Une protection complète contre les menaces internes

Proofpoint ITM protège efficacement et de manière proactive les données et les employés de l'entreprise contre les menaces provenant du réseau de l'entreprise.

Proofpoint ITM: les points forts

- Identification des risques pour les utilisateurs
- Prévention et clarification rapide sur les incidents internes
- Prévention des flux de données non autorisés (Data Loss Prevention)
- Respect de la protection des données et des employés
- Mise en service rapide grâce à plus de 350 ensembles de règles fournis
- Aucune connaissance particulière en matière de sécurité n'est requise pour l'utilisation
- On-Prem-Installation

Selon le Verizon Data Breach Investigation Report 2020, 30% des violations de données sont provoquées à l'interne – que ce soit par des motifs malveillants, par ignorance ou simplement par un comportement imprudent. Les employés internes et les sous-traitants contribuent donc largement au scénario de menace globale. En outre, les menaces internes ne sont généralement pas détectées avant longtemps et les entreprises touchées ne réagissent que lorsque le dommage est déjà fait. Les solutions classiques de cybersécurité ne suffisent pas pour se défendre contre les menaces internes et leurs conséquences. La solution innovante Insider Threat Management de Proofpoint adopte une approche différente: Proofpoint ITM utilise des informations contextuelles pour identifier les risques d'incidents de sécurité interne en collectant des données sur les rôles des utilisateurs, l'activité des utilisateurs, les alertes et les événements provenant de systèmes tiers tels que les solutions SIEM, ainsi que les modifications et les changements de données. Proofpoint ITM détecte tout comportement anormal sur la base des règles fournies et peut informer l'équipe de sécurité et les utilisateurs responsables à temps, avant même que des dommages ne surviennent. Si l'incident s'est déjà produit, la solution fournit des informations relatives à ce dernier pour une résolution rapide. Proofpoint ITM offre une protection fiable, proactive et conforme à la RGPD contre les pertes de données, les actions préjudiciables des employés, les dommages causés à la marque et les coûts de remédiation résultant d'une conduite interne malveillante, négligente ou inconsciente.

proofpoint.

Dépliant du fabricant
proofpoint / ITM

Insider Threat Management avec Proofpoint ITM

La plateforme Insider Threat Management (ITM) de Proofpoint met en corrélation les informations sur l'activité des utilisateurs et les mouvements de données, ce qui permet à l'équipe de sécurité informatique d'identifier les risques pour les utilisateurs, de prévenir les pertes de données et de réagir plus rapidement aux incidents de sécurité à l'interne.

Identification des risques pour les utilisateurs

Proofpoint ITM utilise des analyses sophistiquées et s'appuie sur des modèles de menace connus pour identifier et bloquer précocement les menaces internes potentielles. Proofpoint ITM contrôle également les employés et les sous-traitants qui ont accès au réseau de l'entreprise. La confidentialité est toujours préservée: la solution respecte toutes les exigences RGPD.

Protection contre la perte de données

La visibilité complète des mouvements de données de bout en bout – y compris les périphériques USB, le copier/coller, l'impression, la saisie en ligne de commande, le courrier électronique, les applications web et le stockage cloud – permet la détection immédiate des exfiltrations de données non autorisées, la prévention en temps réel et spécifique à l'application en fonction de l'activité de l'utilisateur et la sensibilisation des employés. Une console clairement agencée permet d'avoir une vue d'ensemble rapide.

Réaction rapide aux incidents de sécurité

Avec Proofpoint ITM, tout le contexte entourant les incidents de sécurité internes reste visible. Une réaction efficace à de tels incidents est possible en quelques minutes ou heures plutôt qu'en quelques jours ou semaines. Les utilisateurs concernés et l'équipe de sécurité sont immédiatement informés. Les éléments de preuve nécessaires à la prise de décision et à l'action en justice peuvent être rapidement rassemblés sans qu'il soit nécessaire d'avoir des connaissances approfondies en informatique.

Base de données complète

Les données de surveillance des utilisateurs proviennent de diverses sources, notamment des agents light installés sur les ordinateurs et serveurs, et des plateformes SIEM telles que Splunk, QRadar, McAfee ou LogRhythm. Un serveur dédié est utilisé pour analyser les accès des prestataires externes. Grâce à l'ensemble de plus de 350 règles préconfigurées, Proofpoint ITM peut être mis en service rapidement et efficacement sans avoir besoin de connaissances spécialisées en matière de sécurité.

BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com

BOLL
IT Security Distribution