

Acronis is a Leader in **Cyber Protection**

AI-powered **Cyber Protection**, Cyber Cloud, Cyber Platform

Swiss

Since 2008 Corporate HQ in Schaffhausen, Switzerland

Singaporean

Founded in 2003 in Singapore, currently the International HQ

Dual Headquarters for Dual Protection



Scale & Rapid Growth

\$300M+ billings
50% business growth
100%+ cloud growth



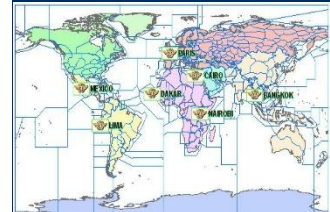
Cyber Reach

100% of Fortune 1000
50,000+ partners
500,000+ businesses
5,500,000+ prosumers



Global Local Presence

1,500+ employees
33+ locations
150+ countries
33+ languages
DCs in 100+ countries in the next 12 months



304 Flight Information Regions (FIR)

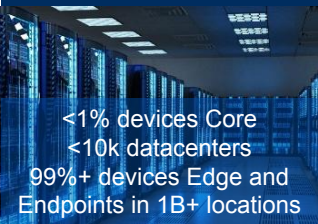


Protecting Digital World Has Major Challenges

Digital workloads are mission critical but very fragile – need protection!

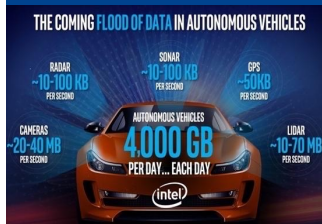
Complexity

Rapid growth of number of systems and locations:
< 50B devices in 2020, 500B+ by 2030



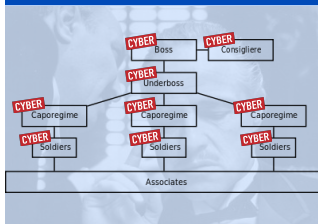
Cost

Accelerating growth rate of amount of data and workloads:
50ZB+ in 2020, 500ZB+ by 2030



Security

Industrialization of cyber crime, AI & exploit automation, ransomware, zero-day exploits, exploit-as-a-service



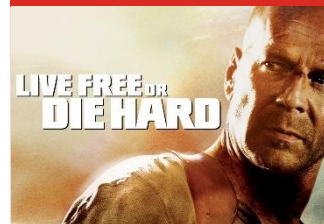
Privacy

A **protection** platform vendor independent from a **production** platform vendor is required to enable freedom of choice



5th Basic Need

The digital world is the 5th basic human need. The world can't go on without IT anymore



Robotic arms in VW (Skoda Auto) car factory

Solution: Integrated and Autonomous **Cyber Protection**

Acronis mission is to protect all data, applications and systems (Workloads)



Acronis Cyber Protection for Humanity

Similarities of biological and computer threats – Acronis partners are “doctors”

Biological

Digital

Prevention
(Proactive, Active)

Vaccination, good hygiene, healthy lifestyle, social distancing

Detection
(Active)

Screening of symptoms, RNA/DNA tests, antibody tests, leukocytes

Response
(Active, Reactive)

Immune system response, antiviral drugs, antibiotics, ICU, healthcare system

Recovery
(Reactive)

Macrophages to remove dead tissue, osteoblasts rebuild, interferons killing cells

Forensics
(Reactive, Proactive)

Genome sequencing, pathogen study, contact tracing to connect cases into clusters

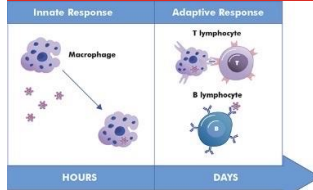
Vulnerability assessments, patch management, smart protection plans, self-protection, cyber protection management

AI-based threat detection, behavioral protection, AI-based injection detection, entropy analysis, rootkit detection in backups

Blocking of malware execution, automatic file recovery from backups, malware removal from backups and production system, new heuristics

Instant recovery from backups, automated disaster recovery, cyber protection management, desktop and assistance

Metadata and memory dump storage with backups for incident investigations, cyber protection recovery and forensics manager



