



ManageEngine



Unified Endpoint Management and Security



(Est. 1996)

Privately held and profitable since inception



A Division of ZOHOO Corporation

(1996 -2021)

IoT management framework



(Est. 2002)

Enterprise IT management solutions



Work. Online

(Est. 2005)

Applications for business, collaboration and productivity



CONTEXTUAL · RELEVANT · EXPERIENTIAL

(Est. 2005)

Technology and soft-skills training for local students



(Est. 2021)

Workflow orchestration software

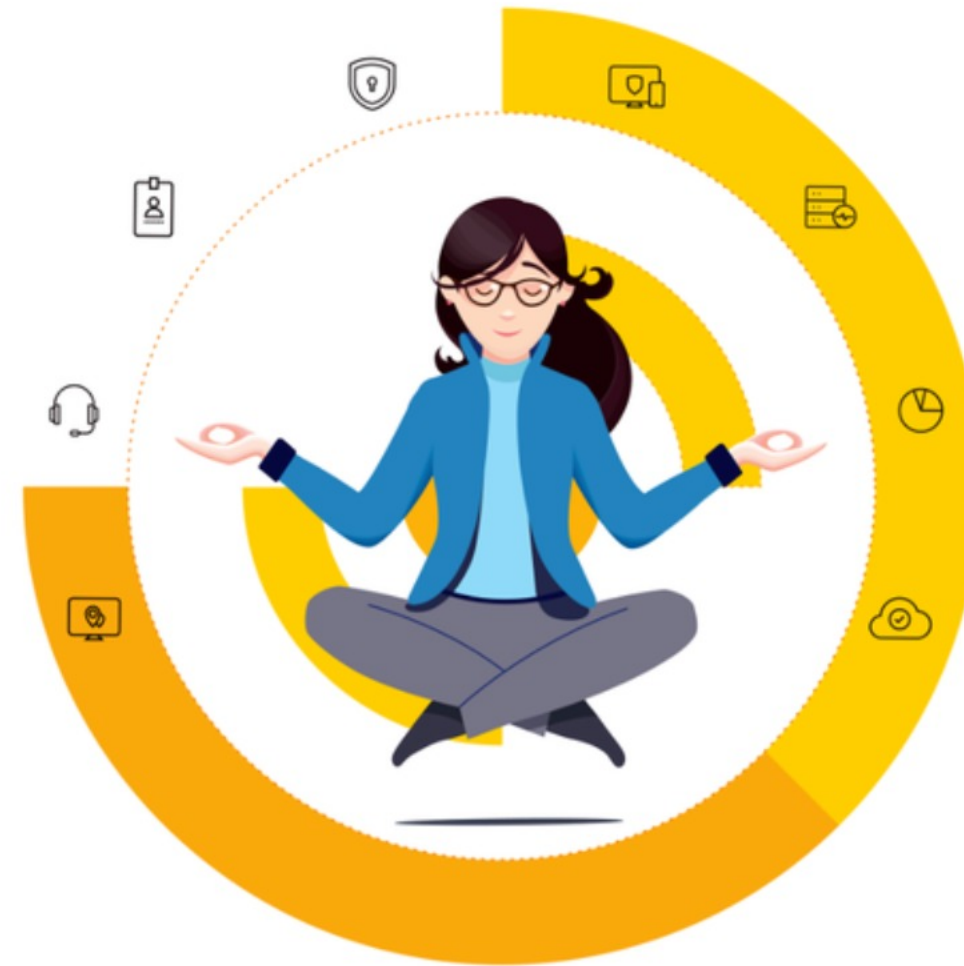


(Est. 2021)

An all-in-one training platform



Bringing IT together



ManageEngine crafts comprehensive IT management software for your business needs

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 a 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 and 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 and Exchange management and auditing
- AD and Exchange backup and recovery
- SSH and SSL certificate management

Unified endpoint management and 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
- Endpoint data loss prevention

IT operations management

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

Security information and event management

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

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

Low-code app development

- Custom solution builder



ManageEngine:

