

# Acronis Detection and Response



## PREVENT ATTACKS IN REAL-TIME AND GAIN DEEP VISIBILITY INTO EVERY CYBERTHREAT

Acronis Detection and Response is a last line of defense that protects your organization against threats that evade your anti-malware defenses. Designed around the zero trust approach, the solution detects and prevents any deviations from legitimate OS behavior and provides real-time visibility, as well as automatic and manual remediation capabilities.

THREAT-AGNOSTIC SECURITY	REAL-TIME THREAT PREVENTION	FOCUSED AND DETAILED VISIBILITY
Add threat detection and response to supercharge your endpoint security. Prevent attacks that evade anti-malware defenses, including new or unknown malware and ransomware, fileless attacks, zero-days, and advanced persistent threats (APTs)	Stop being reactive to security breaches by deploying a proven solution that automatically prevents the damage from occurring. No manual threat hunting, costly infrastructure, or cloud connectivity is required	Empower your security team with granular visibility into attack timelines, origin, tactics, techniques, and procedures (TTPs), as well as information on what the attackers attempted to accomplish, to strengthen your organization's security posture

## PROTECT YOUR ENDPOINTS AND DATA FROM ATTACKS OTHERS MISS


MINIMIZE CYBER RISKS / PREVENT ANY THREAT	ENSURE RAPID INCIDENT RESPONSE	LEVERAGE YOUR EXISTING RESOURCES TO THE FULLEST
<ul style="list-style-type: none"> <li>• Detect and prevent advanced attacks that bypass your anti-malware defenses – new or unknown malware, fileless attacks, zero-day threats, APTs</li> <li>• Add a last-line-of-defense security layer to enhance your current capabilities to stop breaches before they harm your organization's assets</li> <li>• Adopt a "zero-trust" approach and catch any deviations from legitimate OS behavior</li> <li>• Works in air-gapped and offline environments</li> </ul>	<ul style="list-style-type: none"> <li>• Reduce the time needed to respond to threats with automatic prevention capabilities</li> <li>• Empower your SOC team with detailed visibility into every attack</li> <li>• Leverage automatic and manual remediation capabilities</li> <li>• Continuously monitor endpoint and network activity across the entire organization</li> <li>• Get access to detection and incident response services managed by Acronis' security professionals for ultimate protection and peace of mind</li> </ul>	<ul style="list-style-type: none"> <li>• Reduce the need for additional resources with focused and detailed visibility into threats without unnecessary noise</li> <li>• Supplement your other anti-malware solutions – no need for a rip and replace</li> <li>• Low impact on endpoint performance and bandwidth consumption</li> <li>• Optimize your TCO with no need for additional staffing or costly infrastructure</li> </ul>

## BENEFIT FROM A MODERN APPROACH TO THREAT PREVENTION

Acronis Detection and Response adds post-breach threat detection and response capabilities to your security stack. Identify and stop threats that have bypassed other defense layers while empowering your cybersecurity team with deep, forensic analysis on each incident.

AUTOMATIC, REAL-TIME PROTECTION	THREAT-AGNOSTIC PROTECTION	ZERO TRUST APPROACH	NO DATA DELUGE	LOW TCO
Automatically stop threats once detected, unlike solutions that require manual or semi-manual threat hunting and remediation.	Detect and prevent advanced attacks that evade next-generation antiviruses (NGAVs) such as new or unknown malware and ransomware, fileless attacks, zero-day attacks, and APTs.	Increase threat detection accuracy with a zero trust approach, recognizing any deviations from legitimate OS behavior instead of having to identify constantly evolving attack techniques.	Empower your security team with detailed, focused visibility into threats and incidents without the need for manual threat hunting and analysis of overwhelming amounts of data.	Lower your total cost of ownership (TCO) via automated threat hunting and low bandwidth consumption. Leverages existing resources and infrastructure.

## ICSA LABS CERTIFIED SOLUTION

 ICSA Labs Advanced Threat Defense <i>Certified</i>	TEST LENGTH	TEST RUNS	MALICIOUS SAMPLES	PERCENT DETECTED	INNOCIOUS APPS	PERCENT FALSE POSITIVES
	33 days	1162	441	100%	721	0.1%

### FLEXIBLE DEPLOYMENT OPTIONS

**On-premises deployment**  
Leverage your existing IT infrastructure and deploy the solution on your premises

**Cloud deployment**  
Get in a software-as-a-service (SaaS) deployment model to cut maintenance and upkeep costs



**LEARN MORE**

