FINDING AND REMOVING MALWARE

**Dual-engine virus and malware detection**
Emsisoft (A) and Bitdefender (B) engines work together to detect all types of malicious software, including viruses, ransomware, trojans, bots, keyloggers, spyware and more. Signatures for double-detections are avoided for memory use and speed optimization.

**Super fast system scans (1-2 min)**
Scan your device quickly and thoroughly using our efficient dual-engine scanner. Scan time varies depending on which scan type you select.

**PUP/unwanted programs detection**
Alerts you of potentially unwanted programs (adware, browser toolbars, system optimizers, etc.) that can affect your device's performance.

**Advanced infection cleaning**
Smart operation processes ensure the safety and stability of the computer during system cleaning. Checks 70+ autorun/loading points including hidden ones used by rootkits and restores default values if they have been overwritten by malware.

**Safe quarantine of suspicious files**
Detected malware is stored in an encrypted format in quarantine so it can't cause any damage. You can submit a quarantined file to the Emsisoft Lab for detailed analysis.

**Scan exclusions/allow list**
Exclude known good files and folders from scanner detection. Supports wildcards (`?`, `*`) and 44 environment variables as generic shortcuts for common folders (`%temp%`, `%windir%`, etc.).

**Scheduled scans**
Scan the whole system at scheduled times. Includes highly configurable scheduling, logging and scan options.

**Windows Explorer integration**
Right click any file or folder in Windows Explorer to quickly initiate a scan.

**Command line interface included**
A powerful command line interface that features all the functions of the GUI software. Use it to automate common scanning tasks.

**Emergency Kit maker included**
Compile your own fully portable scan tool to clean third-party devices of malware infections. Save the Emergency Kit to a portable device like a thumb drive.

PREVENTING NEW INFECTIONS

**Multi-layered real-time protection**
We use diverse technologies and multiple layers of security to maximize our solutions' protection capabilities.

**Web Protection**
Blocks access to known dangerous websites using a frequently updated block list. Web Protection is host-based and works across all programs, even if the transferred web data is encrypted.

**Anti-phishing**
Blocks access to known fraudulent websites that try to steal online banking passwords or identity details.

**Browser security**
Browser extension/addon for Chrome, Firefox and Edge that blocks access to dangerous websites on a URL level. Uses a privacy-conscious design that doesn't track your browsing history or break your SSL encryption chain.

**File Guard**
Scans all downloaded and executed files with the dual-engine scanner.

**Behavior Blocker**
Detects zero-day malware by monitoring the behavior of all running programs. The Behavior Blocker is the main line of defense against specialized attacks.

**Anti-Ransomware**
Reliably stops ransomware before it encrypts files.

**Exploit prevention**
Generically prevents exploits from injecting code into foreign programs to execute harmful payload.

**System manipulation prevention**
Detects exe-patchers, hidden rootkits, autoruns, host changers, browser settings changers, group policy changers and invisible installers.

**Application hardening**
Controls potentially dangerous procedures within active programs. E.g. prevents commonly attacked software like MS Office from being able to execute dangerous PowerShell scripts, and more.

**Advanced Persistent Threat (APT) protection**
APTs are attacks where an intruder establishes a long-term presence in your network to exfiltrate data. The Emsisoft Behavior Blocker, the Application Hardening and advanced heuristics detect such intrusions before damage is done.

**Fileless malware protection**
Behavior Blocker, Application Hardening, Registry scanning and script monitoring prevent fileless malware infections, which reside only in memory.

**Targeted attack prevention**
Stops customized attacks, including spear-phishing, single-use malware, state trojans and industrial espionage.

**Botnet protection**
Behavior Blocker and signature-based scanner heuristics protect your devices from becoming part of a botnet that criminals use to perform malicious or fraudulent actions.

**False positives verification**
Detected objects can be verified with our reputation online service to ensure that legitimate programs are not unnecessarily alerted or quarantined.
PREVENTING NEW INFECTIONS

Protection exclusions/allow list
Exclude known good files and folders from real-time protection. Supports wildcards (?), (*) and 44 environment variables as generic shortcuts for common folders (%temp%, %windir%, etc.).

