

# Acronis

## Advanced Security + Endpoint Detection and Response (EDR)

### Pour les fournisseurs de services

#### Simplifiez la protection des terminaux

Dans la mesure où plus de 60 % des compromissions impliquent une forme de piratage<sup>1</sup>, les entreprises doivent se doter de solutions de sécurité avancées et faire appel à des fournisseurs aptes à les aider à lutter contre les cybermenaces sophistiquées actuelles. Malheureusement, la plupart des solutions EDR capables de contrer ces menaces présentent plusieurs inconvénients :

- Coûts élevés et complexité, les rendant inaccessibles au plus grand nombre
- Long retour sur investissement, formation intensive et exigences en matière d'intégration
- Protection incomplète, nécessitant une intégration supplémentaire pour assurer la continuité des activités
- Défis d'évolutivité nécessitant un grand nombre d'experts en sécurité



Les fournisseurs de services en début d'activité ne disposent ni des compétences ni des moyens nécessaires pour lancer leur propre service EDR. En raison des surcoûts, même les fournisseurs déjà bien implantés dans le domaine de la cybersécurité risquent de perdre leurs clients issus des marchés intermédiaires ou de PME s'ils essaient de développer leurs propres services de détection et de réponse avec les meilleures solutions du secteur. Ils pourraient également se retrouver en concurrence avec les services MDR de leur éditeur de solutions.

#### Acronis Advanced Security + EDR, conçu pour les fournisseurs de services

Acronis sait que les fournisseurs de services doivent proposer une offre de services performante tout en tenant compte des exigences et des budgets propres à chaque client.

Pour ce faire, ils ont besoin d'une solution de sécurité avancée en mode SaaS, adaptée au maintien de leurs marges et à leurs compétences internes, offrant une gestion multitenant, une protection renforcée et un niveau

d'automatisation et de convivialité assurant une activation et une montée en charge rapides au sein des environnements propres à chaque client.

Conçu pour les fournisseurs de services, **Acronis Advanced Security + EDR** simplifie la protection des terminaux : la solution permet de détecter, d'analyser et de neutraliser rapidement les attaques avancées, tout en assurant efficacement la continuité des activités. Éliminez les coûts et la complexité qu'impliquent plusieurs solutions spécialisées et offrez à votre équipe une solution de cyberprotection complète, simple à gérer et à déployer.

# Optimisez vos services de détection et de réponse avec Acronis

<b>Priorisation et analyse avancées des attaques pour une réponse rapide</b>	<b>Fonctionnalités de sauvegarde et de restauration intégrées pour assurer efficacement la continuité des activités</b>	<b>Solution de cyberprotection complète, conçue pour les MSP, en un seul agent</b>
<ul style="list-style-type: none"> <li>• Simplifiez les investigations grâce à la priorisation des incidents potentiels et à la réduction de la désensibilisation aux alertes.</li> <li>• Réduisez le délai d'investigation de plusieurs heures à quelques minutes à grande échelle, avec une corrélation automatisée et des interprétations des attaques guidées par l'intelligence artificielle.</li> <li>• Une mise en correspondance plus claire avec le cadre MITRE ATT&amp;CK® permet de comprendre facilement l'analyse et l'impact des attaques, y compris la méthode utilisée par le cybercriminel pour s'introduire dans l'environnement et propager l'attaque, de même que l'ampleur des dommages causés.</li> </ul>	<ul style="list-style-type: none"> <li>• Fonctionnalités de sauvegarde et de restauration intégrées pour préserver la continuité des activités là où les solutions spécialisées échouent</li> <li>• Correction et restauration optimisées, en un clic</li> <li>• Protection complète et intégrée couvrant tout le cadre de cybersécurité NIST (identifier, protéger, détecter, répondre et restaurer) à l'aide d'une seule solution</li> </ul>	<ul style="list-style-type: none"> <li>• Lancez rapidement et facilement de nouveaux services au moyen d'un seul agent et d'une seule console pour déployer, gérer et monter en charge.</li> <li>• Montez en charge facilement pour répondre aux besoins de nombreux clients, tout en préservant vos marges et en minimisant les dépenses d'exploitation (OPEX), sans devoir faire appel à une équipe étendue d'experts hautement qualifiés.</li> <li>• Collaborez avec un éditeur qui a votre réussite à cœur et soutient votre activité, sans vous faire concurrence.</li> </ul>