Acronis Cyber Singularity

Autonomous, Integrated and Modular **Cyber Protection** for everybody

Acronis Cyber Protect

Cyber Protection

Available on-premises and as a cloud service



Acronis Cyber Cloud

Resellers & Service Providers

15k+ resellers & 30k+ service providers in 2022



Acronis Cyber Platform

Integrating & customizing cyber protection

100k+ certified developers in 2022



Acronis Cyber Infrastructure

Cloud, hardware and software appliances
300+ Acronis DCs, 3,000+ Partner DCs for compute and storage after 2022



Acronis Cyber Services

Premium support, Acronis #CyberFit Academy, marketing, sales and development services



International Space Station (ISS) – autonomous, integrated and modular system

Acronis Cyber Engine – Autonomous

Cyber Protection Innovations: 300+ patents, 75+ new filed every year

Acronis Business

Cloud
Infra

Cloud
Identity

Cloud
Services

Cloud
Infra

Cloud
Identity

Cloud
Services

Independent

Cyber Learning

Self-learning AI with human feedback enforcement, deploys without configuration, adapts to new situations



Cyber Autonomous

Disconnected execution of AI-engine, high frequency of tests and learning, no dependency on connection



Cyber Hybrid

Execution next to data, real-time response to attacks, multiple-level of execution, Acronis Cyber Bus technology for integration



Cyber Bus

Integration technology on Acronis Cyber Platform – connecting systems, syncing data and enabling protection workflows



Cyber SAPAS

Engine collects all metadata and events, enables safety, accessibility, privacy, authenticity and security

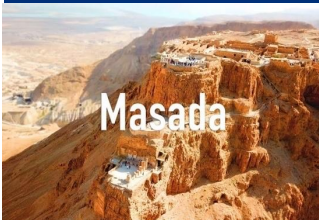


Acronis Cyber Protect

All-in-one protection designed for IT professionals

Proactive Protection

Vulnerability assessment and patch management, malware removal from backups, patching on recovery



Active Protection

Continuous data protection (CDP), malware detection and prevention, self-defense for agents and backups



Reactive Protection

Instant restore, disaster recovery, bare metal recovery, metadata for forensics investigations



Designed for Integration

Integration with RMM, PSA and security suites, SDK and APIs for integration with MSP tools



Productivity & Efficiency

Cyber protection manager, pre-configured plans, data protection map, secure remote connection



Acronis Cyber Protect – Integrated Security

Unique set of technologies for endpoint protection in a single product

Core Anti-Malware Tech

- NextGen engine for real-time and on-demand scans
- AI-based static analyzer
- Dynamic behavioral protection
- Cloud reputation analysis for allow/block lists
- Threat-agnostic heuristics based on data access

Advanced AI-Based Security

- Autonomous Cyber Engine
- URL filtering
- Identity protection
- Script analyzer
- System-health prediction
- Semantic search with similarity discovery
- Automatic smart backup plans, prediction of data importance

Preventive Security

- 0-day attach prevention
- Self-protection of agents & backups
- Vulnerability assessments for discovery of unpatched and unconfigured systems
- Automated patch management for operating system and 3-rd party apps

Security Management

- Secure remote desktop access
- #CyberFit score for workstations
- Point-to-site VPN access to managed corporate networks
- Remote wipe for deprecated devices
- Windows Defender management – enforcing settings, forcing AV-definitions update

Backup Integration

- Automatic backup before patching
- Patching of images on recovery
- “Allow/Deny” list Offline backup malware scanning
- Backup scan and update on recovery
- Automated recovery of damaged files
- Meta-data for forensics

