

IT security management solutions



ManageEngine 

Aligning IT with business

Comprehensive IT management software for all your business needs





Disclaimer

This presentation is confidential and is intended, among other things, to present a general overview of Zoho's ("Zoho") products and services. This presentation is provided for informational purposes only. The contents are not to be reproduced or distributed to the public or press. While the information in this presentation is believed to be accurate and reliable, Zoho makes no representation regarding, and assumes no responsibility or liability for, the accuracy or completeness of, or any errors or omissions in, any information contained herein.

ManageEngine is the enterprise IT Management software division of ZOHU Corporation

Privately held and profitable since inception



(Est. 1996)



(1996-2021)

Enterprise Internet of Things & Unified Network Management Solutions



(Est. 2002)

Enterprise IT Management Solutions



(Est. 2005)

Application for Business, Collaboration, and Productivity



(Est. 2021)

Workflow orchestration software

ZOHIO Corp. Offices Worldwide





ManageEngine:

A bootstrapped, private, and profitable company

19+

years in the
industry

180,000+

Organizations across the
globe use our products

90+

products and free tools for
IT management

3,500+

ManageEngine
employees

190+

countries

BRINGING IT TOGETHER



Available for
Enterprise IT | Managed service providers (MSPs)
as
Self-hosted on-premises
Self-hosted in public cloud (AWS, Azure)
Zoho Cloud-native

Enterprise service management

- Full-stack ITSM suite
- IT asset management with CMDB
- Knowledge base with user self-service
- Built-in and custom workflows
- Orchestration of all IT management functions
- Service management for all departments
- Reporting and analytics

Identity & access management

- Identity governance and administration
- Privileged identity and access management
- AD and Azure AD management and auditing
- SSO for on-premises and cloud apps with MFA
- Password self-service and sync
- Microsoft 365 & Exchange management and auditing
- AD & Exchange - backup and recovery
- SSH and SSL certificate management

Security information & event management

- Unified SIEM for cloud and on-premises
- AI driven user and entity behavior analytics
- Firewall log analytics
- Data leakage prevention and risk assessment
- Regulatory and privacy compliance

Unified endpoint management & security

- Desktop and mobile device management
- Patch management
- Endpoint device security
- OS and software deployment
- Remote monitoring and management
- Web browser security
- Monitoring and control of peripheral devices

IT operations management


- Network, server and application performance monitoring
- Bandwidth monitoring with traffic analysis
- Network change & configuration management
- Application discovery & dependency mapping
- Cloud cost and infrastructure monitoring
- End user experience monitoring
- AIOps

Advanced IT analytics

- Self-service IT analytics
- Data visualization and business intelligence for IT
- Hundreds of built-in reports and dashboards
- Instant, flexible report creation
- Out of the box support for multiple data sources

IT security management solutions





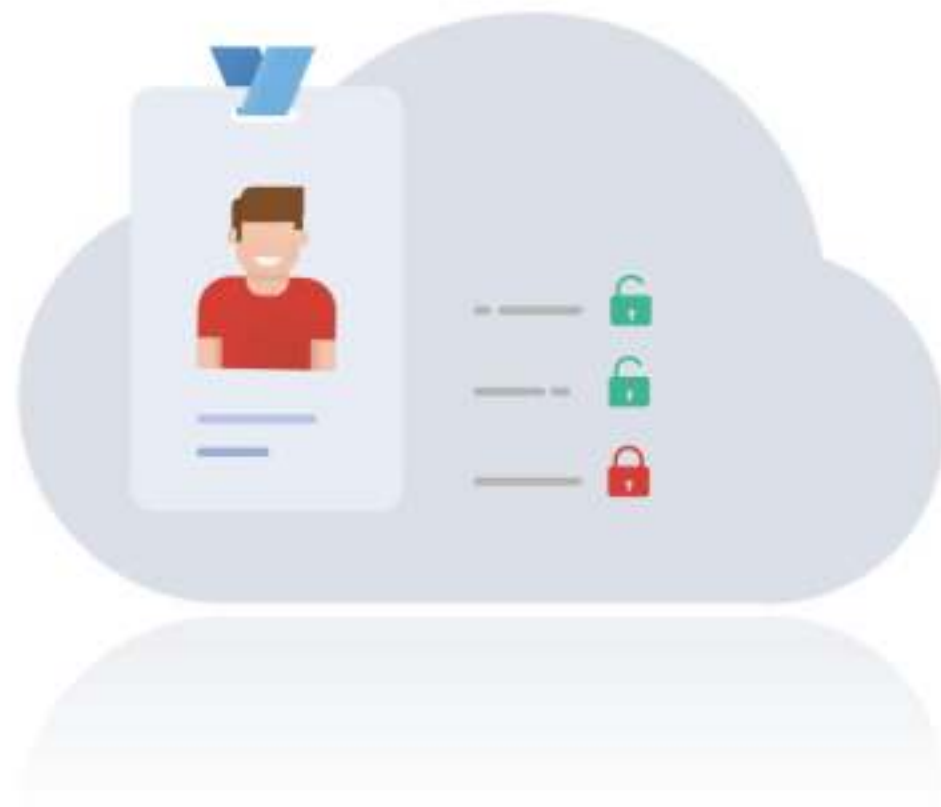
There is one thing even a billion-dollar company can't afford: **a security breach**

- 7 out of 10 businesses are not prepared to respond to a cyberattack ([2018 Hiscox Cyber Readiness Report](#))
- 34 percent of data breaches involved internal actors ([Verizon](#))
- 61 percent of companies have over 500 accounts with non-expiring passwords ([Varonis](#))
- 4.1 billion records were exposed from data breaches in the first half of 2019 ([RiskBased](#))
- \$3.92 million is the average cost of a data breach as of 2019 ([Security Intelligence](#))