## Optimisé par une technologie primée de protection des terminaux

<p><b>Prix de la rédaction</b></p>	<p><b>Gagnant des tests AV-TEST</b></p>	<p><b>Certification VB100</b></p>	<p><b>Certification de protection antimalware pour terminaux octroyée par ICSA Labs</b></p>	<p><b>Certification AV-Comparatives</b></p>
------------------------------------	---	-----------------------------------	---	---

## Résilience optimale avec Acronis

Grâce à Acronis, une seule plate-forme vous offre une protection complète des terminaux et la continuité des activités, en accord avec les normes et bonnes pratiques du secteur telles que le cadre NIST. Vous pouvez ainsi identifier les ressources et données vulnérables, les protéger de façon proactive, détecter et bloquer les menaces, réagir aux attaques et en réparer les dommages.

### Acronis : continuité des activités conforme au cadre NIST

 <b>Identifier</b>	 <b>Protéger</b>	 <b>Détecter</b>	 <b>Répondre</b>	 <b>Restaurer</b>
<b>Advanced Security + EDR</b>				
<ul style="list-style-type: none"> <li>• Inventaire des matériels</li> <li>• Détection des terminaux non protégés</li> </ul>	<ul style="list-style-type: none"> <li>• Évaluation des vulnérabilités</li> <li>• Prévention des exploits</li> <li>• Contrôle des terminaux</li> <li>• Configuration de la sécurité</li> </ul>	<ul style="list-style-type: none"> <li>• Flux de cybersécurité sur les menaces émergentes</li> <li>• Recherche des indicateurs de compromission face aux menaces émergentes</li> <li>• Protection antimalware et antiransomware</li> <li>• Détection des comportements anormaux basée sur l'intelligence artificielle</li> <li>• Filtrage des URL</li> </ul>	<ul style="list-style-type: none"> <li>• Analyse rapide des incidents</li> <li>• Correction des ressources par isolement</li> <li>• Sauvegardes riches en données d'investigation numérique</li> </ul>	<ul style="list-style-type: none"> <li>• Restauration rapide après une attaque</li> <li>• Restauration en masse en un clic</li> <li>• Restauration en libre-service</li> </ul>
<b>Acronis Cyber Protect Cloud</b>				
<ul style="list-style-type: none"> <li>• Inventaire des logiciels</li> <li>• Classification des données</li> </ul>	<ul style="list-style-type: none"> <li>• Gestion des correctifs</li> <li>• Prévention des fuites de données (DLP)</li> <li>• Intégration des sauvegardes</li> <li>• Scripts de cyberprotection</li> </ul>	<ul style="list-style-type: none"> <li>• Protection de la messagerie</li> </ul>	<ul style="list-style-type: none"> <li>• Investigation via une connexion à distance</li> </ul>	<ul style="list-style-type: none"> <li>• Reprise d'activité après sinistre pré-intégrée</li> </ul>

## Principales fonctionnalités EDR

### Priorisation des incidents

Surveillez et mettez automatiquement en corrélation les événements sur les terminaux en priorisant les séquences d'événements suspects sous forme d'alertes.

### Interprétation automatisée des incidents en correspondance avec le cadre MITRE ATT&CK®

Simplifiez la réponse et augmentez la réactivité aux menaces, grâce aux interprétations des attaques guidées par l'intelligence

artificielle et mises en correspondance avec le cadre MITRE ATT&CK®. En quelques minutes, vous pouvez comprendre :

- Comment le cybercriminel a infiltré le système
- Comment il a effacé ses traces
- Quels dommages l'attaque a causés et par quels moyens
- Comment l'attaque s'est propagée



