Acronis

#CyberFit

Apprenez à stopper les attaques de ransomware avec Acronis Cyber Protect

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

Agenda

- Pourquoi la cyberprotection est-elle essentielle ?
- Pourquoi les ransomwares se multiplient-ils toujours en 2024 ?
- Comment Acronis vous aide à vous protéger contre les ransomwares ?
- Demo

Ransomware, la cybermenace la plus urgente en 2024

L'attaque la plus répandue, la plus destructrice et la plus coûteuse contre le temps de fonctionnement des entreprises et l'intégrité des données.

Haute fréquence

- Les ransomwares frappent une entreprise **toutes les 11 secondes**
- **80% des entreprises** ont été attaquées
- **25 % des brèches** comprennent une charge utile de type ransomware

Une complexité croissante

- **80 % des brèches** sont des attaques nouvelles ou inconnues de type "zero-day" (par exemple, l'attaque Kaseya 2021)
- **Ransomware as a service** (RaaS)
- **Nécessite une pléthore de solutions ponctuelles** - protection des points d'extrémité, protection des données, sécurité du courrier électronique, EDR/XDR

Risques et pertes pour le SMB

- **7 entreprises sur 10** ne sont pas prêtes à répondre à une attaque
- Montant moyen de la rançon : **812 360$**
- Coût moyen du 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

Attaques récentes de ransomware

- **Deutsche Bank** (Allemagne, worldwide)
  - L'une des plus grandes banques du monde avec 1,5 Milliards de $ d'actifs
  - Attaque de **vol de données** par le ransomware **ClopExposition**
  - limitée des données des clients en Allemagne

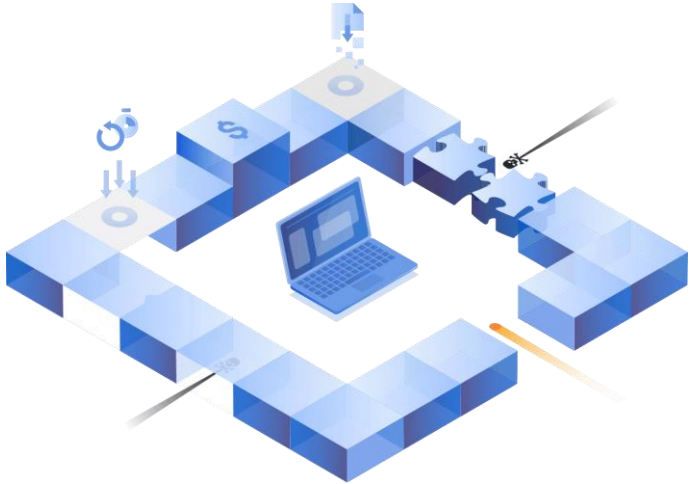
- **Coaxis** (France)
  - ESN spécialisé dans les solutions pour cabinets d'expertise comptable.
  - Attaque par le **groupe de Cybercriminel Lockbit 3.0**.
  - **25% des serveurs chiffrés** entrainant des retards concernant les déclarations de TVA et les déclarations sociales du mois de décembre

- **Schneider Electric** (France)
  - Schneider Electric est le numéro 1 mondial de la distribution électrique, capitalisation de 103 Milliards d'Euro.
  - Attaque de **vol de données** par le groupe de **Cybercriminels Cactus**
  - La sensibilité et la nature des données n'a pas été révélé pour le moment

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

Cesser de s'appuyer sur des approches traditionnelles inadéquates

	Intrusion initiale *Les ransomwares s'attaquent aux terminaux, aux serveurs, aux services en nuage et aux applications*	**Exécution** *Les ransomwares échappent aux défenses, se déplacent latéralement, exfiltrent et chiffrent les données critiques.*	**Prévention de la recuperation des données** *Le ransomware corrompt ou supprime les snapshots VSS*	**Demande de rançon** *Les attaquants retiennent la clé de décryptage et menacent de divulguer des données sensibles*
Anti-malware / anti-ransomware traditionnels	**La couche antivirus classique détecte les menaces connues** grâce à la correspondance des signatures, **mais ne peut pas identifier les "zero-days"** (menaces inconnues jusqu'à présent).	L'anti-malware comportemental identifie les processus malveillants en fonction de ce qu'ils font, **et non de ce à quoi ils ressemblent.** *Les ransomwares peuvent être bloqués après le chiffrement de certains fichiers*	Les logiciels anti-virus et anti-malware comportementaux peuvent ne pas bloquer les ransomwares à temps pour empêcher **la corruption ou la suppression des snapshot VSS**	Les mesures de lutte contre les logiciels malveillants **ne permettent pas de récupérer les données cryptées.**

