

OpenText Core Endpoint Protection

Sécurisez les utilisateurs où qu'ils se trouvent grâce à une protection en temps réel ultra-efficace

Avantages

- Gestion et contrôle 100 % à distance des nœuds d'extrémité
- Fonctionnement hautement automatisé et économique
- Déploiement fluide
- Efficacité supérieure contre les menaces « zero-day »
- Solutions spécialement conçues pour les fournisseurs de services gérés et les PME

Les entreprises de toutes tailles sont constamment attaquées. Compte tenu de la diversité, du volume et de la vitesse des attaques, il n'a jamais été aussi crucial d'arrêter les logiciels malveillants, les ransomware, le phishing, le cryptomining malveillant et d'autres attaques nuisibles ciblant vos utilisateurs et vos systèmes.

OpenText™ Core Endpoint Protection résout ces problèmes et bien plus encore, en fournissant une console de gestion intuitive et primée. Avec plus de 40 intégrations tierces, une API RESTful, ainsi qu'une détection, une prévention et un traitement entièrement automatisés des nœuds d'extrémité, OpenText offre une protection complète des nœuds d'extrémité pour compléter la stratégie de cyberrésilience d'une organisation. OpenText exploite la puissance du cloud computing et du machine learning en temps réel pour surveiller et adapter en permanence les défenses des nœuds d'extrémité de chaque système aux menaces uniques auxquelles un utilisateur final ou un système est confronté.

Adoptez une approche proactive, prédictive et multicouche de la sécurité

OpenText Core Endpoint Protection repose sur la plate-forme BrightCloud™ Threat Intelligence d'OpenText™. Cette plate-forme combine le meilleur de l'intelligence artificielle et du machine learning pour aider les entreprises à lutter contre l'évolution rapide des menaces. BrightCloud est plébiscité par plus de 140 fournisseurs de réseaux, de solutions de sécurité et de technologies.

Optimisée par ces renseignements sur les menaces de classe mondiale, la protection multi-boucliers d'OpenText inclut des boucliers de comportement en temps réel, de système central, de menaces Web, d'identité, de phishing, d'évasion et hors ligne pour la détection, la prévention et la protection contre les attaques complexes. La technologie brevetée OpenText Evasion Shield détecte, bloque et corrige (met en quarantaine) les attaques par injection de script évasif, qu'elles soient basées sur des fichiers, sans fichiers, brouillées ou chiffrées. Elle empêche également l'exécution de comportements malveillants dans PowerShell, JavaScript et VBScript avec sa technologie Script Shield.

Surveillez, consignez et confinez les infections, même lorsque le nœud d'extrémité est hors ligne

Contrairement aux approches traditionnelles, qui n'ont qu'une seule opportunité de détecter et d'arrêter une menace, la protection OpenText nouvelle génération fonctionne en trois étapes :

1. Elle empêche de manière prédictive les logiciels malveillants de s'infiltrer dans le système. Elle empêche ensuite l'exécution de logiciels malveillants et de fichiers inconnus s'ils présentent un comportement malveillant.
2. La protection OpenText surveille et consigne l'activité du fichier jusqu'à ce qu'elle puisse le classer correctement si un fichier précédemment inconnu (infection potentielle, par exemple) s'exécute.
3. Toutes les modifications apportées aux unités locales sont automatiquement restaurées à leur état pré-infection si le fichier est considéré comme une menace.

Non seulement cette stratégie multi-étapes est plus efficace contre les menaces modernes, mais elle réduit également les risques de faux positifs. Il n'y a jamais de signatures ou de définitions à mettre à jour, car la prévention des menaces s'effectue en temps réel à partir du cloud. Les mises à jour de l'agent OpenText sont automatisées et prennent généralement trois secondes, tout en étant totalement transparentes pour l'utilisateur.

Les alertes et les traitements en cas d'infection sont automatisés, tandis que des rapports réguliers sont planifiés pour le contenu, le calendrier et la circulation. Notre console de gestion basée sur le cloud vous offre visibilité et contrôle sur n'importe quel périphérique avec l'agent OpenText installé. Vous pouvez gérer plusieurs sites et emplacements et tirer parti de puissantes commandes d'agent à distance. L'un des principaux avantages de notre approche basée sur le cloud réside dans le fait que le traitement intensif de la détection et de l'analyse des logiciels malveillants est effectué dans le cloud.

Renforcez la solidité grâce à une cybersécurité intuitive et automatisée

Les solutions OpenText aident votre entreprise à rester cyberrésiliente. Les solutions OpenText vous aident à prévenir et à vous protéger contre les menaces grâce à une capacité rapide de détection, de réponse et de récupération des données. Elles aident également votre organisation à s'adapter et à se conformer à l'évolution des réglementations.

OpenText Core Endpoint Protection offre une protection avancée contre les attaques modernes toujours plus nombreuses et en constante évolution. Grâce à la sécurité automatisée des nœuds d'extrémité, vous n'avez plus besoin de ressources dédiées de sécurité informatique ni d'experts à votre disposition pour assurer la conformité numérique de votre entreprise. Cela signifie moins d'infections et d'incidents liés à la sécurité, sans oublier moins de cas de traitement et de pertes de productivité.

Responsabilisez les employés chargés de la protection avec des politiques avancées

OpenText fournit les outils essentiels qui renforcent considérablement les positions des entreprises en matière de cybersécurité. Nos outils protègent et donnent au personnel chargé de la protection les moyens d'obtenir des informations exploitables et des options de réponse flexibles. Nos nouvelles fonctions incluent :

- **Isolation des périphériques** : en cas de menace, il est essentiel d'empêcher sa propagation sur le réseau. Notre fonction d'isolation des périphériques vous permet d'isoler rapidement les périphériques affectés, ce qui stoppe la progression des logiciels malveillants tout en préservant les communications essentielles. Cette fonctionnalité est cruciale pour endiguer et analyser rapidement les menaces, protégeant ainsi l'intégrité de votre réseau.
- **Visualisation de l'arborescence des processus** : comprendre les tenants et les aboutissants d'une menace est essentiel pour une cybersécurité efficace. Grâce à la visualisation de l'arborescence des processus, les équipes chargées de la protection obtiennent des informations approfondies sur les systèmes. Cette fonction vous permet de suivre les origines et les chemins des processus, offrant ainsi une visibilité claire sur les menaces potentielles.

Ces améliorations légères mais puissantes apportées à votre toolkit de sécurité sont des composants clés qui peuvent vous aider à répondre aux exigences en matière de cyberassurance. Elles représentent l'engagement d'OpenText à fournir des solutions de protection sans imposer de complexité inutile ou ralentir vos opérations.

OpenText Cybersecurity fournit des solutions de sécurité complètes pour les entreprises et les partenaires de toutes tailles. De la prévention à la détection, en passant par la réponse, la récupération, l'enquête et la conformité, notre plate-forme unifiée de bout en bout aide les clients à développer leur cyberrésilience via un portefeuille de sécurité global. Grâce à des informations exploitables issues de nos renseignements en temps réel et contextuels sur les menaces, les clients d'OpenText Cybersecurity bénéficient de produits hautement efficaces, d'une expérience conforme et d'une sécurité simplifiée pour les aider à gérer les risques métiers.