Understanding IT security solutions by ManageEngine

- Identity and access management: control and track employee access to protect internal systems from malicious entities
- Security information and event management: secure your IT environment and ensure compliance with regulatory mandates
- Endpoint security management: detect, disrupt, and prevent malicious attacks before they cause any major damage to endpoints
- Network security management: detect, prevent and respond to threats entering your network through the use of security policies, software tools, and IT services
- Data security management: protect the integrity and privacy of sensitive data, both in storage and in transit

Identity and access management





You need identity and access management solutions to:

- Grant the right users the right access to the right enterprise assets
- Extend access to your information systems across a variety of applications and tools without compromising security
- Protect sensitive enterprise systems, assets, and information from unauthorized access or use
- Ensure user credentials are not compromised and do not serve as a network entry point
- Bolster regulatory compliance by implementing comprehensive security audit and access policies

ManageEngine's identity and access management solutions

Active Directory management

- **ADManager Plus:** Active Directory, Microsoft 365, and Exchange management and reporting
- **ADSelfService Plus:** Password self-service, endpoint MFA, conditional access, and enterprise SSO

Identity governance and administration

- **AD360:** Workforce identity and access management for hybrid ecosystems
- **M365 Manager Plus:** Microsoft 365 management, reporting, and auditing
- **Identity Manager Plus:** Secure single sign-on for enterprise applications

Privilege access management

- **PAM360:** Complete privileged access security for enterprises
- **Password Manager Pro:** Privileged password management
- **Password Manager Pro MSP:** Privileged password management for MSPs
- **Access Manager Plus:** Secure remote access and privileged session management
- **Key Manager Plus:** SSH Key and SSL/TLS certificate management

Active Directory management





ManageEngine 
ADManager Plus

Active Directory, Microsoft 365, and Exchange
management and reporting

Why ADManager Plus?

- Automate user provisioning in AD, Microsoft 365, and Exchange with all necessary entitlements, licenses, etc.
- Bulk assign, modify, or revoke Microsoft 365 users' with CSV
- Create and manage users' Exchange mailboxes in mass
- Bulk manage users' group membership; Assign time-bound file server permissions
- Automated cleanup of stale user accounts
- Built-in AD, Microsoft 365, and Exchange report library to view detailed information about users, their Microsoft 365 licenses, group membership, Exchange mailboxes, etc.
- Manage users' accounts on-the-fly, right from the reports
- Role-based access to user management features for help desk technicians

One-click AD user management and reporting with purpose-built features and reports

- One-click AD, Microsoft 365, Exchange, and G Suite User creation via customizable reactive templates
- Bulk management of AD objects via CSV import
- Secure group membership and file server permissions management
- Automation for routines such as AD cleanup
- 200+ built-in reports on AD, Microsoft 365, Exchange and more with on-the-fly management, and custom report builder
- Secure OU-specific delegation of management tasks to help desk
- Approval-based workflow to streamline management and ensure compliance
- Protection against data loss with AD backup and recovery
- Out-of-the-box integration with help desk software, HRMS applications, and databases



ManageEngine 

ADSelfService Plus

Password self-service, endpoint MFA,
conditional access, and enterprise SSO

Why ADSelfService Plus?

- Empower end users to perform password reset and account unlock without compromising on security
- Enable MFA for endpoints (Windows, macOS, and Linux) and enterprise applications
- Provide secure, one-click access to enterprise applications by enabling SSO
- Deliver password and account expiration notifications directly to end users
- Utilize enterprise single sign-on for one-click access to cloud as well as on-premises apps
- Synchronize password and account changes across multiple on-premises and cloud apps
- Enforce a multi-platform granular password policy
- Allow end users to update their personal details in AD and perform comprehensive corporate directory searches

Give your employees the right amount of independence

- Self-service password reset and account unlock
- Endpoint MFA for major OSs
- SSO for cloud applications
- Real-time password synchronizer
- Custom password policy enforcer
- Password expiration notifier
- Directory self-update and corporate search
- Comprehensive reports and instant notifications
- Automatic and forced enrollment of users for self-service password reset and MFA

Identity governance and administration





ManageEngine[®]
AD360

Workforce identity and access management
for hybrid ecosystems

Why AD360?

- Manage identities throughout their entire lifecycle—from provisioning and deprovisioning, through every change in between
- Use real-time change auditing and user behavior analytics (UBA) to detect insider attacks and mitigate threats
- Step up security by enabling MFA for endpoints and enterprise applications
- Enable secure, one-click access to enterprise applications by implementing SSO
- Use the pre-built automation policies or roles to reduce the burden of identity management
- Get unparalleled insights into the state of your IT environment with over 1000 reports
- Protect identities, their attributes, mailbox data, and files by automatically backing them up at regular intervals



A complete suite for IAM and IT compliance

- Identity lifecycle management
- Identity governance with UBA
- Multi-factor authentication for endpoints and enterprise applications
- Single sign-on (SSO) and self-service password management
- Identity analytics
- Active Directory and Microsoft 365 data protection
- Identity automation and role-based delegation with workflow
- Identity orchestration



ManageEngine

M365 Manager Plus

Microsoft 365 management, reporting, and auditing

Why M365 Manager Plus?

- Audit even the most granular user activities, and get notified of critical activities and changes
- Monitor Microsoft 365 service health around the clock, and receive instant email notifications on service degradations
- Search for emails with personally identifiable information (PII), insider information, and malicious content to ensure email security and compliance
- Get out-of-the box reports on Exchange Online, Azure Active Directory, OneDrive for Business, Skype for Business, and more



Protect your Microsoft 365 setup from cyberattacks

- Reports for IT regulatory compliance
- Reports on Exchange and Azure admin activities, litigation hold, and more
- Mail traffic monitoring to detect spam and malware
- Detect loss of sensitive data to enable faster disaster recovery
- Critical alerts on OneDrive for Business, Microsoft Teams, Yammer, Office Sway, and more



ManageEngine
Identity Manager Plus

Secure single sign-on for enterprise applications



Why Identity Manager Plus?