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

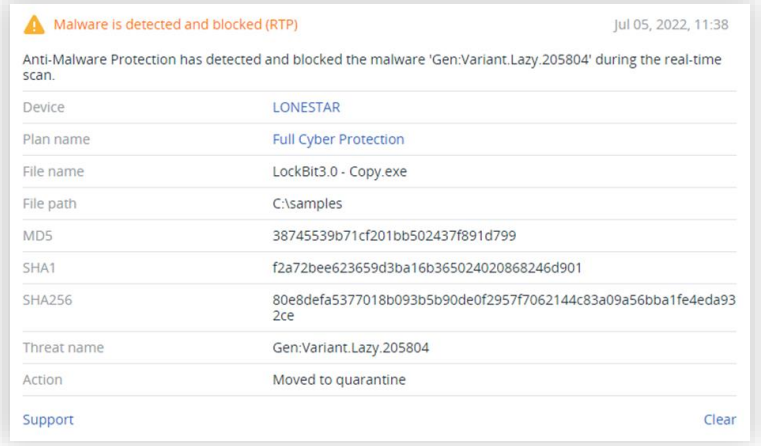
Protégez votre entreprise avec facilité et rapidité - en augmentant la sécurité et la productivité tout en réduisant les délais et les coûts d'exploitation.

Protection complète contre les ransomwares

	Intrusion initiale *Les ransomwares s'attaquent aux terminaux, aux serveurs, aux services en nuage et aux applications*	**Exécution** *Les ransomwares échappent aux défenses, se déplacent latéralement, exfiltrent et chiffrent les données critiques.*	**Prévention de la recuperation des données** *Le ransomware corrompt ou supprime les snapshots VSS*	**Demande de rançon** *Les attaquants retiennent la clé de décryptage et menacent de divulguer des données sensibles*
Anti-malware / anti-ransomware traditionnels	**La couche antivirus classique détecte les menaces connues** grâce à la correspondance des signatures, mais ne peut pas identifier les "zero-days" (menaces inconnues jusqu'à présent).	L'anti-malware comportemental identifie les processus malveillants en fonction de ce qu'ils font, **et non de ce à quoi ils ressemblent.** *Les ransomwares peuvent être bloqués après le chiffrement de certains fichiers*	Les logiciels anti-virus et anti-malware comportementaux peuvent ne pas bloquer les ransomwares à temps pour empêcher **la corruption ou la suppression des snapshot VSS**	Les mesures de lutte contre les logiciels malveillants **ne permettent pas de récupérer les données cryptées.**
Acronis Cyber Protect Cloud	Détecte les menaces de logiciels malveillants inconnus grâce à la **protection contre les exploits.**	Détecte les nouveaux processus malveillants grâce **à la détection comportementale basée sur l'IA**	La récupération ne dépend pas des snapshots VSS	Récupère automatiquement les données affectées **en restaurant les modifications** à **partir du cache local.**

