required to access the vault. When a user accesses the data vault, using the correct credentials, stored data will automatically be decrypted. Vice versa, after a user closes the vault,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

File and Folder Encryption (Disk Encryption)

The Disk Encryption feature secures data by enabling encryption for specific folders or entire drives on a client machine. Once encrypted, the data within these folders or drives cannot be altered or transferred through any means, ensuring robust protection against unauthorized access.

eScan
Business DLP

eScan®
Enterprise Security



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 the copy/paste option disabled, a user is prohibited from copying any information to the clipboard.

Application Control

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

eScan Business DLP

eScan Enterprise Security

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.

Role-Based Access (RBA

This module allows the creation of roles tailored to the specific responsibilities and tasks a user needs to perform. Role-Based Access (RBA) is used to control system access, ensuring that only authorized users can perform certain actions based on their roles within the organization. It helps define who can access which resources and what actions they are allowed to perform. User roles are defined based on the responsibilities and tasks, with access permissions granted accordingly. Roles can vary, from administrator to group admin, each with its own set of access rights. After a role is created, its settings can be adjusted to manage access to different areas of the eScan Management Console and networked devices.

Disable Print Screen

This will block any screenshot and/or screen-grab process, like Windows Snipping Tool, from capturing desktop screen images. 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.

Web Protection

eScan is equipped with Advanced Web Protection that protects from accessing dangerous, phishing, and fraudulent pages. It allows admins to define the list of sites to restrict or whitelist on endpoints connected to the network. As a result, when a URL points to a known phishing or fraudulent website or to malicious content such as spyware or viruses, the webpage is blocked and an alert is displayed.

Logging and Reporting

Incident Response, Reporting, and Forensics

eScan Business DLP provides comprehensive Incident Response, Reporting, and Forensics 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 Business DLP maintains comprehensive logs and reports of DLP violations and actions taken, ensuring full traceability for compliance audits and regulatory requirements.
- **Forensics:** Is the process of investigating and analyzing data loss incidents to understand the cause, impact, and response actions. It involves the detailed examination of logs and reports related to DLP violations to ensure accountability, traceability, and compliance with regulatory requirements.

eScan Business DLP

eScan Enterprise Security

Integrations

Active Directory (AD) Integration

eScan Business 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 Business 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.

Uniform Management

Asset Management

eScan's Asset Management module helps admins to keep track of hardware information and a list of software installed on the endpoints. Besides, it allows you to view the hardware changes that have been made to the configuration of the systems in the network. It also allows exporting the detailed report of the same to have deeper knowledge.

Key Highlights

- Secure eScan Management Console
- License Management
- Task deployment
- Policy Templates
- Policy Criteria
- Update Agent
- Auto Grouping
- Active Directory Synchronization
- Message Broadcast
- Session Activity
- Customize Setup
- Manage updates
- Sophisticated File Blocking & Folder 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