SentinelOne

FICHE TECHNIQUE

# Singularity™ Cloud

## Server/VM Workload Detection & Response

**La gestion de votre cloud hybride est complexe. La protection de ses workloads, la détection des menaces et la réponse aux incidents, par contre, ne doivent pas l'être.** SentinelOne offre les performances EDR exceptionnelles dont votre SOC a besoin pour protéger les machines virtuelles Linux et Windows Server exécutées sur Amazon Web Services (AWS), Azure, Google Cloud et votre centre de données.

Composant de Singularity Cloud, Server/VM Workload Detection & Response assure la protection des workloads exécutés dans les instances de cloud virtuel et les serveurs physiques contre les menaces, telles que les attaques zero-day et les malwares sans fichier. La télémétrie EDR persistante corrélée contenant des métadonnées cloud offre une visibilité sur les workloads éphémères à des fins d'investigation numérique, permettant d'alimenter les analyses, la réponse aux incidents et la chasse aux menaces.

### Efficacité opérationnelle

Le déploiement, la gestion et la mise à jour des agents sont d'une grande simplicité grâce à des fonctions d'automatisation compatibles avec les pratiques DevOps en matière de gestion des configurations et de provisionnement.

### Visibilité EDR avec contexte de cloud hybride

Les données télémétriques sur les événements sont mises en correspondance avec les tactiques, techniques et procédures (TTP) MITRE ATT&CK et comprennent diverses métadonnées (ID de compte et d'instance, balises personnalisées, etc.).

### Automatisation performante de la sécurité

Puissantes et intuitives, les fonctionnalités d'automatisation réduisent les délais de détection et d'intervention, afin de répondre aux besoins de tous les membres de l'équipe SOC – de l'analyste débutant au chasseur de menaces confirmé.

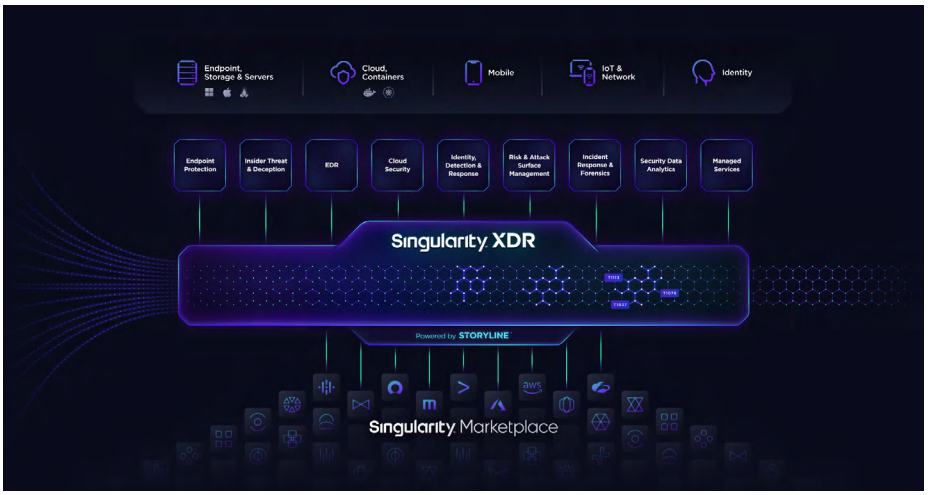
Outre les performances EDR inégalées obtenues dans les simulations MITRE ATT&CK, SentinelOne offre des fonctionnalités uniques, comme la technologie Storyline™, pour automatiser la visualisation des attaques et accélérer le tri des incidents.

aws Azure docker Google Cloud

**146 %** d'augmentation du nombre de ransomwares visant Linux avec du nouveau code en un an. L'IA comportementale de SentinelOne permet de réduire le risque pour vos serveurs physiques et workloads de machines virtuelles.

