Acronis

#CyberFit

Découvrez l'EDR/MDR Acronis conçu pour les MSP.

Nous commençons bientôt !

Acronis

- **Bienvenue à notre webinaire !**
- **Le webinaire est enregistré**
- **Veuillez soumettre vos questions via l'interface Zoom « Q&A »**

#CyberFit

Grégory Laroche

Senior Solutions Engineer
Acronis

La croissance des logiciels malveillants

300 000

Nouveaux échantillons de logiciels malveillants par jour en 2024

moins de 2 jours

Durée de vie moyenne des souches de logiciels malveillants

Vecteurs de cyberattaque typiques

Comment les attaquants s'introduisent-ils dans les entreprises ?

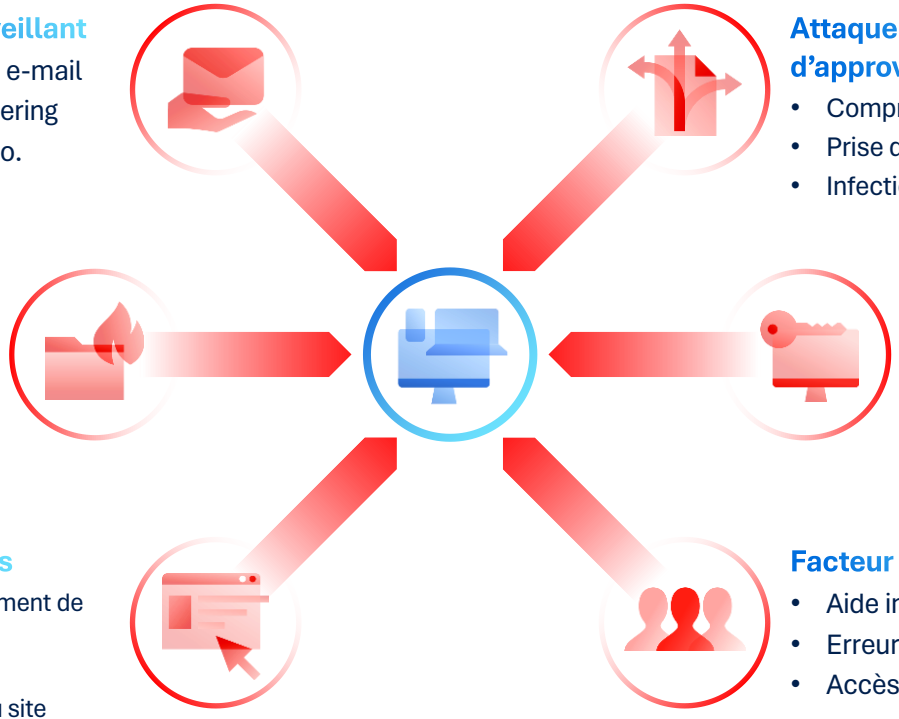
Message malveillant

Pièce jointe à un e-mail

- Social engineering
- ChatGPT & Co.

Attaque de la chaîne d'approvisionnement

- Compromis complet avec le fournisseur
- Prise de contôle d'un SaaS/MSP
- Infection de dépendance



Exploitation des services

- Service non corrigé
- Attaques sans fichier
- Mauvaise configuration

Informations d'identification connues

- Mot de passe par force brute
- Credential stuffing / phishing (hameçonnage)
- Dropper payant / Initial Access Broker

Cloud/sites Web malveillants

- Utilisation abusive d'un emplacement de confiance
- Téléchargement manuel
- Redirection / prise de contrôle du site

Facteur humain

- Aide interne
- Erreur humaine / complexité
- Accès physique

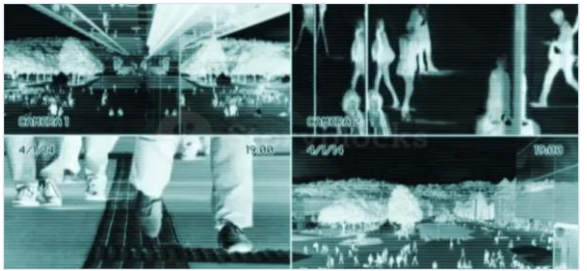
E-mails malveillants et outils utiles

QR Codes + MFA proxy

- E-mails avec des **QR codes** pour masquer les URL du filtrage
- Détourner des sessions pour contourner l'authentification multifacteur (par exemple **le kit d'hameçonnage de W3ll** qui contourne l'authentification multifacteur et détourne les comptes Microsoft 365)

Utiliser l'infrastructure

- Utilisez vos outils pour déployer des logiciels malveillants **(LOTL attack)** e.g. PSA, RMM and GPO
- Installer et **abuser d'applications propres**
- **MFA fatigue**/bombing/SIM swapping



Modifier les outils de protection

- **Supprimer les journaux** et les sauvegardes de sécurité
- **Désinstaller les outils** de sécurité
- **Ajouter des exclusions** pour C :\
- **Utiliser la sauvegarde** pour exfiltrer des données

