HAFS
Smart Distributeur Africa

SECPOINT®

About SecPoint® - Best Cyber Security

A PROPOS

Made in Denmark

SecPoint® est une entreprise européenne de sécurité informatique de premier plan et des plus innovantes, dont le siège se trouve au Danemark.

C'est l'entreprise la plus compétitive dans le domaine de la sécurité informatique avec une large gamme de produits, y compris des UTM, des produits de Pen-Testing et des services Cloud, offrant des solutions faciles à utiliser pour tous les besoins de sécurité informatique.

SecPoint® a conçu le Cloud Penetrator en 2001, le Penetrator Appliance en 2003, le Protector UTM en 2005 et le Portable Penetrator en 2007. Depuis lors, les trois variantes ont connu un développement continu, avec de nombreuses mises à jour du micrologiciel offrant de nouvelles fonctionnalités intéressantes.

SecPoint® est présent dans le monde entier depuis 1999 et son siège social se trouve à Copenhague, au Danemark. Elle fournit des produits de sécurité haut de gamme à des clients du monde entier, via des bureaux au Danemark, en Suède, en Italie, aux Pays-Bas et en Grèce. Nous disposons actuellement d'un réseau de plus de 500 partenaires dans le monde entier.

Nous avons actuellement plus de 1200 clients Protector et 1600 clients Penetrator qui comptent sur les produits de sécurité informatique avancés de SecPoint® pour le bon fonctionnement de leur entreprise.

Chiffre d'affaires inférieur à 20 millions d'euros. Équipe de plus de 50 personnes réparties dans les différents bureaux.

