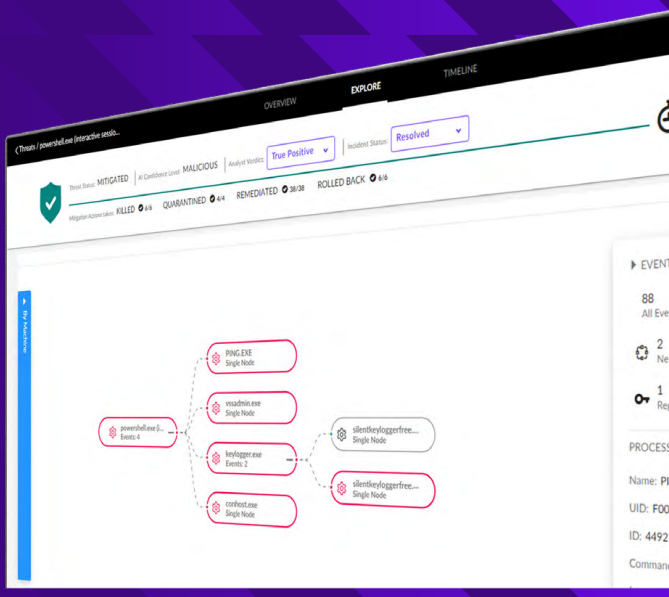
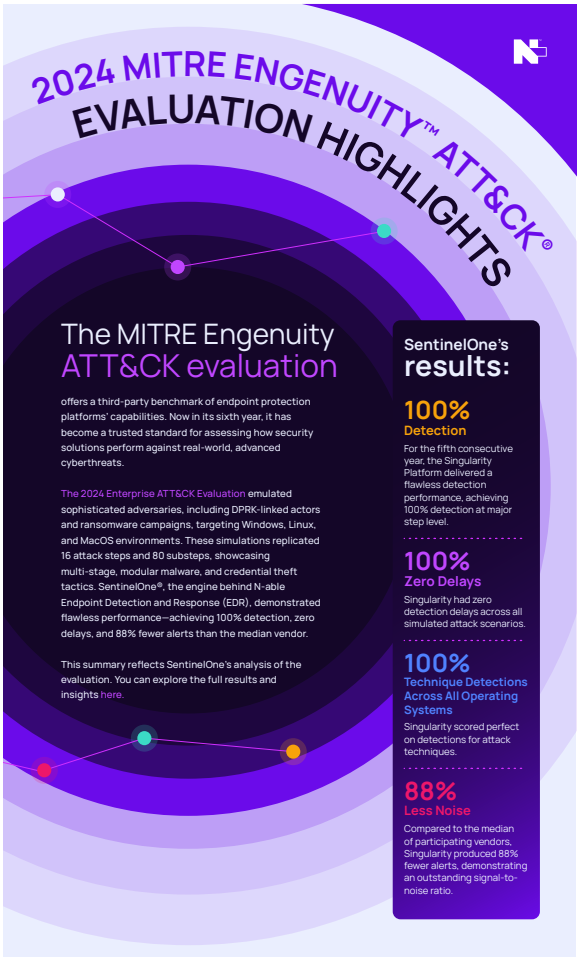
N-ABLE™ Fiche produit

N-able EDR optimisé par SentinelOne®



Détection optimisée avec l'IA. Visibilité approfondie des menaces. Réponse en temps réel.

Conçu pour les équipes de sécurité exigeant rapidité, clarté et contrôle, N-able EDR™ (optimisé par SentinelOne) offre une détection par IA, une visibilité approfondie des menaces et une réponse en temps réel, ce qui permet aux MSP et aux équipes informatiques de neutraliser les menaces avant qu'elles n'aient le temps de se propager.



Performance validée et éprouvée

Lors des **évaluations MITRE Engenuity ATT&CK® 2024**, SentinelOne a atteint un taux de détection de 100 % sans aucun retard, démontrant sa capacité à se défendre contre les attaques les plus avancées d'aujourd'hui.

Une fonctionnalité optimisée par SentinelOne, désigné leader dans :

- L'évaluation ATT&CK® 2024 de MITRE Engenuity™
- Le classement Gartner® Magic Quadrant™ pour la protection des points de terminaison

EDR Control

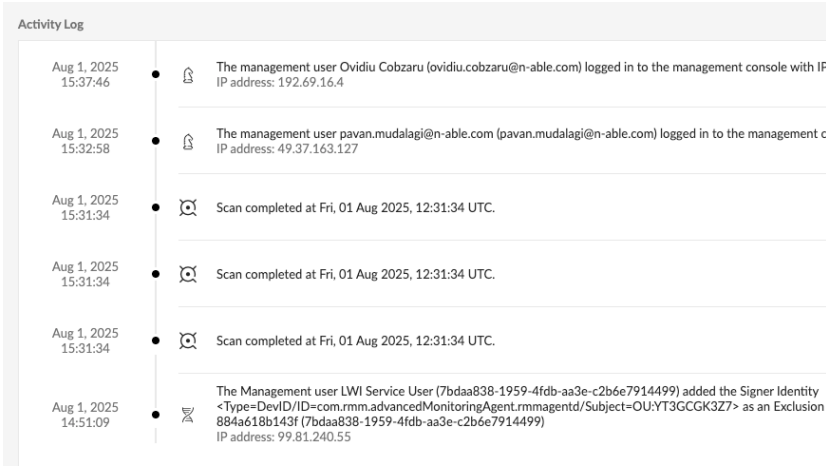
Fonctionnalités EDR essentielles à un tarif compétitif

