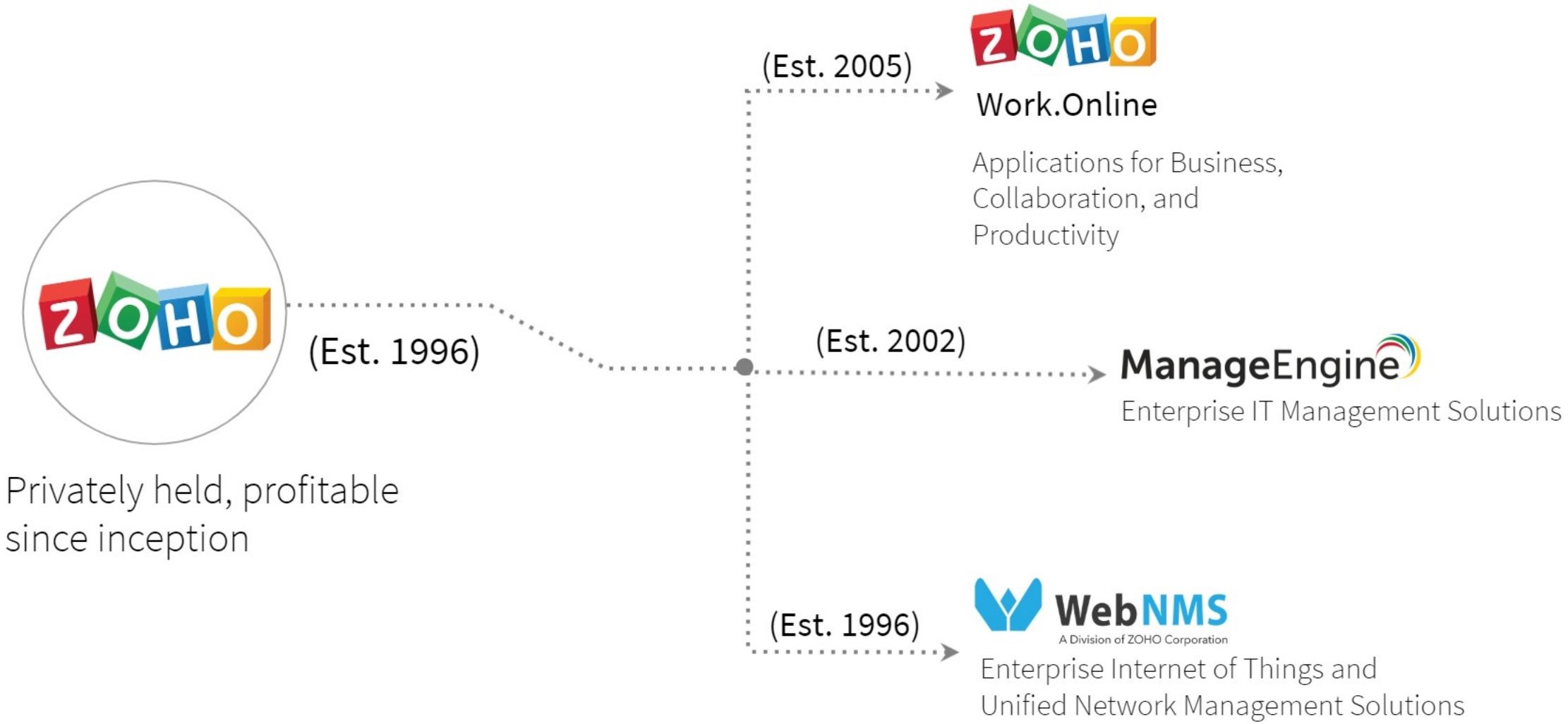
IT Management, Simplified

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

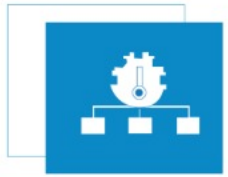
Active Directory
Exchange Server
Self- service Portal
Recovery and Backup

Endpoint Management

Desktop Management
Mobile Device Management
OS Deployment
Patch Management
Browser Management