A bootstrapped, private, and profitable company

20+

years in the
industry

280,000+

Organizations across the
globe trust ManageEngine

120+

products and free tools for
IT management

4,500+

ManageEngine
employees

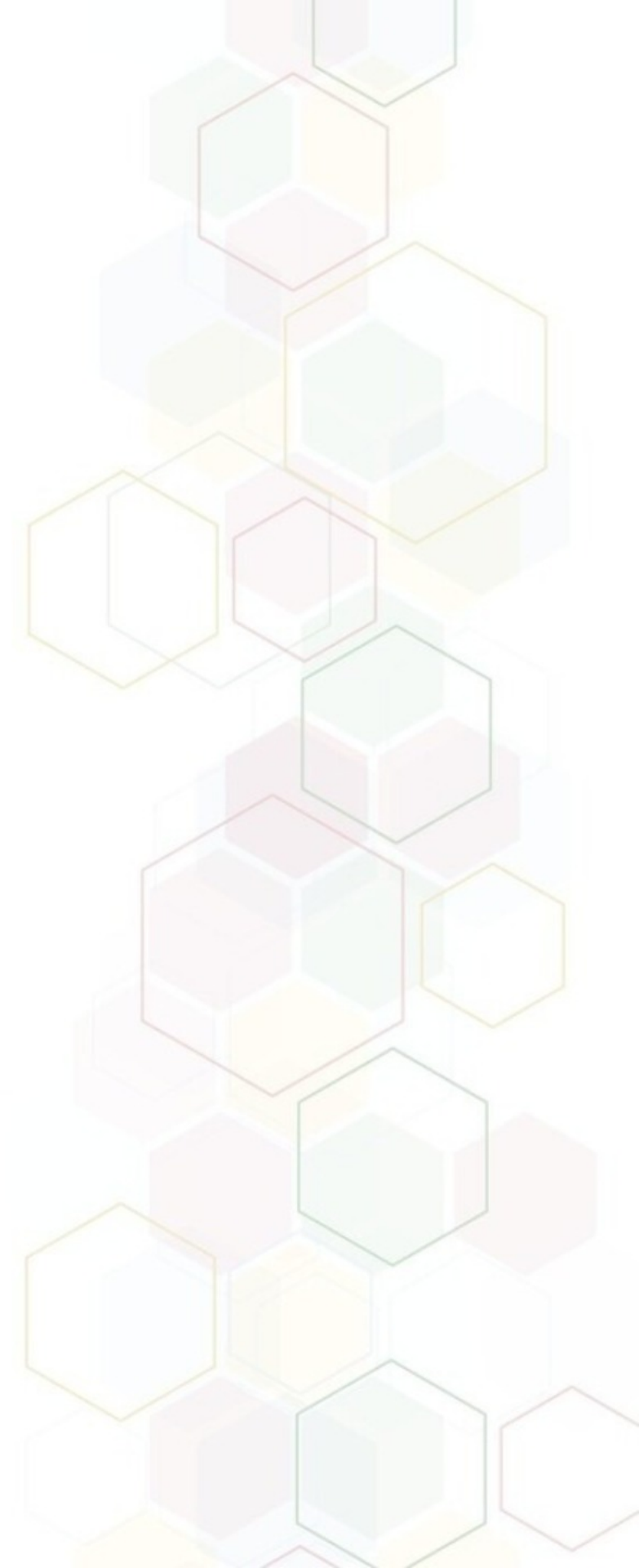
190

countries

ManageEngine 

Browser Security Plus

Product Overview



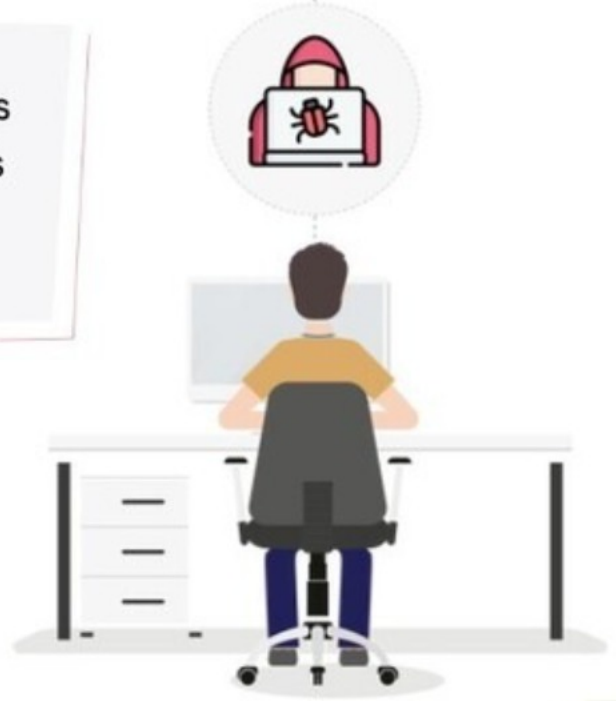


Why do you need Browser Security?



