8 real-world MSP use cases with Acronis XDR

Introduction

Threats are more complex with attacks transpiring beyond endpoints. Nearly 40% of breaches involved compromised credentials and over 15% involved phishing.[1] While traditional phishing is straightforward, web application phishing is far more elaborate, and attacks on cloud-based email and collaboration accounts has intensified. With 29% of businesses citing data loss because of security breaches,[2] holistic protection is about more than just stopping cyberthreats.

To answer sophisticated attacks, extended detection and response (XDR) is essential. But the XDR market offers few options for MSPs that are affordable, easy to use and integrated. Additionally, many XDRs do not ensure recovery and business continuity. Up against these challenges, MSPs are unable to find an XDR they can right size for their IT resources, services and client needs.

Acronis XDR is built for MSPs and helps partners of all sizes offer competitive, XDR-based services to protect at-risk attack surfaces, recover clients from attacks and ensure cyber resilience.

Here are 8 practical use cases with Acronis XDR:

1 Expand protection and visibility across endpoints and the most vulnerable attack surfaces.

Maintaining visibility is a constant challenge for MSPs as client IT environments grow and increase in complexity. MSPs can fortify telemetry beyond endpoints and protect email, identity and Microsoft 365 applications with Acronis XDR. This enables technicians to gain critical insight into attacks and augment response actions whether the threat originated from or spread beyond an endpoint.

2 Detect and block advanced cyberattacks before a breach.

Advanced cyberthreats are notorious for evading conventional detection. Acronis XDR monitors and correlates events spanning endpoints, email, identity and Microsoft 365 environments. The solution detects and analyzes complex cyberthreats within minutes. Additionally, MSPs and clients can enjoy peace of mind knowing that common threats are blocked with Acronis' award-winning, behavioral-based protection.

3 Rapidly respond to threats before the damage is done.

Unlike many market-leading XDRs, Acronis XDR has preintegrated recovery to ensure business continuity. Reducing the impact of an attack is paramount to minimizing the financial, reputational and operational ramifications for clients. Before threats can do damage, Acronis XDR empowers IT to quarantine malicious processes, isolate workloads, remove dangerous URLs and files, and suspend compromised accounts.

[1] Verizon. "2024 Data Breach Investigations Report".
[2] InfoSecurity Magazine 2024.

Additionally, with many businesses under pressure to mitigate cyber risk, Acronis XDR empowers MSPs to limit client attack surfaces against future attacks with proactive and active security measures in place — such as patching vulnerabilities, blocking harmful email addresses and forcing password resets.

4 Enable clients to satisfy compliance and protect sensitive data.

Regulatory compliance requirements often include demonstrating ongoing measures to reduce cyber risk and protect sensitive data. When combined with Acronis Advanced Data Loss Prevention and Advanced Disaster Recovery, Acronis XDR protects clients against data loss, unauthorized access and transfer of sensitive data to help businesses maintain compliance, qualify for cyber insurance and satisfy industry regulations. Forensic data is also collected from backups to aid future investigations. Acronis XDR classifies and prioritizes incidents concerning sensitive data — giving IT technicians improved visibility into high-value assets.

5 Consolidate solutions and centralize management.

Juggling multiple-point solutions is both costly and taxing on MSP businesses. Not only does this deplete resources but also leads to technician burnout when security tool management becomes burdensome. Acronis XDR is a part of Acronis Cyber Protect Cloud, a robust solution ecosystem built for MSPs that helps them rapidly launch, scale and tailor their services with an MSP-class platform. With a consolidated approach, MSPs can enhance cost efficiency and simplify management with a unified service.

6 Accelerate incident investigations.

Alert fatigue is a predominant problem that contributes to technician burnout. With Acronis XDR, IT can leverage AI-prioritized incident lists to ensure legitimate incidents are addressed, and AI-generated attack summaries enable IT to act fast and swiftly grasp the context of attacks. MSP technicians can reduce time on analysis from hours to minutes with AI-generated attack interpretations across the MITRE ATT&CK Framework.

7 Ensure business continuity amid attacks.

XDR with recovery capabilities as an MSP is a rarity on the XDR market. The integrated recovery and disaster recovery included in response in Acronis XDR stands out against conventional XDR solutions. With built-in recovery, the solution ensures client business continuity and protects against data loss. After an attack, MSPs can roll back attack-specific damage or perform full recovery.

8 Demonstrate the competitive value of services.

Point solutions are costly and often do not give MSPs the flexibility to provision protection practically or efficiently — inhibiting the business from scaling. Acronis XDR has customizable widgets that enable IT to tailor security per client or across all MSP services. IT can schedule and automatically send reports to clients in their desired format.

About Acronis

Acronis is a global cyber protection company that provides highly efficient, natively integrated cybersecurity, data protection and endpoint management for MSPs. Acronis solutions identify, prevent, detect, respond, remediate and recover from advanced cyberthreats to ensure business continuity. Acronis Cyber Protect Cloud 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.

Don’t have the resources to implement on your own? Outsource security with Acronis MDR

EXPLORE MORE

Sign up for a 1:1 discussion to learn more about Acronis XDR

SIGN UP NOW

Acronis

Learn more at
www.acronis.com