- Helps fast-track cloud application adoption
- Improves user experience by eliminating the need to remember multiple passwords
- Reduces costly password-related help desk calls
- Enhances productivity by providing users one-click access to all their applications
- Helps admins manage and control access to applications from a centralized console
- Obtains valuable insights into application usage and user accesses

A secure cloud-based SSO for enterprises

- Standardized SAML-based SSO for enterprise applications
- Centralized access to enterprise applications
- Built-in directory
- Application usage and access audit
- Automated user lifecycle management for cloud applications
- Leverage existing identities in Microsoft 365, G Suite, or Zoho credentials
- Built-in reports for deep insights

Privileged access management





ManageEngine 
PAM360

Complete privileged access security
for enterprises

Why PAM360?

- Scan and discover privileged accounts across the network
- Onboard privileged credentials into a secure, unified vault
- Centralize the enforcement of privileged access policies for all categories of users. Regulate, monitor, and audit access to all critical assets
- Enable users to launch one-click connections to remote hosts; video-record privileged sessions with session shadowing capabilities to achieve dual control over privileged access
- Delegate just-in-time controls for domain accounts through on-demand, time frame-based privilege elevation
- Create baseline behaviors and detect anomalies in privileged account activity by correlating privileged access data with endpoint event logs
- Accelerate remediation with prompt access to advanced analytics on privileged access



Holistic privileged access security for enterprise IT

- Complete privileged access governance
- Enterprise credential vault
- Just-in-time privilege elevation
- Privileged session monitoring
- Privileged user behavior analytics and context-aware event correlation
- Secure remote access
- Application credential security
- Ticketing system integrations
- SSH key management and SSL certificate management
- Comprehensive reporting, audit and compliance




ManageEngine

Password Manager Pro

Privileged password management

Why Password Manager Pro?

- Privileged credential vaulting and randomization
- Role-based access controls for insider threat mitigation
- Secure remote access provisions with encrypted access gateways and direct login capabilities
- Session recording and shadowing of privileged users
- Compliance auditing and reporting



Secure your enterprise credentials and protect access to your critical devices

- Privileged account discovery and vaulting
- Granular access control mechanism
- Approval workflows for privileged access requests
- Automated password resets
- Application password management
- DevOps credential security
- SSH key management
- Lifecycle management for SSL certificates
- Compliance auditing and reporting
- Secure mobile access



Password Manager Pro MSP:

Manage the passwords of multiple customers in a single instance

- Securely store client passwords
- Launch direct connection to remote IT resources
- Selectively share among MSP admins and clients
- Automatically reset passwords
- Control privileged access to client network
- Gain visibility on password access
- Entrust concurrent control of the password vault to the MSP administrator, the end user, or both



ManageEngine

Access Manager Plus

Secure remote access and privileged
session management

Why Access Manager Plus?

- Secure remote access management and session governance
- Establish privileged sessions to underlying systems (Windows and Linux) via a centralized console
- Define roles and access rights for users and provide them with granular access to critical systems
- Monitor privileged sessions in real-time and record every privileged user session for post session review
- Leverage extensive audit trails for forensic investigations
- Enhanced regulatory compliance

Secure remote access for privileged sessions

- One-click RDP, SSH, SQL, and VNC sessions
- RemoteApp support for Windows
- Bi-directional remote file transfer
- Jump box support for Windows and Linux
- Privileged session management and recording
- Live monitoring and collaboration
- In-depth audit trails



ManageEngine

Key Manager Plus

SSH key and SSL/TLS certificate management

Why Key Manager Plus?

- Gain complete visibility over your SSH and SSL environments
- Discover all SSH keys and SSL certificates across your network and consolidate them in a secure repository
- Avoid proliferation of keys and certificates by centralizing their creation and deployment
- Tighten security by periodically rotating keys to prevent their misuse
- Launch remote SSH sessions to target specific endpoints
- Integrate out-of-box with leading certificate authorities to automate SSL certificate life cycle management
- Detect vulnerabilities in SSL configurations and expedite remediation
- Receive timely SSL expiration alerts, stay on top of certificate renewals, and reduce downtimes



Take total control over your SSH key and SSL/TLS certificates

- Automated discovery and vaulting of SSH keys and SSL/TLS certificates
- Centralized key creation, deployment, and periodic rotation
- One-click remote SSH connections to target endpoints
- Policy based CSR generation and signing
- Out-of-the-box integration with Let's Encrypt, DigiCert, Microsoft CA, and more
- SSL vulnerability scanning and certificate expiry alerting

Security information and event management



You need security information and event management solutions to:

- Preempt internal threats, data exfiltration, and user account compromises using machine-learning based user and entity behavior analytics.
- Automate incident response with predefined and customizable workflows to save critical response time.
- Identify malicious communications with blacklisted IPs, URLs, and domains by corroborating data from threat intelligence services.
- Analyze all network activity to detect and defend against malware, brute-force attacks, cryptojacking, and other threats.
- Monitor active virtual private network (VPN) connections and get alerts about unusual VPN activities.
- Ensure compliance with data privacy and security regulations such as PCI DSS, SOX, HIPAA, and the GDPR with predefined report templates.

ManageEngine's security information and event management (SIEM) solutions

- **Log360:** Integrated SIEM with advanced threat analytics and ML-driven UEBA
- **EventLog Analyzer:** Comprehensive log and IT compliance management
- **ADAudit Plus:** Real-time Active Directory, file, and Windows server change auditing
- **SharePoint Manager Plus:** SharePoint reporting and auditing
- **M365 Security Plus:** Microsoft 365 security
- **Cloud Security Plus:** Cloud security monitoring and analytics
- **FileAnalysis:** File security and storage analysis



ManageEngine 
Log360

Integrated SIEM with advanced threat analytics
and ML-driven UEBA

Why Log360?

