The challenge

A hacker's most coveted entity in a cybersecurity attack is an organization's data so developing effective data defense strategies is vital for business continuity. However, the sheer volume of new and unfiltered information makes distinguishing exactly what is important and worth protecting difficult to determine. If highly critical information is not tracked, it can result in misuse or unauthorized disclosures that can be incredibly costly to recover from. To address this issue, an efficient data loss prevention tool has to be implemented that prioritizes the detection and safeguarding of sensitive data in particular.

The solution

ManageEngine Endpoint Data Loss Prevention (Endpoint DLP Plus), is an integrated software that can be leveraged to automate the process of locating, tagging, and controlling the movement of data across a network. It identifies and protects sensitive data contained in endpoints, mitigates accidental data disclosures, and helps eliminate external and internal cyberattacks.

Insider threat prevention with Endpoint DLP Plus

Endpoint DLP Plus strategically curbs insider risks by first, accounting for all digital assets considered sensitive by discovering an organization's confidential data and classifying it based on source and context. Second, it helps IT administrators create rules that function as virtual boundaries to prevent sensitive data from being leaked by negligent users, or hijacked by malicious actors. Lastly, it provides detailed reports to help flag suspicious user behavior and proactively stop unauthorized file actions.

Data discovery

- Stay on top of the data influx by continuously locating archived as well as newly created files containing sensitive information.
- Deploy policies to detect all structured and unstructured sensitive items.
- Create groups of target computers according to department, function, project or role in order to focus the search efforts and to find specific types of sensitive documents.
- Receive real-time metrics to track evolving data trends and changes in security posture.

Data classification with pre-defined templates

- Categorize sensitive data into groups based on similar attributes.
- Utilize the numerous pre-defined templates to silo common forms of sensitive content, such as personally identifiable information (PII).
- Classify various types of PII, such as financial and health records based on country using nation-specific pre-defined templates.

Data classification with custom templates

- Create custom templates to pinpoint miscellaneous sensitive items not covered by the pre-defined templates.
- Utilize fingerprinting technique to find sensitive files that follow company-specific or frequently used formats.
- Implement RegEx to identify documents with strings of a specified length or specific combination of characters.
- Launch a keyword search to locate content containing unique texts.

Cloud upload protection

- Enhance web protection by allowing only select browsers to be used to process sensitive data.
- Inhibit files containing sensitive items from being exported to various cloud storage software.
- Disallow sensitive content from being transferred via third-party file sharing application.

Device control

- Label authorized USB and peripheral devices as trusted so that all others will be blocked by default.
- Enable printer security by blocking the downloading of confidential information.
- Permit the superimposition of watermarks on sensitive documents that are allowed to be printed.

False positives remediation

- Allow trusted users to override restrictive policies.
- Permit personnel to request override permission through the self-service portal.
- Review reasons for requested overrides directly from the console.
- Fine-tune policies when necessary to suit user needs.

Data containerization

- Label trusted or highly secure applications as 'Enterprise apps' to ascertain that sensitive information is processed only within these select software applications.
- Ensure that all data emerging from Enterprise apps are automatically tagged as sensitive by default.
- Restrict the transfer of data from enterprise apps to non-enterprise applications to prevent unverified and vulnerable software from accessing confidential content.

Clipboard tool regulation

- Enforce clipboard monitoring to prevent screenshots being taken of sensitive content.
- Prohibit users from importing content from work to non-work spaces and apps.

Email security

- Choose which organizational domains to trust for transferring sensitive content.
- Authorize sending information to legitimate Outlook email addresses.
- Block uploading of work content through personal emails.

Reports and Alerts

- Visually navigate the dashboard highlights for a quick overview of network health.
- Conduct forensic analysis to gauge the security profile of each endpoint.
- Receive alerts about blocked attempts at transferring data.

Server hardware requirements

Number of managed devices	Processor	RAM	Hard disk space
1 to 250	Intel Core i3 (2 core/4 thread) 2.0 GHz 3MB cache	2GB	5GB
251 to 500	Intel Core i3 (2 core/4 thread) 2.4 GHz 3MB cache	4GB	10GB
501 to 1000	Intel Core i3 (2 core/4 thread) 2.9 GHz 3MB cache	4GB	20GB
1001 to 3000	Intel Core i5 (4 core/4 thread) 2.3 GHz 6MB cache	8GB	30GB
3001 to 5000	Intel Core i7 (6 core/12 thread) 3.2 GHz 12MB cache	8GB	40GB
5001 to 10000	Intel Xeon E5 (8 core/16 thread) 2.6 GHz 20MB cache	16GB	60GB
10001 to 20000	Intel Xeon E5 (8 core/16 thread) 2.6 GHz 40MB cache	32GB	120GB

When managing more than 3,000 computers, it is recommended to use an additional SQL Server.

Software requirements

Supported OSs for Server
Windows 7 / 8 / 8.1 / 10 / 11 / Servers 2003 / 2003 R2 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022

Supported OSs for agents

Windows OS*	Windows Server OS*
Windows 11	Windows Server 2022
Windows 10	Windows Server 2019
Windows 8.1	Windows Server 2016
Windows 8	Windows Server 2012 R2
Windows 7	Windows Server 2012
	Windows Server 2008 R2

* - recommended for managing 5000 or more endpoints.