RSA

RSA NETWITNESS® ENDPOINT

DÉTECTEZ LES MENACES PLUS VITE. RÉDUISEZ LEUR TEMPS D'IMPLANTATION. AUTOMATISEZ LA RÉPONSE.

FONCTIONNALITÉS PRINCIPALES

- *EDR, NDR, SIEM, UEBA, O&A sur une plate-forme unique et complète*
- *Visualisation des processus*
- *Authentification continue basée sur les menaces*
- *Agent inviolable unique pour les journaux, le noyau des points de terminaison et la collecte des métadonnées*
- *Premier système UEBA intégré, basé sur les points de terminaison*
- *Algorithmes étendus de détection de l'analytique du comportement*
- *Moteur de notation des risques innovant et personnalisable*

À l'heure où les surfaces d'attaque se multiplient, il est devenu de plus en plus complexe de se protéger contre les attaquants, qu'il s'agisse de logiciels malveillants courants, de menaces et de logiciels criminels provenant de personnel interne jusqu'aux attaques parrainées par l'état, ou encore d'attaques d'hacktivistes et de terroristes. Toutes les menaces ne naissent pas égales, pourtant des silos de technologies non connectées pour la prévention, la surveillance et l'investigation restent inefficaces pour permettre aux centres d'opérations de sécurité (SOC, Security Operations Centers) d'éliminer rapidement les faux positifs et de fournir des indicateurs ciblés (par opposition aux alertes cloisonnées libres). Ce qu'il faut, c'est une solution complète et collaborative permettant aux analystes de la sécurité de détecter et de répondre aux menaces les plus importantes pour leur organisation.

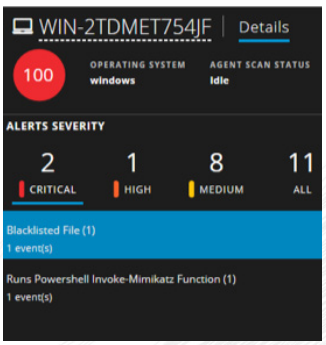
Compte tenu de la mobilité actuelle des collaborateurs, qui travaillent de plus en plus hors site, sur des réseaux non fiables avant de se reconnecter à des environnements de confiance, les points de terminaison restent plus que jamais le vecteur d'attaque le plus vulnérable.

Élément clé de l'offre RSA NetWitness Platform, RSA NetWitness® Endpoint est une solution de détection et de réponse entièrement intégrée pour les points de terminaison. Elle propose une surveillance continue des points de terminaison afin de proposer aux analystes de la sécurité une visibilité approfondie et une analyse puissante de toutes les menaces sur les points de terminaison d'une organisation. À la place des signatures ou des règles, elle tire profit d'une surveillance comportementale unique et continue, et de l'apprentissage automatique avancé pour approfondir la recherche sur les points de terminaison afin de mieux analyser et identifier les attaques cachées de type « zero-day » (non basées sur des logiciels malveillants) que d'autres solutions de sécurité des points de terminaison peuvent complètement ignorer.

UN AGENT LÉGER COMME UNE PLUME ET PARTICULIÈREMENT INNOVANT

RSA NetWitness Endpoint fournit un agent unique, à la fois inviolable et évolutif, qui apporte des renseignements immédiats, des actions de réponse et l'ingestion de métadonnées à partir des journaux Windows et des processus de base des points de terminaison. Cette visibilité approfondie et des renseignements exploitables offrent une vue à l'échelle de l'organisation sur tous les points de terminaison pour connaître le cycle de vie complet des attaques et des investigations de réponse aux incidents sur les systèmes d'exploitation Windows, macOS et Linux.