Les ransomwares sont morts – Vive les ransomwares

Toujours facile à distribuer - et toujours très rentable

Augmenter la pression

- **Contacter** directement les clients finaux
- **Déclencher des amendes** pour atteinte à la vie privée, par exemple le RGPD
- **Attaques DDoS** pour détourner l'attention du SOC

Connaître la cible

- Trouver le stockage des données et **lire les e-mails**
- Tirer les leçons du **plan d'intervention** en cas d'incident
- Résolvez des cas d'assistance réels pour **gagner la confiance**

Adapter les techniques

- À la recherche de données dans le cloud (E.g. BlackCat/Sphynx encryptor attack Azure storage)

Arrêtez les ransomwares, la cybermenace la plus urgente de 2024

L'attaque la plus généralisée, la plus destructrice et la plus coûteuse sur la disponibilité de l'entreprise et l'intégrité des données

Haute fréquence

- Un ransomware frappe une autre entreprise **toutes les 11 secondes**
- **80% des entreprises** ont été attaquées [au cours des dernières années]
- **25 % des violations** incluent une charge utile de ransomware

Une complexité croissante

- **80 % des violations** sont des attaques **zero-day nouvelles** ou inconnues (par exemple, l'attaque Kaseya 2021)
- **Ransomware en tant que service (RaaS)**
- **Nécessite** une pléthore de solutions ponctuelles pour y répondre : protection des terminaux, protection des données, sécurité des e-mails, EDR/XDR

Augmentation des pertes des PME

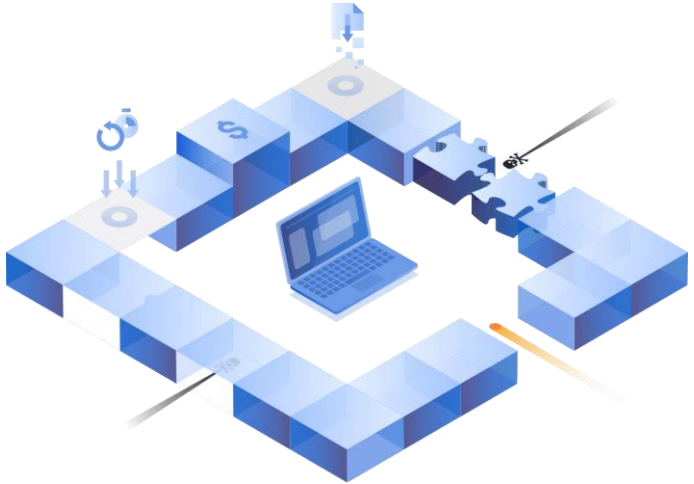
- **7 entreprises sur 10** ne sont pas prêtes à répondre à une attaque
- Rançon moyenne payée : **812 360 $**
- Coût moyen des temps d'arrêt : **5 600 $/minute**

Sources: "Data Breach Investigations Report', Verizon, 2022"; "Cost of data breach report", 2022, IBM Security & Ponemon Institute; "Cyber Threats Report", Acronis, 2022 ", "After The Fall: Cost, Causes and Consequences of Unplanned Downtime", ServiceMax

La protection est complexe : les défis des PME en 2024

Les entreprises sont confrontées à de nouvelles attaques de plus en plus sophistiquées visant la continuité des activités et les données critiques.

- Les ransomware continuent de progresser : ils restent la cybermenace la plus répandue et la plus destructrice.
  - La fréquence et **la sophistication des attaques** ne cessent de croître
  - **ChatGPT** est là, par exemple pour écrire des phising parfaits.
- **Manque de talents** en matière de cybersécurité et d'opérations informatiques
- **La multiplicité des outils** accroît les inefficacités et les lacunes potentielles en matière de couverture
- **La multiplicité des agents, des consoles et des licences** ajoute à la complexité et aux coûts.
- Un Framework de sécurité complet introduit **des coûts élevés et une grande complexité**
- L'intégration, la culture et la rétention des talents technologiques **restent un défi**



Comment les entreprises peuvent-elles faire face aux risques : continuité de l'activité et protection des données dans le cadre du programme NIST

Acronis Cyber Protect Cloud

IDENTIFY

- Inventaire des logiciels et matériels
- Découverte des endpoints non protégés
- Classification des données

PROTECT

- Évaluation de la vulnérabilité
- Contrôle des dispositifs
- Gestion de la configuration de la sécurité
- Gestion des correctifs
- DLP
- Intégration des sauvegardes

DETECT

- Fil d'information sur les menaces émergentes
- Prévention des exploits
- Recherche des IOCs de menaces émergentes
- Détection comportementale basée sur l'IA/ML
- Anti-malware et anti-ransomware
- Filtrage des URL

RESPOND

- Priorité et analyse rapides des incidents
- Remédiation de la charge de travail avec isolation
- Sauvegardes avec Forensic
- Investigation par connexion à distance

RECOVER

- Reprise rapide des attaques
- Récupération de masse en un clic
- Auto-récupération
- Pré-intégration avec la reprise après sinistre

Acronis Cyber Protect

Cybersécurité de nouvelle génération

Moteur de détection comportementale avancé basé sur l'IA pour la prévention des attaques de type "zero-day".

