Acronis

WHITE PAPER

Multilayered cybersecurity: part of modern cyber protection

Integrated technologies for a better defense

Data is your most important business asset. As the world has become increasingly digital, data has grown in volume and value. In fact, this most valuable resource of modern society doubles in volume every year and that growth rate is likely to accelerate even further. Of course, this creates a challenge: do you store data securely and how can you be sure that every operation with data is secured? Today, loss of data means loss of everything: business, identity, future, and even life in some cases.

Traditionally, businesses like yours have approached this challenge from two different angles. Antivirus and anti-malware solutions handled system security, providing a safe environment, while a backup solution managed data to ensure that a copy of it was always available. Anti-malware and backup agents are typically installed in the same endpoint but they don't talk to each other and can't guarantee fast data recovery in the event of an incident.

Acronis Cyber Protect solves this challenge while adding other essential functionality into the newly established cyber protection space.

Why enhance cybersecurity?

Modern cyberattacks, data leaks, and ransomware outbreaks all show the same thing: cybersecurity is failing. This failure is the result of weak technologies and human mistakes caused by clever social engineering. In cases where a backup solution was working well and wasn't compromised, it usually takes hours and days to restore systems (with data) to an operational state. Backup is essential for when cybersecurity solutions fail, but at the same time backup solutions can be compromised, disabled, and perform slowly, causing businesses to lose a lot of money due to downtime.

To solve these problems, Acronis has developed Acronis Cyber Protect: a cyber protection solution that combines anti-malware and backup into a single agent running under a family of Windows operating systems. This integration lets you maintain optimal performance, eliminate compatibility issues, and ensure rapid recovery. If a threat is missed or detected, while your data is being altered it will be restored from a backup immediately – because of its one agent, it knows that data was lost and needs to be restored.

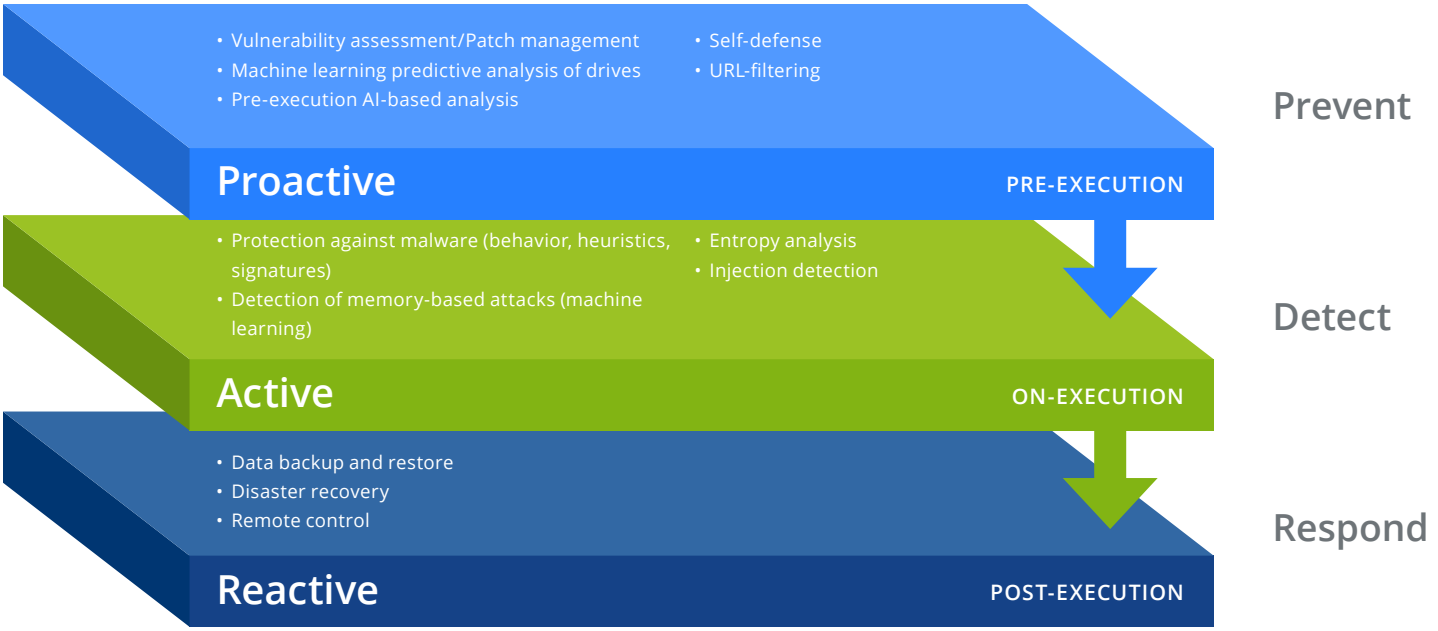
This isn't possible with an anti-malware agent separate from a backup product with it's own agent. Your anti-malware solution may stop the threat but some data may already be lost. A backup agent won't know about it automatically and, in the best case, data will be restored slowly – if at all.

