



+

Acronis

Discern Security + Acronis Cyber Protect Cloud

Integration Data Sheet

Turn Acronis protection data into continuous posture insights, prioritized risk, and accountable action.

Acronis Cyber Protect Cloud integration with Discern

Discern connects Acronis protection telemetry with broader security and business context so teams can continuously assess posture, identify configuration and coverage gaps, prioritize what matters most, and coordinate remediation. Discern helps transform fragmented posture and tool data into a defensible plan with measurable progress.

Key benefits

Turn telemetry into actionable insight

Unify protection events, policy status, configuration, and coverage data into a context-rich posture view.

See risk the way the business does

Combine asset criticality, control gaps, and business context so teams know what to fix first and why.

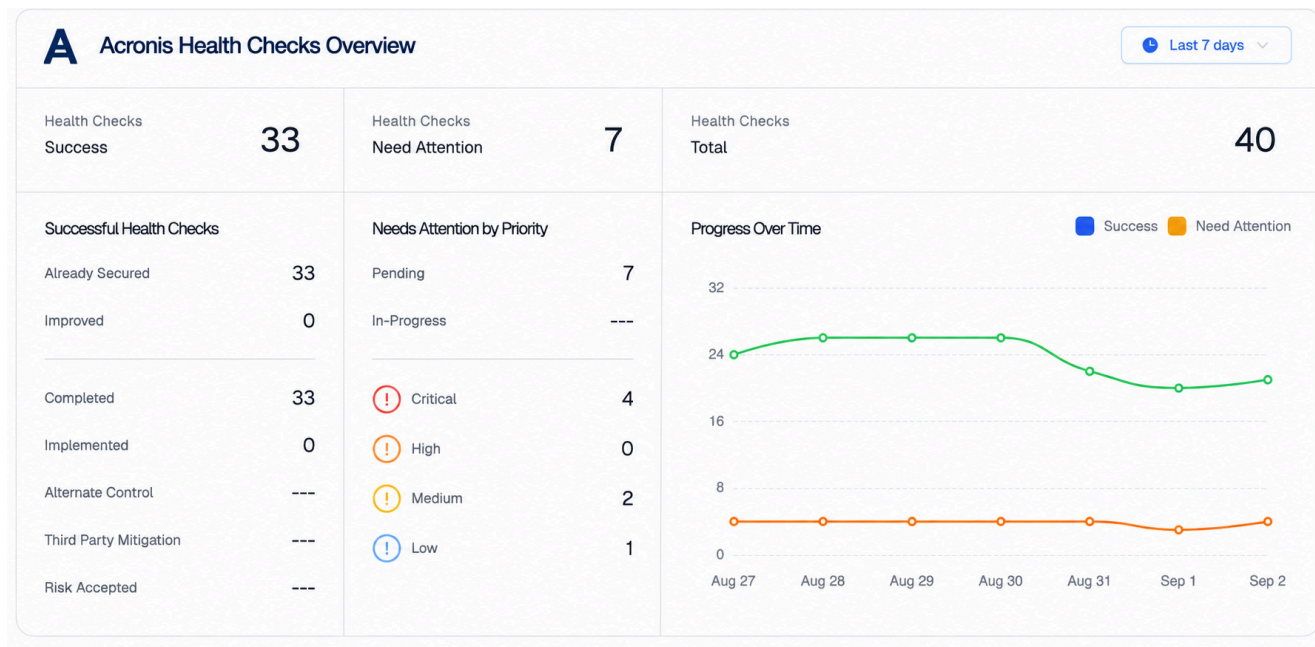
Find and close coverage gaps

Surface unprotected, offline, outdated, or misconfigured endpoints and workloads before blind spots become risk.

Accelerate remediation with guardrails

Create tickets, assign owners, enforce approvals, and track progress from finding to fix without losing governance.

Future-state Acronis health posture view



Illustrative planned integration experience. Actual fields and availability depend on Acronis APIs and enabled services.



How the integration works

Acronis security and endpoint telemetry is enriched with security-stack and business context, then converted into prioritized, trackable actions.

