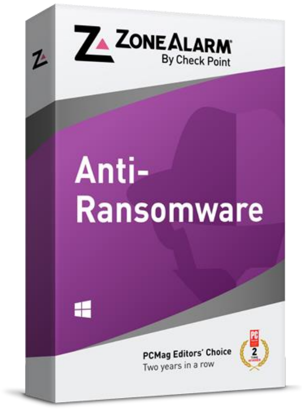

ZoneAlarm Anti-Ransomware

Windows

ZoneAlarm Anti-Ransomware is part of ZoneAlarm's new product line with the latest innovative zero-day, enterprise- grade threat prevention technology, and is the result of years of research and development. It offers ZoneAlarm's award-winning Anti-Ransomware protection combined with ZoneAlarm's new advanced Chrome Extension, which includes zero-day phishing protection and safe downloads of files.

Anti-Ransomware

Detects, blocks, and removes ransomware attacks and, in addition, restores any encrypted files by employing behavior-based technologies that don't rely on signature updates.

File Protection
Uses real-time behavior analysis to detect and block ransomware threats, even those that other PC security solutions don't catch.

Auto File Restoration
The only anti-ransomware protection that immediately and automatically restores any encrypted files.

PC Shield
Blocks any malicious attempts to lock your PC and ensures you have continuous access to it.

Works online and offline (24/7)
Protection is on even when your PC is not.

Product Features

ZoneAlarm's Web Secure includes the latest zero-day threat prevention for your browser and online activities.

Anti-Phishing
Protects your device(s) in real-time from new and unknown phishing sites using static, heuristic, and machine-learning techniques.

Threat Extraction
Downloads files confidently and securely, eliminating possibilities of malicious attachments and behaviors.

Technical Support

Free customer support, including in-depth information, forum, and 24/7 live chat.

Compatible with all antivirus protection

An additional layer of security to any traditional antivirus **protection in place.**

How ZoneAlarm Anti-Ransomware works

ZoneAlarm Anti-Ransomware utilizes advanced security engines and algorithms to detect, block, and remediate ransomware attacks. By using behavioral technologies that do not rely on signature updates, the Anti-Ransomware capability is able to identify and remediate zero-day ransomware attacks.

ZoneAlarm Anti-Ransomware utilizes a multi-layered security architecture, providing a complete solution

LAYER 1: **Ransomware behavioral analysis**

Real-time customized behavioral analysis that identifies most ransomware before it starts encrypting data.

- Purpose-built advanced algorithms perform ongoing behavioral analysis of all activities in the OS with special emphasis on detecting specific ransomware behaviors

LAYER 2: **Illegitimate data encryption identification**

Identifies ransomware that manages to evade initial behavioral analysis and begins encrypting data.

- An independent file-tracking engine looks for evidence that data files, such as documents and images, are being illegitimately and systematically encrypted.
- The file-tracking engine keeps close track of any changes to files, checking which processes are modifying data files, and what is the nature of the modification. It is designed to differentiate between legitimate and illegitimate activities.
- If there is ransomware actively encrypting data, the algorithms will pick up this activity quickly.

LAYER 3: **Automated forensic analysis and malware quarantine**

Detected ransomware is automatically analyzed and quarantined

- Ransomware (or other malware) detected by the engines described above (layers 1 & 2) automatically triggers forensic analysis
- The analysis begins with the detected indicator of compromise (IOC) being used as the investigation anchor.

The forensic analysis uses Anti-Ransomware's powerful ability to automatically trace the attack activity and analyzes all its elements in order to identify the full attack model.

- The generated attack model includes identification of the malicious elements and activities of the Ransomware.
- Using ZoneAlarm Anti-Ransomware Client's malware removal capability, all malicious components of the malware – as identified by the generated forensic attack model - are terminated and quarantined.

LAYER 4: **Data restoration**

Data is automatically backed up and restored in the event that encryption starts before the ransomware was identified.

- Ongoing snapshots of data files are automatically taken before the files can be modified.
- Several factors help minimize the storage required for snapshots:
  1. A file snapshot is taken only when we suspect an attempt to modify the file might be illegitimate. File snapshots must be maintained only until a determination is made on the nature of the modification. If it isn't ransomware, then the snapshots may be discarded.
  2. Users typically modify very few data files.
  3. Maintaining a short history is sufficient.
- Anti-Ransomware will allocate no more than 2GB of storage for file snapshots. In most cases, much less space is needed.
- The data-file snapshots are stored on the endpoint file system and protected from tampering by Check Point Endpoint self-protection kernel drivers.
- After malware quarantine is performed by layer 3 above, data files are automatically restored from the snapshots.

How ZoneAlarm Web Secure works

Anti-Phishing **- Blocks and alerts you of phishing attempts**

Prior to enabling you to insert your credentials, the system will thoroughly scan and examine every field on the page, including the site's URL, title, the layout of the page, form, signature, and visible text and links for potential deceptive threats. The dedicated spaces for your credentials, such as email address, become blocked until the scan has finished.

The system will determine whether the site is trustworthy or not using Check Point's ThreatCloud™, the world's biggest threat database. If the site is determined to be fraudulent, you will be immediately alerted and blocked from accessing it; nevertheless, you will have the option to continue on to the site should you wish.

Threat Extraction **- Allows you to safely download files**

ZoneAlarm Threat Extraction removes exploitable content from common files, such as Microsoft Word, Excel, PowerPoint, and Adobe PDF. It removes high-risk macros, active and embedded objects, and external links that can be maliciously exploited to infect your computers and networks.

Reconstructs your files with known safe elements and promptly delivers you safe content or sanitized versions of potentially malicious files in PDF format. It applies a 'prevent' mode type of deployment as opposed to 'detect' mode which traditional detection technologies often use.

System Requirements:

Microsoft® Windows® (7 SP1, 10)
32 or 64-bit, 2 GB RAM
2 GHz or faster processor
2 GB of available hard-disk space Periodic Internet Connection

FIND OUT MORE:

Website:	www.zonealarm.com
Blog:	www.blog.zonealarm.com
Contact:	info@zonealarm.com

ZoneAlarm
By Check Point