ManageEngine

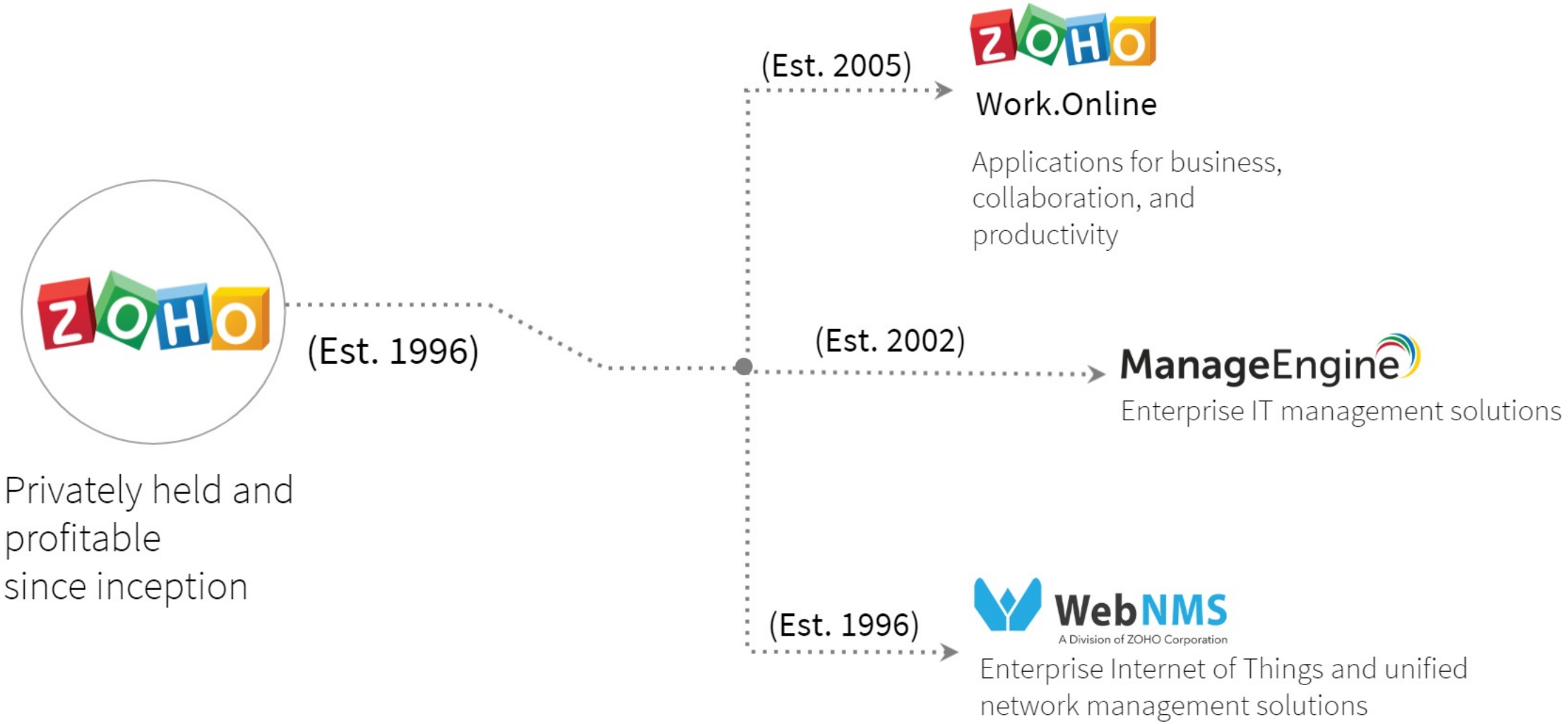
IT management simplified

Real-time IT management solution for the new speed of business

ManageEngine

- Enterprise IT management software division of Zoho Corporation
- Founded in 1996 as AdventNet
- Privately held, rock- solid supplier and partner
- Headquartered in Pleasanton, California
- Millions of customers across industries

