GUIDE D'ÉVALUATION

Guide d'évaluation des solutions Proofpoint de sécurité des données

L'évaluation d'un produit logiciel pour vous assurer qu'il est adapté aux besoins de votre entreprise est une étape essentielle du processus d'achat. Un moyen courant d'y parvenir consiste à réaliser une validation de concept. En acquérant une expérience pratique d'un produit logiciel, vous pouvez déterminer rapidement si les besoins de votre entreprise et les cas d'utilisation pertinents sont pris en charge. Une validation de concept réussie élimine les conjectures et offre une expérience tangible. C'est la raison pour laquelle les validations de concept sont aussi importantes dans le processus de prise de décision.

Dressons une analogie avec l'achat d'une voiture : vous n'envisageriez pas d'acheter un nouveau véhicule sans l'avoir d'abord essayé, n'est-ce pas ? C'est cette expérience pratique de nos solutions de sécurité des données que nous vous offrons au moyen d'une validation de concept entièrement hébergée qui vous aide à comprendre comment votre entreprise peut se protéger contre les fuites de données et les menaces internes.

Défis associés aux validations de concept

Malgré les avantages de la réalisation d'une validation de concept, plusieurs défis peuvent empêcher son bon déroulement. Parmi les défis les plus courants :

- Absence de cas d'utilisation clairement définis
- Obtention des validations et des approbations internes
- Ressources humaines limitées
- Pas d'accès aux machines de test

Proofpoint offre une approche innovante des validations de concept qui élimine ces défis et vous permet de tester nos logiciels de manière rapide et efficace.

Validation de concept Proofpoint : rapide et efficace

Nous proposons un moyen facile et rapide d'acquérir une expérience pratique de nos solutions de sécurité des données. Notre validation de concept se déroule dans un environnement entièrement hébergé, qui met à votre disposition tous les outils dont vous avez besoin pour défendre les données et bloquer les menaces internes. Pendant deux semaines, vous pourrez tester les cas d'utilisation les plus courants. Une fois la validation de concept réalisée, Proofpoint vous aidera à documenter vos conclusions, afin que vous puissiez partager les résultats avec vos équipes.

1. Mise en route

Vous pouvez démarrer la validation de concept des solutions Proofpoint de sécurité des données le premier jour sans aucune configuration ni approbation nécessaire. Nous vous fournirons deux machines virtuelles et des identifiants de connexion pour vous permettre de simuler les actions des utilisateurs. Vous aurez également accès à notre environnement SaaS de sécurité des données afin d'étudier les actions des utilisateurs. La console centralisée vous permet de bénéficier d'une visibilité approfondie sur les comportements des utilisateurs grâce à une vue chronologique de leurs activités ainsi qu'à des métadonnées détaillées et des captures d'écran. Vous pourrez également trier les alertes, gérer les incidents, traquer les menaces et gérer les règles à partir de la même console, avec une vue multicanale sur les endpoints, la messagerie électronique, le cloud et le Web.

2. Cas d'utilisation

Pendant deux semaines, vous pourrez tester les scénarios utilisateur et les cas d'utilisation les plus courants :

- Utilisateur interne malintentionné essayant d'exfiltrer des données sensibles
- Utilisateur faisant preuve de négligence à l'égard des données sensibles
- Utilisateur faisant preuve de négligence à l'égard des données dans des applications d'IA générative
- Utilisateur compromis (attaque de phishing) entraînant la divulgation de données à un cybercriminel
- Utilisateur compromis (attaque par téléphone, ou TOAD) entraînant la divulgation de données à un cybercriminel
- Utilisateur faisant preuve de négligence à l'égard de la navigation Web

3. Conclusion

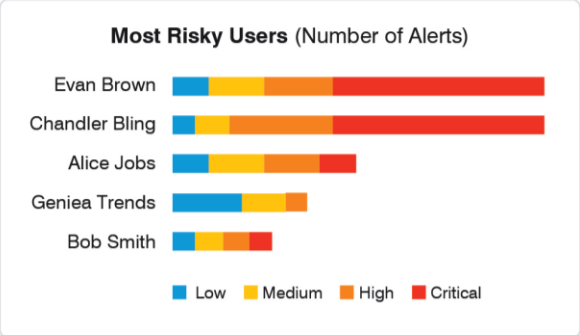
Une fois la validation de concept terminée, vous comprendrez mieux comment Proofpoint peut accélérer votre programme de prévention des fuites de données (DLP) ou de gestion des menaces internes. Une synthèse sera élaborée pour mettre en avant les cas d'utilisation et les avantages.

