






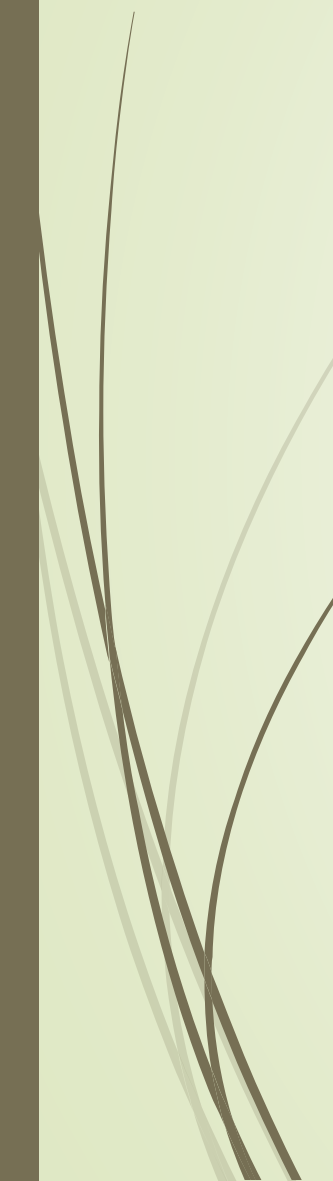
WINDOWS FEATURES: -

- **Content Discovery:** PATROL DLP in Windows helps organizations locate sensitive data within their Windows-based environments, ensuring that all instances of sensitive data are identified and protected.
- **Content Classification:** It classifies data based on predefined policies, helping organizations to categorize data by sensitivity and apply appropriate protection measures.
- **Data Monitoring:** PATROL DLP continuously monitors data flows within Windows systems to detect and prevent unauthorized data access or transfers in real-time.
- **Real-time Inspection:** Windows PATROL DLP systems inspect data in real-time to identify and block unauthorized data transfers or policy violations as they happen.
- **Policy Creation:** Organizations can create and customize data protection policies tailored to their specific needs and regulatory compliance requirements within their Windows environments.
- **Endpoint Protection:** Windows PATROL DLP extends its protection to Windows-based endpoints (computers, servers) to ensure data security no matter where it is accessed or stored.

- 
- **Network Monitoring:** PATROL DLP in Windows environments monitors network traffic for suspicious data transfers or policy violations, helping organizations maintain data security.
 - **Behavior Analytics:** Windows PATROL DLP solutions may use behavioral analysis to identify unusual or suspicious data transfer patterns, aiding in the detection of insider threats or data leakage.
 - **Data Masking:** This feature can dynamically obscure sensitive data within Windows applications or documents, ensuring that only authorized users see the complete data.
 - **Data Redaction:** Windows PATROL DLP can redact sensitive information from documents or files before sharing them, enhancing data privacy and security.
 - **Shadow IT Detection:** PATROL DLP in Windows environments identifies and controls the use of unauthorized or unapproved IT services and applications, reducing security risks.

- 
- **User Training:** Windows PATROL DLP may include user education and training features to raise awareness about data security best practices and compliance policies.
 - **Compliance Reporting:** Windows PATROL DLP solutions generate reports to demonstrate compliance with data protection regulations and internal policies, particularly important for Windows-based systems that handle sensitive data.
 - **Data Retention:** Windows PATROL DLP can help enforce data retention policies, ensuring that data is not retained longer than necessary and complies with legal requirements.
 - **Cloud PATROL DLP:** Extending data protection to cloud services within Windows environments ensures data security in cloud-based applications and storage.
 - **Audit Trails:** Windows PATROL DLP systems maintain detailed logs of data access and transfer activities, enabling auditing and forensic analysis.
- 


- 
- **Data Archiving:** Archiving critical data in a secure manner is essential for compliance and legal purposes within Windows environments.
 - **User Activity Monitoring:** Windows PATROL DLP monitors user actions and behaviors to detect and prevent unauthorized data access or sharing, enhancing security.
 - **Endpoint Visibility:** Windows PATROL DLP provides visibility into endpoint devices running Windows, their status, and data usage, aiding in security monitoring and management.
 - **Insider Threat Detection:** PATROL DLP helps identify and mitigate insider threats within Windows environments by monitoring user behavior and data access patterns.
 - **Regulatory Compliance:** Windows PATROL DLP ensures that organizations using Windows-based systems meet regulatory requirements regarding data protection and privacy.
 - **Email Security:** PATROL DLP features in Windows extend to secure email communications, ensuring that sensitive data is not leaked through email.