Of course, Acronis Cyber Protect strives to make data recoveries unnecessary by detecting and eliminating threats before they can damage your environment. This is achieved with enhanced, multilayered cybersecurity functionality, which we'll explore in depth in this white paper.

Dealing with emerging threats

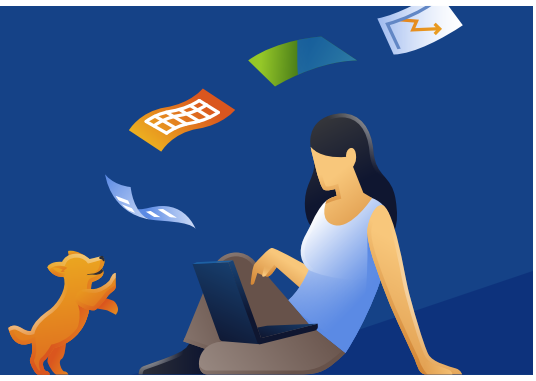
Today, a proper cybersecurity solution requires multilayered threat protection. This should be delivered through a set of smartly integrated technologies each of which should work on dedicated stages of threat prevention. For example, if a security product uses signature-based detection engines, it won't be able to react to new dangerous threats including zero-day malware strains.

Modern cybersecurity or anti-malware solutions should be able to deliver solid real-time protection. That includes the ability to detect an incoming current, new, or unknown threat the moment it arrives at your endpoint and tries to compromise it. In a typical endpoint security solution, this will be covered by so-called "on-access" or "on-execute" detection methods, which are of course implemented in Acronis Cyber Protect. In addition, admins can run on-demand scans: let's say new software appears on a user's machine, it can be scanned before execution. These real-time detections can be achieved with several technologies, in the case of Acronis Cyber Protect, they include.



Below we review detection technologies in particular. We invite you to familiarize yourself with these topics in our dedicated white papers discussing:

- Vulnerability assessment and patch management
- Acronis Active Protection
- Acronis Any-Data engine
- Acronis AI-based drive health analysis
- Fileless attacks



