



Kaspersky
Next

Simplifions la cyberprotection



L'équilibre entre outils et ressources avant tout

Nous avons une question pour vous. **Quels sont les critères les plus importants pour vos choix en matière de cyberprotection ?** Si vous devez bien évidemment identifier les outils et technologies capables d'assurer la sécurité de votre organisation, vous devez également trouver un équilibre entre ces outils et les ressources disponibles pour mettre en œuvre et utiliser cette protection.

De combien de temps disposez-vous ?

Votre équipe possède-t-elle les compétences adéquates ?

Quel est votre budget ?

Disposez-vous du personnel nécessaire ?

Comment parviendrez-vous à convaincre votre supérieur ?

De nombreux autres facteurs pourraient encore être ajoutés à cette liste. Et pourtant, lorsqu'il s'agit de cybersécurité, nous ne nous concentrons que sur trois aspects essentiels. Tout d'abord, combien de spécialistes en sécurité informatique avez-vous en interne ? Ensuite, quels types de menaces vous préoccupent le plus ? Enfin, comment souhaitez-vous gérer votre sécurité ?

Outre l'analyse des causes profondes, vos spécialistes devraient également disposer des informations, des connaissances et des outils nécessaires à une enquête efficace, comme l'enrichissement par la Threat Intelligence, ou encore le rassemblement des données en un seul et même endroit.

Or, rechercher les traces d'une menace présente dans votre infrastructure se fait de préférence à l'aide d'indicateurs de compromission (IOC). Votre solution EDR doit donc vous permettre d'importer des IOC d'attaques actuellement actives dans votre industrie, et de les rechercher sur tous les terminaux pour vous donner une idée du niveau de danger.

Combien de spécialistes de la sécurité informatique avez-vous en interne ?

Commençons par les spécialistes de la sécurité. Si vous n'en avez pas, vous aurez besoin d'une plateforme de protection des terminaux (EPP) moderne, avec une automatisation avancée pour protéger votre organisation contre le plus grand nombre possible de menaces auxquelles elle risque d'être exposée.

Idéalement, l'EPP devrait également inclure des fonctionnalités de base de détection et de réponse au niveau des terminaux (EDR), comme l'analyse des causes profondes, afin de permettre à l'équipe informatique de visualiser et d'analyser ce qui se passe sur les différents terminaux pour mieux comprendre la menace, sans pour autant être trop complexe, pour faciliter son utilisation.

Si vous disposez d'une petite équipe de sécurité informatique, entre 1 et 3 spécialistes, proposez-lui une gamme plus large de fonctionnalités EDR essentielles permettant des réponses automatisées et/ou rapides et précises en un seul clic, pour mettre des fichiers en quarantaine, isoler un hôte, arrêter un processus, supprimer un objet, etc.

Si vous disposez d'une grande équipe de sécurité informatique ou d'un centre d'opérations de sécurité (SOC), vous devez probablement déployer et gérer une gamme beaucoup plus étendue d'outils spécialisés, ce qui nous amène à notre deuxième question.

Quels types de menaces vous préoccupent le plus ?

Généralement, les organisations font face à trois types de menaces distinctes. Il s'agit des menaces courantes, des menaces nouvelles, inconnues et évasives, et des menaces persistantes avancées (APT) et attaques complexes, chacune d'entre elles nécessitant une protection plus avancée.

Les menaces courantes sont les plus répandues et s'appuient généralement sur des systèmes non protégés ou sur une erreur humaine pour permettre une attaque. Jusqu'à récemment, la grande majorité des entreprises utilisaient l'EPP pour se défendre de ces menaces.

Toutefois, avec l'évolution des cybermenaces, des menaces de plus en plus sophistiquées ciblant auparavant uniquement les grandes organisations touchent progressivement les PME et les plus petites entreprises qui ne disposent pas des ressources internes nécessaires pour y répondre efficacement.