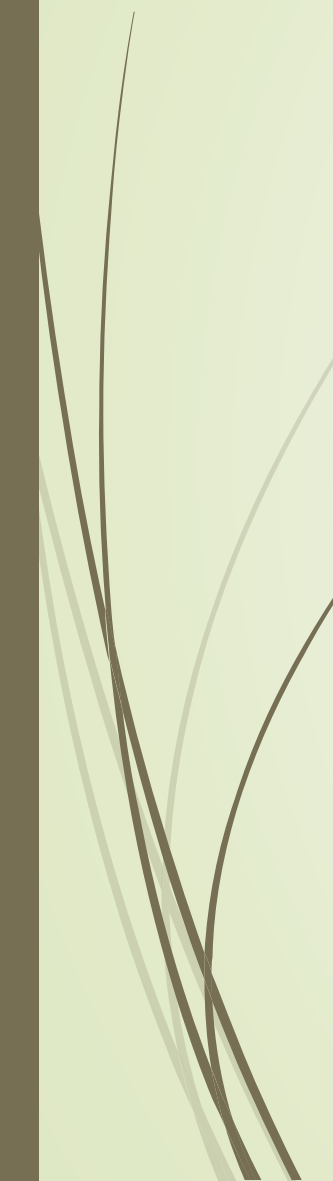
- 
- 
- **Incident Response and Alerts:** Windows PATROL DLP generates alerts when policy violations occur, enabling organizations to respond promptly to potential data breaches or unauthorized data sharing incidents.
 - **Data Encryption:** PATROL DLP in Windows environments may include encryption capabilities to protect sensitive data both at rest and in transit.
 - **Web Content Filtering:** Windows PATROL DLP helps control and monitor web traffic to prevent data leaks through web-based communication and file sharing services.
 - **Policy Enforcement:** Windows PATROL DLP solutions enforce data security policies within Windows systems, ensuring compliance with data protection regulations and internal rules.
 - **Mobile Device Protection:** PATROL DLP extends its coverage to mobile devices running Windows, securing data on Windows-based smartphones and tablets.
 - **Automated Remediation:** Windows PATROL DLP systems can automatically take action to remediate vulnerabilities found in Windows environments, reducing the risk of data breaches.





MAC FEATURES: -

- **Email Security:** PATROL DLP includes features to monitor and secure email communications, ensuring sensitive data is not leaked through emails. It can detect and block unauthorized sharing of data via email.
- **Incident Response and Alerts:** PATROL DLP systems generate alerts when policy violations occur, allowing organizations to respond promptly to potential data breaches or unauthorized data sharing incidents.
- **Data Encryption:** PATROL DLP may include encryption capabilities to protect sensitive data both at rest and in transit, ensuring that even if data is leaked, it remains unreadable to unauthorized parties.
- **Web Content Filtering:** This feature helps in controlling and monitoring web traffic to prevent data leaks through web-based communication and file sharing services.
- **Policy Enforcement:** PATROL DLP solutions enforce data security policies by monitoring and controlling data flows within an organization, ensuring compliance with data protection regulations and internal rules.

- 
- **Mobile Device Protection:** PATROL DLP extends its coverage to mobile devices, securing data on smartphones and tablets and preventing data loss through mobile apps or unauthorized device access.
 - **Automated Remediation:** PATROL DLP systems can automatically take action to remediate vulnerabilities found on open ports or system software, helping to reduce the risk of data breaches.
 - **Application Control:** PATROL DLP can control and monitor the use of applications and their data-sharing capabilities to prevent unauthorized data transfers.
 - **Integration with SIEM (Security Information and Event Management):** This integration allows PATROL DLP to provide data loss events and policy violations to a SIEM system, enhancing overall security monitoring and incident response capabilities.
 - **Content Discovery:** PATROL DLP can identify and locate sensitive data across an organization's network, helping to ensure that all instances of sensitive data are protected.
 - **Insider Threat Detection:** PATROL DLP helps identify and mitigate insider threats by monitoring user behavior and data access patterns.
 - **Regulatory Compliance:** PATROL DLP ensures that organizations meet regulatory requirements regarding data protection and privacy.

- 
- **Content Classification:** It classifies data based on its sensitivity, allowing for more granular control and protection of different types of data.
 - **Data Monitoring:** PATROL DLP constantly monitors data flows and user actions to detect and prevent data breaches or policy violations in real-time.
 - **Real-time Inspection:** PATROL DLP systems inspect data in real-time to identify and block unauthorized data transfers or policy violations as they occur.
 - **Policy Creation:** PATROL DLP solutions enable organizations to create and customize data protection policies tailored to their specific needs and compliance requirements.
 - **Endpoint Protection:** PATROL DLP extends protection to endpoints (e.g., computers, servers, mobile devices) to ensure data is secure no matter where it is accessed or stored.
- 

- 
- **Network Monitoring:** PATROL DLP continuously monitors network traffic for suspicious data transfers or policy violations.
 - **Behavior Analytics:** PATROL DLP can use behavioral analysis to identify unusual or suspicious data transfer patterns, helping to detect insider threats or data leakage.
 - **Data Masking:** This feature can dynamically obscure sensitive data, such as credit card numbers or Social Security numbers, to protect it from unauthorized access.
 - **Data Redaction:** PATROL DLP can redact sensitive information from documents or files before sharing them, ensuring that only authorized recipients see the complete data.
 - **Shadow IT Detection:** PATROL DLP identifies and controls the use of unauthorized or unapproved IT services and applications that may pose security risks.
 - **User Training:** PATROL DLP may include user education and training features to raise awareness about data security best practices and policies.

- 
- **Compliance Reporting:** PATROL DLP solutions generate reports to demonstrate compliance with data protection regulations and internal policies.
 - **Data Retention:** PATROL DLP can help enforce data retention policies, ensuring that data is not retained longer than necessary.
 - **Cloud PATROL DLP:** It extends data protection to cloud services, ensuring data security in cloud-based applications and storage.
 - **Audit Trails:** PATROL DLP systems maintain detailed logs of data access and transfer activities for audit and forensic purposes
 - **User Activity Monitoring:** PATROL DLP monitors user actions and behaviors to detect and prevent unauthorized data access or sharing.
 - **Endpoint Visibility:** PATROL DLP provides visibility into endpoint devices, their status, and data usage, enhancing security monitoring.