+

Sauvegarde et récupération fiables

Sauvegarde d'images complètes et de fichiers, reprise après sinistre et collecte de métadonnées à des fins d'analyse criminalistique de la sécurité

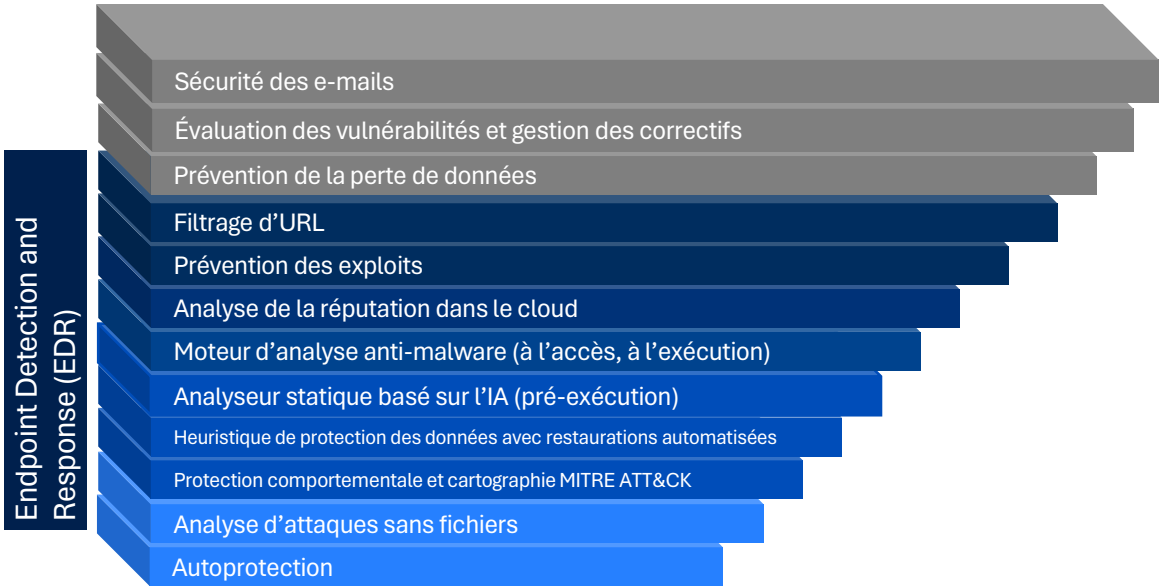
+

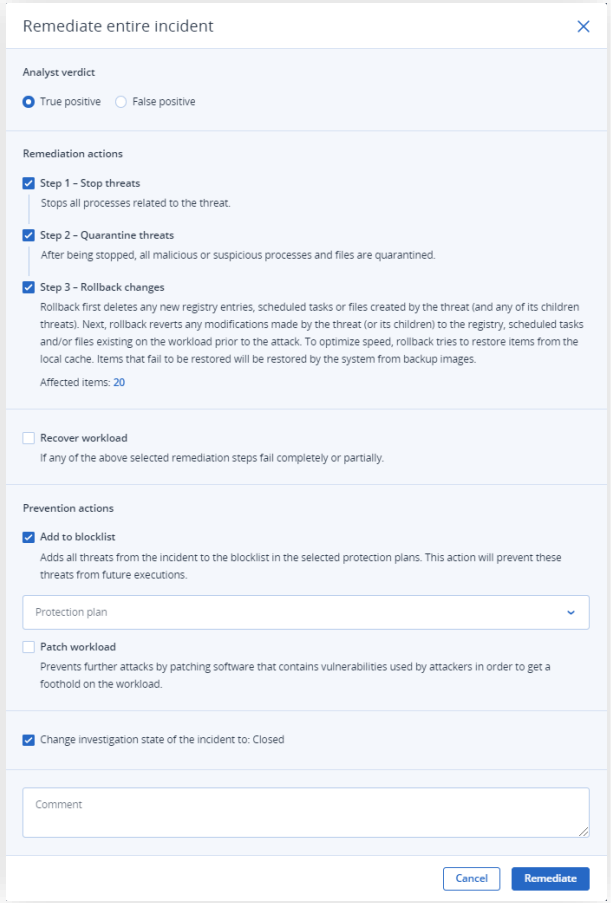
Gestion de la protection de l'entreprise

Filtrage des URL, évaluation des vulnérabilités, gestion des correctifs, gestion à distance, santé des lecteurs

Protégez votre entreprise avec facilité et rapidité - en augmentant la sécurité et la productivité tout en réduisant les délais et les coûts d'exploitation.