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

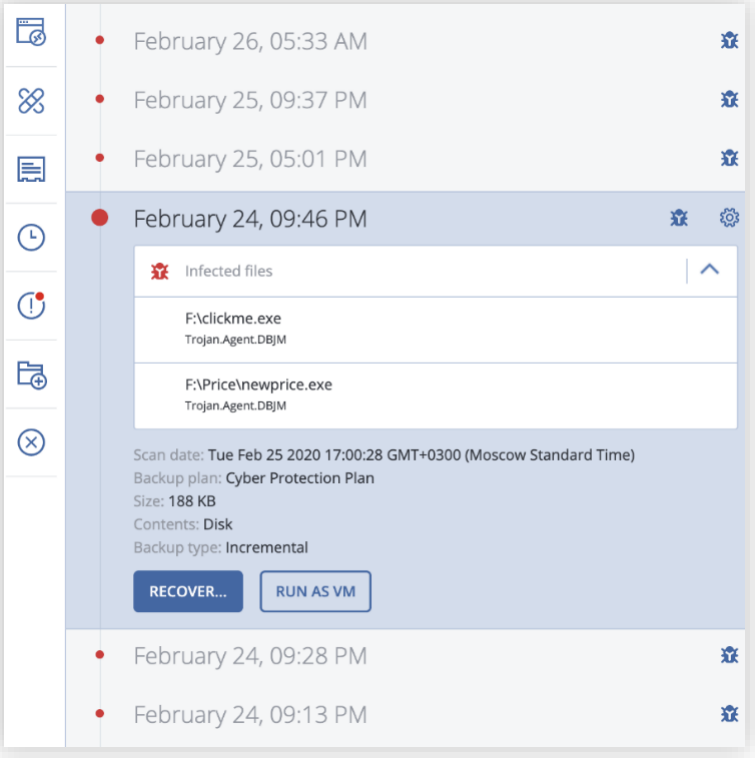


Plusieurs Technologies anti-malware primées

- 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

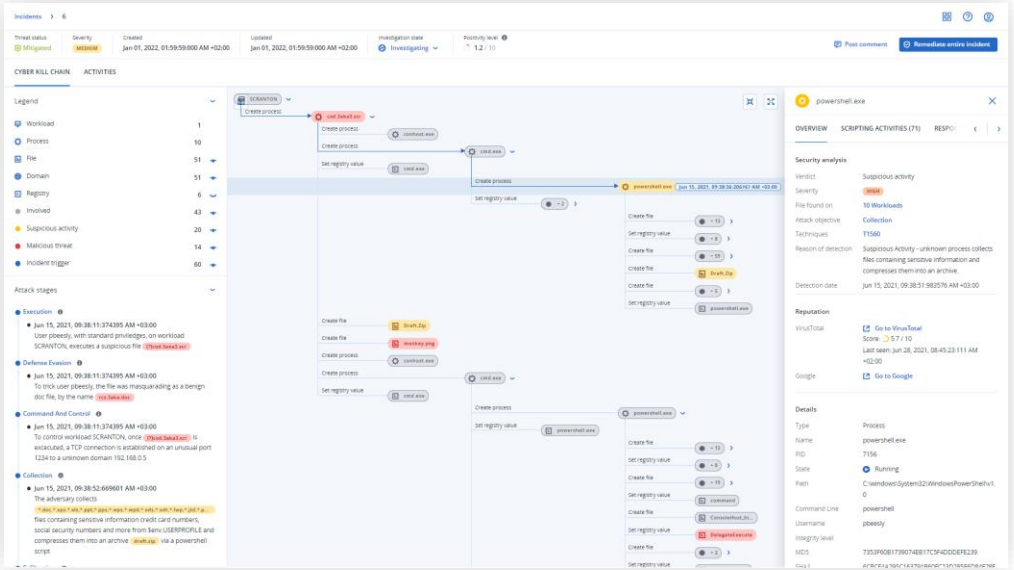
- L'attaque typique d'un ransomware crypte certains fichiers **avant d'être détectée et stoppée**.
- Récupération automatique et quasi-instantanée des fichiers cryptés à partir **du cache local** ou d'une sauvegarde **sans intervention de l'utilisateur**
- **Éliminer les dépendances** à l'égard d'outils 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.



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



Principaux cas d'utilisation d'Acronis Cyber Protect

Cybersecurity

Zero-day and malware protection

Remote work protection

Detect & Respond to security incidents

Data protection

Backup data across your all environments

Post-attack recovery & disaster recovery

Real-time protection of critical data

Administration

Streamlined management

Reduced costs & complexity

Compliance & forensics investigations

Grâce à une protection primée des points d'accès

VB100 Certified

0 false positives

AV-Test Certified

Detection and Blocking of Advanced Attacks – **100% detection**

0 false positives

ICSA Labs Certified

0 false positives

Leader in FrostRadar: Endpoint Security Global

Gold medal for Endpoint protection

4.5 Excellent

IDC MarketScape: Worldwide Cyber-Recovery Leader

Anti-Malware Testing Standard Organization member

Microsoft Virus Initiative member

Anti-Malware Test Lab participant and test winner

VIRUSTOTAL member

Cloud Security Alliance member

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