Acronis Technology Ecosystem

Security integrations – MDR, XDR and SIEM Connector

With Acronis security integrations, you can reduce the time and cost to respond to threats, differentiate yet simplify your service stack by using a unified platform and increase stickiness with customers by offering full-circle protection.

MDR integrations

Acronis MDR is a 24/7/365 managed detection and response (MDR) service built for MSPs of any size and maturity. Delivered via a global network of SOC providers and trusted MSSP partners — and integrating threat response and data protection to deliver unmatched business resilience.

Integration category	Vendor	Region	Description
Acronis MDR partners	Legato OpenText	Global	Global, strategic Acronis MSSP partners with proven track records, ensuring piece of mind for partners that want to outsource their EDR and XDR management.
Acronis MSSP Program	CyberNordic DIAMATIX OpSys	Nordics Bulgaria, UAE Australia	Regional MSSP partners deliver Acronis MDR (based on Acronis EDR and XDR) with localized expertise and compliance alignment, helping to scale services cost efficiently.

XDR integrations

With Extended Detection and Response (XDR) integrations in the Acronis Ecosystem, you can deliver advanced security services - from data collection and enrichment to incident investigation - across critical attack surfaces, without added complexity.

Integration category	Vendor	Description
XDR	Fortinet FortiGate Microsoft 365 Fortinet FortiMail Workspace Security Microsoft Entra ID	These integrations enhance Acronis EDR and XDR with telemetry and response actions across these tools.

Start your free 30-day trial of Acronis Cyber Protect Cloud

TRY NOW

Browse the Acronis Ecosystem

SEE ALL INTEGRATIONS

Copyright © 2003-2025 Acronis International GmbH.

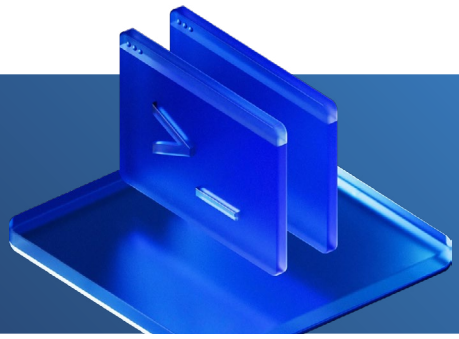
Integrations enabled through Acronis SIEM Connector

The Acronis SIEM Connector makes integration seamless. Integrated directly into protection plans, it uses the Acronis agent as the data writer — eliminating the complexities around generating certificates and applying custom settings to a syslog server — and exports alerts, events, activities and tasks in either CEF or JSON format to a designated file path for ingestion by any SIEM platform. This simplifies data consolidation.

Integration category	Vendor	Description
SIEM	Coralogix Elastic Exabeam Exium Fluency Fortinet FortiSIEM Google Security Operations (SecOps) Graylog SIEM IBM QRadar LogSign Lumu for MSPs ManageEngine EventLog Analyzer ManageEngine Log360 Microsoft Sentinel NetWitness Logs Rapid7 InsightIDR RocketCyber SentinelOne Singularity Data Lake Splunk Trellix	These integrations and many more can be enabled through the Acronis SIEM Connector. The SIEM Connector uses the Acronis agent as a log writer, enabling MSPs to store: • Alerts • Events • Activities • Audit Log on any endpoint or a syslog server in the customer network with an Acronis agent installed, where the SIEM agent can then ingest the logs. The Acronis SIEM Connector supports CEF and JSON log formats.

Try the Acronis SIEM Connector

TRY NOW



Acronis

Learn more at
www.acronis.com

Copyright © 2003–2025 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2025-11