TRITON® AP-WEB

UNE PROTECTION COMPLÈTE EN TEMPS RÉEL CONTRE LES MENACES AVANCÉES ET LE VOL DE DONNÉES

FORCEPOINT
POWERED BY Raytheon

TRITON® AP-WEB

UNE PROTECTION COMPLÈTE EN TEMPS RÉEL CONTRE LES MENACES AVANCÉES ET LE VOL DE DONNÉES

Votre société et ses données font l'objet d'attaques constantes. La protection offerte par les solutions de sécurité traditionnelles ne suffit plus. En réalité, elles peuvent vous exposer à un risque de perte de données et de procès. Protéger votre réseau et vos données contre les menaces avancées, le harponnage et les kits d'exploits est primordial pour la survie de vos activités dans un monde numérique en pleine croissance et risqué.

Personnalisable, avec la possibilité de l'étendre

Les sociétés ont besoin de solutions personnalisables pour répondre à leurs besoins tout en respectant leur budget, afin de se prémunir contre ces types de menaces lorsqu'elles font leur apparition. TRITON AP-WEB confère une protection en temps réel face aux menaces avancées et au vol de données. Cette solution propose de nombreuses options de déploiement et différents modules pour vous aider à adapter votre kit de protection sur le Web à vos besoins.

Que vous ayez besoin d'une protection pour des utilisateurs sur site ou distants, que vous ayez besoin de défenses intégrées contre le vol de données ou d'une solution pour les utilisateurs mobiles, TRITON AP-WEB fournit la couverture adéquate et la protection dont vous avez besoin. Ni plus, ni moins.

Les défis de la sécurité sur le Web

La plupart des solutions de sécurité actuelles ne sont pas en mesure de neutraliser les menaces avancées dès leur apparition. TRITON AP-WEB est une solution de défense avancée contre les menaces, qui agit en temps réel.

RÉDUISEZ LES RISQUES

Des déploiements de sécurité complexes, non coordonnés et impliquant plusieurs fournisseurs augmentent les risques pour la sécurité. TRITON AP-WEB offre une protection totalement intégrée sur l'ensemble de la chaîne de frappe.

METTEZ UN TERME AU VOL DE DONNÉES

Les solutions de DLP autonomes sont trop complexes à déployer. TRITON AP-WEB offre une DLP totalement intégrée et facile à déployer, avec la meilleure protection disponible sur le marché.

PROTÉGEZ UNE FORCE DE TRAVAIL MOBILE

Étendez votre protection en toute transparence des locaux jusqu'aux travailleurs distants et mobiles avec la même solution.

« Nous avons besoin d'une solution qui nous protège contre les menaces Web les plus récentes, qui dispose d'une DLP intégrée et qui optimise la productivité du personnel. [Forcepoint] fait tout cela, tant sur site qu'en mode SaaS. Il n'est pas étonnant que Forcepoint soit leader sur le marché. »

– Ben Schoenecker, Spécialiste de la sécurité informatique
AllSouth Federal Credit Union

TRITON AP-WEB

ANALYSE EN TEMPS RÉEL POUR UNE PROTECTION CONTRE LES MENACES AVANCÉES

TRITON AP-WEB surclasse les défenses antivirus traditionnelles en utilisant huit domaines d'évaluation de la protection au sein d'un modèle de notation complexe doté d'une fonction d'analyse prévisionnelle avec le moteur ACE (Advanced Classification Engine) de Forcepoint™. Plusieurs moteurs de contenu en temps réel analysent l'ensemble du contenu des pages Web, les scripts actifs, les liens Web, les profils contextuels, les fichiers et les exécutables.

ACCÈS SIMPLIFIÉ AU TABLEAU DE BORD POUR CONSULTER LES DONNÉES D'EXPERTISE

Le tableau de bord des menaces sophistiquées de la solution TRITON AP-WEB fournit des rapports approfondis sur la victime de l'attaque, les données qui étaient ciblées, la destination prévue des données et la manière dont l'attaque s'est déroulée. Les incidents de sécurité incluent la saisie du vol de données lorsque cela est possible. Les défenses analysent les communications entrantes et sortantes.

