SOLUTION BRIEF

Fortinet and Acronis Cyber Protect Cloud Security Solution

Unified Cyber Protection with Advanced Security Monitoring

Executive Summary

The Fortinet and Acronis integrated solution combines Acronis Cyber Protect Cloud comprehensive data protection and cybersecurity capabilities with Fortinet FortiSIEM powerful security information and event management features. This integration enables organizations to enhance their security posture by centralizing threat detection and response operations, allowing teams to monitor, detect, and respond to security incidents from a single pane of glass while leveraging Acronis' advanced cyber protection technologies.

The Challenge

MSP organizations face increasingly sophisticated cyberthreats while managing complex IT environments, often with limited security resources. These security teams also frequently struggle with siloed security tools that create visibility gaps, delay incident response, and increase management overhead. Adding to the challenge, the growing volume of security alerts from multiple customer environments and disparate systems can lead to missed critical threats and increased vulnerability to data breaches and ransomware attacks. To address these challenges, organizations need integrated solutions that consolidate security monitoring and incident data collected from multiple locations.

Joint Solution

The integration of Acronis Cyber Protect Cloud and Fortinet FortiSIEM enables organizations to streamline security operations, improve threat detection capabilities, and enhance incident response times by consolidating Acronis security events, alerts, and audit logs into the FortiSIEM unified security management platform.

Solution Components

Acronis Cyber Protect Cloud provides data protection, cybersecurity, and endpoint management tools in one solution.

Acronis SIEM Connector is a specialized integration component that enables Acronis Cyber Protect Cloud to transmit Alerts and Audit Logs to third-party SIEM systems. The connector converts Acronis security data into Common Event Format (CEF) and sends it via syslog, ensuring compatibility with major SIEM platforms.

Fortinet FortiSIEM provides the centralized IT/OT event collection, advanced detection analytics, incident management, and other NOC/SOC functions that today's security teams need. Built on UEBA analytics, a unique CMDB, and GenAI assistance, this intuitive analyst experience supports all aspects of threat investigation, incident response, and compliance validation for organizations of any size.

Solution Components

- Acronis Cyber Protect Cloud
- Acronis SIEM Connector
- Fortinet FortiSIEM

Solution Benefits

- Enhanced threat detection through integration of Acronis' cyber protection technologies with FortiSIEM correlation capabilities
- Improved operational efficiency with centralized security monitoring and alerting
- Faster incident response through automated alert prioritization
- Simplified compliance with consolidated logging and reporting capabilities
- Unparalleled security protection with the Fortinet Security Fabric

FORTINET FABRIC-READY

Solution Integration

The integration between Acronis Cyber Protect Cloud and Fortinet FortiSIEM operates via the Acronis SIEM Connector, which streams security events and alerts from Acronis to FortiSIEM in real time using the CEF over syslog. When Acronis Cyber Protect Cloud detects a security event—such as malware, ransomware activity, or policy violation—the SIEM Connector formats these alerts in CEF and forwards them to a secure syslog server. FortiSIEM can then consume this data.

FortiSIEM receives these alerts, normalizes the data, and correlates it with other security events from across the network. This integration enables security analysts to view Acronis security events alongside other security data in the FortiSIEM unified dashboard, prioritize alerts based on severity, and initiate rapid response actions when threats are detected. The combined solution enhances an organization's security posture by providing visibility into security events while leveraging Acronis' cyber protection capabilities.

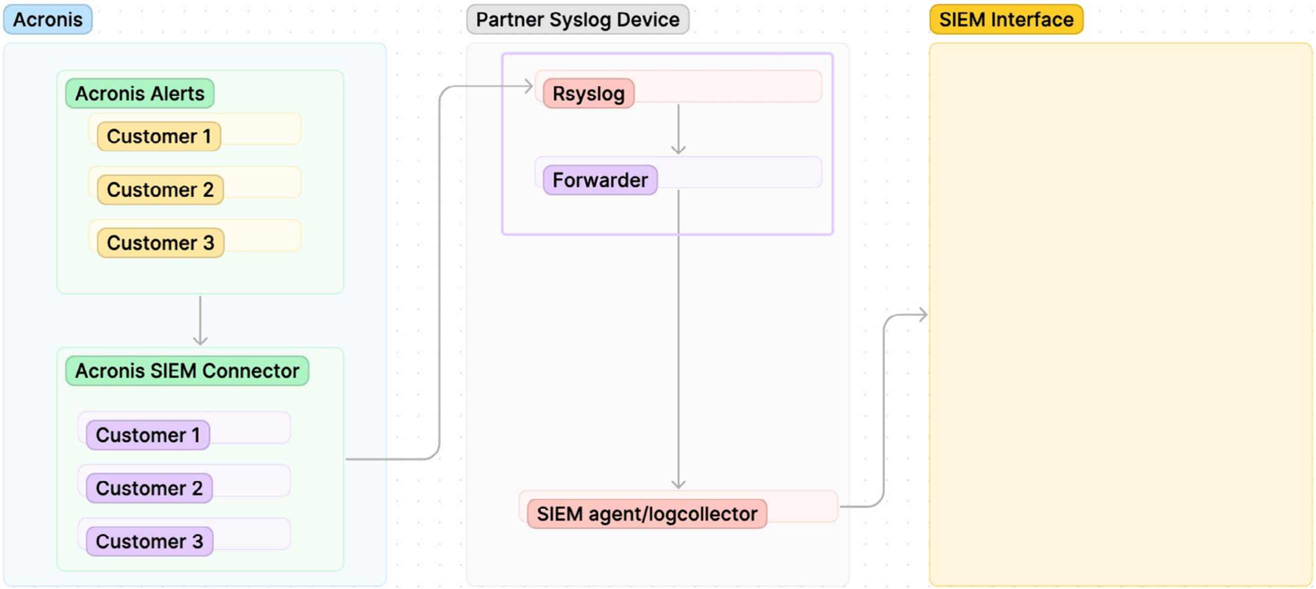

Figure 1: Acronis SIEM Connector architecture

Learn more about this integration.

The Acronis SIEM connector enables MSPs to see Acronis alerts in any SIEM solution that ingests CEF syslog format data. The SIEM connector is a CEF forwarder that sends Acronis alert data to a secure syslog server.

Joint Use Cases

Use Case #1: Ransomware Detection and Response

When Acronis detects ransomware activity on protected endpoints, it immediately triggers alerts, which are forwarded to Fortinet FortiSIEM. Security teams can view these high-priority events in the FortiSIEM dashboard, correlate them with other network activities, and orchestrate a coordinated response across the security infrastructure to prevent lateral movement and minimize damage.

Use Case #2: Security Policy Compliance Monitoring

The integrated solution enables continuous security policy compliance monitoring across all Acronis-protected systems by sending Acronis Audit Log data to Fortinet FortiSIEM. When Acronis detects policy violations such as missing patches, disabled protection features, or unauthorized configuration changes, these events are transmitted to FortiSIEM for centralized monitoring, alerting, and reporting.

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs), and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate, and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 15 offices worldwide and employees in 50+ countries. Acronis Cyber Protect is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses. Learn more at www.acronis.com.