DATA SHEET

SERVICES DE SÉCURITÉ MANAGÉS

Services de sécurité des terminaux

Face à des équipes de plus en plus mobiles, les risques de sécurité associés à l'usage de terminaux personnels au travail (BYOD) inquiètent les entreprises.

La connexion de smartphones, tablettes, ordinateurs portables et autres appareils sans fil aux réseaux d'entreprises est une porte ouverte aux menaces en tous genres. D'où l'importance capitale de bien sécuriser tous les terminaux. Le problème est que les solutions traditionnelles ne font plus le poids face aux exigences actuelles de sécurité : identification des risques, élimination des faux positifs et endiguement des infections à toute heure du jour et de la nuit.

Avec Endpoint Security Services (ESS), NTT gère un nombre de plus en plus important de solutions de sécurité des terminaux. ESS, c'est une solution unique conçue pour augmenter la vitesse et la précision des interventions humaines au moyen de la technologie EDR (Endpoint Detection and Response).

Pour la sécurité des terminaux, ne vous contentez pas des solutions traditionnelles

Un anti-virus classique ne détecte et ne protège les utilisateurs que contre des malwares connus. Votre sécurité ne tient alors qu'à une bonne automatisation et à des signatures à jour. C'est ainsi que des failles de sécurité sur le réseau passent parfois inaperçues et laissent le champ libre à des infections généralisées.

Pour protéger leurs données en transit contre tout accès illicite, de plus en plus d'entreprises chiffrent leur trafic réseau. Seulement voilà, un hacker déterminé pourra toujours se reporter sur les terminaux où les données sont visibles et accessibles en clair. Chaque terminal connecté devient ainsi un point d'entrée potentiel sur le réseau.

Les délais de réponse sont un autre problème dans un monde où les experts en sécurité doivent être disponibles 24/24h. Il suffit d'un clic malencontreux d'un salarié distrait pour qu'un malware se propage rapidement de machine en machine. Il est alors crucial d'identifier la compromission et de stopper l'infection au plus vite.

Certaines solutions intègrent des fonctionnalités de détection des attaques, de protection et de confinement automatique des terminaux présentant des signes de compromission. Si l'automatisation permet d'agir vite, le nombre élevé de faux positifs peut entraîner la mise en quarantaine de terminaux parfaitement sains. De même, la capacité d'application du jugement humain s'en trouve fortement limitée.

Avantages d'Endpoint Security Services :

- Augmentation de la vitesse et de la précision des interventions humaines/automatisées
- Réduction du temps d'analyse manuelle des journaux des terminaux
- Baisse des interruptions de service dues aux faux positifs
- Recommandations et bonnes pratiques pour renforcer la sécurité

Les opérations de remédiation débutent souvent par une analyse de la cause racine. Pour ce faire, il est nécessaire de passer au crible d'énormes quantités de données de journaux (logs) générées par tous les terminaux d'un même groupe ou réseau. Or, sans l'appui d'un moteur d'analyse des logs et d'experts chevronnés, des preuves et des indicateurs de compromission essentiels risquent de passer inaperçus, laissant l'attaque échapper à tout contrôle.

Schéma 1 : L'offre ESS de NTT gère un nombre croissant de produits de sécurité des terminaux. Elle se décline en trois formules pour mieux répondre aux besoins spécifiques de votre entreprise.

Endpoint Monitoring (EPM)

- Conformité aux règles de sécurité

Endpoint Detection (EPD)

- Conformité aux règles de sécurité
- Gestion des politiques
- Analytique avancée

Endpoint Response (EPR)

- Conformité aux règles de sécurité
- Gestion des politiques
- Analytique avancée
- Confinement à distance

Choisissez le degré de sécurité adapté à vos besoins

L'offre ESS de NTT est disponible sur la NTT Global Managed Security Service Platform. Elle allie les fonctionnalités de solutions EDR leaders aux capacités de Threat Intelligence et d'analytique avancée de NTT. Nous disposons également d'un centre opérationnel de sécurité (SOC) actif 24h/7j, où notre équipe d'experts se tient à votre disposition pour assurer un service managé (MSS) de support de votre solution de sécurité des terminaux. Vous réduisez ainsi le temps passé à analyser les logs des terminaux, bénéficiez de la vitesse et de la précision d'une automatisation validée par le jugement humain, diminuez les faux positifs et les interruptions de service associées, et recevez des conseils sur les bonnes pratiques de sécurité.

Les trois degrés de protection Endpoint Security Services

Endpoint Monitoring (EPM) : Ce niveau de service inclut une surveillance de la conformité, de la sécurité et des bonnes pratiques, ainsi que des rapports de conformité aux politiques internes. EPM établit des bases de référence au moyen des logs et tendances observées, ce qui lui permet d'envoyer des alertes personnalisées, d'établir des rapports de conformité et de recommander de bonnes pratiques d'utilisation des équipements de détection et de protection des terminaux.

Endpoint Detection (EPD) : Ce service allie les fonctionnalités de détection de solutions EDR leaders aux capacités de Threat Intelligence et d'analytique avancée de NTT. Par rapport à l'EPM, l'EDP montre d'un cran avec des technologies de machine learning, d'analyse comportementale et de modélisation de la kill-chain, le tout supervisé par des analystes experts en examens de preuves. Les indicateurs de compromission envoyés par l'équipement de sécurité sont suivis en temps réel, puis recoupés avec les services de sécurité cloud et réseau. Des corrélations peuvent ainsi être établies et renseignées par la Threat Intelligence de NTT . Enfin, les recherches et les recommandations sont compilées dans des rapports d'incident de sécurité clairs et concis, présentant un résumé des événements et des actions de remédiation conseillées.

Endpoint Response (EPR) : Ce service fait appel aux fonctionnalités d'isolement à distance des technologies EDR pour offrir un support rapide, efficace et 24h/7j de confinement de terminaux compromis. En cas d'alerte, la compromission est d'abord recoupée avec les watch-lists de NTT et soumise au jugement et à l'analyse approfondie d'experts. Ce processus permet de réduire le nombre de faux positifs susceptibles de paralyser des équipes entières. Et en cas d'incident avéré, vous bénéficiez d'une analyse pointue et de recommandations pour la remédiation.

A propos de NTT

NTT est un leader mondial des services technologiques. Convaincus qu'ensemble nous accomplissons de grandes choses, nous avons conjugué les capacités de 28 entreprises remarquables afin de créer un leader des services technologiques. En partenariat avec vous, nous mettons notre gamme complète de capacités hors pair au service de vos collaborateurs, stratégies, opérations et technologies. Ensemble nous préparons le futur connecté.

Vous souhaitez en savoir plus sur nos services de sécurité managés ?

Rendez-vous sur **hello.global.ntt**