DÉFENSES INTÉGRÉES CONTRE LE VOL DE DONNÉES

Les meilleures défenses intégrées contre le vol de données sur le marché (en option) détectent et interceptent les tentatives de vol de données et offrent une conformité réglementaire pour la prévention des pertes de données (DLP). Voici quelques exemples de ces capacités : la détection des chargements à cryptage personnalisé, le vol des mots de passe, les fuites de données lentes (« Drip DLP »), ainsi que la reconnaissance optique des caractères (ROC) pour le texte contenu dans les images et la sensibilisation aux destinations de géolocalisation.

SANDBOXING INTÉGRÉO

Découvrez comment mieux protéger les actifs de votre société en analysant le comportement des programmes malveillants avec le service optionnel de sandboxing intégré.

Modules de protection améliorée

MODULE DÉMATÉRIALISÉ OU HYBRIDE POUR LE WEB	**Étendez la protection Web et l'application des politiques aux utilisateurs distants** Déployez une solution TRITON AP-WEB 100 % sur site, avec notre offre de dispositif évolutif. Choisissez un déploiement 100 % dématérialisé ou déployez un réseau hybride. C'est à vous de choisir, en fonction de vos besoins en matière de réseau.
MODULE DE DLP SUR LE WEB	**Ajoutez un puissant moteur de DLP sensible au contenu pour une protection sortante supplémentaire contre le vol de données** Le Module de DLP sur le Web offre des défenses isolantes contre le vol de données, et permet une conformité réglementaire avec plus de 1 700 politiques et modèles prédéfinis. Il inclut également la meilleure protection du marché, avec notamment la technologie « Drip DLP » contre les fuites de données lentes, la reconnaissance optique des caractères (ROC) contre le vol de données dans les images, ou encore la détection des chiffrements personnalisés pour détecter les fichiers cryptés à des fins criminelles.
MODULE DE SANDBOXING SUR LE WEB	**Intégrez le sandboxing comportemental pour une analyse automatique et manuelle des fichiers malveillants** Analysez les fichiers suspects dans un environnement virtuel et regardez au-delà de la simple exécution de fichier pour bénéficier du plus haut degré de protection contre les programmes malveillants avancés. Des rapports d'expertise détaillés sont automatiquement fournis lorsque des fichiers malveillants sont détectés.
TRITON AP-MOBILE	**Étendez les politiques et la protection aux utilisateurs d'appareils iOS et Android** Autorisez l'utilisation des appareils mobiles sur votre lieu de travail en appliquant vos politiques de sécurité existantes aux appareils mobiles pour les protéger contre les menaces avancées, les programmes malveillants mobiles, les attaques de hameçonnage, les usurpations et bien plus encore.
TRITON APX	**La solution recommandée par Forcepoint pour une protection avancée** Étendez la protection dont vous disposez grâce à TRITON AP-WEB, TRITON AP-EMAIL, TRITON AP-DATA ou TRITON AP-ENDPOINT pour bénéficier d'une protection puissante et unifiée sur l'ensemble des canaux d'attaque.

Autres capacités

PROTECTION DES UTILISATEURS DISTANTS
Gérez les utilisateurs qui travaillent dans la société, dans les succursales et à distance avec une seule console et une seule politique grâce aux modules dématérialisés ou hybrides.

PROTECTION DES UTILISATEURS MOBILES
Étendez les politiques et les paramètres de sécurité aux appareils Android ou iOS en y intégrant la solution TRITON AP-MOBILE.

INSPECTION SOUPLE DU SSL
Les capacités d'inspection approfondie du SSL vous permettent de surveiller le trafic HTTPS tout en préservant les exigences de vie privée et réglementaires.