THE ACRONIS CLOUD BRAIN

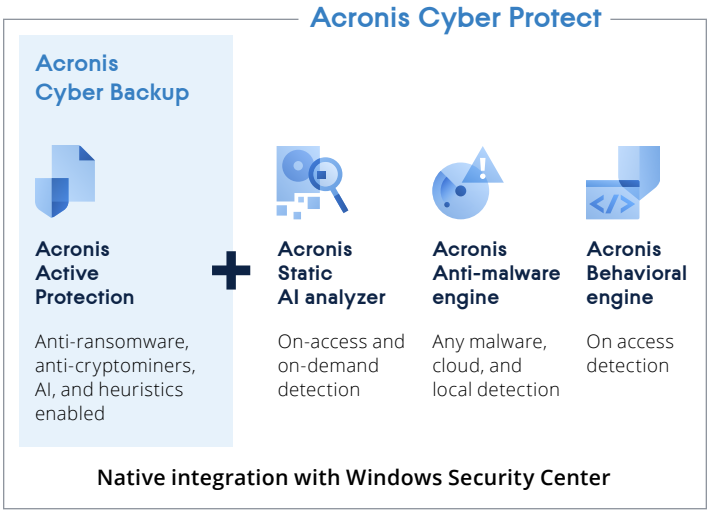
This technology offers cloud-delivered detection from Acronis data centers around the globe. When the Acronis Cyber Protect agent on an endpoint detects something suspicious, it sends metadata to the cloud for further analysis and research including sandboxing, AI-enabled processing, and so on. Additionally, threats can be analyzed by human experts when needed. After that, a detection record will be created and instantly made available for all other endpoints connected to Acronis Cloud. This allows for better protection faster than regular on-agent signature bases and heuristic rule updates, which normally take hours to release.

BEHAVIORAL ENGINE (PLUS ACRONIS ACTIVE PROTECTION)

Static detection methods, like signatures, are very easy to bypass. Cybercriminals can just pack and obfuscate malicious files and signature detection will not work. That's why behavioral engines were introduced. These are typically a set of behavior rules which will react to a known bad behavior or abnormal behaviors from known good processes. For example, a program that tries to maliciously edit the registry, delete files, try to reside on system folders, or make injections into other processes is likely malicious.

Behavioral engines will detect and stop processes exhibiting these behaviors. The Acronis Behavioral Engine analyzes suspicious kernel-level events as well as events coming from the Windows operating system. These heuristic rules are easily updatable and let Acronis security specialists quickly react to new developing threats. Additionally, the Acronis Behavioral Engine is a very powerful tool for the detection of fileless threats – like in memory or script-based attacks. By analyzing certain process behaviors in memory, Acronis can also determine if it's a threat. For example, if malicious code is executed in the context of a web browser, via a vulnerability or by infecting or creating a malicious website. Acronis' behavior detection engine is able to identify it by analyzing the browser's thread behavior, block it, and report it to the administrator.

Acronis Active Protection, introduced in 2017, is a separate behavior-based engine enhanced by AI. It works in close collaboration with the new general-purpose Acronis Behavioral Engine that can detect any kind of threat and was fully developed in-house for Acronis Cyber Protect. To review all of the innovations implemented in Acronis Active Protection – like stack trace analysis and detection of injections into legitimate processes – you can learn more in this white paper.



MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Acronis incorporated machine learning technology in 2018 as a part of Acronis Active Protection's anti-ransomware technology. With the help of machine learning models and artificial intelligence decision-making, we analyze Windows executable stack traces to add additional layers of confidence to our Acronis Active Protection behavioral heuristics.

In 2019, Acronis launched a static AI-based detection engine on VirusTotal. This engine processes Windows executables and dynamic link libraries (DLLs) to determine whether or not a process is malicious through a set of unique parameters. The machine learning model is trained on both malicious and clean files in the Acronis Cloud Brain, which already processed dozens of millions of files - keeping in mind such details as the presence of a digital certificate and its validity. Files are constantly analyzed in the Acronis Cloud Brain where the model is also trained via sandboxes and other security tools. We use a supervised training approach and a gradient boosting technique with various decision trees based on many situations or patterns of malicious behavior.

The model is constantly optimized by Acronis engineers

and can be easily updated on each endpoint from the cloud. As a result, only relevant parameters are included in the training, helping to ensure the best possible results. If a process' behavior remains undetermined after detection, it's automatically analyzed by another model and, as we review results later, our detection models are adjusted accordingly. For top malware types and families, we have separate models that deliver the best detection results.

A good machine learning model doesn't need much data in terms on quantity. It needs relevant, good quality data. That's why it's important to train models to catch common threat features and traits. Ransomware's key traits, for example, are the ability to encrypt data and make a connection to the command and controls center.