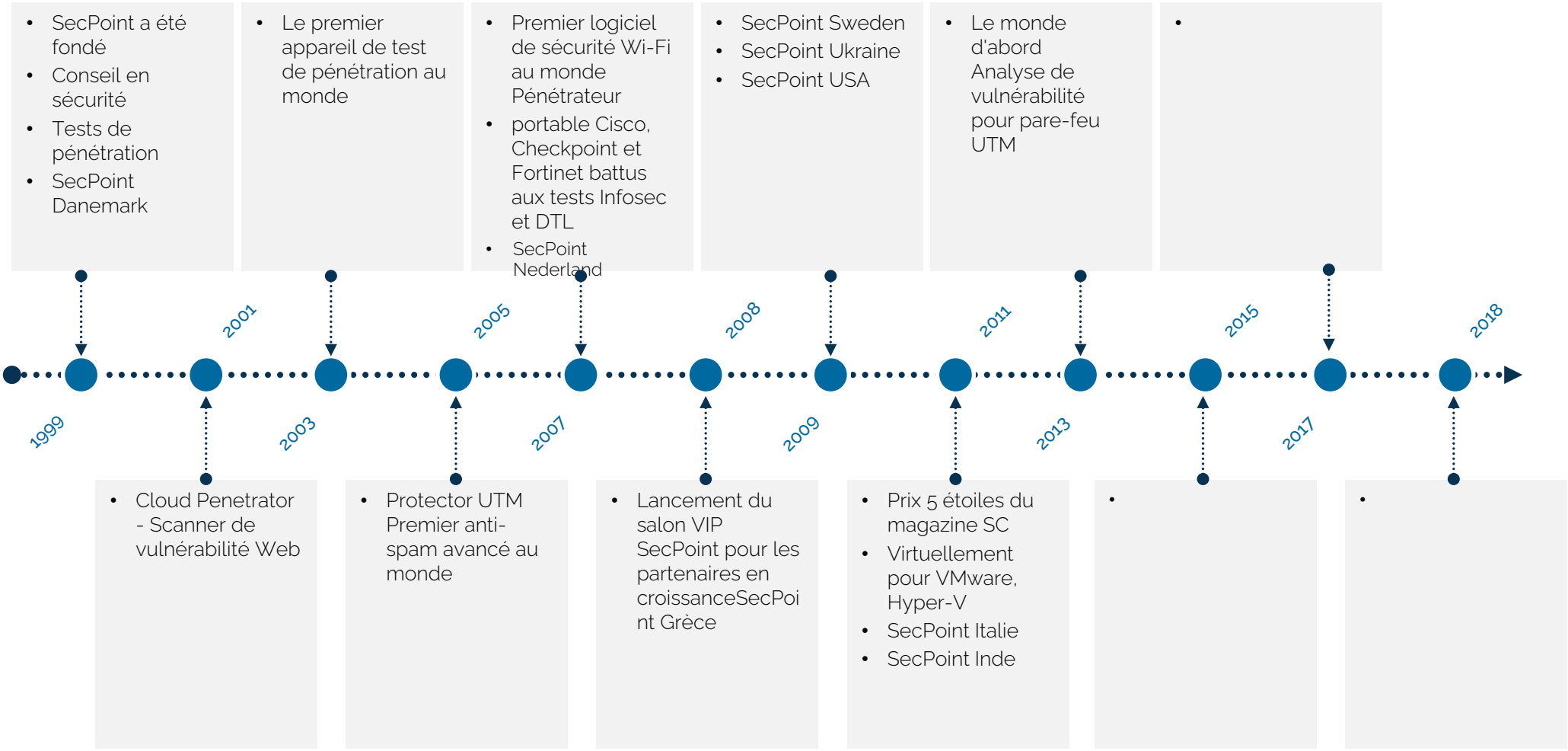
SecPoint Offices

SecPoint® a des bureaux au Danemark, en Suède et aux Pays-Bas. Un réseau de vente composé de centaines de revendeurs et de distributeurs agréés dans le monde entier. SecPoint® met à la disposition de tous ses partenaires un gestionnaire de compte dédié, afin qu'ils reçoivent une assistance personnalisée en cas de doutes ou de questions, ainsi qu'une formation et du matériel de vente pour leur assurer le meilleur rendement possible. Il existe également une boutique en ligne interactive réservée aux partenaires, qui permet de créer des unités de démonstration gratuites pour que les clients puissent les évaluer. Les partenaires sont également libres de fixer leurs propres prix.

Removing Complexity

Avec SecPoint® 'No Hidden Cost Policy', les clients ont la possibilité d'obtenir la solution dont ils ont besoin sans aucun coût supplémentaire. Les produits sont dotés de nombreuses fonctionnalités, mais les clients n'ont pas besoin de les payer séparément. Le concept est simple. Les autres entreprises cachent toujours leurs prix. Elles affichent aux entreprises leur prix le plus bas, ce qui revient à payer le prix de l'appareil, mais avec des fonctionnalités négligeables. Avec SecPoint®, les clients bénéficient de toutes les fonctionnalités sans coût supplémentaire et sans modules de sécurité supplémentaires, car tout est déjà inclus dans le produit que le client achète en premier lieu.

SECPOINT - HISTOIRE CHRONOLOGIQUE



SECPOINT – BUREAUX MONDIAUX

- O

Pour obtenir des informations de contact complètes et actualisées, veuillez consulter le site : https://www.secpoint.com/contact.html

1999

Denmark

2007

The Netherlands

2008

Greece (Hellas)
& Cyprus

2009

Sweden

Ukraine

U.S.A.

2011

Italy

India

SecPoint a des bureaux régionaux en Europe, en Asie et en Amérique.

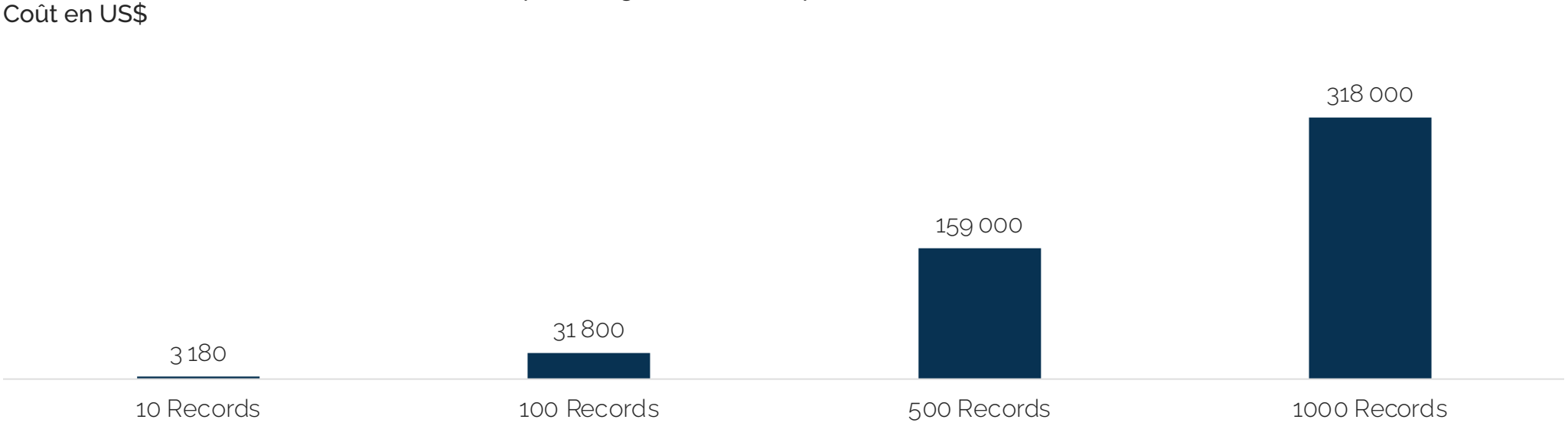
SecPoint attache une grande importance à la qualité et à la rapidité de son support.