IT Service Management

Help Desk
Asset Lifecycle
CMDB and ITIL
Customer Support



IT Operations Management

Network Performance
Application Performance
End-user Experience
Network Change and Configuration
Converged Infrastructure
Storage Infrastructure
Bandwidth and Traffic
SQL Server Monitoring

On Demand

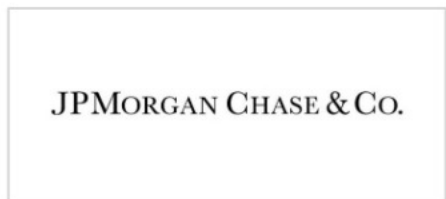
Application Performance
Helpdesk Software
Active Directory Recovery and Backup
Mobile Device Management
Patch Management
Log Management

IT Security

Log Management
Firewall Analysis
Vulnerability Analysis
Privileged Password
Network Anomaly Detection

2 Million Users

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



ManageEngine

Device Control Plus

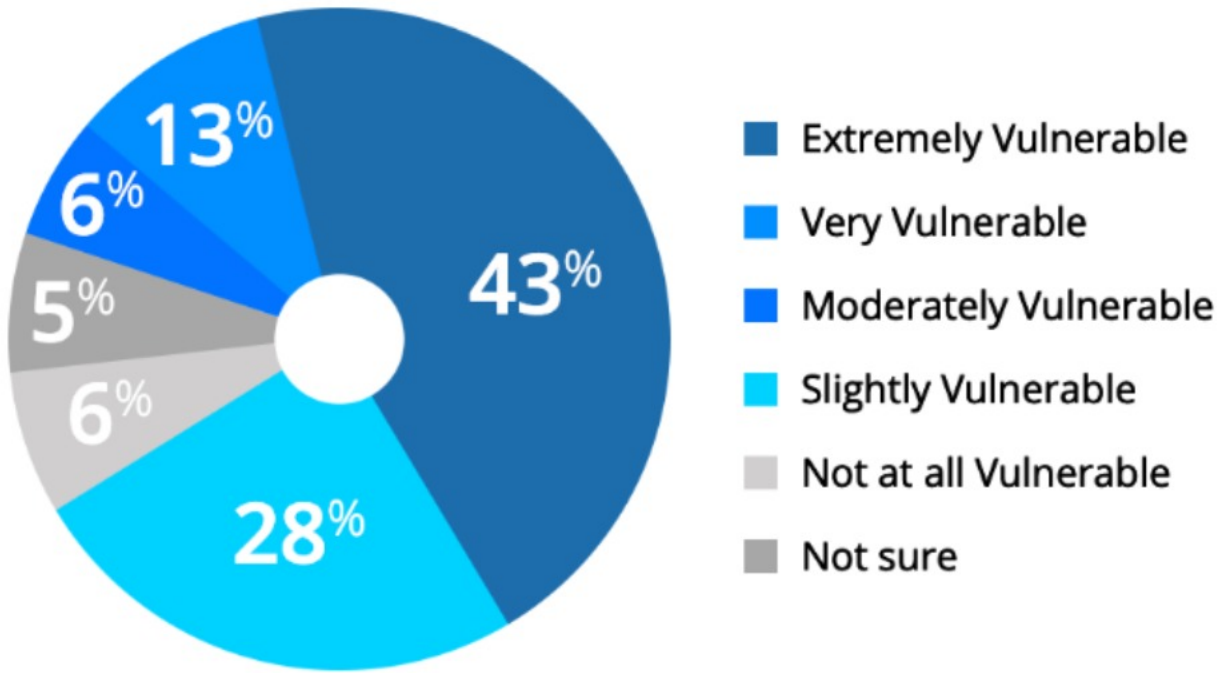
Automated solution for centralized device control and file security management

What is Device Control Plus?

Device Control Plus is complete device control and file movement management software which supports the detection and zero-trust based management of various in-built and external peripheral devices. The information security capabilities of this product aids organizations in securing their network perimeter and effectively mitigating data loss.

Why is device control important for your organization?

Traditional device control capabilities still leave organizations with massive amounts of **unprotected files. A robust software solution is needed to prevent data loss.**



Many business across various sectors are threatened by insider attacks or data loss via improper device usage. Yours could be one of them.