EDR Control fournit les fonctionnalités EDR de base pour une posture de sécurité solide et une réponse efficace aux incidents. Parmi les différentes fonctionnalités offertes, citons l'intégration MITRE ATT&CK, le déploiement automatisé des agents, la configuration des stratégies et l'accès à des informations exploitables telles que la découverte des points de terminaison non protégés, qui aide les équipes à réduire les risques et à améliorer la couverture.

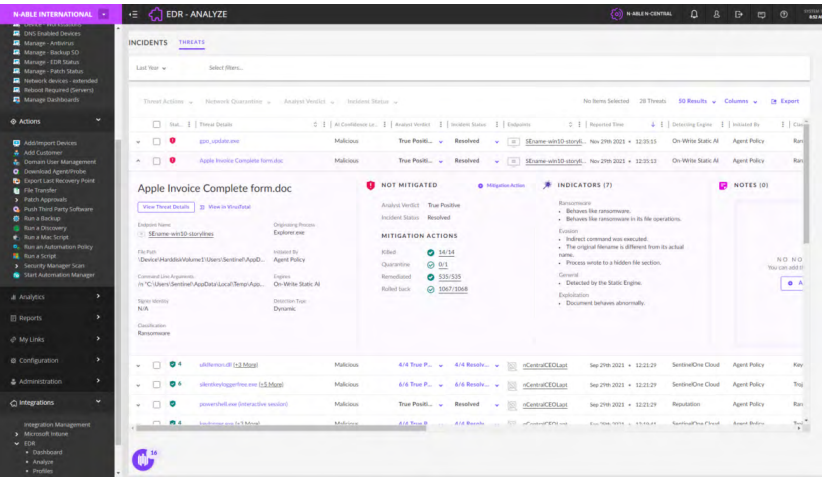
Fonctionnalités incluses

- **Intégration MITRE ATT&CK :** profitez d'une corrélation des techniques en temps réel ; 100 % de détection lors des simulations
- **Gestion mutualisée :** sécurisez et automatisez les environnements clients
- **Déploiement automatisé des agents :** installez, configurez et mettez à jour les agents à grande échelle
- **Configuration des stratégies :** sur tous les points de terminaison avec un agent EDR installé
- **Solution multiplateforme :** compatibilité avec Windows, macOS et Linux, y compris les anciennes versions*

*Compatibilité Linux non disponible pour N-Sight/N-Central



NGAV et remédiation



Moteurs de détection par IA statique et comportementale

- Analyse des fichiers, des actions et du comportement du réseau pour prévenir les menaces, de façon autonome, en s'appuyant sur des stratégies basées sur MITRE ATT&CK

Renseignements sur les menaces par IA et indicateurs de menaces

- Détection et réponse aux menaces en temps réel (même hors ligne), grâce à plusieurs moteurs de détection par IA statique et comportementale

Récupération avec correction et restauration en un clic brevetées

- Isolement automatique des points de terminaison infectés, éradication des processus malveillants et restauration des fichiers à leur état antérieur à l'infection

Rapports d'enquête sur les incidents

- Création d'une chronologie détaillée de l'attaque à partir des journaux, pour une enquête approfondie et complète (EDR Control : données d'investigation détaillées sur les incidents détectés ; EDR Complete : toutes les données d'investigation, indépendamment des incidents détectés)

Protection avancée des points de terminaison

Stratégies détaillées, mises à jour et administration contrôlées

Découverte des points de terminaison non protégés (Rogues)

- Analyse du réseau pour détecter les points de terminaison invisibles, en identifiant les appareils vulnérables nécessitant une attention immédiate

Vue des activités

- Suivi de toutes les actions au niveau de la console : connexions, modification des stratégies, exclusions et mises à jour des points de terminaison, pour une visibilité complète lors des audits

Vue des applications

- Visibilité de toutes les applications tierces exécutées sur les points de terminaison