CONTRÔLE PRÉCIS DES RÉSEAUX SOCIAUX
Les contrôles des réseaux sociaux offrent une grande souplesse. Les contrôles vidéo limitent ou empêchent de visionner des vidéos virales, de divertissement et de surveillance, tout en permettant l'accès à des vidéos éducatives sur YouTube.

CONTRÔLE DES APPLICATIONS ET DES PROTOCOLES
L'Agent réseau offre un contrôle précis sur des centaines de protocoles et d'applications pour une stratégie de sécurité améliorée.

CRÉATION DE RAPPORTS SOUPLE
Quatre tableaux de bord personnalisables et plus de 60 rapports prédéfinis et personnalisables offrent des informations techniques et professionnelles faciles à lire, ainsi que de précieux renseignements sur les niveaux de menace et bien plus encore.

PLUSIEURS OPTIONS DE DÉPLOIEMENT
Optez pour un déploiement sur site avec un dispositif physique, un déploiement hybride pour protéger les utilisateurs distants, ou un déploiement totalement dématérialisé.

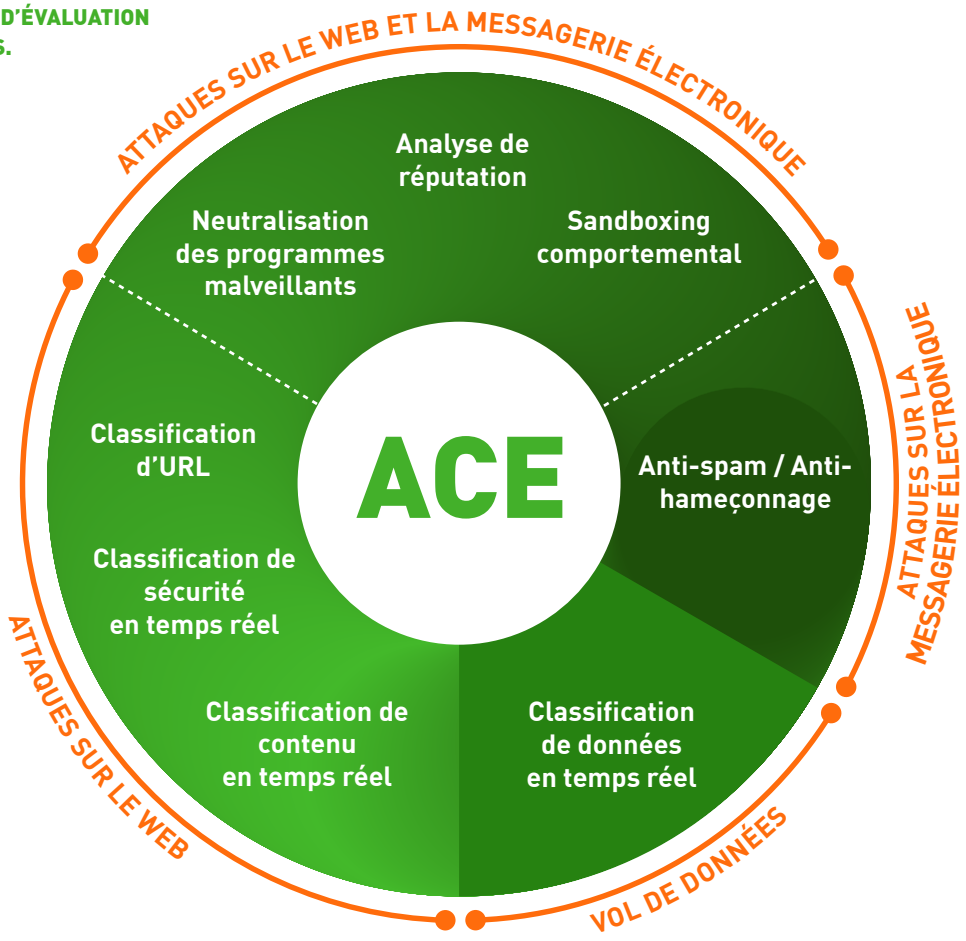
La puissance sous-jacente aux solutions TRITON

Moteur de classification avancée (ACE)