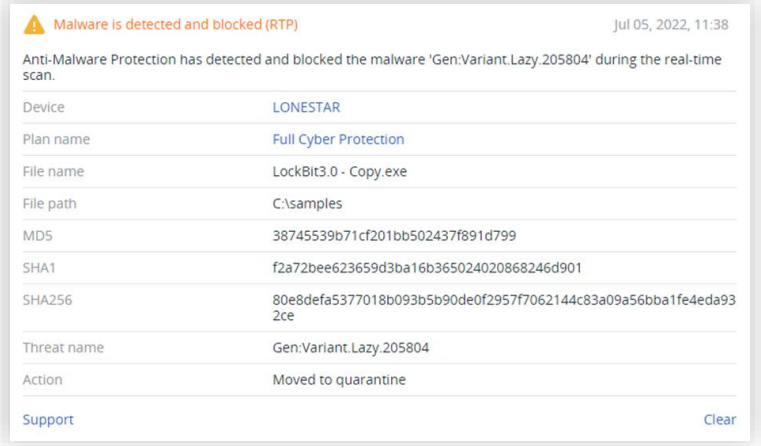
Pile de protection Acronis





Détecter les ransomwares, y mettre fin et s'en remettre grâce à un anti-malware comportemental basé sur l'IA

Protéger les données critiques des clients sur les terminaux, les serveurs, les dossiers réseau et les sauvegardes

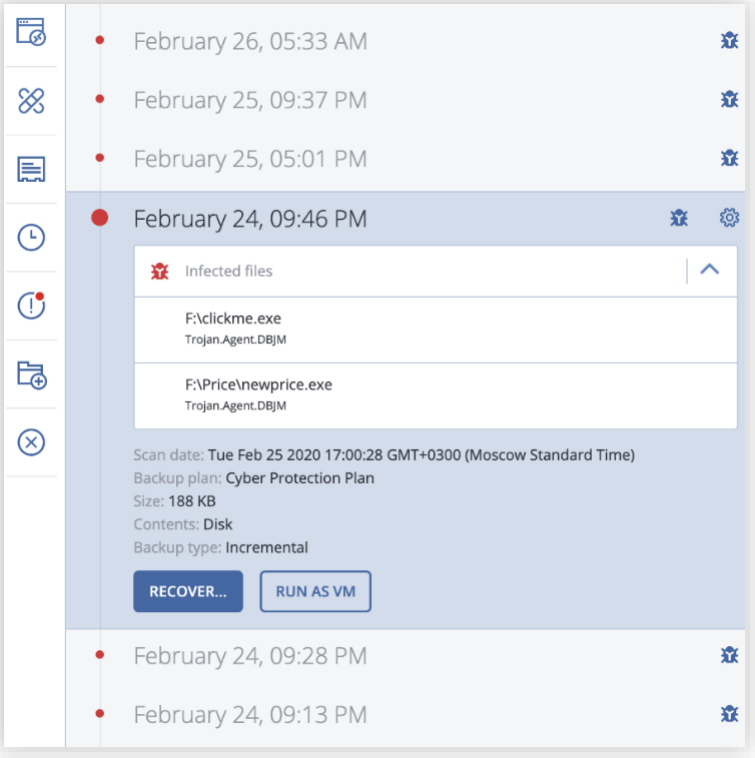


Plusieurs Technologies anti-malware primées

- Détection des ransomwares basée sur l'IA, **le comportement et les signatures**, y compris dans les sauvegardes locales.
- **L'analyse entropique** pour attraper les ransomwares avancés
- Protection des données **dans les dossiers du réseau**
- Protection côté serveur des données contenues **dans des dossiers partagés sur le réseau local**
- Protection des données **dans les sauvegardes**
- **Prévention des exploits** pour empêcher les ransomwares de tirer parti des vulnérabilités ouvertes
- **Filtrage des URL** pour empêcher les téléchargements à partir de sites web malveillants

Récupération automatique des données et réparation des dommages

- L'attaque typique d'un ransomware crypte certains fichiers **avant d'être détectée et stoppée**.
- Récupération automatique et quasi-instantanée des fichiers cryptés à partir **du cache local** ou d'une sauvegarde **sans intervention de l'utilisateur**
- **Éliminer les dépendances** à l'égard d'outils tiers et de **snapshot VSS vulnérables**
- La détection automatique, l'arrêt et la récupération des ransomwares sont **pré-intégrés à la sauvegarde et à la reprise après sinistre** d'Acronis sans frais supplémentaires.