As organizations are becoming more flexible, adoption of cloud has increased to enable the distributed workforce to do business.

Browsers become an tool that workers use to access cloud, making browsers a popular attack surface.





What is Browser Security Plus?



Browser Restriction

Reduce the attack surface across your organization by streamlining employees' access to web through tried-and-tested browsers.

Standardize browsers

Provision browsers with configurations, bookmarks, add-ons and extensions, homepage and start-up settings etc., to standardize the appearance across your organization.

Implement security restrictions

Enforce restrictions to employees' access to the web, further reducing the attack surface.

Periodic maintenance

Regularly monitor the dashboard to verify compliance to stipulated standards and to detect new potentially harmful components on the web.

Supports popularly used browsers in organizations



Google Chrome



Microsoft Internet Explorer



Microsoft Edge



Mozilla Firefox



Brave



Yandex



Vivaldi



Cốc Cốc



Naver Whale



Browser Security Plus features - Explained

Add-on Management

- Monitor the usage of Chrome, Firefox and Edge extensions and IE plug-ins present in the network.
- Detect and remove potentially harmful browser add-ons.
- Silently distribute mission-critical Chrome and Edge extensions and Firefox add-ons to users.
- Block Chrome and Edge extensions that seek permissions involving threats.

Benefits:

- Protect your employees from spyware and malware disguised as add-ons.
- Improve employees' productivity by equipping them with necessary mission-critical add-ons.



Enforce browser configurations

- Configure settings like VPN, proxy, printer settings etc. to improve productivity and settings like safe browsing, autofill, password management etc. to ensure security, all from a central console.
- Standardise the look of browsers across your organization with control over default browser, homepage and configure bookmarks for end-users, centrally.

Benefits:

- Configurations once set and deployed by the IT admin can not be overridden by the end-users.
- Protect employees on the web by reducing attack surface.

