

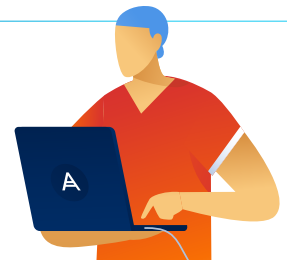
Acronis Advanced Security + XDR

Built for service providers

Modernize your security service stack

Cyberattacks become increasingly sophisticated and every business is vulnerable. To protect their clients, MSPs offering security services have had to choose between solutions that:

- Are insufficient — do not provide the needed level of protection.
- Offer incomplete protection — focus on partial remediation, and not business continuity.
- Introduce a high level of complexity — time consuming to implement, integrate and manage.
- Come at insurmountable cost — have heavy resource requirements and long-time-to-value.



Acronis XDR, the most complete security solution for MSPs

With Acronis XDR, MSPs get complete, natively integrated protection built for them to swiftly prevent, detect, analyze, respond to and recover from incidents across the most vulnerable attack surfaces.

Incidents > 2

Threat status: Not mitigated | Severity: HIGH | Investigation state: Investigating | Positivity level: 7 / 10 | Incident type: URL blocked | Created: May 13, 2024 ... | Updated: May 14, 2024 ...

CYBER KILL CHAIN | XDR | ACTIVITIES

Execution (1)

OVERVIEW

Details

First detected at: May 13, 2024 15:05:36:177
 Threat name: URL.UserBlockList
 Description: An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Link. Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via Exploitation for Client Execution. Links may also lead users to download files that require execution via Malicious File.

Severity: HIGH
 Tactic: Execution

Natively integrated	Highly efficient cybersecurity	Built for MSPs
<ul style="list-style-type: none"> Proactively prevent risks, actively stop threats and reactively ensure unmatched business continuity across NIST. Easily manage and scale with a single platform and agent to deliver all cybersecurity, data protection and endpoint management services. Ensure compliance and protect sensitive data with behavior-based DLP and best-of-breed disaster recovery. 	<ul style="list-style-type: none"> Protect endpoints with visibility across the most vulnerable attack surfaces, including email, identity and Microsoft 365 apps. Streamline analysis guided by AI and unlock rapid, single-click response. Improved performance on endpoints via a single agent for complete security: XDR, EDR, MDR, anti-malware and anti-ransomware, DLP, data protection, endpoint management and monitoring. 	<ul style="list-style-type: none"> Unlock superior ROI via a centralized platform that streamlines daily tasks and reduces costs. A SaaS-based, multitenant platform with role-based access that's easy to manage and scale across disparate client IT environments. Extend additionally with 200+ integrations, including ones commonly used by MSPs — SIEM, PSA, RMM tools.

Powered by award-winning endpoint protection

Editors' choice

AV-TEST participant and test winner





ICSA Labs endpoint anti-malware certified

Frost Radar™: Endpoint Security growth & innovation leader

IDC MarketScape: Worldwide Cyber-Recovery 2023: Leader

Unmatched business resilience with Acronis

With Acronis you can count on a single platform for holistic endpoint protection and business continuity. Aligned with established industry standards such as NIST, Acronis enables you to govern your cybersecurity strategy with ease, identify and proactively protect vulnerable assets and data, detect and stop threats, and respond to and recover from attacks.

 Govern	 Identify	 Protect	 Detect	 Respond	 Recover
Advanced Security + EDR					
<ul style="list-style-type: none"> Centralized policy management. Role-based management. Information-rich dashboard. Schedulable reporting. 	<ul style="list-style-type: none"> Hardware inventory. Unprotected endpoint discovery. 	<ul style="list-style-type: none"> Vulnerability assessments. Device control. Security configuration management. 	<ul style="list-style-type: none"> Threat telemetry across endpoints, identity, email, Microsoft 365 apps. AI- and ML-based behavioral detection and anti-ransomware. Exploit prevention and URL filtering. Search for IoCs. 	<ul style="list-style-type: none"> AI-based incident prioritization. AI-guided analysis. Remediation and isolation. Forensic backups. 	<ul style="list-style-type: none"> Rapid rollback of attacks. One-click mass recovery. Safe recovery.
Acronis Cyber Protect Cloud					
<ul style="list-style-type: none"> Provisioning via a single agent and platform. 	<ul style="list-style-type: none"> Software inventory Data classification. 	<ul style="list-style-type: none"> Patch management. DLP. Backup integration. Cyber Scripting. 	<ul style="list-style-type: none"> Email security. 	<ul style="list-style-type: none"> Investigation via remote connection. Scripting. 	<ul style="list-style-type: none"> Preintegrated with disaster recovery.

Modernize your security service stack today

Don't resort to multiple tools and XDRs with siloed focus on stopping threats. Modernize your service stack with Acronis XDR — built for MSPs to provide unmatched business continuity with ease and speed.

[LEARN MORE](#)



Don't have the resources to implement XDR on your own?

Acronis MDR is a simplified, reliable and efficient service built for MSPs and delivered via a platform that amplifies security effectiveness with minimal resource investment.

[→ Learn more about Acronis MDR](#)

Choose the protection suite that best fits your needs

Feature	Advanced Security + EDR	Advanced Security + XDR
Behavior-based detection	✓	✓
Anti-ransomware protection with automatic rollback	✓	✓
Vulnerability assessments	✓	✓
Device control	✓	✓
File- and system-level backup	✓ Pay as you go	✓ Pay as you go
Remediation, including full reimaging	✓	✓
Inventory collection	✓ (via Advanced Management)	✓ (via Advanced Management)
Patch management	✓ (via Advanced Management)	✓ (via Advanced Management)
Remote connection	✓ (via Advanced Management)	✓ (via Advanced Management)
Business continuity	✓ (via Advanced Disaster Recovery)	✓ (via Advanced Disaster Recovery)
Data loss prevention (DLP)	✓ (via Advanced DLP)	✓ (via Advanced DLP)
#CyberFit Score (security posture evaluation)	✓	✓
URL filtering	✓	✓
Exploit prevention	✓	✓
Real-time threat intelligence feed	✓	✓
Automated, tunable allowlisting based on profiling	✓	✓
Event monitoring	✓	✓
Automated event correlation	✓	✓
Prioritization of suspicious activities	✓	✓
AI-generated incident summaries	✓	✓
Automated MITRE ATT&CK® attack chain visualization and interpretation	✓	✓
Single-click response to incidents	✓	✓
Full threat containment including endpoint quarantine and isolation	✓	✓
Intelligent search for IoCs including emerging threats	✓	✓
Forensic data collection	✓	✓
Attack-specific rollback	✓	✓
Integration with Advanced Email Security (email telemetry)	✗	✓
Integration with Entra ID (identity telemetry)	✗	✓
Integration with Collaboration App Security (Microsoft 365 apps telemetry)	✗	✓
Delete malicious email attachment or URLs	✗	✓
Search for malicious attachments across mailboxes	✗	✓
Block malicious email address	✗	✓
Terminate all user sessions	✗	✓
Force user account password reset on next login	✗	✓
Suspend user account	✗	✓
MDR service	✓	✓