Vue des automatisations

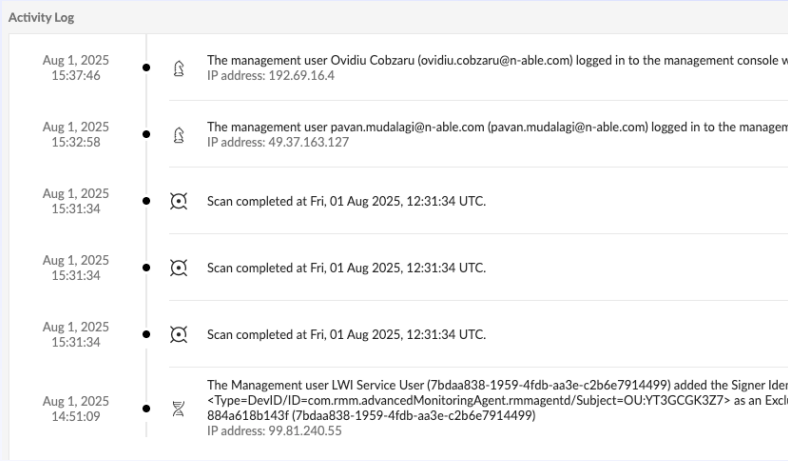
- Affichage de l'état des mises à niveau des agents sur l'ensemble des points de terminaison

EDR Complete

Inclut toutes les fonctions EDR Control, plus la fonction Threat Hunting avancée avec la fonctionnalité Deep Visibility. Celle-ci sonde les points de terminaison afin d'extraire les métadonnées des 14 derniers jours (jusqu'à 365 jours désormais) et de fournir des informations sur la sécurité. Il est possible de créer des règles STAR™ personnalisées pour définir des règles de sécurité temporaires ou permanentes et permettre une réponse autonome. Vigilance MDR propose des services gérés de sécurité 24h/24 et 7j/7.

Fonctionnalité Deep Visibility

- **Technologie avancée ActiveEDR Threat Hunting avec contextualisation via un scénario visuel** : visibilité des activités des points de terminaison, détaillant la cause profonde des menaces, les mouvements et les relations pour permettre une réponse autonome
- **Règles STAR™ personnalisées :** enrichies avec des événements bénins ; créez les règles nécessaires pour bloquer les menaces
- **Rétention des données sur 14 jours (jusqu'à 365 jours désormais) :** pour effectuer une chasse aux menaces et des recherches rétroactives



Modules complémentaires facturables

RemoteOps

- Enquêtez, atténuez et répondez à distance aux menaces en exécutant des scripts intégrés ou personnalisés, directement depuis la console EDR. Peut être activé à la fois dans EDR Control et EDR Complete.

Découverte du réseau

- Identification des angles morts et des points de terminaison non gérés, avec un déploiement d'agent en temps réel pour garantir une couverture complète
  - EDR Control : visibilité partielle via la découverte des faux points d'accès au réseau (Rogues)
  - EDR Complete : visibilité totale et recommandations d'actions

Nouveau Rétention des données (30/60/90/180/365 jours)

- Conservez les données sur le long terme pour comprendre l'ampleur d'une attaque et garantir la conformité tout en répondant aux exigences de cyber-assurance

Nouveau Cloud Funnel

- Transférez directement les données XDR enrichies vers votre propre stockage dans le Cloud, aux fins de conservation à long terme des données, de conformité et d'analyses avancées

Nouveau AI Security Analyst

- Véritable agent optimisé avec l'IA, assurant la détection, l'investigation et la réponse aux menaces

Vigilance MDR (optimisé par SentinelOne Vigilance MDR)

SOC 24h/24 et 7j/7 et experts en sécurité pour superviser, examiner et traiter les menaces identifiées par EDR :

- SOC géré pour une couverture permanente via le service Managed Endpoint Detection and Response de N-able EDR.
  - **Modèle « Follow-the-Sun » :** surveillance et réponse continues à l'échelle mondiale
  - **MTTR réduit :** temps moyen de réponse (MTTR) supérieur à la moyenne du secteur
  - **Contexte humain :** détection automatisée des menaces complétée par une analyse et une réponse humaine

Inclus par défaut dans EDR Control et EDR Complete

Console de gestion : bénéficiez d'un accès direct au compte, d'un tableau de bord personnalisable, de contrôles d'accès basés sur des rôles et d'un accès API

Rapports : générez des analyses sur l'empreinte de sécurité des points de terminaison avec des statistiques et des tendances exploitables. Assurez la conformité en détectant les violations de la sécurité au niveau des points de terminaison et en produisant des rapports de conformité.

« Nous avons rapidement constaté qu'un grand nombre de clients étaient friands du « shadow IT », des logiciels non approuvés par l'entreprise. L'adoption de la solution EDR nous a permis de remédier rapidement à ce problème ».

Dirk Geertis, IT Infrastructure System Engineer, ITC Belgium

Parler à un spécialiste

N-ABLE™

La mission de N-able est de protéger les entreprises contre des cybermenaces en constante évolution en leur proposant une plateforme unifiée de cyberrésilience qui leur permet de gérer, protéger et récupérer. Notre infrastructure technologique évolutive inclut des fonctionnalités optimisées avec l'IA et des intégrations tierces de pointe, et offre la flexibilité nécessaire pour utiliser des technologies d'excellence afin de transformer vos flux de travail et d'obtenir des résultats probants en matière de sécurité. Notre approche centrée sur les partenaires permet d'associer nos produits à des experts, à des formations et à des évènements animés par des pairs qui donnent à nos clients les moyens de se protéger, de gagner en résilience et de réussir. n-able.com/fr

---