ManageEngine: The enterprise IT management division of Zoho Corporation



ManageEngine **solutions**

Active Directory management

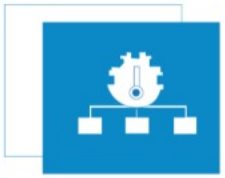
Active Directory
Exchange Server
Self- service portal
Recovery and backup

IT service management (ITSM)

Help desk
Asset life cycle
CMDB and ITIL
Customer support

Endpoint management

Desktop management
Mobile device management
OS deployment
Patch management
Browser management



IT operations management (ITOM)

Network performance
Application performance
End-user experience
Network change and configuration
Converged infrastructure
Storage infrastructure
Bandwidth and traffic
SQL server monitoring

On-demand

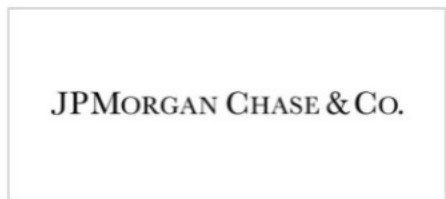
Application performance
Help desk software
Active Directory recovery and backup
Mobile device management
Patch management
Log management

IT security

Log management
Firewall analysis
Vulnerability analysis
Application control
Privileged password management
Network anomaly detection

2 million users

3 of every **5** Fortune **500 companies** are ManageEngine customers



ManageEngine

Endpoint DLP Plus

An integrated endpoint data loss prevention software designed for sensitive data protection and insider risk mitigation.

Why do you need a **data loss prevention** solution?

- Data is one of the most valuable entities within an organization and is often the prime target of cybersecurity attacks.
- Being unaware of where data is stored or how it's processed leaves it vulnerable to accidental loss or insider threats.
- Data breaches can compromise the integrity of a business and result in reputational and financial damage that can take a significant amount of time to recover from.

Why do you need **an Endpoint DLP solution** specifically?

The domain level of a network where most endpoints are located, is often the most dynamic and at risk due to the following reasons:

- Endpoints are ubiquitous and also often the first mode of access for the majority of employees within an organization, making them hotspots for insider attacks due to easy access and accidental data disclosure due to lack of awareness or protocol.

- Endpoints contain valuable data but their security is often overlooked in favor of protecting more specialized data reservoirs (i.e file servers) leaving them more vulnerable to data breaches.

Roadblocks to effective **Endpoint Data Loss Prevention**

- Exponential rise of cybersecurity threats targeting sensitive data on endpoints can be challenging to consistently avert.
- Shortage of resources such as time and personnel to manage the data security details and user access permissions of every individual computer.
- Absence of endpoint security solutions for data leakage prevention which are versatile enough to satisfy all organization specific needs.
- Lack of understanding regarding the importance of sensitive content protection for endpoints in particular.

How can ManageEngine **Endpoint DLP Plus** can help?

ManageEngine Endpoint DLP Plus is dedicated cybersecurity solution for effective endpoint data protection. It aids in proactively combating insider and external threats to preemptively prevent the leakage of sensitive data. Endpoint DLP Plus offers a multitude of robust capabilities that enable IT admins to instantly discovery and classify structured and unstructured forms sensitive data and to also strategically define domain boundaries to prevent the data from being intentionally or unintentionally disclosed.

Features at a glance

- Data discovery
- Data classification
- Data containerization
- Email security
- Cloud protection
- Device Control
- Clipboard protection
- False positive remediation
- Business overrides
- Reports

Endpoint **Data Discovery**

Sensitive content can be dispersed across numerous endpoints, it can be difficult to track making it easier to tamper with discreetly or illicitly extract sensitive data.

With Endpoint DLP Plus, swiftly pinpoint of the locations of data at rest, in motion and in use, as well as newly generated and archived sensitive data.