## Réponse en un clic aux attaques pour assurer efficacement la continuité des activités

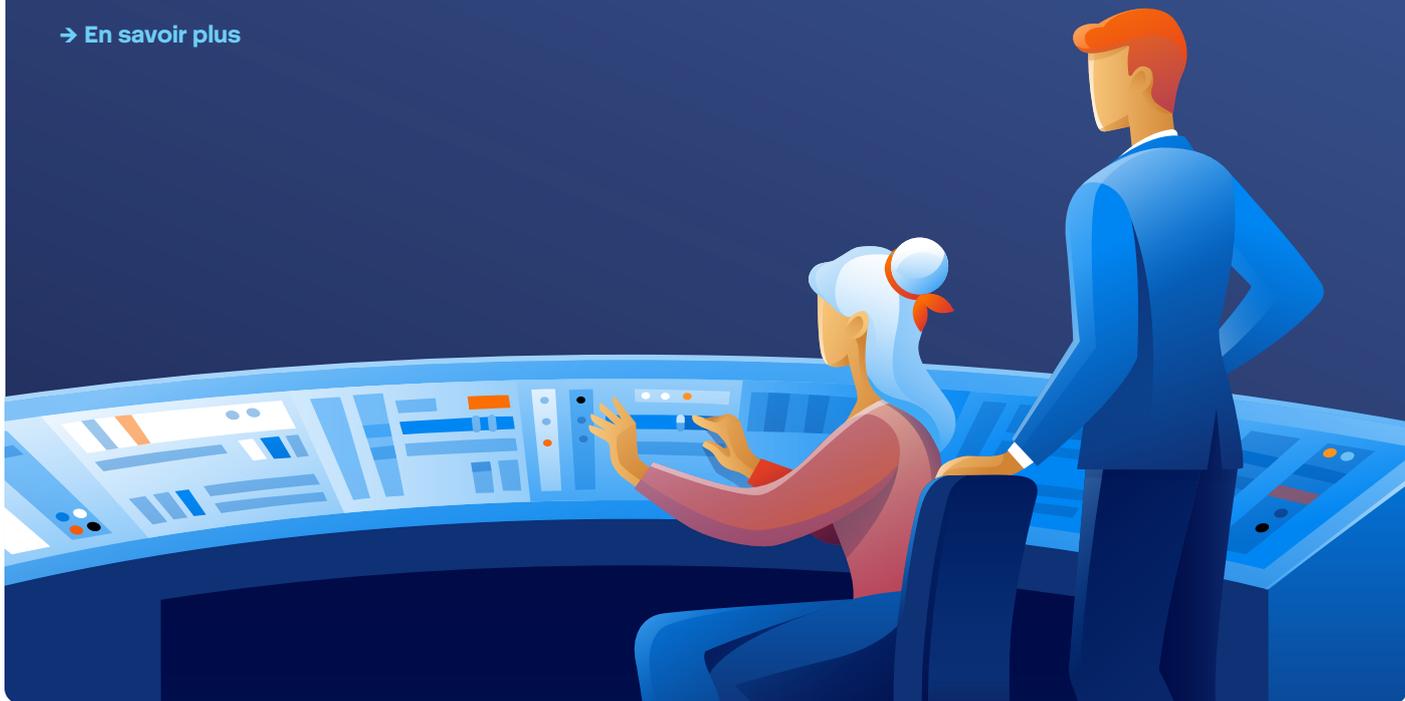
Profitez de fonctionnalités de cybersécurité, de protection des données et de gestion des configurations de sécurité des terminaux intégrées via une réponse en un clic aux incidents :

- **Corrigez** en isolant les terminaux et en mettant en quarantaine les menaces.
- **Enquêtez** au moyen de connexions à distance et de sauvegardes riches en données d'investigation numérique.
- **Prévenez les attaques futures** en éliminant les vulnérabilités.
- **Préservez la continuité des activités** grâce aux rétablissements spécifiques aux attaques et aux fonctionnalités intégrées de sauvegarde et de restauration.

### Simplifiez la protection des terminaux

Vous n'avez plus besoin d'une multitude d'outils et de compétences en sécurité de pointe pour protéger les terminaux. Simplifiez la protection des terminaux avec Acronis EDR.

→ [En savoir plus](#)



1. Source : « 2022 Data Breach Investigations Report », Verizon