- Perform end-to-end security auditing for all data and IT assets
- Spot suspicious incidents with rule-based correlation engine
- Contain persistent and insider attacks with ML-driven user and entity behavioral analytics (UEBA)
- Detect threats by correlating business-contextual information with external feeds using advanced threat analytics
- Resolve and remediate security threats with automated workflows
- Simplify compliance audits for PCI DSS, FISMA, HIPAA, SOX, GLBA, GPG 13, and the GDPR mandates with audit-ready report templates



A comprehensive SIEM solution for all your network security challenges

- Agentless and agent-based log collection
- Over 1000+ predefined report and alert profiles
- Real-time Active Directory auditing
- Integrated compliance management
- Robust event correlation engine
- User and entity behavior analytics
- Streamlined incident management
- Augmented threat intelligence platform




ManageEngine

EventLog Analyzer

Comprehensive log and IT compliance management

Why EventLog Analyzer?

- In-depth auditing capabilities of network perimeter devices' logs, user activities, and a lot more to meet security auditing needs
- Augmented threat intelligence bundled with a global IP threat database and STIX/TAXII feed processor to detect malicious inbound or outbound traffic
- Comprehensive log management which also includes a custom log parser to analyze any human-readable log format
- High-speed log processing which processes log data at 25,000 logs/second to detect attacks in real time
- Built-in incident management which raises tickets in help desk consoles to ensure accountability and speed up incident resolution



Gain insights into potential threats in your network and stop them before they turn into an attack

- Comprehensive log collection
- In-depth log auditing and analysis
- Real-time event log correlation
- Built-in file integrity monitoring
- Secure log archival
- Dynamic threat intelligence
- Efficient log forensics
- Streamlined incident management
- Integrated compliance management



ManageEngine 
ADAudit Plus

Real-time Active Directory, file, and Windows server
change auditing

Why ADAudit Plus?

- Obtains answers to what's buried in event logs in a Windows network
 - Who logged in from where?
 - What caused an account to lockout?
 - Which user was added to an admin group?
 - Who deleted a file?
 - And more
- Analyzes log data that demands expertise and time using native tools
- Transforms event log data into actionable reports and alerts
- Enables you to know who did what, when, and from where in your Windows ecosystem with just a few clicks

Get complete visibility into AD and Windows servers activity

- Receive notifications for changes to AD—on-premises and Azure
- Detect group policy setting changes and Group Policy Object (GPO) management actions
- Get a consolidated audit trail of **privileged user activities**
- Continuously track **Windows user logon** activity
- Detect and analyze Active Directory **account lockouts**
- Audit access to **Windows, NetApp, EMC, and Synology files** and folders
- Track logons and changes across **Windows member servers and workstations**
- Get to know the **active time spent by employees** at their workstations
- Leverage **user behavior analytics (UBA)** to detect threats and anomalies
- Get prepackaged IT **compliance reports** for SOX, GDPR, and other mandates



ManageEngine

SharePoint Manager Plus

SharePoint reporting and auditing

Why SharePoint Manager Plus?

- Audit log reports and analyze all activities in your SharePoint environment to ensure security
- Carry out critical management tasks (grant and revoke permissions, create or delete groups and more) from a central console
- Get insights on user behavior with details on traffic and search with the help of usage analytics
- Ensures seamless collaboration with out-of-the-box Microsoft 365 reports to manage your online SharePoint
- Categorize reports into sections covering statistics, security, activity, usage analytics, and Microsoft 365 for easy analysis
- Meet compliance requirements that outlines audit log data archival for forensic analysis



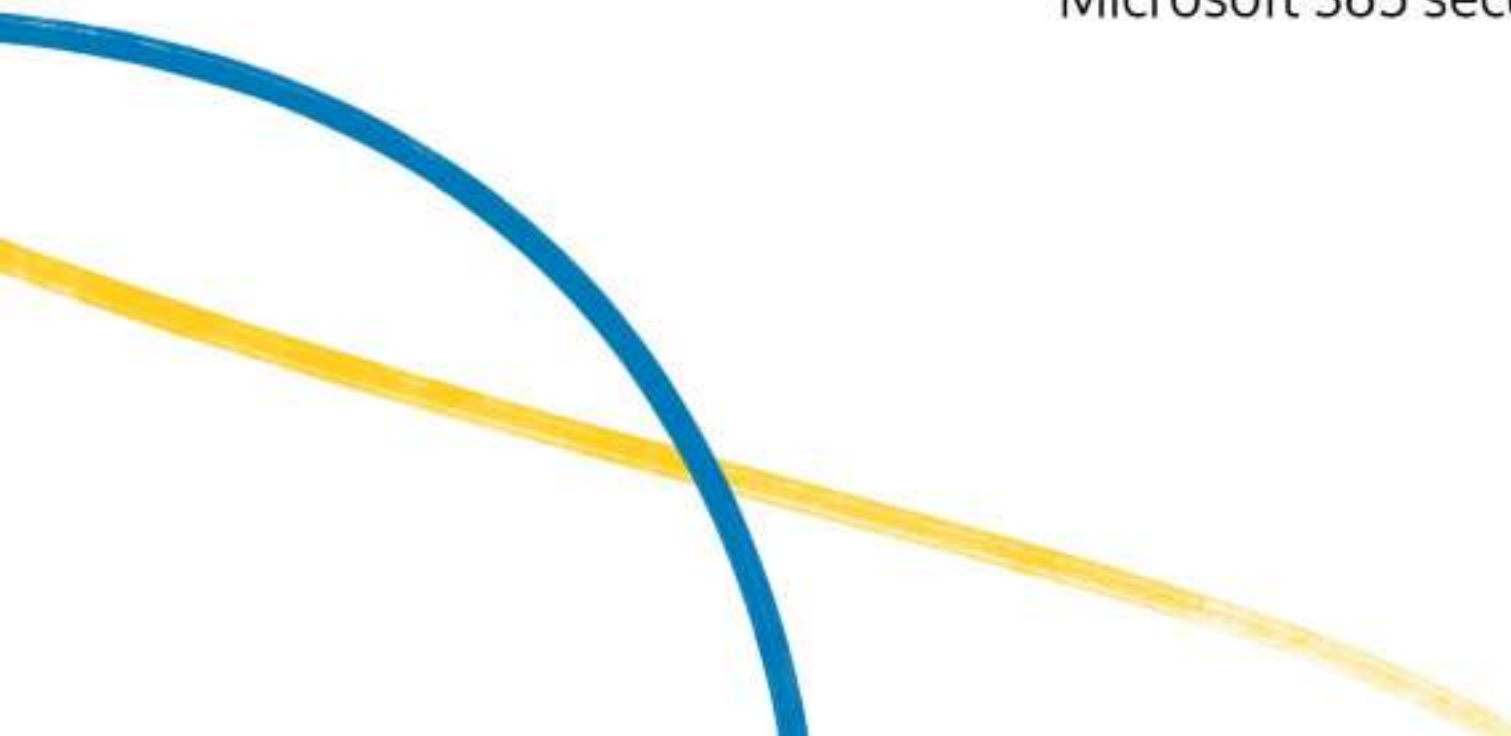
Ensure server security and make your SharePoint auditing easier than ever