Hourly automatic updates
The protection software always keeps itself up-to-date, including detection patterns and functional improvements.

Emergency network lockdown mode
Click the on/off switch to instantly take your devices offline. Can also be controlled remotely via the Management Console.

Shutdown & uninstall prevention via password
Set a local security admin password to ensure that attackers won’t be able to disable or uninstall protection even if they gain full access to the device.

Windows Firewall monitoring and hardening
Checks if the Windows Firewall is enabled and protects it from being manipulated by third-party software.

Windows RDP attack detection
Checks if the Windows Remote Desktop service (RDP) is enabled and alerts you when it is under brute force attacks.

ENDPOINT DETECTION AND RESPONSE (EDR)

Suspicious behavior tracking
Suspicious process activity is analyzed in the cloud and accessible through the Incidents panel.

Local detections on devices
Analyze all threats detected by the local disk scanner and real-time protection.

Quick allow/quarantine/block everywhere
Allow, quarantine or block a specific file in your entire workspace with a single click.

Device isolation
Take selected devices offline with a single click while keeping them connected with the console for further threat analysis.

Execution tree & timeline
Trace potential threats back to their origin to see how they entered your workspace.

MITRE ATT&CK tactics & techniques
Standardized classification of malware behavior patterns.

CENTRALIZED MANAGEMENT

Management Console included (Simplified)
Centralized security management has never been easier. See the protection status of all your devices on a single dashboard at MyEmsisoft.

Industry leading mirror view
Using the Management Console feels like you’re in front of the protected device. All settings and features can be controlled, changed and applied in real-time.

Web access & mobile app
The Management Console can be accessed via web browser or used as a mobile app, so you can take care of your security needs from any device.

“Local only” management mode
Disables all cloud based management features but still enables automatic updates, licensing and online lookups of malware findings. Provides maximum privacy.

“Local & remote” management mode
Allows protection settings to be configured locally on the protected device and remotely via the Management Console. Provides maximum flexibility for users and admins.

“Remote only” management mode
Disables access to settings and simplifies the user interface on the protected device. Recommended for larger organizations. Provides maximum control for admins.

Traffic caching relay devices (multiple)
Configure one or more of your devices to act as a relay for all Internet data transfers. Relays cache software updates to reduce the total amount of Internet traffic. Only data from and to Emsisoft servers is allowed through.

Incident investigation tools
See all alerts of all your devices on a single dashboard. Drill down to device level to check detection logs and details.

Forensics & audit logs
See exactly what happened in your workspace and who performed certain actions or configuration changes.

Remote scans & quarantine
Initiate a malware scan remotely at any time and watch the scan status live. All scan types are supported. Check quarantined objects on any device for further analysis.

Device isolation
Take devices offline within seconds if you suspect a malware infection. Remote management for incident investigation is still possible but all other network communication is blocked.

Device health & system overview
The device dashboard shows security-related information on device health, including current protection status, firewall and RDP service. Also shows real-time system parameters like storage, memory, IP addresses, critical system events and device hardware properties.

Email, webhook & push notifications
Receive real-time notifications for specified events such as malware findings or device issues. You can process notifications by email or webhooks, or have them pop up on your device as a push notification for urgent situations.

Advanced reporting
View real-time data analysis and scheduled snapshots. Reports can be template-based and fully customized.
**CENTRALIZED MANAGEMENT**

<table>
<thead>
<tr>
<th>Protection policies for device groups</th>
<th>Smart designed policies in hierarchical order with inheritance and highlighting of edits on each level. Includes support for policy templates for use in multiple workspaces.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission policies for user groups</td>
<td>Define how much your users can do with their Emsisoft protection. Use smart defaults for admins and non-admin accounts.</td>
</tr>
<tr>
<td>Invite Emsisoft partners (MSPs) to manage workspace</td>
<td>Invite an Emsisoft Security Hero to handle your workspace. Suitable for organizations that lack internal resources for ongoing security monitoring and management.</td>
</tr>
<tr>
<td>REST Web API for all features</td>
<td>For developers who need to integrate security management into their own workflows and tools. All functionality of MyEmsisoft is also available via API.</td>
</tr>
</tbody>
</table>