Currently, one training session for the Acronis static detection model takes only 20 seconds and we have more than 10,000 data updates each day specifically to retrain the model. This means we're able to constantly improve its effectiveness against new and emerging threats. Today, Acronis Cyber Protect analyzes Windows, macOS and Linux operating systems.

WHITELIST DATABASE

A whitelist is a huge database that contains information on clean/non-malicious applications. This can be stored both in the cloud and locally, the local version allowing for quicker reactions and being a necessary component for businesses who require a closed perimeter and only want to receive data rather than share with a global network. These are typically government and military and this restriction makes sense given the nature of data they work with.

In the case of a cloud implementation, this is again a part of the Acronis Cloud Brain and is located in Acronis data centers. What is more interesting, cyber protection products from Acronis are also able to populate a whitelist from a backup, a unique and useful feature if you have custom software. Imagine using an app created in-house by your developers. This app allows some system access, so only a few people in your company can use it. The traditional whitelisting system would encounter such an app, raise a flag, and mark

it as suspicious. The only way to clean that file is by downloading and analyzing it, which isn't always possible. Your admin at the same time has to deal with false alarms, lost time, and lost productivity.

Now imagine that you enrolled a new machine with this app into the network. A full backup will be done and (if you have Acronis Cyber Protect) will be scanned by various anti-malware engines. When Acronis Cyber Protect sees the new app in a backup that is not in the current whitelist, it will be analyzed immediately, sandboxed if needed, and can be "cleared" in a matter of 24 hours or more (depending on the configuration set by Acronis engineers). After that, the whitelist will react properly when it encounters this app on any new machines you enroll.

This approach minimizes false positives and lets Acronis specialists create more accurate and aggressive heuristic detection rules, leading to a better detection rate and better protection, overall.