Acronis Cyber Protect – Unique Advantages

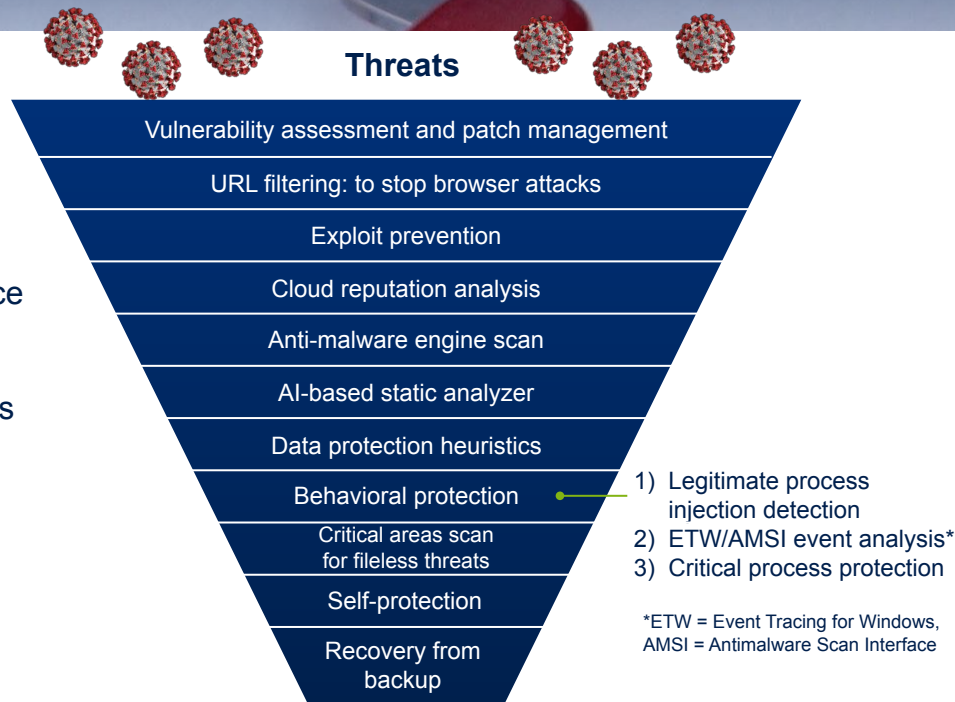
Complete, integrated, autonomous endpoint protection

	Automatic instant recovery	No dependency on connectivity	Forensic data in backups	Application protection	Multi-layer detection
Acronis	Damaged files recovered automatically. Three layers of data protection: local cache, local backup and cloud backup	Autonomous execution of AI-based engine: real-time protection in environments with poor connectivity, high frequency of local scans	Metadata and memory dumps stored in backups for future forensic investigation	Prevention of DLL-injections, registry settings protection, protection from DNS spoofing; application sandboxing coming soon	Real-time and on-demand scanner, AI-based detection engine, behavioral protection, signature engine – augmenting protection, allow-lists
Legacy Vendors	Recovery of files from a local cache – limited in number of files and size of files for recovery	Limited local detection capabilities without access to Cloud-based detection engine, delays with database updates for signature-based solutions	Limited or no data collection by traditional endpoint security solutions; for EDR packages forensic data collection limited to production system	System-level protection, specific application protection is not offered	Signature-only scans missing zero-day attacks, AI-only scanners prone to false-positive detections, allow-lists from production data only

Acronis Cyber Protect – Protection Funnel

All-in-one protection in a single product

- **Acronis expertise in backup and low-level I/O gives advantage in heuristics**
- New malware techniques, for example RIPlace using symlinks for encrypting files evade discovery by Microsoft, Symantec, Sophos, McAfee, CrowdStrike, Malwarebytes scanners
- Acronis protects against malware's evasive techniques working with low-level data
- Agent and backups self-protection: automatic recovery as last layer of protection



WastedLocker Ransomware: Garmin paid \$10M

Acronis successfully prevents WastedLocker at multiple levels

Vulnerability assessment and patch management

URL filtering: to stop browser attacks

Exploit prevention

Cloud reputation analysis

Anti-malware engine scan

AI-based static analyzer

Data protection heuristics

Behavioral protection

Critical areas scan for fileless threats

Self-protection

Recovery from backup

Malware is detected and blocked (RTP) Today, 20:07

Anti-Malware Protection has detected and blocked the malware 'Trojan.GenericKD.43531595' during the real-time scan.