Benefits:

- Reduce information sprawl for optimal visibility.
- Newly generated as well as archived sensitive data will be promptly detected to ensure all valuable digital assets are accounted for.

Data classification using **templates**

- Endpoints can harbor large volumes of unstructured information. To improve data-driven decision-making, Endpoint DLP Plus enables IT admins to create rules for automating the detection and categorization of specific types of sensitive documents.
- They can select from a wide array of pre-defined templates that correspond to common types of sensitive documents. Endpoint DLP Plus will then search across endpoints for documents that match the template attributes and will consolidate and label the discovered files accordingly.
- To find sensitive files whose formats are organization specific, Endpoint DLP Plus provisions admins with advanced mechanisms such as keyword search, fingerprinting and RegEx.

Containerization of sensitive data

Streamlining the flow of data can be conducive to a better security posture, to achieve this admins can use the data containerization capability to:

- Designate specific business-friendly and secure applications as trusted.
- Confine sensitive data to these trusted apps to ensure that it circulates in authorized spaces only.
- All data originating from enterprise apps can be automatically labeled as sensitive.
- Audit & block any attempts to transfer data from trusted apps to unauthorized apps

Optimal Cloud Protection

With many workforces going remote, cloud services have become an increasingly popular way to store and transfer data. To prevent data disclosure via cloud, Endpoint DLP Plus can be used to:

- Allow employees to utilize verified browsers only.
- Prohibit the upload of work content to unverified web domains.
- Stop the transferring of sensitive content to third-party cloud storage and applications.

Email Security

Many employees often opt for email for quick collaboration and though it is convenient it can be a risk if not properly controlled. With Endpoint DLP, admins can:

- Ensure that sensitive content is not illicitly attached and leaked via email.
- Inhibit work information from being sent via personal emails by whitelisting trusted email domains for authorized information exchange.
- Add verified Outlook email domains to the trusted list.

Device Control and **Clipboard Regulation**

- Users can attempt to utilize hardware utilities, such as peripheral devices to transfer data. Endpoint DLP Plus can be used to control the usage of USB drives and other devices.
- Some printers can be permitted to process sensitive content and watermarking can also be enabled in these scenarios.
- To prevent images of sensitive files from being taken or transferred, limit the use of clipboard tools that are used for screen capture purposes.

Handle **False positives & business overrides**

- From onboarding to long term implementation, easily cater to changing user needs.
- By using the self-service portal, users can report false positives, the reason can be reviewed by IT admins and related policies can be easily modified, if required.
- Trusted users can also be allowed to override a policy after stating a valid reason for transferring sensitive data.

Extensive reports and **insights**

- Endpoint DLP Plus' dashboard offers multiple infographics for easy navigation and overview of data trends.

- A plethora of data security analytics are available so that admins can easily grasp the efficacy of applied policies and data protection framework.

- Actionable insights are also provided so that admins can make informed decisions to strengthen their endpoint DLP strategies.

Editions

Free Edition Up to 25 computers	Professional suitable for computers in LAN & WAN
» Suitable for SMBs » Fully functional » Up to 25 computers	» Discover and classify sensitive data » Utilize pre-defined & custom templates » Containerize data to trusted apps » Ensure email security » Monitor cloud uploads » Restrict clipboard actions » Control peripheral devices » Manage false positives » Grant business overrides » Mitigate insider risks » Access smart audit reports

How does Endpoint DLP Plus **benefit your organization?**

- Simplified set up and centralized deployment of policies
- Restriction of major avenues of data transfer
- Expedient detection and mitigation of insider threats
- In-depth understanding of company data leading to better data-driven decision making
- Conservation of resources such as time and digital space.
- Data security and significant return on long term financial investment

Useful **resources**

- Pricing store
- System requirements
- Architecture
- User guide
- FAQs
- Free trial

Learn more

https://www.manageengine.com/endpoint-dlp/