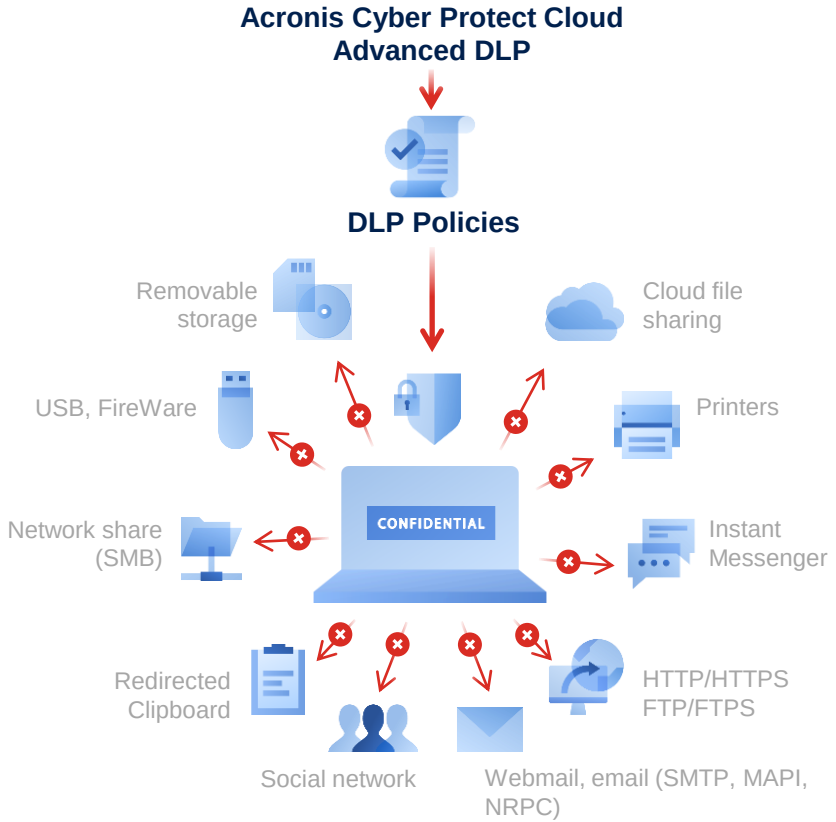
Empêcher l’exfiltration de données sensibles

Bloquez les tentatives d’exfiltration de données sensibles. Améliorez la conformité en toute simplicité grâce à l’intégration avec la protection contre la perte de données (DLP)

Empêchez les fuites de données sensibles vers des sources non autorisées via des périphériques et des canaux réseau (70+ canaux contrôlés)

Classer automatiquement les données soumises à des cadres réglementaires communs (RGPD, HIPA, PCI-DSS) pour détecter et empêcher l’exfiltration de données sensibles

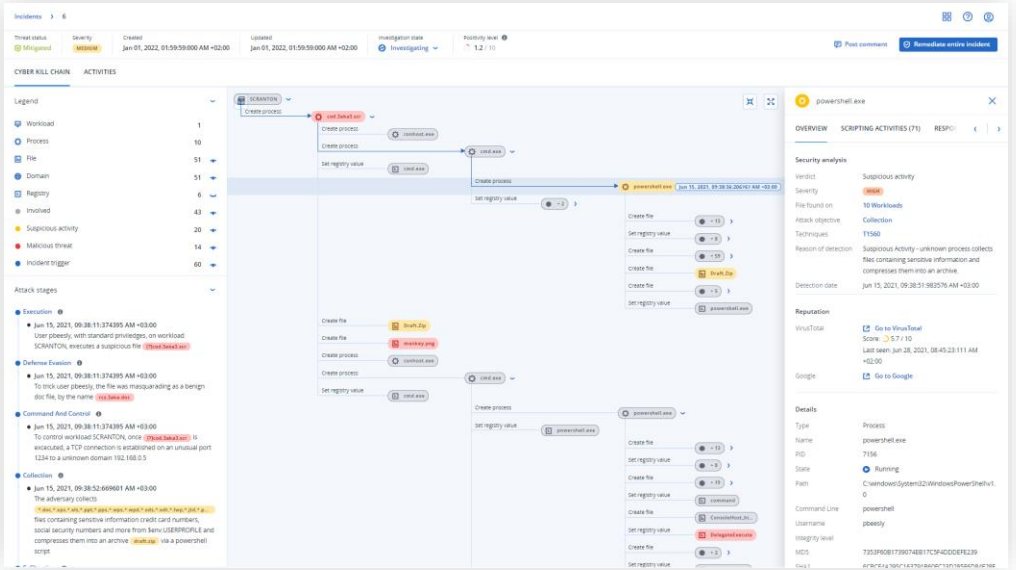
Gérez facilement des politiques spécifiques à l’entreprise grâce à la création et à l’extension automatisées de politiques basées sur le comportement.



Complétez votre défense en profondeur avec la détection et la réponse aux points d'accès (EDR)

DÉTECTION et RÉPONSE aux attaques avancées qui échappent aux autres défenses des points finaux - pré-intégrées avec les capacités IDENTIFIER, PROTÉGER et RÉCUPÉRER - sans efforts d'investigation importants.