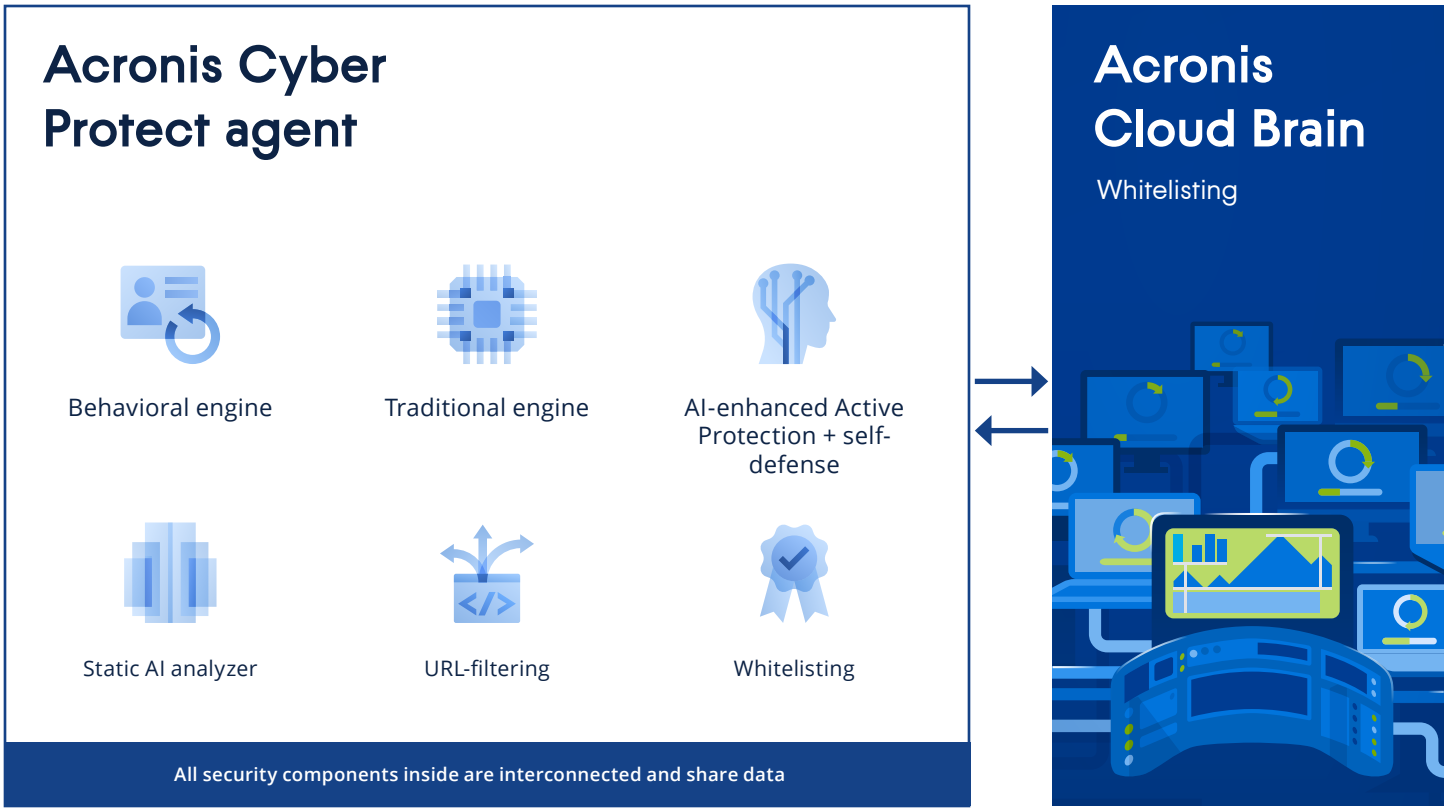
URL-FILTERING

The ability to filter and recognize phishing attempts and malicious URLs is also an integral part of any modern security solution. As the majority of threats today come from the internet, it's important to properly control internet access for specific websites that are known to be unsafe. In addition, legitimate websites can also be compromised and until they are fixed, they also can be blocked by URL- or web-filtering.

Typically, URL-filtering functionality is delivered from a cloud reputation base, in the case of Acronis, the Acronis Cloud Brain detects and blocks malicious URLs using:

- **Acronis' signatures**
- **Acronis' AI-based detection technology**
- **Intelligence from industry partners including the Anti-Phishing Working Group**

It's wise to keep local detection rules for malicious and phishing URLs in case of internet connection disruptions, a capability included in all of our cyber protection solutions. Acronis URL-filtering is enhanced by a machine learning model that's built by analyzing links and page structure (headers, content, and so on).