Le moteur ACE de Forcepoint fournit une protection contextuelle en ligne et en temps réel pour le Web, la messagerie électronique, les données et la sécurité mobile et s'appuie sur une analyse prédictive et un calcul composite des risques pour offrir la sécurité la plus efficace du marché. Il sécurise les contenus en analysant les communications entrantes et sortantes à partir de la meilleure protection du marché basée sur les données pour éviter le vol de ces dernières. Des classificateurs conçus pour l'analyse de la sécurité, des données et du contenu en temps réel — le résultat d'années de recherche et de développement — permettent au moteur ACE de détecter chaque jour davantage de menaces que les moteurs antivirus traditionnels (la preuve est mise à jour quotidiennement sur le site http://securitylabs.forcepoint.com). Le moteur ACE est la principale défense intégrée dans les solutions TRITON® de Forcepoint, et est pris en charge par le réseau Forcepoint ThreatSeeker® Intelligence Cloud.

UN ENSEMBLE INTÉGRÉ DE CAPACITÉS D'ÉVALUATION DES DÉFENSES DANS 8 DOMAINES CLÉS.

- 10,000 analyses disponibles pour étayer des inspections approfondies.
- Le moteur de sécurité prédictive permet de toujours garder plusieurs longueurs d'avance.
- Le fonctionnement en ligne surveille les menaces et les **bloque**.



ThreatSeeker® Intelligence Cloud

Le ThreatSeeker Intelligence Cloud, géré par Forcepoint Security Labs™, propose les informations de sécurité collectives essentielles pour tous les produits de sécurité Forcepoint. Il réunit plus de 900 millions de postes de travail, y compris des contributions de Facebook. Conjointement avec les défenses de sécurité ACE, il analyse jusqu'à 5 milliards de requêtes par jour. Ce vaste ensemble de connaissances sur les menaces à la sécurité permet au ThreatSeeker Intelligence Cloud d'offrir des mises à jour de sécurité en temps réel qui neutralisent les menaces avancées, les logiciels malveillants, les attaques de hameçonnage, les leurres et les arnaques, et propose les dernières évaluations Web. Le ThreatSeeker Intelligence Cloud est sans égal en termes de taille et dans son utilisation des défenses en temps réel d'ACE pour analyser les contributions collectives. (Lorsque vous optez pour une solution de sécurité sur le Web, le ThreatSeeker Intelligence Cloud aide à réduire votre exposition aux menaces sur le Web et au vol de données.)

Architecture TRITON

Avec la meilleure sécurité de sa catégorie, l'architecture unifiée TRITON de Forcepoint offre une protection par pointer-cliquer combinée à des défenses en ligne et en temps réel de Forcepoint ACE. Les défenses en temps réel inégalées d'ACE sont soutenues par Forcepoint ThreatSeeker Intelligence Cloud et par l'expérience des chercheurs de Forcepoint Security Labs. Résultat : vous bénéficiez d'une architecture unique et unifiée avec une interface utilisateur centralisée et des renseignements de sécurité unifiés.

TRITON APX

TRITON APX confère de nombreux avantages clés aux sociétés qui souhaitent déployer la meilleure protection possible contre les menaces avancées sur la chaîne de frappe divisée en 7 étapes. Ces avantages peuvent se résumer en trois points :

- **Déployer une sécurité adaptative –** Déployez des solutions de sécurité adaptative nécessaires pour les technologies et menaces en constante évolution.
- **Protéger partout –** Les données sont votre périmètre. Protégez vos informations critiques contre le vol, que ce soit sur site, en mode SaaS ou sur les périphériques mobiles.
- **Élever le QI de la sécurité –** Combattez le manque d'aptitudes en cybersécurité en fournissant des renseignements prédictifs exploitables à travers tout le cycle de vie des menaces.

CONTACT
www.forcepoint.com/contact

[BROCHURE_TRITON_AP_WEB_FR] 400002FR.011416

FORCEPOINT
POWERED BY Raytheon