- Détection rapide et analyse des incidents grâce à **l'interprétation automatique des attaques dans le cadre de MITRE ATT&CK®.**
- **Une véritable continuité des activités** avec une protection dans le cadre du NIST, y compris une reprise intégrée.
- Déploiement et mise à l'échelle rapides grâce à une plateforme conçue **pour réduire le coût total de possession** et le délai de rentabilisation



Acronis

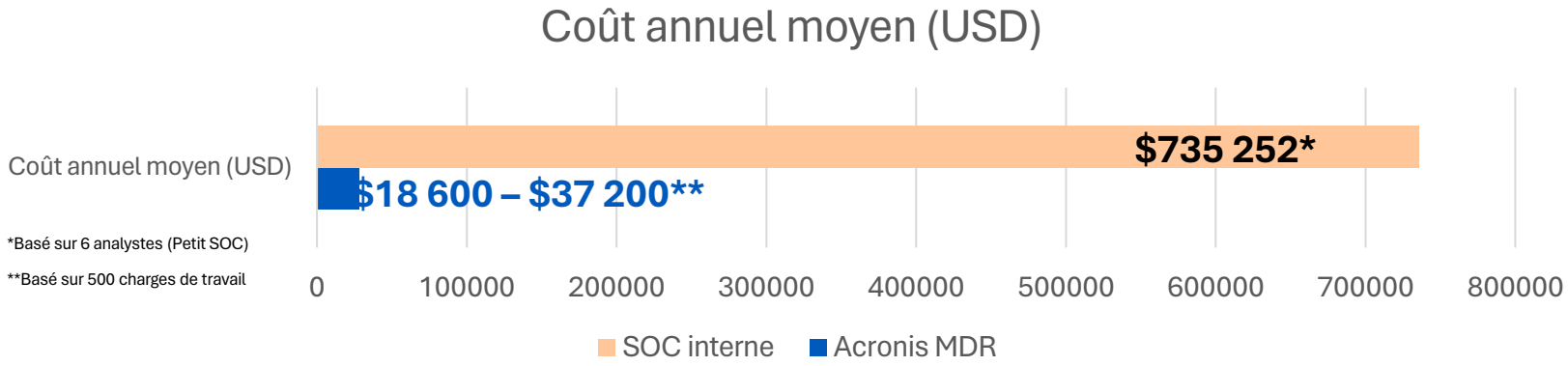
Acronis MDR

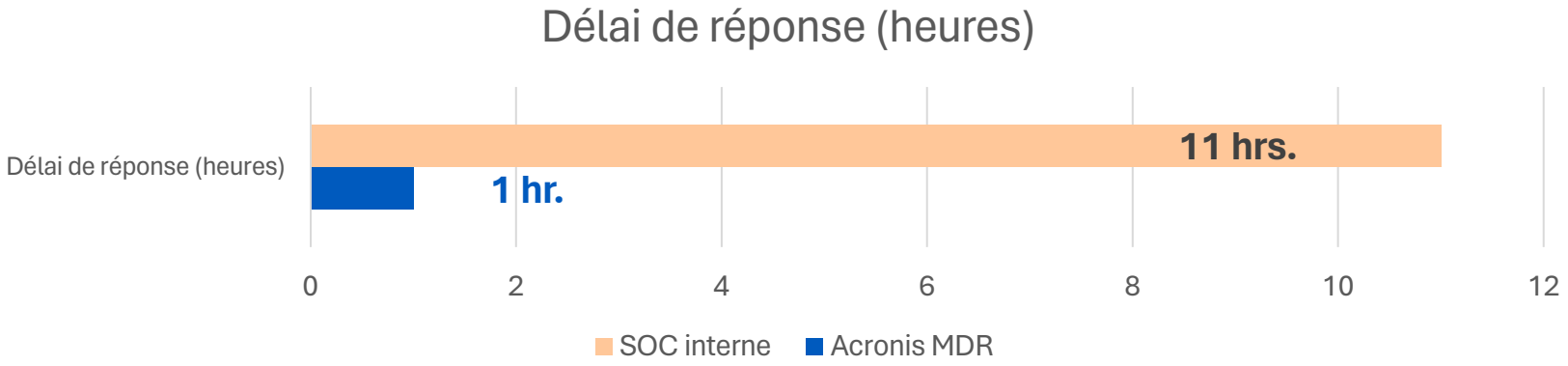
Grégory Laroche

Senior Solutions Engineer
Acronis

#CyberFit

Pourquoi externaliser vos services de sécurité via MDR ?





Acronis MDR propulsé par Novacoast

Service de sécurité simplifié, continu et efficace pour les points finaux, conçu pour les fournisseurs de services afin d'offrir à leurs clients une résilience inégalée avec un investissement minimal en ressources.