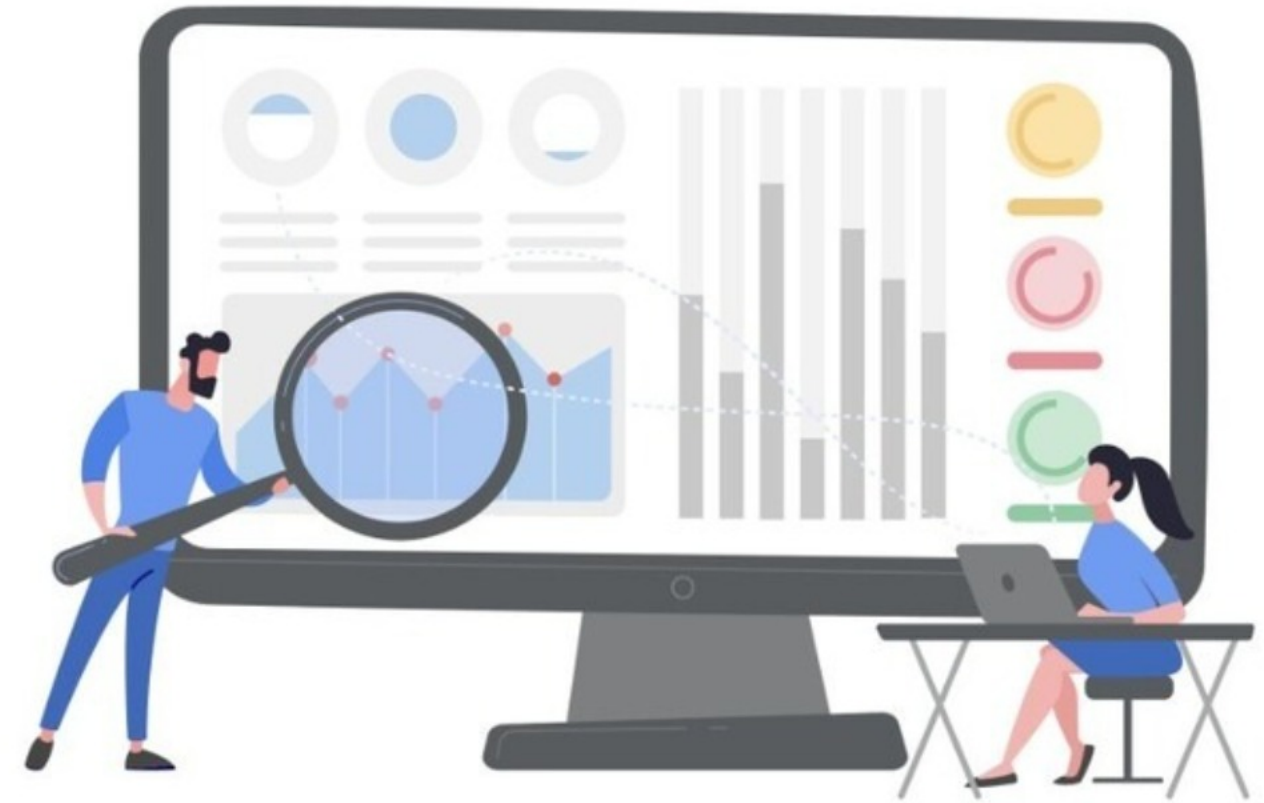


Web activity tracking

- Keep track of users' activity and browsing patterns on the web.
- Discover the Shadow IT web applications used across your organization.

Benefits:

- Stay aware of employees who visit unapproved websites and webapps.

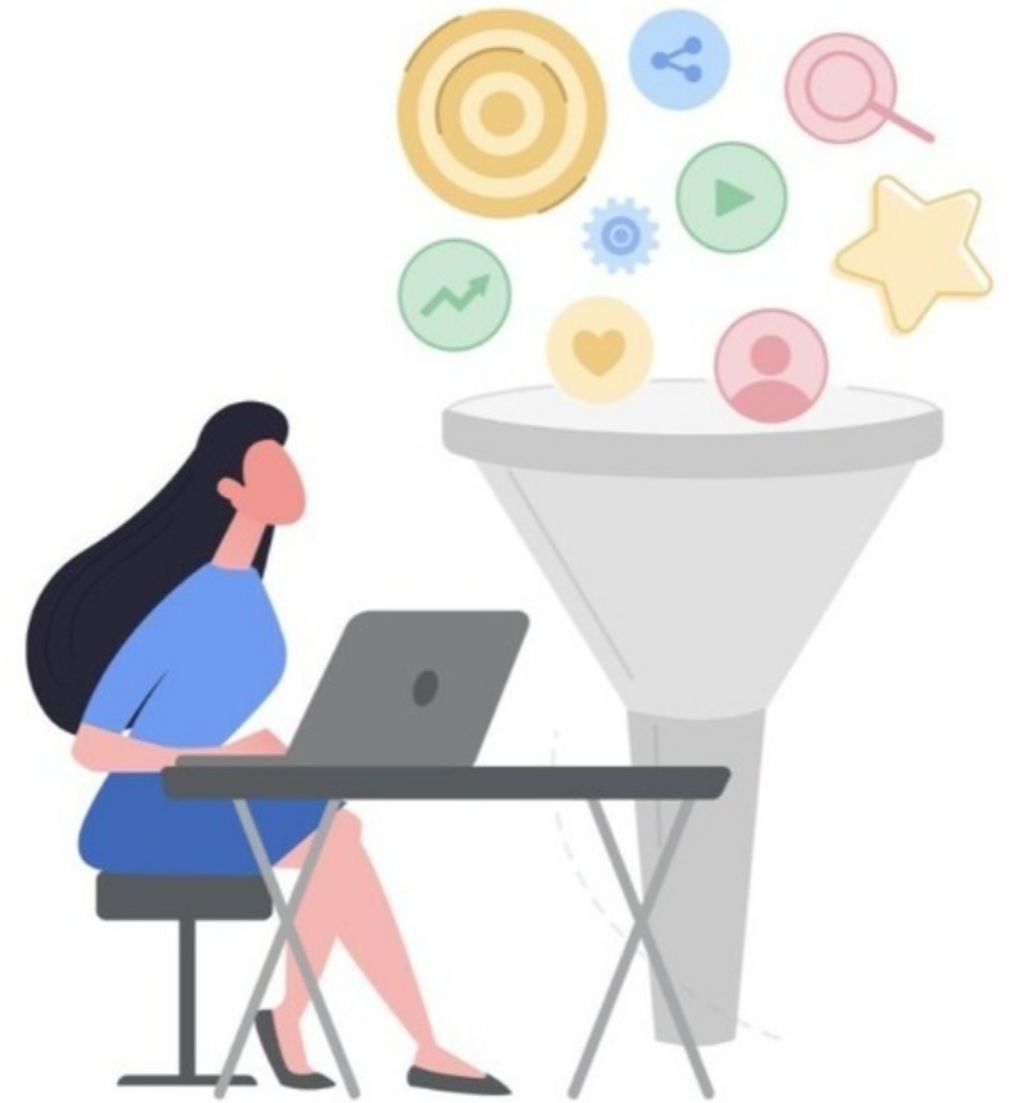


Web filter

- Restrict access to detected Shadow IT applications.
- Customize message to be displayed on block screen.
- Enables IT admins to restrict downloads based on criteria like file type, size, website of initiation, time range etc., to ensure security without compromising employee's productivity.

