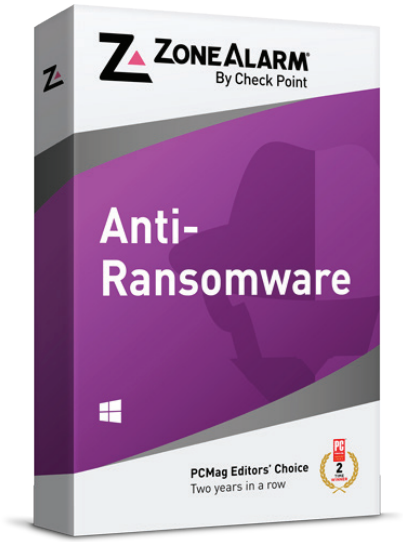
ZoneAlarm Anti-Ransomware

ZoneAlarm Anti-Ransomware analyzes all suspicious activities on your PC. It detects Ransomware attacks, blocks them and immediately restores any encrypted files. ZoneAlarm Anti-Ransomware is the result of years of research and development and offers the best Enterprise-Grade protection against Ransomware threats.



Auto File Restoration

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

Compatible with all antivirus

Additional layer of security to any traditional antivirus

File Protection

Detects and blocks Ransomware threats, even those that other PC security solutions don't catch.

Works online and off

Protection is on even when the PC is offline

PC Shield

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

Second year in a row: PCmag rates ZoneAlarm Anti-Ransomware Editor's choice.

"The most effective ransomware-specific security tool"

PC Magazine Editor's Choice, July 2017

"ZoneAlarm Anti-Ransomware is a clear winner"

PC Magazine Editor's Choice, June 2018

System Requirements

Microsoft® Windows® (7 SP1, 8.1+, 10)

32 or 64-bit, 2 GB RAM

2 GHz or faster processor

1.2GB of available hard-disk space

Periodic Internet Connection

Supported OSs

Windows 7 SP1 (must have SHA-2 support).

Windows 8.1+

Windows 10

Compatibility

ZoneAlarm Anti-Ransomware is compatible with all other antivirus, firewall and PC security software.

ZONEALARM By Check Point www.zonealarm.com

Same technology used to protect Fortune 500 companies and home PC users.

HOW ZONEALARM ANTI-RANSOMWARE WORKS

ZoneAlarm Anti-Ransomware Client utilizes advanced security engines and algorithms to detect, block and remediate ransomware attacks. By using behavioral technologies which do not rely on signature updates, the Anti-Ransomware capability is able to identify and remediate zero-day ransomware attacks.
Anti-Ransomware utilizes a multi-layered security architecture, providing a complete solution:

LAYER 1: Ransomware behavioral analysis
Real-time customized behavioral analysis 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
• Because many ransomware behaviors, such as various evasion tricks, are common to other malware our behavioral analysis also has the capability to detect and block other types of malware.

LAYER 2: Illegitimate data encryption identification
Ransomware that manages to evade initial behavioral analysis and begin encrypting data is identified

• 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 change 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 is in play, actively encrypting data, the algorithms will pick this up quickly, typically not more than a few dozen files have been encrypted

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 a the investigation anchor
• The forensic analysis uses Anti Ransomware's powerful ability to automatically trace the attack activity and analyze 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 where 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
  - A file snapshot is taken only when we suspect an attempt to modify the file might be illegitimate
  - Users typically modify very few data files
  - Maintaining a short history is sufficient
    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
• Anti-Ransomware will allocate no more than 1GB of storage for file snapshots. In most case 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

FREQUENTLY ASKED QUESTIONS

• Our Anti-Virus (AV) has successfully stopped ransomware in the past, why do I need ZoneAlarm Anti-Ransomware Client?
Traditional AV can be effective in detecting attacks by known ransomware. However, ransomware is constantly evolving, mutating and incorporating new evasion tricks. Many ransomware attacks are capable of evading AV detection, as evident by the numerous infections suffered by businesses around the world – virtually all of which are utilizing AV.
• If I use ZoneAlarm Anti-Ransomware Client feature, do I still need my endpoint Anti-Virus (AV)?
We recommend using AV on all PCs – it is still an important part of an effective multi-layered approach to security, and it is still an effective means for preventing basic malware attacks that are still quite prevalent. ZoneAlarm Anti-Ransomware Client can deployed alongside any third party AV or as part as ZoneAlarm Anti-Virus package.
• Can ZoneAlarm Anti Ransomware work in parallel to other Anti Virus?
Yes, ZoneAlarm Anti Ransomware can run in parallel to any other Anti virus (i.e. Check Point/ZoneAlarm, Symantec/Norton, McAfee, F-Secure, AVAST, AVG, Bit defender, Microsoft etc.)
• How much storage is required for Anti-Ransomware's file snapshots?
We recommend allocating 1GB of storage for file snapshots. The storage capacity can be configured by the customer.
• Do I still need my backup if I use the ZoneAlarm Anti-Ransomware Client?
Yes.
Anti-Ransomware focuses only on recovering data encrypted by ransomware, not on general purpose

backup.
In order to ensure data recovery in other cases such as disk failure, a conventional backup is recommended.

• **How are file snapshots protected?**

File snapshots are protected by the ZoneAlarm Anti-Ransomware Client self-protection kernel driver, which prevents any attempt to access to the data by processes that are not part of ZoneAlarm Anti-Ransomware Client and signed by Check Point.