Storage Guardian

Acronis

Acronis Cyber Protect Cloud Integration with Storage Guardian

CyberSecurity Reinvented: Acronis and Storage Guardian Unite For Ultimate Protection

Acronis Cyber Protect Cloud integration with Storage Guardian

The integration of Acronis Cyber Protect Cloud with Storage Guardian's Incident Response Planner brings together NIST 2.0 framework into the Acronis EDR and MDR ecosystem by leveraging our workflows together with Storage Guardian's covert way of communicating for tabletop exercises and preparing for zero-day events. The templates including PICERL approach (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) and ISHP (Initial Security Handling Procedures) are hosted for you allowing quickly gathering templates and customizing them for each customer at a low cost.

Acronis Cyber Protect Cloud for Service Providers

Service providers that are focused on Acronis EDR and MDR from their SOC team, can leverage the integration for users to have the ability to share the Runbook templates with their customers to prepare for tabletop exercises, engage management in the process of CyberSecurity, get a hold of organizations that are not typically part of the IT such as management teams, insurance brokers or other stakeholders that are often not included in the notification of an incident.

ABOUT ACRONIS CYBER PROTECT CLOUD

The only single-agent solution that natively integrates cybersecurity, data protection and management to protect data, endpoints and systems.

THE WORLD'S BEST BACKUP AND RECOVERY

Full-image and file-level backup and recovery safeguard data on more than 20 platforms — with near-zero RPOs and RTOs.

ENHANCED WITH ESSENTIAL CYBER PROTECTION AT NO ADDITIONAL COST

Acronis' advanced AI-based behavioral detection engine stops malware, ransomware and zero-day attacks on client endpoints and systems.

WITH PROTECTION MANAGEMENT BUILT FOR SERVICE PROVIDERS

Thorough post-incident investigation and proper remediation tools keep costs down for service providers — digital evidence is collected and stored in a secure central repository.

Benefits for service providers

- **Enhanced Incident Monitoring:** Allows SOC/NOC teams to track and manage incidents efficiently.
- **Rapid Stakeholder Engagement:** Supports quick communication via covert methods like SMS.
- **Zero-Day Readiness:** Helps organizations prepare for and practice responses to emerging threats.
- **Resilience in Communication Disruptions:** Ensures coordination even when traditional channels fail.
- **Seamless Integration** – Easily integrates with existing SP workflows and IT environments without disruption.
- **Faster Disaster Recovery** – Reduces downtime with structured incident response planning and automated recovery processes.

Acronis Cyber Protect Cloud integration with Storage Guardian use cases

Storage Guardian's NIST 2.0 Cyber Incident Response integration with Acronis Cyber Protect Cloud provides a cost-effective, comprehensive solution for incident response, enabling seamless tabletop exercises, real-time SOC/NOC monitoring, and secure stakeholder engagement via covert methods, ensuring organizations stay resilient against zero-day threats and communication disruptions.

Pain point 1

There is no centralized tool to manage and broadcast fluctuating alerts from the SOC team to key stakeholders. Currently, alerts are often relayed to a single individual—sometimes via voicemail, who then has to manually inform others. This delays incident response, creates communication gaps, and makes it difficult to coordinate effectively across different teams, including insurance companies and other critical stakeholders.

Pain point 2

Most service providers and IT professionals conduct successful tabletop exercises, but they often lack integration with Acronis and ready-to-use templates for post-exercise reporting. Without these resources, engaging management and ensuring compliance with the NIST 2.0 framework becomes more challenging.

Pain point 3

Incident response plans are often stored on paper or within the same network that has been breached, making them inaccessible during a crisis. Additionally, there is no tool to dynamically manage fluctuating incidents, align SLAs with the SOC team, and streamline communication between stakeholders. Without an integrated solution, organizations struggle to declare incidents promptly, create service tickets, and coordinate an effective remediation process.

Scenario 1

The integration of Acronis Cyber Protect Cloud with Storage Guardian's Incident Response Planner offers a powerful, all-in-one solution combining CyberSecurity and disaster recovery. It delivers proactive threat protection and structured incident response in a single platform, easily integrated into existing IT environments with minimal disruption. The solution is scalable, ensuring businesses and service providers can meet evolving needs while minimizing downtime and enhancing compliance. Features like enhanced monitoring, zero-day readiness, and faster recovery help businesses stay ahead of threats and improve efficiency. For example, a healthcare provider used the solution to proactively detect cyber threats and automate backups, ensuring minimal disruption and rapid recovery during attacks, safeguarding critical data and maintaining operations with little downtime.

> Recently our Ransomware insurance provider mandated us to have an Incident Response plan to comply with insurance using the Storage Guardian's DR Runbook we were able to comply with insurance provider requirements.
>
> **Sarah Mitchell, Head of IT Security, Financial Services Firm**

> I have worked with Storage Guardian for over 15 years on numerous disaster recovery and data protection initiatives. Throughout our collaboration, I have found their expertise to be highly professional and consistently aligned with my expectations, both for myself and my customers. Their commitment to preparedness and excellence has been invaluable, and I highly recommend them.
>
> **Booki Yakobi, Director of IT Operations, "Infinity Networks"**

About Storage Guardian

Storage Guardian is a comprehensive data protection and disaster recovery solution designed to help businesses effectively manage and respond to CyberSecurity incidents. It provides a structured, scalable approach to incident response, enabling companies to detect, plan for, and recover from cyber threats with minimal disruption. The platform integrates seamlessly with existing IT environments, offering features like enhanced incident monitoring, covert communication during disruptions, and faster recovery. With its focus on simplicity, adaptability, and compliance, Storage Guardian helps organizations maintain business continuity, reduce downtime, and improve overall security posture.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore and headquartered in Switzerland, Acronis now has more than 2,000 employees and offices in 34 locations worldwide. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.

Acronis

Learn more at
www.acronis.com