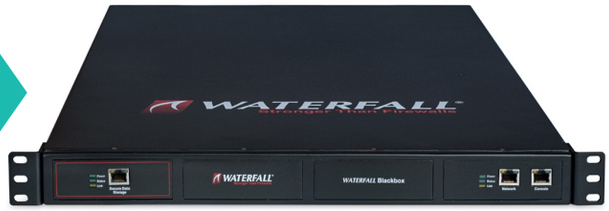
WATERFALL®
Stronger Than Firewalls

Fiche technique

Waterfall BlackBox™ : In Logs We Trust™



Lorsqu'une cyber-attaque est découverte, les spécialistes forensiques examinent les différents logs du réseau compromis pour localiser et analyser les traces laissées par les intrus. Les logs, ou fichiers journaux, constituent les informations de référence essentielles pour une investigation et une réponse de qualité à l'incident. Ils contiennent les traces et des renseignements sur l'attaque et l'attaquant. Mais l'agresseur, une fois qu'il a pénétré votre réseau, peut prendre les commandes et supprimer ou altérer les informations compromettantes dans les logs. Effacer ses traces est l'une des règles de base du cyber-assaillant... Cette vulnérabilité touche tous les systèmes d'archivage de logs, locaux, centralisés et sur le cloud.

Pour offrir aux archives de logs une sécurité renforcée, Waterfall a créé la BlackBox. Étudiée pour les équipes de réponse aux incidents , les experts forensiques et tous les professionnels de l'audit informatique, elle garantit la conservation de données de log fiables. Brevetée, et basée sur technologie brevetée et innovante de sécurité unidirectionnelle de Waterfall, la BlackBox établit une barrière physique entre le réseau et les données de log. Ainsi, les données envoyées à la BlackBox sont stockées physiquement « à l'extérieur » du réseau, inaccessibles à quiconque chercherait à effacer ses traces, et inaltérables.

Caractéristiques principales

Capacité

- Sources de log multiples:
  - » Syslog TCP/UDP
  - » SNMP
  - » Fichiers
  - » Autres (Bases de données, MQ, protocoles industriels)
- Transmission de log en temps réel à haute vitesse (1Go/s, latence en ms)Variable storage sizes
- Différentes tailles de stockage

Gestion des données

- Les logs de toutes les sources sont centralisés et stockés dans une base de données relationnelle interne
- Chiffrement à clé publique de tous les logs, côté interne
- Base de données cyclique, limites de dépassement de volume

Extraction de logs

- Utilisation de port hors réseau dédié
- Application d'extraction de données conviviale
- Vidage complet, partiel avec fonctions de recherche et de filtre

Fonctions additionnelles

- Gestion de versions multiples de fichiers
- Affichage en temps réel des statistiques
- Module interne de maintenance de l'ensemble des composants système

Format

La BlackBox s'adapte aux exigences de votre mission. Elle est proposée en deux formats.

Figure 1: *1U à monter sur rack*

BlackBox à monter sur rack

La BlackBox 1U à monter sur rack est installée et réside sur votre topologie de réseau. Elle collecte activement et en continu toutes les données de log applicables.

Dimensions:
450mm X 45mm x 500mm

Figure 2: *Field Deployable Carry-On BlackBox*

Carry-On BlackBox

Portable, la Carry-On BlackBox déployable sur le terrain est destinée aux membres de l'équipe de réponse et à tout le personnel de terrain. Elle peut être installée et résider sur votre topologie de réseau pour collecter en continu les logs applicables. Elle peut aussi être déployée par l'équipe forensique sur le site d'une brèche de sécurité présumée pour recueillir tous les logs suspects, et être ensuite soit accessible sur site, soit « transportée » là ou l'équipe forensique effectue les analyses.

Dimensions:
450mm X 180mm X 420mm

La BlackBox 1U à monter sur rack et la Field Deployable Carry-On BlackBox sont toutes deux configurées avec alimentation redondante et transmission de log en temps réel à haute vitesse (1Go/s, faible latence).

Les deux formats sont disponibles en l'une des deux capacités de stockage interne suivantes:

- Basic - 0.5 TB
- Extended - 8.5 TB

À propos de Waterfall Security Solutions

Waterfall Security Solutions est le leader mondial des solutions de cybersécurité industrielle employant la technologie de communications unidirectionnelles imposées par le matériel. Au service de la protection des systèmes de contrôle industriel et des infrastructures critiques contre les cyberattaques provenant de réseaux extérieurs, les produits Waterfall constituent une alternative évolutive aux pare-feu. Chaque jour plus nombreux, les clients de Waterfall sécurisent avec son aide infrastructures nationales, entreprises de services publics, usines, centrales électriques et nucléaires, plateformes onshore et offshore, raffineries et autres sites industriels. Déployés en Amérique du Nord, en Europe, en Asie et au Moyen-Orient, les produits Waterfall prennent en charge les principales plateformes, applications, bases de données et protocoles de la surveillance industrielle à distance.

WATERFALL®
Stronger Than Firewalls

Pour plus d'informations, contactez-nous:
+33 (0) 1 46 14 87 28 | france@waterfall-security.com
www.waterfall-security.com