Les menaces évasives se sont ajoutées aux menaces courantes. Elles utilisent des outils légitimes dans les attaques, des scénarios prêts à l'emploi pour contourner l'EPP, ont un faible coût et sont facilement disponibles sur le Dark Web, ce qui augmente considérablement les risques de cybersécurité pour les organisations qui utilisent des solutions EPP traditionnelles.

Par conséquent, si vous êtes surtout préoccupé par les menaces courantes et utilisez l'ancien système EPP, vous devriez sérieusement envisager de l'accompagner d'au moins une fonctionnalité EDR de base. Si vous avez répondu « menaces évasives », vous aurez besoin des fonctionnalités EDR essentielles décrites ci-dessus. Et s'il s'agissait d'« APT et d'attaques complexes », tournez-vous vers la détection et la réponse étendues (XDR), pour faire face à ces attaques sophistiquées, ciblées et avec le plus grand potentiel de dommages.

Pour les organisations exposées à ce type d'attaque, la puissance du XDR s'explique par **la vue unique et la visibilité totale qu'elle offre entre les outils et les couches de cybersécurité**, permettant aux équipes de sécurité surchargées de détecter et de résoudre les menaces plus rapidement et plus efficacement, et de capturer des données plus complètes et contextuelles pour les aider à prendre de meilleures décisions en matière de sécurité et à prévenir de futures attaques.

Comment souhaitez-vous gérer votre sécurité ?

La gestion dans le cloud peut contribuer à simplifier vos opérations et constitue une option intéressante pour de nombreuses entreprises en raison des coûts réduits et de la maintenance gérée. Mais la gestion sur site présente également des avantages non négligeables, en particulier si vous vous préoccupez de la souveraineté des données.

Il ne reste plus qu'à déterminer vos préférences en matière de sécurité. Vous pouvez opter pour un système sur site, un système dans le cloud ou un système hybride.

Vous pourriez également décider de ne pas gérer tout ou partie de votre sécurité en interne et confier cette responsabilité à un fournisseur de confiance, à un fournisseur de services managés (MSP) ou à un prestataire de services de sécurité gérés (MSSP) offrant des services de détection et de réponse gérés (MDR).

Bilan

Répondre à ces questions vous donnera immédiatement une idée plus claire des types d'outils dont vous avez besoin pour construire une base de sécurité forte et adaptée à vos besoins, qu'il s'agisse d'EPP, d'EDR ou de XDR, et de leur niveau respectif (élémentaire, essentiel ou expert). Ainsi, vous vous assurez non seulement de ne pas investir dans du matériel pour lequel vous dépenserez des ressources précieuses mais dont vous aurez du mal à tirer le meilleur parti, mais vous serez également à même d'identifier les mesures de sécurité réellement utiles dans vos activités quotidiennes.

Comment Kaspersky peut vous aider

Avec seulement trois niveaux de produits, Kaspersky Next sécurise l'infrastructure d'une entreprise en combinant une protection et des contrôles des terminaux (EPP) exceptionnels avec la transparence et la rapidité de l'EDR, ainsi que la vision complète et la puissance du XDR. Les entreprises peuvent donc choisir les outils utiles dans l'immédiat, puis les mettre à niveau lorsque leurs besoins de protection évoluent.



Kaspersky Next
EDR Foundations

En savoir plus



Kaspersky Next
EDR Optimum

En savoir plus



Kaspersky Next
XDR Expert

En savoir plus

Actualités des cybermenaces : securelist.com

Actualités dédiées à la sécurité informatique : business.kaspersky.com

Sécurité informatique pour les PME : kaspersky.fr/business

Sécurité informatique pour les entreprises : kaspersky.fr/entreprise

kaspersky.fr

© 2024 AO Kaspersky Lab.
Les marques déposées et les marques de service sont
la propriété de leurs détenteurs respectifs.

Pour en savoir plus à propos de Kaspersky Next,
consultez le site : <https://go.kaspersky.com/next>

Choisissez le niveau qui vous convient le mieux et
répondez à un bref questionnaire dans notre outil
interactif :

https://go.kaspersky.com/Kaspersky_Next_Tool