Acronis Cyber Protect Cloud → Discern

Planned data used from Acronis:

- Endpoint/device inventory
- Agent and protection status
- Configuration and policy information
- Agent and component versions
- Protection and security telemetry
- Vulnerability information
- Backup security status
- Tenant/customer context for MSP environments

Availability depends on Acronis APIs, licensing, and enabled services.

Discern AI Security Loop

OBSERVE	Collect posture and security signals across the stack.
ORIENT	Add asset criticality, control gaps, and business context.
PRIORITIZE	Focus teams on the highest-risk issues first.
ACT	Drive tickets, owners, approvals, and remediation workflows.
MEASURE	Track progress, control health, and measurable risk reduction.

Integration profile

Integration	API-based
Platform	Acronis Cyber Protect Cloud
Deployment	No additional Discern endpoint agent
Primary users	MSPs, MSSPs, security, and IT teams
Use cases	Posture, coverage, prioritization, and remediation

Planned Acronis health checks

Examples of checks: Discern plans to evaluate against Acronis configuration, protection status, agent health, and coverage.

MALWARE & THREAT PROTECTION

- Ensure Anti-malware Protection Is Enabled and Properly Configured
- Ensure Generative AI Protection Controls Are Enabled
- Ensure Windows Defender Antivirus Protection Is Enabled
- Ensure Active Protection Is Enabled Against Ransomware and Suspicious Activity
- Ensure Endpoint Detection and Response Is Enabled
- Ensure Microsoft Security Essentials Protection Is Enabled

WEB, DATA & BACKUP PROTECTION

- Ensure URL Filtering Is Enabled to Block Malicious and Risky Websites
- Ensure Data Protection Map Is Enabled for Sensitive Data Visibility
- Ensure Backup Scanning Is Enabled to Detect Malware in Backup Data

VULNERABILITY & PATCH MANAGEMENT

- Ensure Patch Management Is Enabled and Configured for Regular Updates
- Ensure Vulnerability Assessment Is Enabled for Continuous Risk Detection

PROTECTION PLAN & AGENT HEALTH

- Ensure Complete Protection Plan Is Enabled for Workloads
- Ensure Acronis Agent Installer Is Up to Date
- Ensure Acronis Agent Components Are Up to Date
- Ensure Acronis Agent Has Protection Components Installed
- Ensure Acronis Agent Auto-Update Is Enabled
- Ensure Acronis Automatic Agent Update Is Not Suspended

AVAILABILITY & COVERAGE

- Acronis-Protected Device Is Offline

Example health-check detail view

Acronis Health Checks						
Health Check Name	Status	Priority	Resource type	Security Benefit	Effort	Productivity Impact
Ensure Antimalware Protection Is Enabled and Properly Configured	✓	Critical	Organization	High	Medium	Low
Ensure Generative AI Protection Controls Are Enabled	✓	High	Organization	High	Medium	Medium
Ensure Windows Defender Antivirus Protection Is Enabled	✓	High	Organization	High	Low	Low
Ensure Active Protection Is Enabled Against Ransomware and Suspicious Activity	⚠	Critical	Organization	High	Medium	Medium
Ensure URL Filtering Is Enabled to Block Malicious and Risky Websites	✓	High	Organization	High	Low	Low
Ensure Data Protection Map Is Enabled for Sensitive Data Visibility	⚠	High	Organization	High	Medium	Medium
Ensure Backup Scanning Is Enabled to Detect Malware in Backup Data	✓	High	Organization	High	Medium	Low
Ensure Patch Management Is Enabled and Configured for Regular Updates	⚠	Critical	Organization	High	High	Medium
Ensure Endpoint Detection and Response Is Enabled	✓	Critical	Organization	High	Medium	Low
Ensure Vulnerability Assessment Is Enabled for Continuous Risk Detection	⚠	High	Organization	High	High	Medium
Ensure Microsoft Security Essentials Protection Is Enabled	✓	High	Organization	Medium	Low	Low

