Forcepoint

Fiche technique

Forcepoint Data Detection and Response

Détection et réponse continues pour protéger vos informations les plus sensibles

Avantages et fonctions clés :

- **Détection des menaces et réponse en continu :** Forcepoint DDR surveille en permanence l'activité des données\ pour détecter les menaces de sécurité et y répondre dynamiquement, aidant à contenir et à atténuer les menaces avant qu'elles ne causent des dommages significatifs.
- **Analyse avancée des données et classification de l'IA :** en tirant parti de l'analyse des données avancées et de Forcepoint DSPM AI Mesh, Forcepoint DDR identifie les vulnérabilités des données et les activités suspectes, permettant une gestion proactive des menaces.
- **Visibilité complète des données :** Forcepoint DDR fournit une visibilité étendue sur les environnements cloud et de terminaux, empêchant les violations de données en s'assurant que les vulnérabilités potentielles sont traitées.
- **Amélioration des enquêtes sur les incidents :** en offrant des détails de niveau scientifique en traçant le cycle de vie d'un fichier, Forcepoint DDR améliore les enquêtes sur les incidents de sécurité, ce qui conduit à des décisions de remédiation plus précises et à une réduction des faux positifs.

Les entreprises sont aux prises avec une augmentation alarmante des violations de données, entraînée par l'adoption rapide du cloud computing et des technologies d'IA. Ces violations de données affectent les entreprises dans le monde entier, entraînant des pertes financières considérables et une atteinte à la réputation. Le défi réside dans la capacité de détecter et d'intervenir face à ces violations avant qu'elles ne se produisent en assurant la protection des données sensibles.

Forcepoint Data Detection and Response (DDR)

Forcepoint DDR powered by GetVisibility est une solution clé pour relever ces défis. Elle fournit une détection continue des menaces et une visibilité améliorée des risques liés aux données, en veillant à ce que les entreprises puissent efficacement voir les changements apportés aux données susceptibles d'entraîner des violations de données. En tirant parti des réponses basées sur l'IA, Forcepoint DDR offre la neutralisation des menaces, en aidant les entreprises à maintenir des mesures de sécurité robustes. Sa visibilité étendue sur le cloud et les terminaux, combinée au suivi de la lignée des données, en fait un outil essentiel pour la protection des informations sensibles, la réduction des pertes financières et le maintien de la confiance des clients.

Détection des menaces en continu et réponses basées sur l'IA

Forcepoint DDR fournit une détection en continu des menaces et une visibilité améliorée des risques liés aux données, en veillant à ce que les entreprises puissent identifier, surveiller et répondre aux menaces. En s'appuyant sur les réponses alimentées par AI Mesh de Forcepoint, Forcepoint DDR agit pour neutraliser les menaces, en offrant une défense robuste contre les violations de données.

Visibilité étendue sur le cloud et les terminaux

Forcepoint DDR offre une visibilité étendue sur les environnements cloud et de terminaux. Cette vue complète aide les entreprises à prévenir l'exfiltration des données et à s'assurer que les vulnérabilités potentielles sont surveillées et traitées. L'inclusion du suivi de la lignée des données améliore encore la capacité de contrer avec précision les violations potentielles.

Productivité améliorée et réduction des coûts

Grâce à une détection des menaces en continu et des réponses dynamiques, Forcepoint DDR permet aux équipes de sécurité de se concentrer, en les aidant à hiérarchiser les données et les changements d'autorisations en vue de détecter les violations de données potentielles en action. Cela améliore la productivité et soutient les objectifs organisationnels de réduction des coûts, de réduction des risques et de maintien de la confiance des clients.

Ajout clé à Forcepoint DSPM

Alors que les entreprises cherchent à sécuriser leur posture de données, en réduisant les données à risque sur le cloud et les emplacements sur site, Forcepoint DDR apporte une visibilité en continu des risques à Forcepoint DSPM. Au lieu d'avoir besoin d'exécuter d'abord une analyse de découverte complète des emplacements des données, Forcepoint DDR permet une surveillance continue de la posture de sécurité des données immédiatement après leur déploiement. Même sans analyses de découverte préalables, Forcepoint DDR détecte et active les mesures correctives pour les nouveaux risques liés aux données dès qu'ils se produisent. Cela permet de prévenir en permanence les nouveaux risques pour la posture globale de sécurité des données.

En intégrant ces fonctionnalités avancées, Forcepoint DDR protège non seulement les données, mais sécurise également l'avenir des organisations à l'ère de la GenAI et du cloud computing.

CARACTÉRISTIQUES	AVANTAGES
Surveillance continue	Obtenez une visibilité continue sur les activités de données à risque pour permettre aux entreprises de détecter les menaces potentielles et d'y répondre.
Alertes automatisées	Réduit le temps de réponse aux violations de données potentielles en hiérarchisant et en envoyant des alertes en fonction des menaces de risques pour les données détectées.
Détection des mouvements de données	Veille à ce que les données restent dans les limites autorisées, en protégeant la propriété intellectuelle et les informations sensibles.
Application des violations de politique	Garantit la conformité aux réglementations en matière de protection des données en détectant et en émettant des alertes en cas de violation des politiques.
Outils de conformité	Simplifiez la conformité aux exigences réglementaires grâce à une surveillance continue et des historiques de données détaillés pour simplifier les audits et les rapports de conformité.
Gestion proactive des risques	Définit et active l'application de ce qui constitue un risque au sein de l'entreprise à l'aide de politiques de gouvernance personnalisables.
Suivi des fichiers surexposés	Augmente la visibilité de l'exfiltration des données, en révélant une chaîne d'événements malveillants ou une violation accidentelle.
Intégration d'outils de sécurité tiers	Améliore la réponse aux incidents et la gestion des menaces grâce à l'intégration aux solutions SIEM et SOAR.
Couverture du cloud et des terminaux	Permet aux entreprises de comprendre et de sécuriser pleinement leurs données en fournissant une visibilité étendue sur l'écosystème des données.
Type de données et classification de sensibilité détaillés	Fournit une visibilité du contexte des données, permettant aux équipes de sécurité d'évaluer les risques et d'y répondre efficacement.
Classification de l'IA (AI Mesh)	Fournit une précision supérieure de la classification des données, efficace et hautement formable.
Capacités d'analyse forensique	Accroître la précision des corrections et réduire les faux positifs grâce à des enquêtes approfondies sur les incidents de sécurité.
Enquêtes dynamiques sur les incidents	Accélère les temps de réponse aux incidents, réduisant l'impact des incidents de sécurité et améliorant en permanence la posture de sécurité globale de l'entreprise.
Visibilité de la lignée des données	Permet aux entreprises de comprendre pleinement le cycle de vie de leurs données grâce à un suivi historique détaillé des fichiers non structurés.

Forcepoint

forcepoint.com/contact