ANALYSE PLUS APPROFONDIE DES COMPORTEMENTS DES UTILISATEURS ET DES ENTITÉS



RSA NetWitness Platform fournit des modèles d'apprentissage automatique basés sur des données approfondies relatives aux processus des points de terminaison, afin de détecter rapidement les anomalies dans les comportements des utilisateurs et des machines, le tout dans une seule et même plate-forme complète. RSA NetWitness Endpoint and RSA NetWitness UEBA, les offres de produits clés de RSA NetWitness Platform, offrent une visibilité étendue et approfondie qui stimule les fonctionnalités de détection et de réponse pour les analystes de la sécurité, quel que soit le front sur lequel opèrent les pirates. Les menaces telles que l'utilisation erronée ou abusive de PowerShell, les scripts malveillants, les accroches de noyau et de

La plate-forme RSA NetWitness aide les équipes SOC et IT à obtenir des renseignements sur toute l'étendue d'une attaque, au niveau du réseau et des points de terminaison, et fournit aux analystes de sécurité les renseignements exploitables dont ils ont besoin pour rationaliser l'analyse des menaces et les actions de réponse.

RSA

PRINCIPAUX AVANTAGES

- *Réduction du temps moyen de détection, d'investigation et de réponse*
- *Accélération de la réponse aux incidents et réduction du temps d'implantation*
- *Visibilité inégalée sur les anomalies de comportement des points de terminaison pour la détection précoce des menaces*
- *Authentification basée sur les menaces qui localise les utilisateurs suspects et les comptes corrompus*
- *Analyse des causes premières plus rapide*
- *Évaluation de la portée complète de l'attaque sur les points de terminaison et les réseaux*

processus, la modification du registre, l'exfiltration de mémoire et les attaques sans fichier sont rapidement détectées par la capacité de RSA NetWitness Platform à corréler des millions d'événements à l'aide d'une analyse manuelle ou d'une personnalisation des règles et des signatures.

AMÉLIORATION DU TEMPS DE RÉPONSE, RÉDUCTION DE L'IMPACT DE LA VIOLATION

L'un des aspects essentiels de l'efficacité des mesures correctives consiste à comprendre dans quelle mesure une attaque ciblée s'est étendue sur votre réseau. RSA NetWitness Endpoint apporte cette visibilité étendue et approfondie sur les menaces qui donne aux équipes de sécurité la possibilité de répondre de manière ciblée pour corriger rapidement les incidents sur tous les points de terminaison de l'entreprise. RSA NetWitness Endpoint rassemble rapidement toutes les données les plus stratégiques qui sont nécessaires à une procédure d'enquête approfondie, et identifie instantanément tous les points de terminaison infectés afin de comprendre immédiatement toute l'étendue d'une attaque.

Les équipes de sécurité peuvent isoler un point de terminaison sur le réseau, ce qui empêche la communication des pirates et les mouvements latéraux des menaces, et peuvent bloquer et mettre en quarantaine les menaces sur tous les points de terminaison infectés. Les enquêtes approfondies et les intégrations de métadonnées avec RSA NetWitness Platform permettent aux entreprises de voir et de comprendre le champ d'application complet d'une attaque sur la télémétrie du réseau et des points de terminaison, optimisant ainsi la réponse aux opérations de sécurité.

RSA NETWITNESS PLATFORM

Avec plus de 30 ans d'expertise en matière de sécurité, RSA reste un leader du marché grâce à des solutions innovantes qui répondent aux défis les plus importants des opérations de sécurité dans le monde entier. L'intégration du nouveau produit RSA NetWitness Endpoint étend RSA NetWitness Platform et ses offres avancées en termes de SIEM et de défense contre les menaces, et tire profit de sa visibilité omniprésente sur les journaux, le réseau et les points de terminaison.

À PROPOS DE RSA

Les solutions RSA® Business-Driven Security™ offrent aux organisations une approche unifiée de la gestion du risque numérique qui repose sur une visibilité intégrée, des informations automatisées et des actions coordonnées. Avec des solutions permettant une détection et une réponse rapides, un contrôle d'accès des utilisateurs, une protection du consommateur contre les fraudes et une gestion intégrée des risques, les clients de RSA peuvent se développer et s'adapter en permanence au changement induit par la transformation. Pour plus d'informations, accédez au site rsa.com/fr-fr.

09/20 Fiche produit H17630-1 W386667.