SOC externalisé, 24/7/365, de classe mondiale

Amplifiez l'efficacité de la sécurité grâce à une surveillance et à une assistance externalisées 24/7/365 par une équipe SOC de classe mondiale

Remédiation de pointe, y compris la récupération

Assurer la continuité de l'activité grâce à une remédiation qui comprend une reprise sans faille et des options d'externalisation complète

Visibilité prioritaire des menaces sur une plateforme unique pour tous vos services

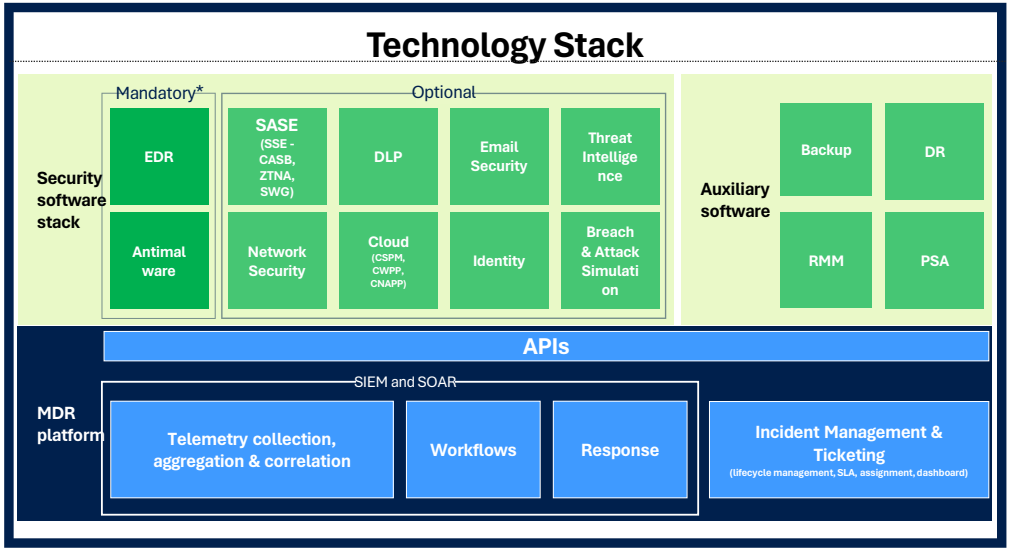
Obtenir une **visibilité prioritaire sur les incidents de sécurité** dans une plateforme qui intègre les services de protection des données, de cybersécurité et de gestion des points d'accès

SOC externalisé, de classe mondiale, 24/7/365

Amplifier l'efficacité de votre équipe en matière de sécurité et optimiser l'affectation des ressources

Services de protection des points d'extrémité externalisés via le partenaire MDR certifié d'Acronis – Novacoast :

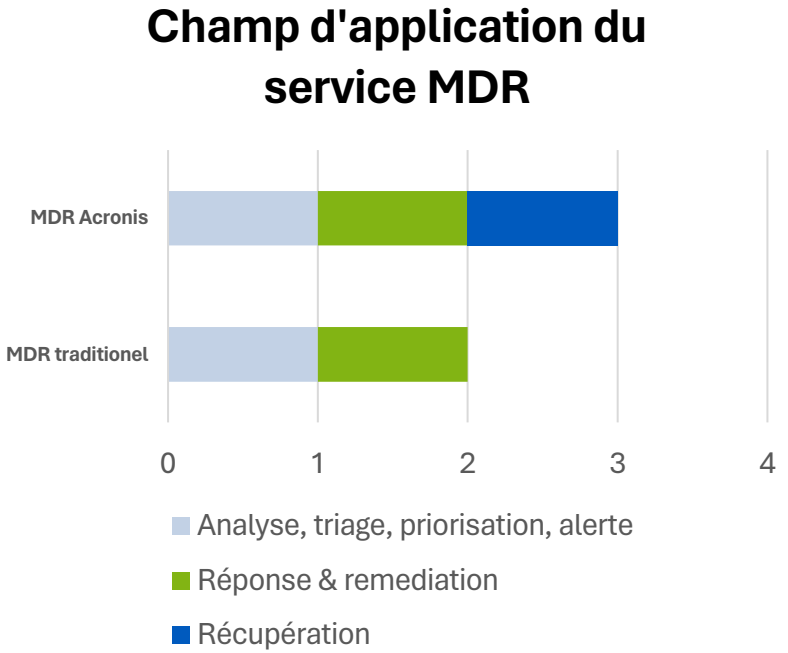
1. Approvisionnement sans effort – déploiement en un seul clic, le SOC externalisé s'occupant de tout le reste
2. Surveillance continue, 24 heures sur 24 et 7 jours sur 7, des points d'accès des clients – afin d'identifier les menaces
3. Enquêtes accélérées menées par des analystes de sécurité experts – exploitant une télémétrie riche, des renseignements sur les menaces et des analyses forensiques approfondies
4. Triage et hiérarchisation des événements – avec alertes en temps réel
5. Isolement des points d'extrémité et confinement des menaces – afin d'éviter toute propagation
6. Réponse rapide, y compris la récupération – peut être entièrement externalisée
7. Rapports continus – démontrez votre valeur aux clients



Remédiation de pointe, y compris la récupération

Réussir là où les solutions ponctuelles et les MDR qui en découlent échouent. Exploitez toute la puissance de la remédiation et de la récupération intégrées pour une résilience inégalée.

