SOLUTION BRIEF

Fortinet and Acronis Security Solution

AI-Guided Prevention, Protection, Response, and Recovery for the Most Vulnerable Attack Surfaces, Designed for MSPs

Executive Summary

Fortinet and Acronis have partnered to deliver an award-winning security solution designed for MSPs to modernize their service stacks and unlock unmatched resilience. Get complete, natively integrated, AI-guided protection to swiftly prevent, detect, analyze, respond to, and recover from incidents across the most vulnerable attack vectors: endpoints, email, identity, networks, and Microsoft 365 apps.

The Challenge

Cyberattacks have become increasingly sophisticated, targeting multiple vectors beyond the endpoint, and every business is vulnerable. To protect their clients, MSPs offering security services have had to choose between insufficient, incomplete protection, or complex solutions that are expensive and time-consuming to deploy and maintain.

Acronis and Fortinet have partnered to deliver complete, natively integrated protection, accessible for organizations of any size and specifically built for MSPs. With the integration of Acronis XDR and FortiGate Next-Generation Firewall (NGFW), service providers can easily and quickly prevent, detect, analyze, respond to, and recover from incidents across the most vulnerable attack surfaces.

Joint Solution

Acronis and Fortinet have partnered to deliver an industry-leading security solution to address these challenges. With this Fabric-Ready integration and using the Acronis CyberApp Integrations framework, you can benefit from an easy-to-setup, easy-to-use interaction between both technologies that leverages the rich API capabilities of the Fortinet FortiGate NGFW.

Solution Components

Fortinet FortiGate NGFWs protect data, assets, and users across today's hybrid environments. Built on patented Fortinet security processors, FortiGate NGFWs accelerate security and networking performance to effectively secure the growing volume of data-rich traffic and cloud-based applications. FortiGate NGFWs, backed by FortiGuard AI-Powered Security Services, help you prevent cyberattacks and mitigate security risks with consistent, real-time protection and responses against even the newest and most sophisticated threats.

Acronis XDR, designed for service providers, enables you to simplify endpoint protection by rapidly detecting, analyzing and remediating advanced attacks while ensuring unmatched business continuity. Eliminate the cost and complexity of multiple point products and enable your team with one complete cyber-protection solution that is simple to manage and deploy.

Solution Components

- Fortinet FortiGate Next-Generation Firewall
- Acronis Cyber Protect Cloud Advanced Security + XDR

Solution Benefits

- Consolidate cybersecurity, data protection, and management to proactively prevent risks, actively stop threats, and reactively ensure unmatched business continuity
- AI-guided analysis and remediation and response automation, streamlining analysis and response to just minutes
- Built for MSPs to unlock up to 60% better ROI compared to point solutions
- Leverage the Fortinet FortiGate NGFW for unparalleled network security protection

FORTINET FABRIC-READY

Solution Integration

When a network artifact is involved in a security incident, a new Fortinet node will be created in the XDR Graph, offering both the reputation details and the ability to block said resource in FortiGate.

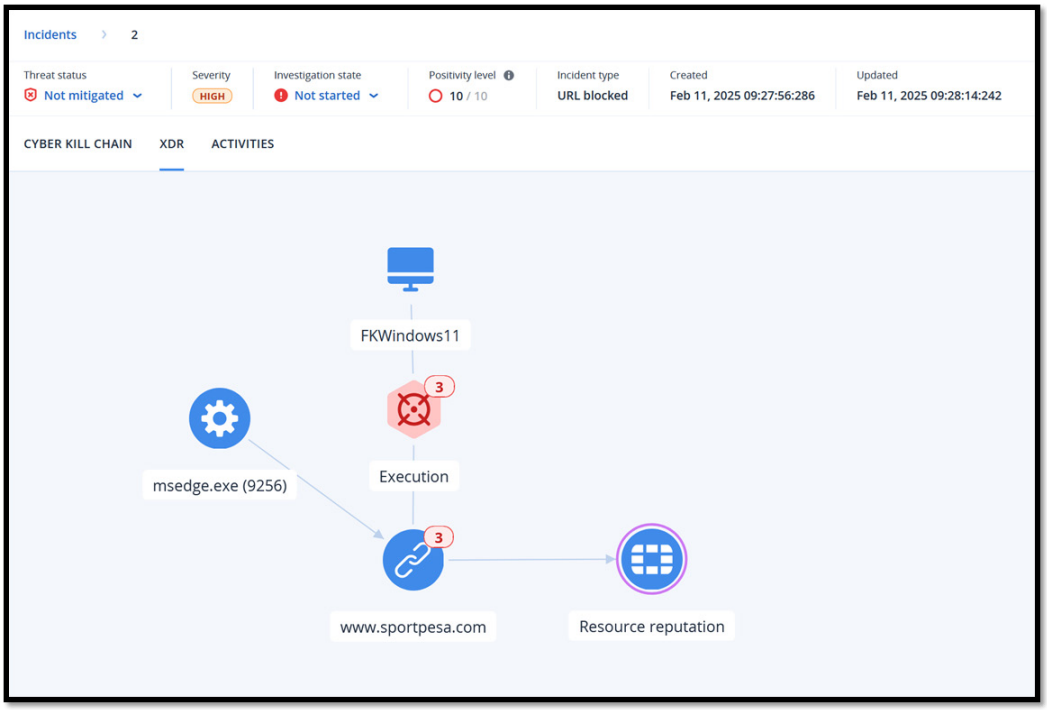

Figure 1: Access Fortinet's resource reputation info and response actions from within the XDR

Figure 2: Block multiple resources and consult the status of the actions

Use Cases

Swiftly react to network-based security threats with Fortinet's intelligence

Security analysts can leverage Fortinet's advanced threat intelligence capabilities to obtain a verdict more quickly and easily, centrally accessing specific details of any network artifact detected by Acronis Cyber Protect Cloud XDR.

Expand response capabilities by enabling corporate-level blocking of any network threat using FortiGate NGFW

Prevent recurring threats, massive malware infections, or APT group campaigns. This blocking can be adapted to each company's network architecture, allowing the selection of policy or policies that will be used for the blockings.

Extend visibility, protection, and response to the most vulnerable attack surface

Correlate data from FortiGate NGFW and Acronis XDR to get visibility and response capabilities across multiple attack vectors, including endpoints, email, identity, networks, and Microsoft 365 apps.

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 govern, identify, protect, detect, respond, and recover from modern cyber threats with minimal downtime, ensuring data integrity and business continuity.

April 19, 2025 9:26 AM / MKTG-1249-0-0-EN