- SharePoint reporting and management
- SharePoint security and auditing
- SharePoint permission and group management
- Microsoft 365 management
- Audit log archival
- Usage analytics

ManageEngine 

M365 Security Plus

Microsoft 365 security



Why M365 Security Plus?

- Prevent security breaches with predefined granular audit reports on user and admin activities, failed logon attempts, file access, and role changes. Or create custom audit profiles to suit your security requirements
- Provide quick remediation for critical events with real-time alerts
- Stay on top of service outages with around-the-clock monitoring of health and performance of Microsoft 365 features and endpoints
- Scrutinize emails with automated content search to detect personal information such as Social Security numbers and login credentials
- Create custom help desk roles and delegate routine tasks to non-admin users without the elevation of their permissions in Microsoft 365. Leverage advanced delegation features to ease the admin workload



An exclusive solution to fortify Microsoft 365 environments

- Granular auditing of user activities
- Around-the-clock monitoring
- Real-time alerting of critical activities and changes
- Automated content search
- Help desk delegation



ManageEngine 
Cloud Security Plus

Cloud security monitoring and analytics



Why do you need cloud security management solutions?

- Monitor large volumes of cloud data that is spread across different locations
- Improve visibility into cloud operations and threat management
- Identify patterns and pinpoint potential security vulnerabilities in the cloud infrastructure
- Protect your critical enterprise data that is stored and processed in cloud environment
- Assess risk and generate reports for the entire cloud environment

Why Cloud Security Plus?

- Centrally manage public clouds
- Easily search through log data
- Track every activity that happens in Microsoft Azure
- Get granular insights on Google Cloud Platform events
- View detailed reports for your AWS cloud environment
- Proactively monitor your Salesforce environment
- Instantly know about critical changes and other security threats with real-time alerts

Log management and monitoring for your public cloud platforms

- **Securing AWS Cloud platform**

- Amazon S3 log management
- Amazon S3 bucket logging
- AWS IAM activity reporting
- Auto-configuration of AWS
- AWS ELB traffic analysis
- AWS security group change auditing
- Amazon RDS activity reporting
- Forensic analysis using CloudTrail logs

- **Securing Azure cloud platform**

- Microsoft Azure virtual machine (VM) activity reporting
- Microsoft Azure DNS auditing

- **Salesforce log management**

- **Google Cloud platform log management**



ManageEngine 
FileAnalysis

File security and storage analysis



Why FileAnalysis?

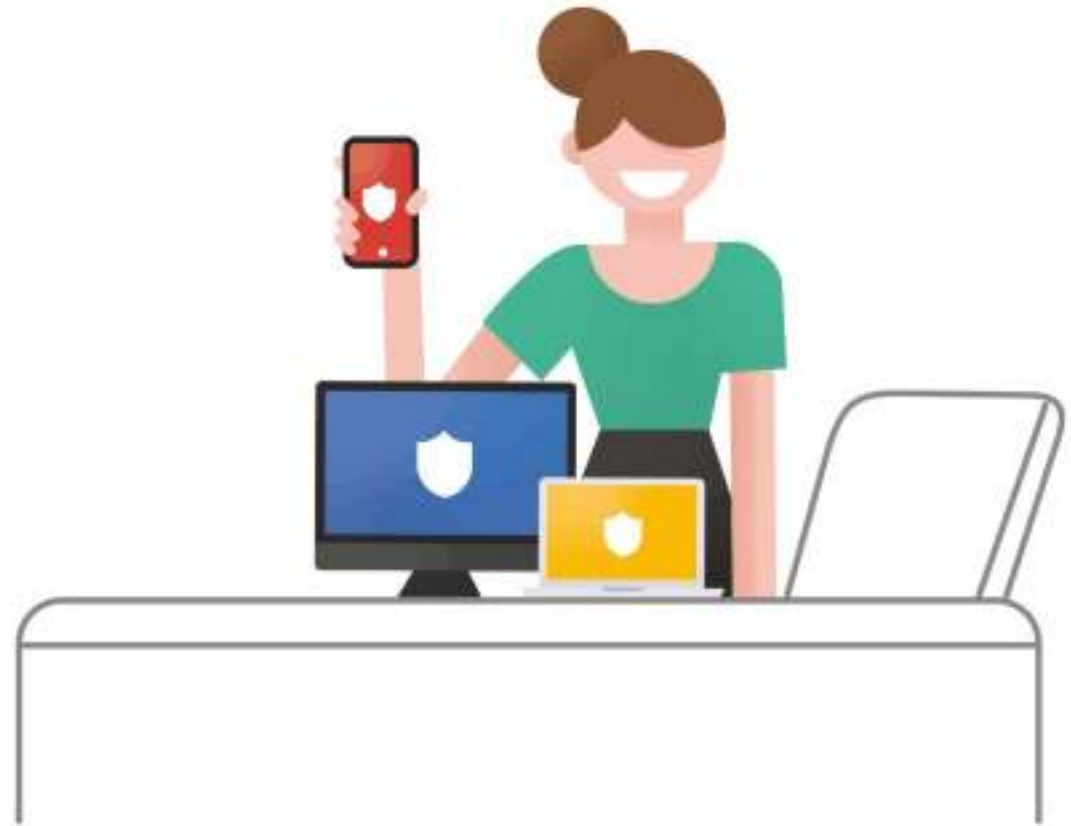
- Find folders and shares with excessive permissions, such as those open to everyone or those that allow full control access
- Identify privileged users and analyze effective permissions to identify who has access to do what to your critical files
- Locate security vulnerabilities such as files with broken or improperly inherited permissions, ransomware-infected files, and more
- Find and manage files owned by inactive, disabled, or deleted users