Device	VM-1-NAB00
Plan name	full protection
File name	wasted_locker_ransomware.bin
File path	C:\samples
MDS	2cc4534b0d0e1c8d5b89644274a10c1
SHA1	735ee2c15c0b7172f65d93f0fd33b9186ee69653
SHA256	905ea119ad8d3e54cd228c458a1b5681abc1f35d7f8297
Threat name	Trojan.GenericKD.43531595

1. Anti-Malware scan engine blocks WastedLocker

Vulnerability assessment and patch management

URL filtering: to stop browser attacks

Exploit prevention

Cloud reputation analysis

Anti-malware engine scan

AI-based static analyzer

Data protection heuristics

Behavioral protection

Critical areas scan for fileless threats

Self-protection

Recovery from backup

Malware is detected and blocked (RTP) Jul 26, 2020, 04:16

Anti-Malware Protection has detected and blocked the malware 'Malware.GenericML' during the real-time scan.

Device	DESKTOP-32F1F4M
Plan name	Default
File name	sample.exe
File path	C:\Users\VP_Research\Desktop
MDS	2cc4534b0d0e1c8d5b89644274a10c1
SHA1	735ee2c15c0b7172f65d93f0fd33b9186ee69653
SHA256	905ea119ad8d3e54cd228c458a1b5681abc1f35d7f82977a23812ec4ef0288a
Threat name	Malware.GenericML
Action taken	Moved to quarantine

2. Pre-execution detection with static AI-based analysis of files

Vulnerability assessment and patch management

URL filtering: to stop browser attacks

Exploit prevention

Cloud reputation analysis

Anti-malware engine scan

AI-based static analyzer

Data protection heuristics

Behavioral protection

Critical areas scan for fileless threats

Self-protection

Recovery from backup

Suspicious activity is detected Jul 26, 2020, 01:03

Device	DESKTOP-32F1F4M
Process	C:\Users\VP_Research\AppData\Roaming\Provider
Monitored because	Process certificate is not valid
Suspicious because	Binary format has been changed for several files.
Action	Revert using cache
Affected files	E:\Aa\Images\12x.png E:\Aa\Images\download.jpg E:\Aa\Images\Acronis\Storage\2016.png E:\Aa\Images\download.png E:\Aa\Images\front_sap2.jpg E:\Aa\Images\saas_dragon.png E:\Acronis_updates\Updates\Malware_Update\ave\db1\Plugins\update.xt E:\Acronis_updates\Updates\Malware_Update\ngmp.zip E:\Acronis_updates\Updates\VAPM_Update\va_pm_db.db

3. Behavioral engine detection during execution with full rollback

Acronis Cyber Protect – Scenario Analysis

0-day Maze ransomware sample infected 9 machines in Xerox, 2 more were not patched sufficiently and were rendered inoperable.

Acronis Cyber Protect

- 9 machines recovered immediately
- 2 machines restored from the cloud within 1 hours due to CDP
- Back to business in 1 hours

Detection time: **0h**
detected by Active Protection heuristics*

Total loss: **\$100** (\$50/hour x 2)

CrowdStrike and CommVault with Immutable Backups

- Ransomware not detected
- 11 machines locked out
- 8 hours of data lost since last backup (no active protection, no CDP)
- 3 hours for image backup recovery
- 33 hours downtime, 88 recovery time

Detection time: –
No detection after 25 days (25 Aug 2020)

Total loss: **\$6,050**

Webroot and Veeam Backup

- Ransomware not detected
- 11 machines locked out
- Backups deleted (no self-protection)
- No data recovery possible
- Ransom is paid

Detection time: –
No detection after 25 days (25 Aug 2020)

Total loss: **\$200,000**

* An MD5 hash of the recent sample: fa73f50d62ba1a469c4bd2cac80df838

Acronis Cyber Protect – Detection Times

VirusTotal detection time delays for modern ransomware stain

Ragnar Locker

- Acronis **0 hours**
- Bitdefender **0 hours**
- CrowdStrike +168 hours
- Kaspersky +168 hours
- Microsoft +168 hours
- SentinelOne > 1 week
- Symantec +204 hours
- TrendMicro +291 hours
- Webroot +395 hours

