



FICHE PRODUIT

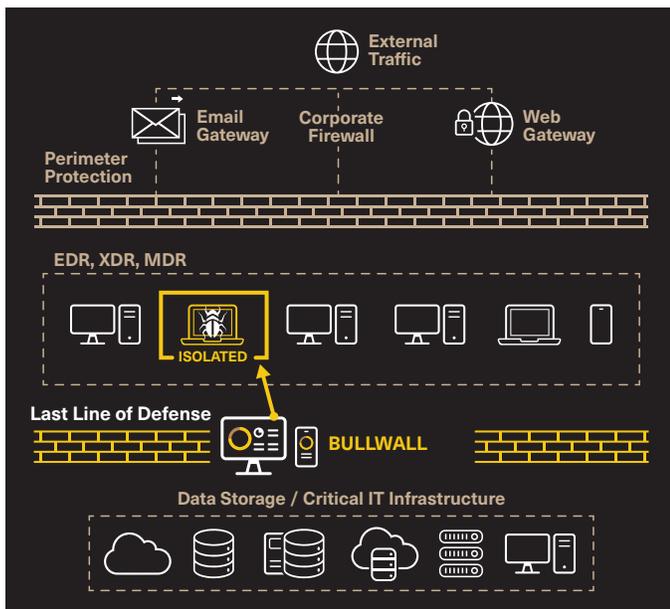
BULLWALL RANSOMWARE CONTAINMENT

L'INTERRUPTEUR DE RANSOMWARE



La plupart des organisations ont déjà investi et mis en place de solides couches de sécurité, pourtant elles continuent d'être impactées par les rançongiciels (ransomwares). Les attaquants déjouent constamment les solutions de sécurité les plus robustes ; l'évolution des méthodes et des tactiques empêche les éditeurs de solutions de sécurité traditionnelles d'y faire face. **La protection des postes de travail n'est plus suffisante.**

BullWall Ransomware Containment est une défense active qui interrompt les attaques de ransomware au niveau des partages de données et de l'infrastructure IT critique en isolant automatiquement les utilisateurs et les appareils compromis, protégeant ainsi les données essentielles de l'organisation et limitant les temps d'arrêt.



RANSOMWARE CONTAINMENT LE NIVEAU DONT VOUS AVEZ BESOIN.

BullWall Ransomware Containment détecte et réagit à la seconde même où le chiffrement illégitime démarre. BullWall est la seule solution qui se concentre sur le niveau des fichiers, la partie vulnérable, afin de minimiser la propagation des rançongiciels au lieu de tenter en vain de les reconnaître et de les prévenir.

LA SEULE APPROCHE FIABLE À CETTE CYBERMENACE COÛTEUSE ET INÉVITABLE.

BullWall ne dépend pas de méthodes de détection dépassées telles que les signatures de ransomware, les souches, les modèles ou le comportement. Au contraire, BullWall détecte instantanément l'action malveillante du ransomware : le chiffrement des fichiers. Et ce, sans surcharge du réseau ni



Sans agent et facile à déployer

Rien à installer sur les postes



Protège toute l'infrastructure IT critique



Rapport d'incident Automatisé de conformité

GDPR, NIST, NIS2, DORA



Détection & Réponse Automatisée 24/7

dégradation des performances. BullWall se démarque en surveillant l'activité sur les partages de fichiers, les serveurs d'applications et les serveurs de bases de données.

Grâce à l'apprentissage automatique, BullWall analyse l'activité des fichiers et utilise des capteurs de détection pour identifier les menaces. Dès que BullWall détecte un chiffrement malveillant, il isole le ou les utilisateurs et appareils compromis en quelques secondes, empêchant ainsi davantage de dommages aux partages de fichiers et les répercussions financières et réglementaires.

COMPLÈTE ET DURCIT L'INFRASTRUCTURE DE SÉCURITÉ EXISTANTE

BullWall s'intègre à votre pile de sécurité existante (ITAM, SOC, SIEM, EDR, NAC) via des API Web RESTful et opère en parallèle avec des éditeurs comme Carbon Black, CrowdStrike, McAfee, Symantec, SentinelOne, Sophos, et bien d'autres encore - apportant une couche de protection complémentaire et maximisant les investissements dans les sécurités existantes. BullWall est totalement évolutif, de la PME à la multinationale, quelle que soit la taille de l'infrastructure IT, le volume ou le type d'applications de fichiers utilisées.

BullWall Ransomware Containment démontre régulièrement sa capacité à endiguer le pire des scénarios, en intervenant comme un niveau de défense vital, réduisant les dommages, les perturbations et les coûts des attaques déclenché de ransomware



AGENTLESS



LÉGER



FACILE À INSTALLER



**ENTIÈREMENT
AUTOMATISÉ**



**AUCUNE
SURVEILLANCE REQUISE**



**INTÉGRABLES AUX SOC,
SIEM, NAC, EDR...**



PROTECTION CONTRE LES RANSOMWARES

1

Monitore & Détecte

Monitore l'activité des fichiers en temps réel sur les partages de fichiers SAN/NAS, les machines virtuelles, les contrôleurs de domaine, les serveurs de base de données et les serveurs d'applications, on-prem et dans le cloud.

28 capteurs de détection et des capacités de machine learning permettent de reconnaître instantanément le chiffrement illégitime et l'exfiltration.

2

Isole et quarantaine

Active immédiatement et automatiquement un protocole d'isolation et de confinement des utilisateurs et des appareils compromis à l'origine d'un chiffrement illégitimes.

Déploie des scripts intégrés pour bloquer le chiffrement des fichiers et l'exfiltration des données en quelques secondes.

Alerte le service IT via un tableau de bord intégré, un e-mail, un SMS, une application ou une intégration avec un SIEM, un NAC, un EDR et d'autres solutions de sécurité via une API RESTful.

3

Recuperation & Reporting

Liste automatiquement tous les fichiers chiffrés afin qu'ils puissent être restaurés à partir d'une sauvegarde.

Automatise entièrement les rapports d'incidents de conformité avec un registre détaillé de tout l'historique de l'attaque, adapté aux besoins de communication internes et externes des agences gouvernementales (CNIL/GDPR/DPA)

L'INTÉGRATION AVEC LES PRINCIPALES SOLUTIONS DE SÉCURITÉ



Les ransomwares actuels chiffrent 50 000 fichiers par minute et par machine infectée.

BULLWALL LES STOPPENT

A PROPOS DE BULLWALL

BullWall est un éditeur de solutions de cybersécurité dédié à la protection des infrastructures IT critiques contre les ransomwares. Nous assurons un confinement rapide des attaques actives et protégeons les serveurs en empêchant les intrusions non autorisées.

Plus d'info: www.bullwall.com.