- Endiguement instantané des menaces - en isolant la charge de travail infectée sur le réseau
- Triage et hiérarchisation des événements avec alertes en temps réel - SOC toujours à l'affût des risques, 24 heures sur 24, 7 jours sur 7 et 365 jours par an
- Remédiation rapide - élimination des processus malveillants, mise en quarantaine des menaces
- Assurer une continuité d'activité inégalée - récupération intégrée à partir des sauvegardes sur la base d'un accord initial avec le partenaire
- Obtenez une visibilité prioritaire sur les incidents isolés avec des capacités de remédiation en un seul clic, ou externalisez entièrement votre réponse.



Partenariat entre Acronis et Novacoast

Novacoast est une société internationale de cybersécurité spécialisée dans les services informatiques et le développement de logiciels.

Novacoast

- Plus de **25 ans d'expérience** dans l'industrie
- **5 SOC** - SOC2-compliant- 24x7x365
- Novacoast a construit et maintien des solutions de sécurité informatique **pour certaines des plus grandes organisations privées et publiques du monde** (Managed SIEM, DLP, EDR, PAM, IR, etc.).
- **Plus de 400 employés**, notamment dans les domaines du conseil informatique, des services gérés, du développement et de l'ingénierie.
- Novacoast améliore la télémétrie EDR d'Acronis avec des systèmes **SIEM et SOAR propriétaires pour une analyse supplémentaire**. Basée en Californie du Sud, États-Unis

Acronis MDR : deux niveaux flexibles

Le modèle de licence flexible permet aux partenaires de choisir le niveau de service MDR qui correspond aux besoins de leur entreprise

Standard – A partir de 3.10$

Simplifiez la protection des points d'accès et augmentez l'efficacité de votre équipe en matière de sécurité

Advanced – A partir de 6.20$

Externalisation complète des opérations de sécurité des points d'accès pour une plus grande tranquillité d'esprit et une meilleure résilience de l'entreprise

Advanced MDR fera l'objet d'une licence par charge de travail, en tant que service en plus du pack Advanced Security + EDR (applicable aux modèles de licence par charge de travail et par Go d'Acronis Cyber Protect Cloud)

Inclus	Standard	Advanced
Onboarding MDR	Inclus	Inclus
Support 24/7 par un SOC externalisé	Inclus	Inclus
Surveillance 24/7/365 pour identifier les cyber-menaces	Inclus	Inclus
Triage et hiérarchisation des événements avec alerte en temps réel	Inclus	Inclus
Détection et isolation rapides des cybermenaces par l'équipe SOC	Inclus	Inclus
Conseils sur la manière d'atténuer, d'arrêter et de prévenir les incidents de sécurité	Inclus	Inclus
Escalades de sécurité détaillées et multicanales (dans le produit, par e-mail, par téléphone)	Inclus	Inclus
Remédiation aux menaces de sécurité 24 heures sur 24 et 7 jours sur 7 par l'équipe MDR		Inclus
Externalisation du rollback des attaques et de la récupération des sauvegardes (nécessite un accord avec le MSP)		Inclus
Évaluation du profil de risque des points finaux		Inclus

Qu'est-ce qui rend Acronis MDR unique ?

Remédiation et récupération intégrées

Valeur:

- Optimisation de l'allocation des ressources - possibilité d'externaliser non seulement la réponse, **mais aussi la récupération.**

Console de cyberprotection consolidée

Valeur:

- Provisionnez et gérez tous vos services à partir **d'une console et d'un agent uniques**
- **Améliorez le coût total de possession jusqu'à 60 %** - en rationalisant les processus, en réduisant le nombre de tickets et en augmentant le temps de retour sur investissement.

Véritable partenaire MSP

Valeur:

- Un service et une plateforme MDR **conçus pour s'étendre rapidement à plusieurs clients**
- Mise en œuvre rapprochée de marketing, ventes, support technique

MDRs traditionnels:

- Remédiation en se concentrant de manière cloisonnée sur l'endiguement des menaces et le blocage de leur exécution

MDRs traditionnels & les fournisseurs de cybersécurité pure :

- Une console et un agent distincts - nécessitant des intégrations de facturation, de ticketing et de reporting
- Autres services gérés par les MSP via une console différente

Fournisseurs axés sur les EUCs :

- Extension des solutions et besoins d'intégration
- Mise en œuvre limitée
- Extensibilité limitée

Tests récents de laboratoires indépendants (Jan-Fev/2024)

AV-TEST Product Review and Certification Report

- https://www.av-test.org/en/antivirus/business-windows-client/windows-10/february-2024/acronis-cyber-protect-23.12-242101/

The best Windows antivirus software for business users

- https://www.av-test.org/en/antivirus/business-windows-client/

Acronis

Live demo

Grégory Laroche

Senior Solutions Engineer
Acronis

#CyberFit

Acronis

Q&A

(et un petit sondage)

#CyberFit

Grégory Laroche

Senior Solutions Engineer
Acronis

Acronis

#CyberFit

Merci de votre participation!

Pour plus d'informations, veuillez consulter le site www.acronis.com ou contactez votre gestionnaire de compte

Acronis

Cyber Foundation Program

Share the success of your growing business by helping others

Get your free CSR in a Box training kit