TRY NOW LEARN MORE

How to Defend Your Systems from Ransomware with **Acronis** Backup 12.5

Installation

Protecting your systems from ransomware with Acronis is easy. Simply install Acronis Backup's touch-friendly management console on a server or a PC and deploy backup agents to the machines that you plan to protect. Backup management is completely centralised and you don't need to attend to each system. Any previously installed versions of Acronis Backup will be seamlessly upgraded.

Enabling Acronis Active Protection™

After deploying the agents, enable Acronis Active Protection, which can detect, stop, and reverse unauthorised encryption or modification of files. You can enable the feature on individual machines, groups of machines, or across entire environments. You can control the level of protection from notify-only to complete "stop and revert using cache". You can also whitelist trusted applications and blacklist known malware. In addition, your backup agents are self-protected from ransomware too.

Backup

In addition to enabling Acronis Active Protection, back up all your systems for recovery purposes. With just a few clicks, schedule your backups to local disks, NAS, SAN, centralised deduplicated storage, tape, or secure Acronis Cloud Storage. You can set your retention policies to comply with any internal or government regulations.

System Recovery

When it comes to the most important feature – data recovery – Acronis delivers the most comprehensive solution on the market. If malware damage is irreparable, you can restore an entire system image to dissimilar hardware. Everything is overwritten. There will be no leftovers, backdoors, or remaining traces of malware or its activity.

File Recovery

If only a file is affected, you can quickly browse the backup to find and restore that file. To find a specific file, you can use search and quickly scan the contents of the backup.

BUSINESS REALITY

47%
of businesses were attacked by ransomware in 2016

21+
platforms supported by Acronis Backup 12.5

500,000
businesses rely on Acronis to protect their data and systems

TRY NOW LEARN MORE

ONLY ACRONIS BACKUP 12.5

Delivers **hybrid cloud and on-premises data protection** for businesses of all sizes using a touch-friendly, web-based console to back up and recover all individual workloads.

Includes **Acronis Instant Restore that allows you to reduce RTOs to seconds** by running any physical or virtual Windows or Linux system backup as VMware® or Hyper-V® VM with a few clicks and without standby hardware.

Eliminates the need to recover from ransomware attacks by proactively defending systems with Acronis Active Protection.

Supports the protection of **21 types of physical, virtual, cloud, end-user, and mobile devices,** delivering easy, complete, and affordable data protection.

Includes **Acronis Notary™, which improves regulatory compliance**, establishes the validity of recovery, and ensures authenticity and integrity of your backups with Blockchain.

Gives you **complete control over the location of your data, systems, and backups,** improving regulatory compliance and ensuring data sovereignty.

BEST FOR ANY SCENARIO

Prevention

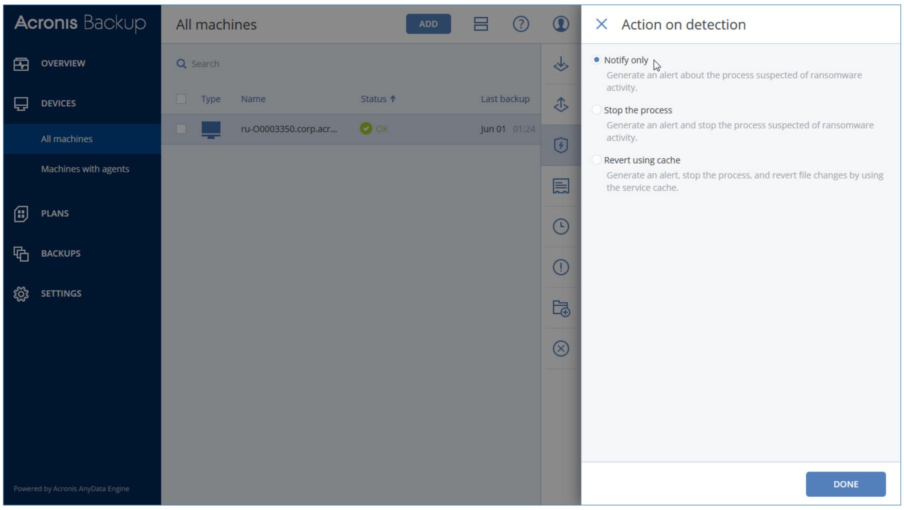
Acronis Backup 12.5 is the only backup solution in the industry with a proactive defence against ransomware: Acronis Active Protection. This technology actively detects suspicious behaviour that affects your data, notifies you, stops the suspicious process, and reverses the changes. It has proven to be effective on the most damaging ransomware types, including WannaCry. It is a perfect complement to your existing antivirus solution.

Data Recovery

For additional protection of your data, perform regular backups with Acronis Backup 12.5, the most complete solution in the market, protecting more than 21 platforms and storing backups on a variety of storage devices. In addition, Acronis Active Protection guards your backups from unauthorised modification or deletion. You can restore your folders, files, databases, and even application items in a few simple clicks using the touch-friendly web-based console.

Bare-Metal Recovery

If your system is damaged beyond repair by malware, Acronis Backup 12.5 can restore your complete disk-image backups to the same or dissimilar hardware. You can even restore your physical system backup to a virtual machine or vice versa. Acronis Universal Restore takes care of the hardware differences, adjusts operating systems settings, and injects the necessary drivers, ensuring reliable operation of your Windows or Linux, 32- or 64-bit, UEFI or BIOS system running on any supported hardware.



Type	Name	Status ↑	Last backup
	ru-O0003350.corp.acr...	✓ OK	Jun 01 01:24

Action on detection

● Notify only
Generate an alert about the process suspected of ransomware activity.

○ Stop the process
Generate an alert and stop the process suspected of ransomware activity.