CLOP

- Acronis **0 hours**
- Bitdefender +19 hours
- CrowdStrike **0 hours**
- Kaspersky +19 hours
- Microsoft **0 hours**
- SentinelOne **0 hours**
- Symantec +19 hours
- TrendMicro **0 hours**
- Webroot +69 hours

DoppelPaymer

- Acronis **0 hours**
- Bitdefender +133 hours
- CrowdStrike **0 hours**
- Kaspersky +11 hours
- Microsoft +11 hours
- SentinelOne **0 hours**
- Symantec +11 hours
- TrendMicro **0 hours**
- Webroot +288 hours

Only Acronis detected all ransomware samples without a delay!














Acronis Cyber Protect – Comparison

Most efficient replacement for traditional endpoint protection

	Acronis	Symantec	Webroot
Core endpoint protection	Real-time anti-malware & anti-ransomware protection	★★★★	★★★★
	On-demand scanning and malware removal	★★★★	★★★★
	Pre-execution AI-based analyzer	★★★★	★★★
	Behavioral analysis and dynamic detection rules	★★★★	★★★
	Zero-day exploit prevention	★★★★	★★★
	Disk and master boot record protection	★★★★	★★★★
	Real-time malicious cryptominer protection	★★★★	★★★★
	Self-protection	★★★★	★★★★
Additional	Vulnerability assessment and patch management	★★★★	★★★
	URL filtering and categorization	★★★★	★★★★
	Email security (often managed by Exchange or Office 365)	★★★★ Q1'21	★★★★
	Firewall (often Windows Firewall managed via domain policies)	★★★★ Q1'21	★★★★
	Data Loss Prevention (DLP)	★★★★ Q4'20	★★★
	Endpoint Detection & Response (EDR)	★★★★ Q1'21	separate
New	Zero-trust assessment and management	★★★★ Q4'20	★★★★
	Cyber protection recovery manager	★★★★ Q4'20	★★★★
	Cyber protection forensic manager	★★★★ Q4'20	★★★★

Acronis Cyber Protect – Industry Recognition

Recognized by top security alliances, tests and certifications

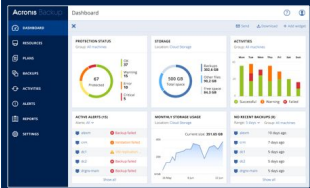
 MVI member	 VIRUSTOTAL member	 Cloud Security Alliance member
 Anti-Malware Testing Standard Organization	 Anti-Phishing Working Group member	 MRG-Effitas participant and test winner
 Anti-Malware Test Lab participant and test winner	 ICSA Labs certified	 NioGuard Security Lab test winner
 AV-Comparatives approved business security product	 VB100 certified	 AV-Test participant and test winner
 FIPS 140-2 certified cryptographic library	 ISO 27001:2013 and ISO 9001:2015 compliant	 GDPR compliant
 GLBA and HIPAA compliant	 TAA compliant	 EU-US and Swiss-US Privacy Shield certified

Acronis #CyberFit Everything

Get your #CyberFit level assessment at go.acronis.com/score

#CyberFit Workloads

Automated assessment and scoring of protection level of workloads



#CyberFit Customers

Assessments, solutions and services for increasing #CyberFit level



#CyberFit Partners

Partner program, partner community, education and partner tools



#CyberFit Countries

Partners, sales and marketing, product capabilities for local needs



#CyberFit Sports

Deployment with top sports team – showcasing Acronis Cyber Protect in demanding IT environments



organizations

incident

hour

victimized



Next Steps

Get #CyberFit with **Acronis Cyber Protect**

Get #CyberFit Score

Run automated assessment tool to check your score

go.acronis.com/score

Download the Product

Download and install Acronis Cyber Protect on all your devices

go.acronis.com/get

Get Trained

Learn about Acronis Cyber Protect capabilities

go.acronis.com/demo

Protect Everybody

Protect protect your customers, employees, friends and family

go.acronis.com/get

Become an MSP

Provide Acronis Cyber Protect service – and get help from Acronis to build your business

go.acronis.com/msp