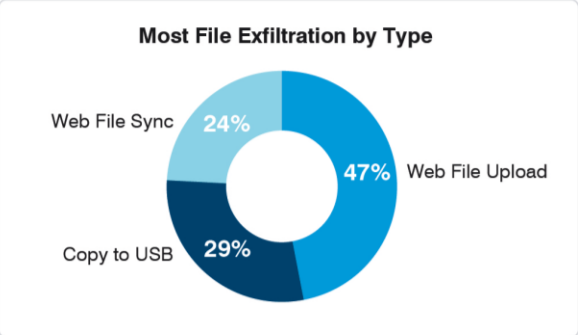
Exemples de critères d'évaluation

- Surveillance proactive des utilisateurs à risque au sein d'un tableau de bord centralisé
- Identification des données qui quittent l'entreprise et des méthodes employées
- Identification de l'événement déclencheur d'une règle et des données sensibles détectées
- Démonstration des changements de comportement des collaborateurs pour préserver la conformité et réduire les risques
- Détection de l'utilisation d'une application non autorisée

- Détection et prévention de l'exfiltration de données sensibles via des chargements sur le Web, des clés USB ou la synchronisation cloud
- Identification et prévention de l'exfiltration de données sensibles par email
- Détection et correction automatique des menaces cloud et de l'exfiltration de données
- Surveillance, détection et prévention de l'exfiltration de données via des sites d'IA générative
- Détection des modifications apportées au nom et au type d'un fichier
- Blocage automatique des emails les plus susceptibles d'entraîner des fuites de données
- Recherche et filtrage des données d'activité pour trouver rapidement des réponses
- Affichage d'une chronologie des activités d'un utilisateur avant, pendant et après un incident
- Affichage d'un historique des activités d'un utilisateur
- Enregistrement de captures d'écran pour la collecte de preuves numériques
- Distinction entre un utilisateur négligent, compromis et malveillant
- Exportation d'un rapport facilement compréhensible des activités des utilisateurs pour les RH et le service juridique
- Formation des utilisateurs grâce à des notifications et des demandes de justification contextuelles

Résumé de la sécurité des données





8
Users browsing to GenAI websites

20
Files automatically remediated for oversharing

45
Blocks of unapproved web file upload

80
Sensitive emails send to unauthorized accounts

Avantages d'une validation de concept Proofpoint

Aucune configuration ni approbation n'étant nécessaire, vous pouvez commencer à tester immédiatement les solutions Proofpoint de sécurité des données dans un environnement entièrement hébergé.

Délai de rentabilisation réduit

Une validation de concept Proofpoint prend moins de deux semaines et offre un moyen facile et rapide d'acquérir une expérience pratique et d'accélérer le processus de prise de décision.

Résultats mesurables

Vous pouvez tester les scénarios utilisateur et les cas d'utilisation les plus courants grâce à un accès total aux solutions Proofpoint de sécurité des données, vous offrant une visibilité multicanale sur les endpoints, la messagerie électronique, le cloud et le Web.

Validation de concept Proofpoint : incomparable à une validation de concept standard

CRITÈRES	VALIDATION DE CONCEPT STANDARD	VALIDATION DE CONCEPT PROOFPOINT
Délai de configuration	Plusieurs semaines ou mois en fonction des approbations	Quelques heures
Durée	Plusieurs semaines ou mois	Moins de 2 semaines
Intervention des clients	Importante	Minimale
Machines de test dédiées	Nécessaires pour la validation de concept	Pas nécessaires pour la validation de concept
Cas d'utilisation	Doivent être clairement définis	La plupart sont disponibles dès la mise en service ; d'autres, plus spécifiques, peuvent être ajoutés