○ Revert using cache
Generate an alert, stop the process, and revert file changes by using the service cache.

Acronis Active Protection™ — Enabling Different Modes of Protection

TRY NOW LEARN MORE

HOW ACRONIS ACTIVE PROTECTION WORKS

The Heuristic Detection Approach

Acronis Active Protection uses a behaviouralheuristic approach that analyses chains of file system events performed by processes and compares it to a database of malicious behaviour patterns.

Behavioural heuristics are reinforced with whitelists and blacklists of various programs. While the heuristic approach is capable of detecting new threats, it operates on the basis of experience/ behaviour results and may cause false positives. White lists reduce and control false positives, while blacklists enforce early prevention before the behaviour starts.

Acronis Active Protection also includes self-protection of backup files and backup agents. No process in the system except Acronis software can modify backup files. There is also a robust self-defence mechanism that eliminates any attack on the backup agent and prevents disruption of the backup software.

In addition, Acronis Active Protection monitors the Master Boot Record (MBR) of the system hard drive and only allows whitelisted process to change the MBR.

Does Acronis Active Protection Protect Any File?

Yes, it defends your system from three distinct vectors of attack:

1. Attack on any file

Acronis Active Protection works in real-time by automatically recovering encrypted files to the latest version.

This provides the protection you need, especially when running scheduled backups. For example, without Acronis Active Protection, you can lose up to 17 hours of work if your system is scheduled to back up at midnight, but is attacked at 5PM. Acronis Active Protection eliminates these losses.

2. Attack on local backup files

Acronis Active Protection actively monitors any local drives and prevents backup files from being modified or deleted.

3. Attack on cloud backups

Files stored in Acronis Cloud Storage are exceptionally safe from direct modification by malicious code. Acronis uses strong end-to-end encryption and only authorised Acronis agent software can access the backup files.

Why Is Acronis Active Protection Better than Antivirus Plus Traditional Backup Software?

The answer to this is simple: your antivirus and backup software are not integrated and therefore not equipped to save your data from ransomware.

Pairing Acronis Active Protection with Acronis Cloud via an Acronis backup agent enables recovery of original data from local caches, local backups, and cloud backups, eliminating the most dangerous ransomware threats.

Acronis Active Protection Protects Against Future Threats

Hackers view attacks on backups as an additional way to increase their income, so you will see more ransomware variants attacking your backups.

The only backup software that can stop future attacks on backups in the cloud is Acronis Backup 12.5 with Acronis Active Protection.

TRY NOW LEARN MORE

SUPPORTED SYSTEMS

Operating Systems for On-Premises Console Installation

- Windows Server® 2016, 2012/2012 R2, 2008/2008 R2*
- Windows Small Business Server 2011, 2008
- Windows MultiPoint Server 2012, 2011, 2010
- Windows Storage Server 2012/2012 R2, 2008/2008 R2
- Windows 10, 8.1, 8, 7
- Linux x86_64 with kernel from 2.6.18 to 4.9 and glibc 2.3.4 or later

Microsoft Windows

- Windows Server 2016, 2012 R2, 2012, 2008 R2, 2008, 2003 R2, 2003*
- Windows Small Business Server 2011, 2008, 2003 R2, 2003
- Windows MultiPoint Server 2012, 2011, 2010
- Windows Storage Server 2012 R2, 2012, 2008 R2, 2008, 2003
- Windows 10, 8.1, 8, 7, Vista, XP SP3

Cloud

- Office 365® mailboxes
- Amazon Web Services EC2® Instances
- Microsoft Azure® VMs

Hypervisors

- VMware vSphere ESX(i) 6.5, 6.0, 5.5, 5.1, 5.0, 4.1, including vSphere Hypervisor (free ESXi)*
- Microsoft Hyper-V Server 2016, 2012 R2, 2012, 2008 R2, 2008
- Microsoft Windows Server 2016, 2012 R2, 2012, 2008 R2, 2008 with Hyper-V
- Microsoft Windows 10, 8.1, 8 (x64) with Hyper-V
- Citrix XenServer® 4.1-6.5*
- Red Hat® Virtualization 2.2-4.0
- Linux KVM
- Oracle® VM Server 3.0-3.3

Applications

- Oracle Database 12, 11*
- Microsoft Exchange® Online
- Microsoft Exchange Server 2016, 2013, 2010, 2007 – including cluster configurations
- Microsoft SQL Server® 2016, 2014, 2012, 2008 R2, 2008, 2005 – including cluster configurations
- Microsoft SharePoint® 2013, 2010 SP1, 2007 SP2, 3.0 SP2

Storage

- Local disks – SATA, SCSI, IDE, RAID
- Networked storage devices – SMB, NFS, iSCSI, FC
- Removable media – ZIP®, Rev®, RDX®, etc.
- External HDDs and SSDs – USB 3.0/2.0/1.1 and IEEE1394 (Firewire)
- Tape drives, autoloaders, and libraries, including media management and barcode support
- Acronis Cloud Storage

File Systems

- FAT16/32
- NTFS
- HFS+ *
- ReFS *
- ext2/ext3/ext4
- ReiserFS3, ReiserFS4 *
- XFS *
- JFS *
- Linux SWAP

Web Browsers

- Google Chrome® 29 or later
- Mozilla Firefox® 23 or later
- Opera 16 or later
- Windows Internet Explorer® 10 or later
- Microsoft Edge® 25 or later
- Safari® 8 or later (running in Apple OS X and iOS)

* Some limitations may apply. **Click here for details.**

Acronis

For additional information, please visit **www.acronis.com**

Technical changes and differences from the illustrations are reserved; errors are excepted. 2017-06