SentinelOne

FICHE TECHNIQUE

Singularity™ EPP+EDR

Prévention, détection, investigation et intervention unifiées

Gartner

Gartner désigne SentinelOne parmi les leaders du Gartner Magic Quadrant 2020 pour les plates-formes de protection des endpoints

La vitesse, la sophistication et l'ampleur des menaces ont évolué, laissant les solutions EDR et de prévention de première génération sur le carreau

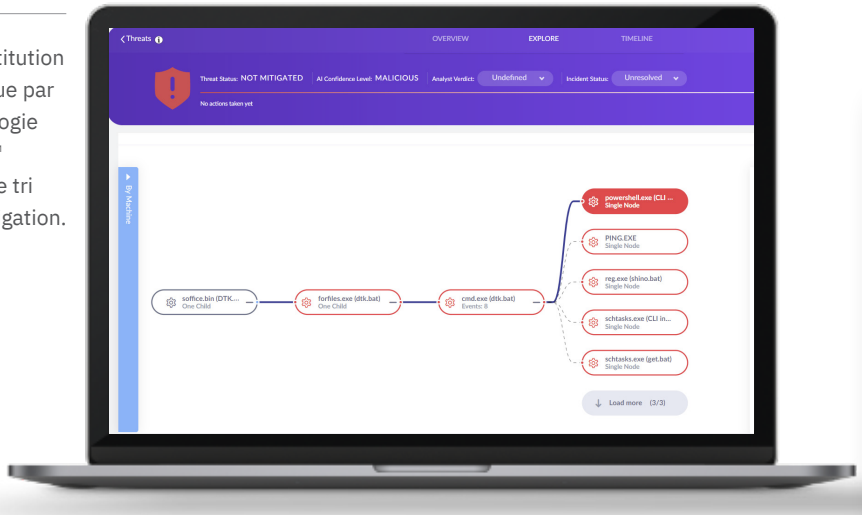
Lorsque les cyberpirates déjouent les mesures de prévention, les fonctionnalités EDR doivent se déclencher en temps réel et de manière autonome sur l'endpoint, que celui-ci soit connecté au réseau ou non. SentinelOne Singularity EPP+EDR réunit des fonctionnalités EDR et de prévention de nouvelle génération au sein d'un agent Sentinel unique pour offrir une protection autonome ultrarapide.

Optimisé par Deep Visibility™ et ActiveEDR™

La fonctionnalité ActiveEDR s'appuie sur l'intelligence artificielle comportementale pour identifier les processus malveillants dès qu'ils surviennent. Elle marque les événements corrélés et en crée automatiquement une reconstitution Storyline™ de l'attaque afin de visualiser et accélérer l'investigation. En mode de protection, l'agent Sentinel non seulement identifie l'attaque, mais la neutralise. Ensuite, grâce à la fonctionnalité de correction en un clic brevetée, un analyste peut annuler toutes les modifications non autorisées. Et cela, sans avoir recours à un script.

Investigation numérique efficace et intuitive

L'EDR ne peut plus être le privilège exclusif d'une minorité. Pour réduire le délai moyen de correction et renforcer la productivité, l'EDR de nouvelle génération doit simplifier la détection et l'intervention. L'intelligence artificielle surveille en permanence tous les événements, sur tous les systèmes d'exploitation et dans tous les environnements, qu'il s'agisse d'un centre de données, d'un fournisseur de services cloud, d'un bureau ou d'un lieu de travail distant. Deep Visibility permet la traque des menaces et l'investigation sans formation préalable, mettant ainsi l'intervention sur incident et la traque des menaces à la portée d'un plus grand nombre de membres de l'équipe de sécurité.



La reconstitution de l'attaque par la technologie Storyline™ accélère le tri et l'investigation.

SINGULARITY EPP+EDR

Prévention et EDR autonomes et ultrarapides pilotés par intelligence artificielle

PRINCIPALES FONCTIONNALITÉS

+ EPP/EDR autonomes et consolidés
+ EPP uniquement, EDR uniquement ou modes combinés avec le même produit
+ Linux, macOS, Windows, Kubernetes et Docker
+ Protection, détection et intervention en ligne/hors ligne
+ Corrélation automatisée des événements sous forme de reconstitutions Storyline
+ Fonctionnalités brevetées de correction et restauration en un clic
+ Respect du framework MITRE ATT&CK®
+ Conservation des données EDR flexible, options de 14 à plus de 365 jours
+ Investigation numérique distante pour tous les systèmes d'exploitation

Gartner peerinsights™

« Un excellent service client, un produit exceptionnel.