SecPoint accorde une grande importance à la qualité et à la rapidité de l'assistance.

COÛT ET RISQUE DU PIRATAGE DES SYSTÈMES D'INFORMATION

Les attaques des pirates informatiques entraînent des coûts pour les organisations qui peuvent avoir plusieurs conséquences telles que:

- La perte de réputation et de confiance nuit à la marque.
- Perte de confiance des clients, de revenus, de rentabilité et de réputation.
- Perte de la capacité d'accepter des options de paiement via VISA, Mastercard et d'autres cartes de crédit.
- Temps d'arrêt des employés pouvant entraîner une perte de production.
- Temps d'arrêt du site web affectant le classement dans Google et perte de nouveaux clients potentiels.
- Les conséquences juridiques de la perte de données confidentielles sur les clients entraînent des amendes et des dommages-intérêts.
- Coût 2010 Selon l'Institut Ponemon, 318 $ par enregistrement compromis.



TYPES D'ATTAQUES COURANTS DES SYSTEMES D'INFORMATIONS

Remote Code Execution	Peut permettre aux attaquants d'exécuter du code sur le système cible et conduire à une compromission totale.
SQL Injection	Ancienne forme d'attaque, mais toujours très populaire. Permet à un attaquant de récupérer des informations sensibles dans la base de données d'un serveur web. peut entraîner la compromission totale du système.
Cross Site Scripting (XSS)	Les attaquants incitent la victime à exécuter une URL malveillante qui peut sembler légitime à première vue.
Format String vulnerabilities	Cela est dû à une mauvaise programmation, qui peut permettre à un attaquant d'imprimer des données à partir d'emplacements dans la mémoire. Il peut également permettre d'écrire des données arbitraires pour compromettre le système cible.

TYPES D'ATTAQUES COURANTS DES SYSTEMES D'INFORMATIONS

Username Enumeration	Permet à un attaquant de deviner les utilisateurs réels de la cible et peut conduire à d'autres attaques.
Denial of Service DoS attacks	Allows an attacker to shutdown or prevent a web server from serving the purpose. This can block a site from receiving orders as an example.
Human mistakes	Cela peut permettre à des attaquants de révéler des fichiers ou des répertoires sensibles qui sont le résultat d'erreurs humaines et de mauvaises configurations.
Sensitive Information Leaking	La fuite d'informations sensibles vers des moteurs de recherche tels que Google et Bing.

POURQUOI LE CLIENT A-T-IL BESOIN D'UN PENETRATOR ?

Pourquoi le client a-t-il besoin d'un pénétrator ?

Perte financière

- L'argument clé est le coût pour le client d'une compromission et d'une fuite ou d'un vol de données sensibles. Il peut s'agir d'informations relatives aux cartes de crédit, d'informations personnelles, de dossiers médicaux, de secrets d'entreprise dont les concurrents peuvent abuser, etc. Même pour les petits clients, les dommages en cas de perte peuvent aller d'un minimum de 5 000 USD à plus. Cela dépend du client et de ses informations. Il peut même s'agir d'une perte de plusieurs centaines de milliers de dollars. Ainsi, si l'on considère le coût d'un compromis, le coût du Penetrator lui-même sera récupéré plusieurs fois au cours du premier mois d'exploitation !