Find and manage files with security vulnerabilities

- Analyze security permissions
- Find users with high privileged access
- Identify files with permission hygiene issues
- Quarantine potential ransomware-corrupted files
- Locate overexposed files and folders
- Manage orphaned files

Endpoint security management



You need endpoint security management solutions to:

- Reduce the need for manual endpoint management and make tedious tasks such as threat detection and response less time-consuming
- Manage inventory of all software and hardware assets across the network in real time
- Set up accurate security configurations across your system to protect the network from internal breaches
- Assign correct user permissions and privileges to software present in the network to help protect your enterprise from external exploits
- Scan systems in the network systematically to identify missing patches, and periodically distribute selected patches to target computers
- Meet regulatory policies that will help boost your companies' compliance with security standards
- Prevent the transfer of confidential data into peripheral devices, as well as the intrusion of files from such devices into managing systems
- Prevents the unauthorized execution of suspicious or potentially dangerous applications that could lead to disastrous complications on endpoints

ManageEngine's endpoint security management solutions

- **Desktop Central:** Unified endpoint management and security
- **Mobile Device Manager Plus:** Comprehensive mobile device management
- **Mobile Device Manager Plus MSP:** Comprehensive mobile device management for MSPs
- **Patch Manager Plus:** Automated multi-OS patch management
- **Patch Connect Plus:** Automatic patching of third-party software
- **Browser Security Plus:** Browser security and management
- **Application Control Plus:** Software discovery and endpoint privilege management
- **Vulnerability Manager Plus:** Prioritization-focused enterprise vulnerability management
- **Device Control Plus:** Data loss prevention for peripheral devices



ManageEngine 
Desktop Central

Unified endpoint management
and security (UEMS)

Why Desktop Central?

- Manage and secure all endpoints without requiring multiple tools from a single dashboard.
- Remediate vulnerabilities and threats, secure browsers, and regulate apps and devices in a few clicks
- Onboard Windows, Mac, Linux, iOS, Android, tvOS, and Chrome OS devices with ease
- Manage and secure your endpoints across multiple remote offices and locations be it working from office or working from anywhere
- Perform regular endpoint tasks from deploying operating systems, patches, software to inventory management, reporting, mobile device management and remotely troubleshooting end-user issues

A complete UEMS solution that manages and secures all your endpoints across multiple locations, from a single dashboard.

- Easy set-up and installation
- Automate patching for Microsoft, third-party, antivirus, and driver updates
- Blacklist applications, and block software installation
- Scan, assess and mitigate threats and unknown vulnerabilities
- Secure end user browsers and keep tabs on the installed plug-ins and extensions
- Prevent data loss and data theft by controlling, blocking and monitoring USB and peripheral devices
- Encrypt devices using BitLocker encryption
- Generate customized audit-ready IT reports for security compliance
- Integrate with help desks like Jira, Zendesk, ServiceNow, Spiceworks, and Freshservice



ManageEngine

Mobile Device Manager Plus

Comprehensive mobile device management

Why Mobile Device Manager Plus?

- Secure multiple device types across Apple, Android, Windows and Chrome.
- Manage and secure both employee-owned (BYOD) and corporate owned devices.
- Enforce OS updates automatically to ensure devices run on the latest OS version.
- Comprehensive app security for store and enterprise apps.
- Secure access to corporate Exchange accounts and email attachments.
- Securely distribute, view, and save business-sensitive content on devices.
- Data loss prevention (DLP) policies to secure data at rest, in use, and in transit.
- Auto-detection and removal of jailbroken and rooted devices from your network.
- Locate, lock, or wipe devices when they leave a particular location, or are lost or stolen.
- Ensure adherence to compliance regulations such as HIPAA, GDPR, and PCI-DSS.

Fortify enterprise security with mobile security management

- BYOD containerization
- OS update management
- Lock down devices to approved apps and restrict device functionality
- Pre-define app permissions and configurations
- Test and deploy enterprise apps
- Blacklist apps and web content
- Secure content management
- Conditional access to MS Exchange accounts
- VPN and per-app VPN
- Enterprise single sign-on to avoid password fatigue
- Mandate encryption on managed devices
- Location tracking and geofencing



Mobile Device Manager Plus MSP:

Comprehensive mobile device management for MSPs:

- Benefit from a unified console with customer segmentation
- Manage Windows, iOS, Linux, Android, and Chrome OS devices
- Enforce security policies to secure data at rest, in use, and in transit
- Manage apps and OS updates without user intervention
- Lock down devices to run a single app or a specific set of apps
- Securely share, view, and save corporate resources on mobile devices
- Remotely view or control devices to troubleshoot issues
- Track device locations and execute remote commands on non-compliant devices



ManageEngine

Patch Manager Plus

Automated multi-OS patch management

Why Patch Manager Plus?

- Support for over 300 third-party applications
- Pre-test and approve patches before deployment
- Keep your remote machines up to date
- Decline patches and disable auto-update of patches
- Vulnerability prompt messages for critical patches
- Agent based monitoring of system health of computers
- Wake on LAN to deploy patches silently & remote shutdown
- Customized, granular reports for IT auditing
- Security news feed about the latest vulnerabilities



Gain complete visibility and control over your patching

- Automated patch management
- Customized deployments policies
- Dynamic monitoring and reporting
- Third party applications patching
- Cross-platform support
- Ensure patch compliance



ManageEngine

Patch Connect Plus

Automatic patching of third-party software



Why Patch Connect Plus?