★★★★★

DIRECTEUR INFORMATIQUE
Soins de santé

Principales fonctionnalités

- **Détection et correction autonomes et en temps réel** des menaces complexes, sans intervention humaine.
- **Protection irréprochable** sous Windows, Linux et MacOS, indépendamment de l'environnement (physique, virtuel, conteneur, cloud ou centre de données).
- **Tri et analyse des causes premières accélérés** grâce à des informations pertinentes sur les incidents et le respect du framework MITRE ATT&CK® le plus rigoureux du marché, avec ou sans service MDR. Investigation en quelques secondes grâce aux mises en corrélation et aux reconstitutions Storyline.
- **Correction et restauration en un clic** pour une intervention simplifiée et un délai de correction réduit.
- **Expérience utilisateur intuitive** de Deep Visibility, S1QL et STAR™ (Storyline Active Response) pour une traque des menaces à la portée de tous les membres de l'équipe de sécurité.
- **Options de conservation des données** adaptées à tous les besoins, de 14 à plus de 365 jours.
- **Déploiement accéléré** grâce à des fonctionnalités d'interopérabilité qui assurent un déploiement rapide et fluide.
- **Cyberveille intégrée** pour la détection et l'enrichissement à partir des principaux flux de cyberveille d'autres sources, ainsi que de nos propres sources propriétaires.

PRÊT POUR UNE DÉMONSTRATION ?

Consultez le site Web SentinelOne pour plus d'informations

PRINCIPAUX AVANTAGES

+ Durée d'implantation réduite
+ Intervention sur incident accélérée
+ Délai moyen de correction réduit
+ Diminution de la désensibilisation aux alertes
+ Productivité des analystes accrue
+ Composant de la plateforme Singularity

SERVICE MDR (MANAGED DETECTION AND RESPONSE)

Vigilance MDR permet aux clients de se concentrer uniquement sur les incidents importants, ce qui en fait la solution complémentaire idéale pour les équipes IT/SOC surchargées.

Consultez le site **https://s1.ai/s1mdr** pour plus d'informations

ATT&CK®

MITRE ATT&CK 2020

- Le plus grand nombre de détections
- Le plus grand nombre de corrélations
- Meilleure couverture de l'enrichissement des données

Gartner

GARTNER MAGIC QUADRANT 2020 POUR LA PROTECTION DES ENDPOINTS

- Quadrant des leaders
- Les fonctionnalités critiques obtiennent le meilleur score pour les trois types de profils de clients définis par Gartner

FORRESTER®

RAPPORT FORRESTER WAVE™ 2020 POUR LES SOLUTIONS EDR

« Acteur de premier plan »

kuppingercole ANALYSTS

MARKET COMPASS 2020 DE KUPPINGERCOLE

Innovateur sur le marché EPDR

SentinelOne place ses clients au centre de ses priorités

Nos évaluations et améliorations continues nous poussent à dépasser les attentes de nos clients.

Gartner peerinsights customers' choice™

97 %

des évaluateurs du rapport Gartner Peer Insights™ « Voice of the Customer » 2020 recommandent SentinelOne.

97 %

Satisfaction des clients (CSAT)

FR FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA

TEVORA

Attestation PCI DSS
Attestation HIPAA

Gartner peerinsights 4,9 ★★★★★

À propos de SentinelOne

Plus de fonctionnalités, moins de complexité. SentinelOne développe des solutions de cybersécurité de pointe qui s'appuient sur une cyberveille autonome, distribuée sur les endpoints, afin de simplifier la pile de sécurité tout en offrant aux entreprises les fonctionnalités dont elles ont besoin. Notre technologie est conçue pour renforcer les équipes de sécurité grâce à l'automatisation et à la neutralisation efficace des menaces.

sentinelone.com
sales@sentinelone.com
+ 1 855 868 3733

S1-SNGL-EPP-EDR-10022020