Gestion de la reputation

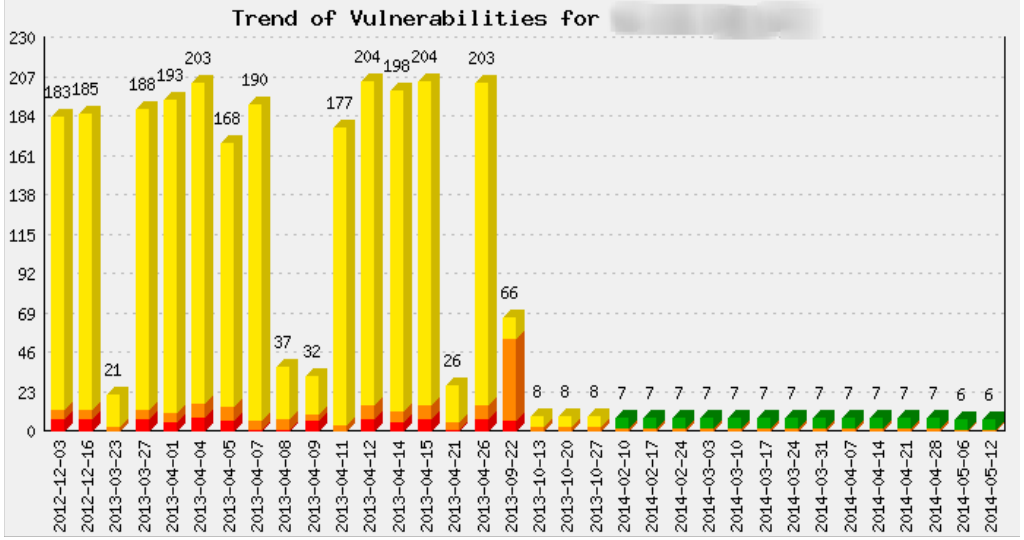
- La direction peut obtenir des rapports clairs et documentés et conserver une bonne réputation grâce à l'analyse et à l'évaluation des vulnérabilités, par exemple toutes les semaines ou tous les mois, selon la manière dont les analyses sont effectuées.

Notification automatique des vulnérabilités découvertes

- Lorsque de nouvelles vulnérabilités sont découvertes, par exemple la vulnérabilité Heartbleed. Cela peut permettre aux clients de prendre rapidement des mesures pour sécuriser leurs sites.

Les tendances en matière de sécurité suivent l'historique de la sécurité

- La direction obtiendra un suivi clair de l'historique des vulnérabilités et de l'ensemble du niveau de sécurité, ce qui lui permettra de suivre l'évolution de la sécurité de son réseau.



Indisponibilité Temps d'arrêt

- Un pirate informatique peut défigurer votre site web en affichant un contenu différent de celui que vous aviez initialement mis en ligne. Le temps de rétablir le service et de trouver ce qui se passe, vos clients ne sont pas en mesure d'utiliser vos systèmes. Dans certains cas, plusieurs jours peuvent s'écouler avant que vous ne soyez à nouveau opérationnel. Veillez à ce que cela n'arrive pas à votre entreprise.

LES AVANTAGES DE SECPOINT

Support Live Chat dédié	Nous fournissons une assistance par chat en direct 24 heures sur 24, 7 jours sur 7, pour tout problème ou question technique que vous pourriez avoir. Visitez simplement www.secpoint.com et cliquez sur l'icône Live Chat et nos sympathiques représentants du support Live Chat s'occuperont du reste.
Développement continu	Nous consacrons beaucoup d'efforts au développement continu de tous nos produits et fournissons des mises à jour gratuites avec des solutions aux menaces les plus récentes. Nous lançons régulièrement des mises à jour de micrologiciels avec de nouvelles fonctionnalités et de nouveaux outils qui sont très importants pour assurer une protection continue, sans frais supplémentaires.Veuillez consulter le journal des modifications pour plus de détails sur la rapidité de notre développement (journal des modifications du Protector) (journal des modifications du Penetrator)
Complexité zéro	Avec la politique de SecPoint "Pas de coût caché", les clients ont la possibilité d'obtenir la solution dont ils ont besoin sans aucun coût supplémentaire. Les produits sont dotés de nombreuses fonctionnalités, mais les clients n'ont pas besoin de les payer séparément.
Zéro stock, même pour le matériel !	Notre boutique en ligne interactive, VIP Lounge, vous permet de créer des identifiants d'unité pour n'importe quel produit en quelques secondes. Vous n'aurez donc jamais à tenir d'inventaire.Pour les commandes de matériel, vous avez la possibilité d'acheter un appareil localement et nous vous aiderons à l'installer et à le configurer. Ainsi, vous n'aurez plus jamais à attendre l'expédition.
Facilité d'utilisation	Les produits SecPoint sont hautement personnalisables et offrent une facilité d'utilisation inégalée. Ils sont assortis d'avantages supplémentaires tels que des mises à jour gratuites du firmware, une assistance gratuite par chat en direct (sept jours sur sept) qui garantit un effort minimal de la part du client et offre une personnalisation et une facilité d'utilisation inégalées.
Historique	SecPoint a conçu Penetrator en 2003, Protector UTM en 2005 et Portable Penetrator en 2007. Depuis lors, les trois variantes ont été continuellement développées et de nombreuses mises à jour du micrologiciel ont permis d'offrir de nouvelles fonctionnalités intéressantes.SecPoint est présent dans le monde entier depuis 1999 et son siège social se trouve à Copenhague, au Danemark. Elle fournit des produits de sécurité haut de gamme à des clients du monde entier, par l'intermédiaire de ses partenaires dans le monde entier.SecPoint a été fondée en 1998 et compte 13 années de développement continu de ses produits. C'est l'entreprise la plus compétitive dans le domaine de la sécurité informatique avec une large gamme de produits, y compris les UTM, le Pen-Testing et les services Cloud, offrant des solutions faciles à utiliser pour tous les besoins de sécurité informatique.
Bureaux	SecPoint possède des bureaux au Danemark, aux Pays-Bas et en Grèce, ainsi que des centaines de revendeurs et de distributeurs agréés dans le monde entier. Elle met à la disposition de tous ses partenaires un gestionnaire de compte dédié, afin qu'ils reçoivent une assistance personnalisée en cas de doutes ou de questions, ainsi qu'une formation et du matériel de vente pour leur assurer le meilleur rendement possible.