- Automate third-party patching with Microsoft SCCM
- Customize third-party patches to comply with organizational policies
- Publish update catalogs to simplify third-party patching
- Execute on-demand administrator actions on client machines remotely
- Get the complete list of patches and system-wise reports of the client machines



Extend third-party patching capabilities to your SCCM server

- Native plug-in for SCCM
- Customized deployment with pre-/post-deployment scripts
- Auto-detection and publishing of third-party patches
- Extensive third-party software catalogs
- Application management to help with third-party application deployment
- Deployment reports that provides complete SCCM deployment data



ManageEngine 
Browser Security Plus

Browser security and management

Why Browser Security Plus?

- Protect your network from web-based cyberattacks
- Enforce security configurations and ensure compliance
- Detect and remove harmful browser add-ons installed on computers
- Keep track of websites and web applications that are being used in your network
- Restrict access to unauthorized websites
- Restrict downloads to trusted websites
- Configure policies to assign the corresponding Java versions to enterprise sites that require them



Ensure security from browser-based threats and attacks

- Browser insights and management
- Browser policy deployment and configurations
- Add-on management
- Java manager
- Browser lock-down and isolation
- Web filter and download restriction
- Data leakage prevention
- Compliance management



ManageEngine

Application Control Plus

Software discovery and endpoint
privilege management

Why Application Control Plus?

- Instant discovery and categorization of authorized and unauthorized applications
- Eliminates untrusted applications by building whitelists and blacklists
- Prevents privilege elevation attacks with endpoint privilege management
- Curbs both security breaches and nonproductive use of employee time by ensuring that only authorized applications are running



Control and authorize application access, prevent malware threats and tackle productivity loss

- Malware prevention
- Rule-based list building
- Endpoint privilege management
- Flexible operation modes
- Improve productivity by blacklisting applications that might hinder productivity



ManageEngine
Vulnerability Manager Plus

Prioritization-focused enterprise vulnerability management

Why Vulnerability Manager Plus?

- Assess and prioritize vulnerabilities based on exploitability, severity, age, and affected system count
- Customize, orchestrate, and automate your entire patching process
- Optimize your system's security and ensure they're compliant with CIS and STIG security guidelines
- Identify high-risk software that are deemed unsafe, and uninstall them from your endpoints in no time
- Deploy pre-built, tested scripts to secure your network from zero-day vulnerabilities
- Obtain details on the cause, impact, and remedies of web server security flaws, and use this information to establish and maintain servers that are secure from attack variants



Gain 360-degree visibility into your security exposure

- Vulnerability assessment
- Patch management
- Security configuration management
- Zero-day vulnerability mitigation
- Web server hardening
- High-risk software and antivirus audit
- Reports with actionable insights into your network security



ManageEngine 
Device Control Plus

Data loss prevention for peripheral devices

Why Device Control Plus?

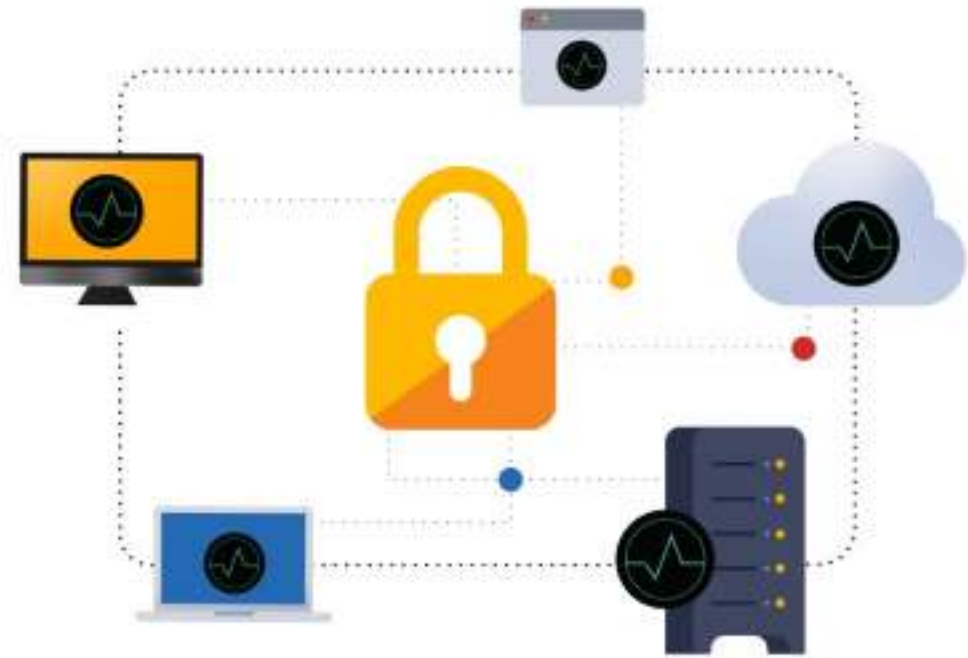
- Crack down on devices with excessive access privileges to safeguard data from intruders
- Automatically keep tabs on unprecedented data transfers to ensure uninterrupted device control
- Control devices with zero-trust approach by continuously assessing trust every time a device requests access to your endpoint
- Prevent various USB and peripheral devices from gaining unauthorized access to your data by assigning strict device policies
- Make it easy and safe for your business to deal with third-party devices by enabling employees to have temporary access when required
- Monitor hack attempts and can spot malicious insider activity



Authorize, authenticate, and audit devices in your network

- Device and port control
- File access control
- File transfer control
- File shadowing
- Trusted device list
- Temporary access for security
- Device activity and data usage activity reports

Network security management



You need network security management solutions to:

- Gain greater visibility across your entire network
- Monitor the status, availability, health, and performance of your IT infrastructure
- Ensure smooth and secure functioning of your organization's online activities
- Protect the network against unauthorized access
- Ensure that customer data remains safe from malicious attacks and unauthorized access and intrusions
- Gain information on possible network attacks and security breaches through extensive log analysis



ManageEngine's network security management solutions

- **Firewall Analyzer:** Firewall configuration and log management
- **Network Configuration Manager:** Network configuration, change and compliance management
- **Netflow Analyzer:** Bandwidth monitoring and traffic analysis
- **OpManager:** Network and server monitoring solution
- **OpUtils:** IP address and switch port management



ManageEngine 

Firewall Analyzer

Firewall rule, configuration, and log management

Why Firewall Analyzer?