**TASK AUTOMATION**

<table>
<thead>
<tr>
<th>Scheduled scans</th>
<th>Scan your devices in regular intervals (e.g. Friday night after work). Includes highly configurable scheduling, scanning and logging options.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line interface included</td>
<td>A powerful command line interface that features all the functions of the GUI software. Use it to automate common scanning tasks.</td>
</tr>
<tr>
<td>Email notifications for relevant events</td>
<td>Get instant email notifications directly from your devices whenever malicious files are detected.</td>
</tr>
<tr>
<td>Monitoring of file shares and connected storage</td>
<td>File servers that are heavily risk-exposed are carefully monitored by real-time protection. Any new devices that connect to your server are automatically covered.</td>
</tr>
<tr>
<td>Protection without logged in users</td>
<td>Protection loads at the earliest possible time when Windows boots and doesn’t require any logged on users to operate.</td>
</tr>
<tr>
<td>Silent mode/gaming mode</td>
<td>Protection changes to auto pilot every time a full screen application runs to prevent interruptions. You can also manually enable silent mode at any time.</td>
</tr>
<tr>
<td>Windows Server OS supported</td>
<td>Emsisoft supports all 64 bit editions of the Windows 10 operating system. Support for Windows Server 2016 and higher is limited to business editions of Emsisoft protection software.</td>
</tr>
</tbody>
</table>

**DEDICATED EMSISOFT BENEFITS**

<table>
<thead>
<tr>
<th>Money back guarantee</th>
<th>For your peace of mind, we offer a 30-day money back guarantee.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware removal assistance</td>
<td>Our dedicated malware removal experts can help you remove infections from your computer system if you need assistance, at no extra cost.</td>
</tr>
<tr>
<td>Always get the latest version</td>
<td>Receive the latest software version within the licensed period at no additional cost. The built-in update feature ensures you always get the latest state-of-the-art protection technology.</td>
</tr>
<tr>
<td>Certified protection</td>
<td>Emsisoft has earned multiple awards and recognition from independent international testing organizations like Microsoft, OPSWAT, AV Labs, Virus Bulletin, AV-Comparatives, AV-Test, and more.</td>
</tr>
<tr>
<td>Privacy conscious design</td>
<td>Emsisoft is recognized as one of the most privacy-conscious cybersecurity companies. We don’t collect or sell user profiles or private data to third parties.</td>
</tr>
<tr>
<td>Email &amp; live chat support</td>
<td>Our friendly support team is dedicated to resolve any problems that you may encounter within the shortest time possible.</td>
</tr>
</tbody>
</table>

**OPTIONAL: EMSISOFT ENTERPRISE SECURITY UPGRADE**

<table>
<thead>
<tr>
<th>Active Directory integration</th>
<th>Synchronizes your domain user accounts with your Emsisoft workspace.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic detection of new devices</td>
<td>Synchronizes your domain devices and alerts your new devices to deploy protection.</td>
</tr>
<tr>
<td>Remote deployment through relay devices</td>
<td>Emsisoft Enterprise Security customers receive priority support.</td>
</tr>
<tr>
<td>Skip-the-line priority support</td>
<td>Should you experience any issues with malware or the software, our dedicated experts are here to immediately help.</td>
</tr>
<tr>
<td>Call-back service (8am-9pm ET)</td>
<td>Drop us a short message and we will call you back to get your issue resolved within minutes.</td>
</tr>
<tr>
<td>Dedicated customer support manager</td>
<td>Get a dedicated Emsisoft Support Hero who knows your situation and requirements.</td>
</tr>
</tbody>
</table>

**System Requirements**

Any system that runs Windows 10 x64, Windows Server 2016/2019 or higher

www.emsisoft.com | support@emsisoft.com