Who's at **risk**?

Financial services

Telecommunication

Technical services

Industrial organization

Healthcare

Government

Roadblocks to effective Device Control

- Numerous device connections occur everyday, which can be overwhelming to keep track of without automatic detection
- Different users/roles require different levels of access, so it can be time consuming to manually assign access permissions each time
- Rudimentary access control such as fully allowing or blocking can be too restrictive, counter-productive and/or unsafe
- Data transfer restrictions can be difficult to enforce without granular policies

A versatile solution for device and data security

- Device control is one of the most fundamental security measures amongst the spectrum data loss prevention protocols.
- With Device Control Plus, secure your network and avert all insider attacks and malicious actors by expediently detecting and managing numerous peripheral devices connected to your network.
- Additionally, safeguard all entreprise-critical data and when required facilitate secure data transfer through capabilities such as file access and transfer control, file tracing and shadowing and granting of temporary device access.

Enforce comprehensive device control in 3 steps

- Select a device type and choose specific devices.
- Configure a policy according to your specific operational requirements.
- Associate the policy with custom computer groups.

Features Overview

- Automatic device discovery
- File access control
- File transfer control
- File tracing
- File shadowing
- Temporary Access
- Extensive reports

Automatic Device Discovery

- Automatically detect 17+ types of in built and external peripheral devices
- Classify each discovered device as trusted, allowed or blocked
- Create a 'Trusted Devices' list comprising of whitelisted devices belonging to highly authorized personnel on the basis of device instance path or wildcard pattern
- Prevent unauthorized devices from entering or conducting illicit activities within your network

File Access Control

- Exercise role-based security by assigning permissions to users based on their titles and job description
- Delegate varying levels of access for optimal control: Read-only, file copying and modifying within devices, file movement from devices to computer
- As an additional precautionary measure, only enable file access for devices that are BitLocker encrypted

File Transfer Control

- Restrict data transfer based on the types of file extensions such that users can only obtain data relevant to their tasks
- Impose regulations regarding the amount of information that can be transferred in order to ensure that users are provided data for their present duties
- Ensure that only the necessary information is moved from the organization and by authorized users

File Tracing

- Immediately obtain logs of all file transfer activities that take place within your organization
- Analyze all salient details regarding these file transfer operations including:

- ✓ File names, extensions and size
- ✓ Initial location from where it was moved
- ✓ Devices used to transfer the data
- ✓ Computers the devices were connected to
- ✓ Users who have initiated the operation

File Shadowing

- File shadowing is a data security best practice to keep critical files within reach
- When a file is transferred or modified within USB devices, the file contents are replicated exactly
- Resulting shadow copies will be maintained in a password-protected network share
- Types of files that get shadowed can be chosen based on file extensions as well as file size

Temporary Access Permissions

- Users can request temporary access through the agent tray's self-service portal for maximum convenience where they will prompted to include device details and reason for their request
- IT admins can review the request and grant access through the console itself or by sending an email with the unique temporary access code/script
- The permissions can be flexibly designated based on time frame comprising specific schedule or based on a duration which the user can activate at the time of their choosing

Extensive Reports

- Obtain detailed logs of all device and file transfer activities taking place within the organization
- Utilize smart filter for easy analysis
- Easily pinpoint any policy disruptions
- Gain insight on how to modify policies in order to meet both network safety and user requirements
- Refer to dashboard info graphics for a bird's eye perspective of device and file-related trends

How does Device Control Plus benefit your organization?

- Maintain optimal cyber hygiene by preventing all unauthorized device intrusions and eliminating potential file-based exploits
- Prevent privilege escalation and thwart all insider attacks
- Ensure swift recovery in the event of any data security emergency
- Promote collaboration by enabling temporary device access for third party users such as consultants and interns
- Always be informed of the device and file access patterns for effective policy creation and enhanced visibility over network

Editions

Features	Professional	Free
Suitable For	Suitable for controlling desktops in LAN	Small Businesses with up to 25 devices in LAN
Supported OS	Windows	Windows

Resources

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