- Analyses firewall policies and rules to provide suggestions for firewall rule optimization
- Helps automate firewall rule administration and determine if a new rule can impact the existing rule set negatively.
- Collects, consolidates, and analyzes firewall logs and maintains a log of configuration changes
- Performs periodic security audits to provide real time security status of firewalls
- Real-time alerts to security events enabling quick response to security threats
- Monitors employee internet usage and alerts when bandwidth is exceeded



Analyze your firewall policy to secure your network

- Firewall policy analysis and administration
- Firewall configuration monitoring and change management
- Firewall compliance and auditing
- Firewall log management
- Network traffic and bandwidth monitoring
- Security and VPN monitoring
- User activity monitoring
- Network forensic audits



ManageEngine

Network Configuration Manager

Network change and configuration management

Why Network Configuration Manager?

- Checks network configurations for industry compliance
- Helps remediate compliance violations with script templates
- Detects authorized and unauthorized changes made to configuration
- Take full control over what configuration changes are uploaded
- Scans and detects network devices running on vulnerable firmware



Analyze network configurations to secure your network

- Configuration change management
- Configuration rollback mechanism
- Firmware vulnerability management
- Encrypted storage of all network configurations
- Network compliance management
- Approval based configuration upload
- Traffic shaping to avoid bandwidth hogs and network disasters



ManageEngine

NetFlow Analyzer

Bandwidth monitoring and traffic analysis

Why NetFlow Analyzer?

- Proactively monitors and identifies network traffic patterns to detect traffic spikes and anomalies
- Helps analyze bandwidth usage trends to identify the root cause network traffic issues
- Detects internal and external security threats such as DDoS/flash-crowd attacks, probes/scans, suspicious flows, etc.
- Helps set real-time alerts for security events to reduce response time and enable faster troubleshooting
- Filters out suspicious traffic by blocking or restricting selected IPs/IP networks
- Helps manage service policies and limit user access to unsafe or non-critical apps

Analyze network traffic activity to identify anomalies and threats

- Network Forensics report
- Advanced Security Analytics Module
 - Network anomaly and security threat detection and classification
 - Network security alerts
- Troubleshooting and traffic shaping
 - Access control list
 - Service policy management



ManageEngine 
OpManager

Network performance monitoring

Why OpManager?

- Real-time network monitoring to track the uptime and availability of devices in your IT infrastructure
- Gain in-depth visibility into your wireless network, track APs and find rogue SSIDs
- Identify and terminate suspicious processes/ services running on physical servers and virtual machines
- Track changes to files/ folders present on your database servers and application log files
- Detect events and execute queries on remote systems to troubleshoot issues from the UI
- Track syslogs and event logs to generate instant alerts on suspicious/unauthorized events

Keep your network secure with end-to-end network visibility

- Real-time network monitoring
- Physical and virtual server monitoring
- WLC monitoring
- Process/ services monitoring
- File and folder monitoring
- Active Directory monitoring
- Exchange monitoring
- MS SQL monitoring
- Syslog/ event log monitoring
- VPN monitoring
- IT workflow automation
- Script monitoring
- Reporting & Fault management



ManageEngine[®] OpUtils

IP address and switch port management

Why OpUtils?

- Proactively monitors the IPv4 and IPv6 address space utilization and logs historical IP usage details
- Enables end-to-end switch port mapping and displays the connected device details, and VLAN name
- Periodically scans the network to detect unauthorized access
- Offers more than 30 networking tools that can scan the services running on a port, and view or remotely update system details
- Alerts instantaneously whenever an unauthorized access to your network is detected

Secure network from unauthorized access

- Real-time network scanning
- Rogue device detection
 - Detection of newly connected network devices
 - Classification of discovered devices as trusted, guest, or rogues
 - Alerts when the validity period of the guest device expires
- Remotely blocking network ports to prevent unauthorized access

Data security management





You need data security management solutions to:

- Protect the confidentiality, availability, and integrity of your data
- Locate sensitive data and analyze its vulnerability
- Detect, disrupt, and prevent sensitive data leaks via endpoints
- Get visibility over every single file access and modification made by users within your file server environment
- Detect and shut down potential ransomware attacks
- Protect the privacy of your customers while adhering to compliance standards



ManageEngine's data security management solution

- **DataSecurity Plus:** File auditing, data leak prevention, and data risk assessment



ManageEngine 

DataSecurity Plus

File auditing, data leak prevention, and data risk assessment



Why Data Security Plus?

- Audit and alert on all file accesses and modifications made in file servers, failover clusters, and workgroup environments in real time
- Prevent data leak by detecting, disrupting, and responding to sensitive data leaks via endpoints like USBs, email, and more
- Assess data risk by leveraging in-depth content inspection and manual tagging capabilities to discover sensitive data and classify files based on their vulnerability



Discover, monitor, and protect your sensitive data from being exposed or stolen

- File integrity monitoring and alerting
- Automated threat response mechanism to combat ransomware
- USB protection
- Email security
- Incident response
- File access auditing
- Data discovery and classification
- Redundant obsolete and trivial, ROT analysis
- Permissions analyzer to identify overexposed files and files with inconsistent permissions
- File storage analyzer

ManageEngine

www.manageengine.com

