Protection sans faille contre les menaces

Endpoint Detection and Response pour se protéger contre les attaques complexes avec des mesures automatisées

Kaspersky EDR Optimum: les points forts

- Protection contre des menaces de plus en plus sophistiquées et fréquentes
- L'outil automatisé permet d'économiser du temps et des ressources
- Vue d'ensemble transparente de l'étendue des menaces complexes dans l'intégralité du réseau
- Fournit des informations sur les causes profondes des menaces
- Réduction efficace des dommages grâce à des contre-mesures rapides et automatisées

Kaspersky a été fondé à Moscou en 1997. Aujourd'hui, le spécialiste de la sécurité est présent dans 200 pays, emploie plus de 4 000 spécialistes hautement qualifiés et est considéré comme l'un des principaux fournisseurs de solutions de sécurité. Les technologies Kaspersky protègent environ 400 millions d'utilisateurs dans le monde et sont utilisées par plus de 270 000 entreprises et organisations. Les solutions et services de cybersécurité de Kaspersky englobent des services managés dans le cloud et des solutions sur site notamment Endpoint Security, Hybrid Cloud Security et Enterprise Security de nouvelle génération, y compris les solutions de sécurisation de l'IoT et des applications industrielles. La plateforme Kaspersky Automated Security Awareness Platform (ASAP) propose une formation en ligne automatisée mais personnalisée sur la sécurité, en fonction des rôles et des compétences de chaque collaborateur.
Des exemples pratiques et des simulations enseignent des compétences qui peuvent être directement mises en œuvre dans la vie quotidienne. Les divers sujets abordés comprennent la gestion des comptes, les mots de passe, les appareils mobiles et les données confidentielles, la sécurité des e-mails, y compris la sensibilisation au phishing et le comportement sur les réseaux sociaux. ASAP offre également une gestion automatisée de la formation, de l'e-mail d'invitation jusqu'à l'évaluation de la réussite de l'apprentissage, et convient en tant que solution cloud évolutive pour toutes les tailles d'entreprise.

kaspersky

Dépliant du fabricant
Kaspersky / EDR Optimum

Prévention des menaces avec Kaspersky EDR Optimum

L'époque des simples logiciels malveillants est révolue depuis longtemps. Les menaces d'aujourd'hui sont plus complexes, plus dommageables pour les entreprises et passent inaperçues plus longtemps. En 2019, 91% des organisations ont été victimes d'une cyberattaque. Kaspersky EDR repousse les menaces les plus avancées et déclenche automatiquement des contre-mesures.

Endpoint Protection et réponse rapide aux menaces

Kaspersky Endpoint Detection and Response (EDR) Optimum assure la sécurité du réseau d'entreprise face à des menaces complexes et sophistiquées grâce à une détection avancée, une investigation simplifiée et des contre-mesures déclenchées automatiquement. EDR Optimum comprend une visibilité étendue, des outils d'investigation simples et des options d'atténuation automatisées qui permettent non seulement de détecter une menace, mais aussi d'en révéler toute l'étendue et les causes profondes afin de réagir immédiatement et de prévenir toute perturbation de l'activité.
La solution combine un kit d'outils de détection et de réponse facile à utiliser et hautement automatisé associé aux fonctionnalités inégalées de détente avancée et de protection des terminaux de Kasperski Endopooint Security for Business, au sein d'une offre unifiée. Des contrôles centralisés simples et un haut niveau d'automatisation libèrent les équipes informatiques et de sécurité pour qu'elles puissent se consacrer à d'autres tâches et permettre un déploiement plus ciblé du personnel – avec un flux de travail rationalisé à partir d'une console unique, disponible pour les configurations sur site comme dans le cloud.

Kaspersky Endpoint Detection and Response

Optimum

Visualiser l'ampleur des menaces

Kaspersky EDR Optimum collecte une multitude d'informations critiques et permet de comprendre immédiatement la relation entre les différents événements grâce à une représentation visuelle du chemin de propagation d'une attaque. L'analyse des indicateurs de compromission (IoC) importés ou générés par l'entreprise elle-même fournit un aperçu détaillé de tous les hôtes du réseau. Pour les menaces détectées sur tous les terminaux à partir des analyses IoC, EDR Optimum répond par des contre-mesures automatisées – ou l'équipe de sécurité lance directement des contre-mesures en un seul clic de souris. Il peut s'agir, par exemple, d'isoler les hôtes affectés et les fichiers infectés, d'analyser l'hôte ou d'empêcher l'exécution d'un fichier malveillant.

BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com

BOLL
IT Security Distribution