## PRINCIPAUX AVANTAGES ET FONCTIONNALITÉS

+ EDR au moment de l'exécution
+ Prise en charge des instances cloud sur AWS, Azure, Google Cloud et votre centre de données
+ Prise en charge des 12 principales distributions Linux
+ Prise en charge étendue de Windows Server (2003 SP2 à 2022)
+ Une seule console de gestion multicloud pour les endpoints, les serveurs, les workloads, etc.
+ Intégrité des workloads garantie
+ Métadonnées intégrées qui simplifient les opérations cloud




# Neutralisation rapide des menaces au moment de l'exécution

La détection des menaces et la réponse aux incidents constituent la dernière ligne de défense d'une stratégie de sécurité cloud multicouche. L'EDR protège les workloads contre les menaces qui échapperaient à l'analyse d'image : malwares de cryptominage chargés à l'exécution, menaces zero-day comme log4j, etc. En réponse à la multiplication des attaques ciblant Linux (DarkRadiation, par exemple), SentinelOne fournit à votre SOC les fonctionnalités nécessaires pour gagner en efficacité et réduire les interventions manuelles. Ainsi, Storyline accélère le tri des incidents ; les actions d'intervention automatisées, personnalisées et en un clic améliorent sa productivité ; tandis que les options d'extension de la conservation des données, le shell distant, RemoteOps et la console de gestion intuitive optimisent la chasse aux menaces.

# Agilité et sécurité optimales

### Plateformes prises en charge

+ AWS EC2
+ Azure VM
+ Google Compute Engine

### Adéquation aux DevOps

+ Automatisation IaC via le bootstrap de machine virtuelle
+ Mise à jour de l'image du système d'exploitation Linux sans dépendance au niveau du Kernel
+ Sécurité n'affectant pas les performances de développement

### Performances des SecOps

+ Investigation numérique et visibilité EDR
+ Tri des incidents accéléré grâce au contexte automatisé fourni par Storyline
+ Correction en un clic, restauration (Windows)
+ Actions d'intervention automatisées personnalisées
+ Chasse aux menaces

## DISTRIBUTIONS LINUX PRISES EN CHARGE

+ RHEL
+ CentOS
+ Ubuntu
+ Amazon Linux
+ SUSE
+ Debian
+ Virtuozzo
+ Scientific Linux
+ AlmaLinux
+ RockyLinux
+ Oracle
+ Fedora

## VERSIONS WINDOWS SERVER PRISES EN CHARGE

+ 2022, 2019, 2016, 2012 R2, 2012 et 2008 R2 SP1
+ Windows Server Core : 2019, 2016 et 2012
+ Windows Storage Server : 2016, 2012 R2 et 2012
+ Versions Windows Server d'ancienne génération : 2008, 2003 SP2+ et 2003 R2 SP2+

## Innovation. Fiabilité. Reconnaissance.

Gartner

**Leader du Magic Quadrant 2021 consacré aux plateformes de protection des endpoints**

MITRE ENGENUITY

**Résultats exceptionnels à l'évaluation ATT&CK**

- 100 % de protection. 100 % de détection
- Couverture analytique exceptionnelle 3 ans de suite
- 100 % en temps réel, 0 retard

Gartner peerinsights. 4,9 ★★★★★

**99 % des évaluateurs de Gartner Peer Insights™**

pour les solutions EDR recommandent SentinelOne Singularity

FedRAMP · AICPA SOC · TEVORA PCI DSS Attestation HIPAA Attestation · VB 100 VIRUS · AAA · SE Labs BEST Innovator WINNER 2021

**À propos de SentinelOne**

SentinelOne (NYSE : S) propose une cybersécurité autonome de pointe, capable de prévenir, détecter et neutraliser les cyberattaques plus rapidement et plus précisément que jamais. Sa plateforme Singularity XDR protège les grandes entreprises mondiales en leur offrant visibilité en temps réel sur les surfaces d'attaque, corrélation entre plateformes et réponse aux incidents optimisée par l'intelligence artificielle. Vous disposez ainsi de plus de fonctionnalités, tout en réduisant la complexité de votre écosystème de sécurité.

**fr.sentinelone.com**

sales@sentinelone.com
+ 1 855 868 3733