Benefits:

- Prevent drive-by attacks.



Java Versions Management

- Map web-applications and websites with specific versions of Java, enabling multiple web-applications and websites to run different versions of Java simultaneously on a single machine.
- Block Java on specific websites/webapps of your choice.

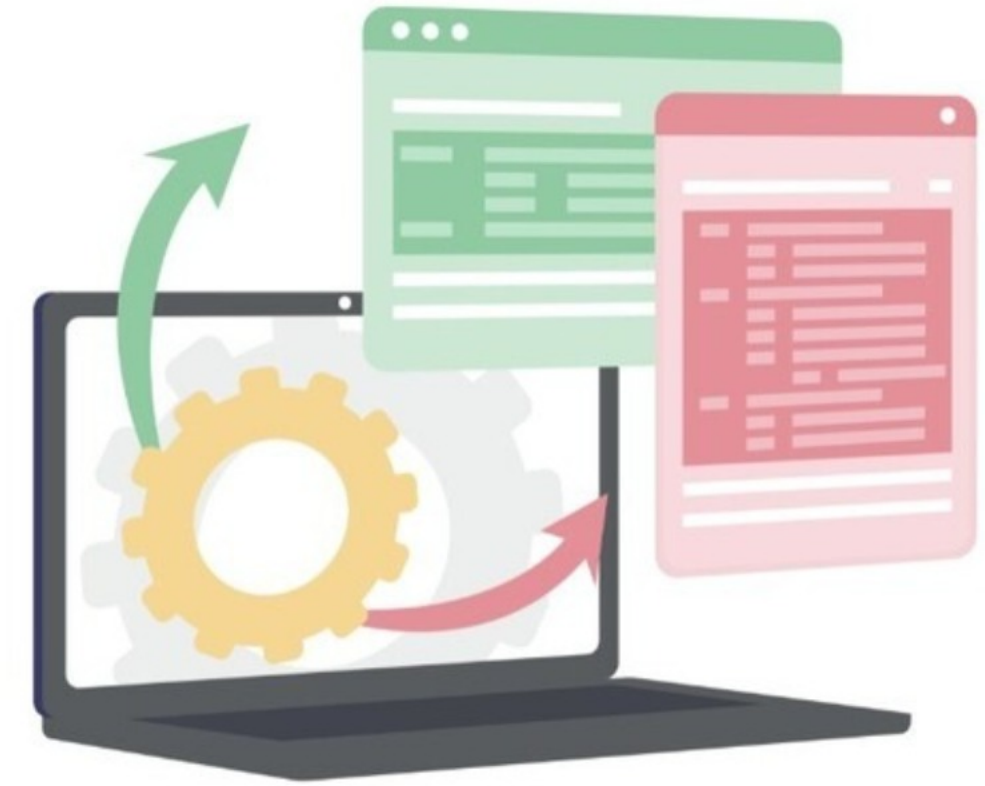
Benefits:

- Ensure compatibility of legacy applications with older versions of Java, without compromising security.



Browser Redirection

- Define a destination browser and direct websites from any browser to the destination browser.



Benefits:

- Streamline employees' web traffic through one tried-and-tested browser to reduce the attack surface.
- Ensure seamless user experience by eliminating compatibility issues in older, legacy websites and applications.

Kiosk Internet Explorer

Lockdown Internet Explorer ensuring access only to trusted web applications.



Compliance

- Allows IT admins to check the compliance of computers with predefined standards like Security Technical Implementation Guides (STIG) and Centre for Internet Security (CIS).
- IT admin can create custom compliance standards with 30+ compliance rules and monitor compliance of computers to the stipulated rules.

Benefits:

- Simplified templates to monitor compliance to existing browser standards.



To know more, visit:

<https://mnge.it/bsp>



Try it for free!

<https://mnge.it/bsp-download>