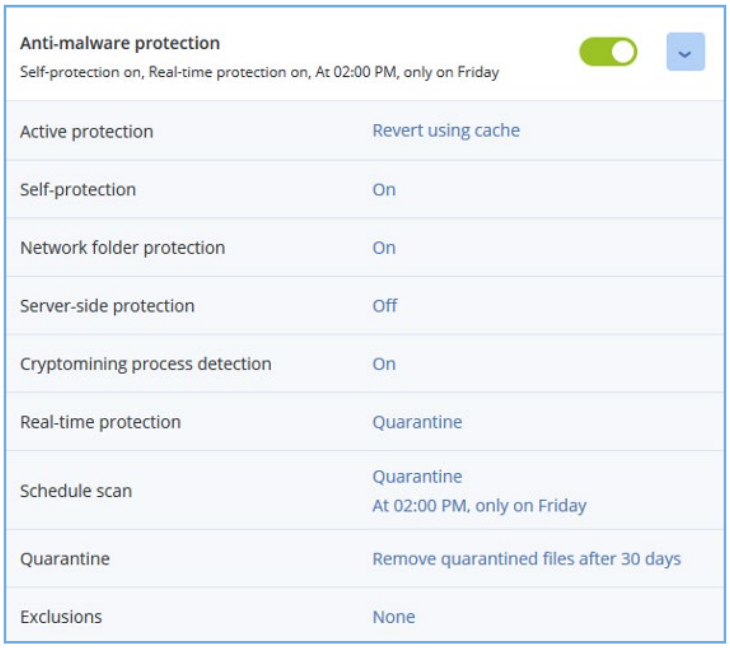


Traditional signature-based anti-malware engine for known threats

While proactive technologies focused on catching zero-day threats are very important, having a signature-based engine as part of your security solution still makes sense because of how responsive it is. It compares the sequence of bytes with a local database on the endpoint agent, a process much faster than other detection technologies that make requests to the cloud. Signature-based detection also offers you the additional reassurance of protection against all known threats that could still be a problem. Eventually, most of the cloud, behavioral, and AI-generated detection methods, make their way to signatures as well, just to make the detection process faster.

However, signature-based engines can vary in effectiveness. Imagine you have a lot of obsolete, incorrect, or corrupted records. This can decrease the performance of your scanning engine. You can also imagine cases when companies don't know the threats and only create a few signatures, limiting what their engine can identify. Acronis Cyber Protection products license one of the best classic engines on the market, ensuring excellent performance and coverage.

Additionally, it's important to know how anti-malware records are updated in these engines. Acronis implemented effective and distributed peer-to-peer-based updates that don't create a bottleneck by relying on one server (source) to distribute updates to a few hundred machines in the network. With P2P updates, as soon as one machine gets a new base, another one can get it as well without having to wait for the update server.



Full Microsoft Windows compatibility

As a member of the Microsoft Virus Initiative, Acronis delivers a recognized certified anti-malware solution for Windows that can replace Windows Defender. Acronis follows all Microsoft recommendations and created a fully ELAM-compatible driver for its products. Early Launch Anti-Malware (ELAM) is a Windows 8 (and newer) security technology that evaluates non-Microsoft Windows boot time device/application drivers for malicious code. It is the first system kernel driver that starts in the Windows operating mode, before any third-party software or driver. In Acronis Cyber Protect, Windows Security Center integration is fully protected by Protected Process Light (PPL, an ELAM-based technology that ensures an operating system only loads trusted services and processes). Acronis Cyber Protect also protects the main anti-malware

services with PPL. This allows Acronis software to achieve the highest level of self-protection, covering the core anti-malware modules other solutions don't.

In the Acronis Cyber Protect management console, admins are able to:

- **Enforce settings across multiple machines**
- **Ensure that anti-malware bases are up-to-date on all machines**
- **See all Windows Defender detection events**

Confirm your cyber protection works

While many security companies say they can protect your data and environment, they aren't all made equal. When you're choosing a cybersecurity solution, we recommend you start by setting your priorities. The ultimate goal for every business is to be profitable. Any disruption in business or loss of credibility costs a lot of money.

Since no solution guarantees 100% security, you will want a solution that provides the ability to be up and running quickly after an incident. A multilayered cybersecurity solution should be able to detect as many threats as possible and provide you with a chance to evaluate its detection capabilities. This can be done by checking various independent tests from companies like AV-Test or AV-Comparatives.

It is always better to test for yourself if you have the ability to do so. And if a threat is missed you should check how quickly you can recover deleted or damaged data or get a user's machine up and running again. Because eventually, the costs associated with a malicious data loss event can be much higher than the immediate losses from the malware itself.

BACKUPS SCAN FOR MALWARE

Anti-malware scanning is typically performed on an endpoint or a server. However, if these machines are being fully backed up (disk images being made), it also makes sense to scan this full disk image at the centralized location it is stored. In this case, a load on an endpoint or a server can be reduced. That's also a good way to check mobile laptops and other machines that are not available on corporate network premises all the time.

Acronis can scan backup files in a centralized location (either in the cloud or on premises). But, Acronis can do more than just scan these full images. Every new slice can be checked for malware. You can learn how in a this white paper.

Acronis

Learn more at
www.acronis.com