

Une sécurisation des points d'accès personnalisée pour chaque besoin

Les menaces provenant du cyberspace deviennent toujours plus fréquentes et plus sophistiquées. La détection et la défense contre les attaques nécessitent des concepts de sécurité avancés, tels que la solution Endpoint Detection and Response (EDR), ainsi qu'une expertise en matière de sécurité, qui peut être celle du client, du revendeur ou du fournisseur de solutions.

Les cybercriminels conçoivent de nouveaux virus, chevaux de Troie, ransomwares et autres logiciels malveillants à un rythme record et les utilisent pour lancer des attaques de plus en plus sophistiquées et difficiles à détecter qui risquent d'avoir des conséquences catastrophiques pour les entreprises visées. Grâce à la solution Endpoint Detection and Response (EDR), il existe depuis quelque temps déjà une méthode de lutte contre les attaques avancées sur les terminaux qui est plus efficace que les solutions classiques de sécurité des endpoints.

Cependant, il n'est pas toujours facile de trouver la bonne solution, car les solutions EDR font désormais partie de la gamme de produits de la plupart des prestataires de services de sécurité. En prenant l'exemple de la gamme de solutions de Kaspersky, on constate que toutes les solutions EDR ne sont pas identiques. En fonction de l'expertise de l'organisation en matière de sécurité, des besoins spécifiques du client et de la relation entre le client et le partenaire de sécurité, différents produits et services peuvent être utilisés.

EDR Optimum: Idéal pour les clients possédant une bonne expertise en matière de sécurité

La plateforme EDR Optimum de Kaspersky s'appuie sur la base éprouvée de la solution de protection des terminaux Kaspersky Endpoint Security for Business Advanced – ou sur des produits comparables – et la complète avec la fonctionnalité EDR: alors que la sécurité classique des endpoints détecte et bloque les logiciels malveillants, le système EDR aide considérablement les responsables de la sécurité à réagir de manière appropriée et conforme. La solution est facile à mettre en œuvre et, comme elle repose sur un agent unique associé à Endpoint Security for Business, elle n'impose pas de charge supplémentaire aux terminaux.

Le modèle de licencing est tout aussi simple. Les revendeurs peuvent ajouter EDR en tant que module complémentaire pour les clients utilisant déjà Endpoint Security for Business Advanced. Si aucun produit Kaspersky n'est déjà utilisé, le client peut commencer



directement avec EDR Optimum et recevoir automatiquement la solution Advanced comme base.

EDR Optimum est plus efficace lorsque le client ou son partenaire dispose d'une bonne expertise en matière de sécurité et peut traduire activement les informations et les rapports fournis par la plateforme en réponses adaptées.

Managed Detection and Response: Kaspersky passe à l'action

Avec la solution MDR (Managed Detection and Response) basée sur le cloud, Kaspersky met les connaissances de ses spécialistes directement à la disposition du revendeur ou de ses clients: Kaspersky surveille les terminaux, recherche de manière proactive les menaces (threat hunting) et se charge lui-même de leur défense ou donne au revendeur des instructions sur la manière de procéder (guided response). La solution MDR est également basée sur la structure de base éprouvée de Kaspersky.

Avec Kaspersky MDR, le revendeur cède au moins une partie des rênes à Kaspersky sans perdre le contrôle. La solution convient donc aux revendeurs disposant de ressources limitées en matière de sécurité informatique, mais aussi à ceux qui ont une bonne connaissance dans ce domaine.

XDR: La plateforme destinée aux experts

Avec son Expert Framework and Targeted Attack Platform (KATA), Kaspersky vise les revendeurs qui gèrent leurs propres Security Operation Centers (SOC) et dont le pain quotidien est la cybersécurité. La solution détecte les menaces multidimensionnelles au niveau des terminaux et du réseau, offre une transparence complète et propose des analyses complexes et des mesures de défense. La plateforme KATA cible les grandes entreprises dans des secteurs tels que la finance, l'énergie, les télécommunications, ainsi que les agences gouvernementales.

Avec ces trois plateformes distinctes dans l'environnement EDR, Kaspersky offre un niveau de flexibilité que peu d'autres fournisseurs peuvent égaler, tant en termes d'options pour les différents clients qu'en termes de licences sur une base mensuelle ou annuelle. Sur demande, Kaspersky peut aussi mener des audits de sécurité chez les clients, une occasion pour les revendeurs de compléter leur modèle commercial avec un service de conformité en matière de sécurité.

EDR et Kaspersky: Les avantages

- Des plateformes EDR adaptées à tous les besoins
- Base éprouvée avec Endpoint Security for Business
- Intégration facile, obtention aisée de la licence
- Transparence totale, défense ciblée
- Solution adaptée aux différents niveaux d'expertise existants en matière de sécurité

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60

vente@boll.ch
www.boll.ch