QUESTIONS À POSER POUR QUALIFIER UN CLIENT EN VUE DE L'ACHAT D'UN PENETRATOR ?

Le diagramme de réseau qu'ils utilisent maintenant ?

Combien d'adresses IP doivent-ils scanner ?

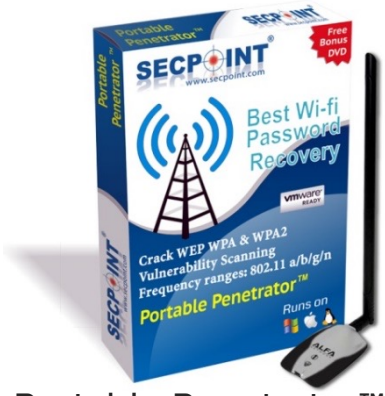
Comment se répartissent les serveurs, les équipements de réseau et les postes de travail ?

Quels types de services et d'appareils doivent être analysés ?

Doivent-ils scanner les adresses IP locales, publiques ou les deux ?

Ont-ils des exigences en matière de conformité ?

SECPOINT PENETRATOR



Portable Penetrator™

Complete Pen-Testing Suite

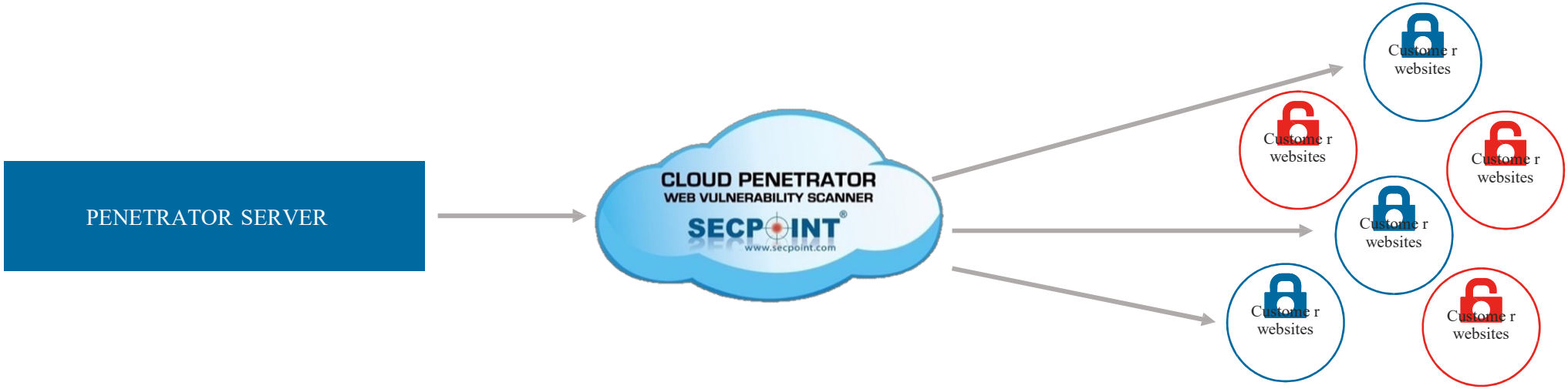
- ✓ Récupération Wi-Fi (WEP/WPA/WPA2/WPS)
- ✓ Nouveau craquage WPS
- ✓ Test de pénétration pour les adresses IP publiques et locales
- ✓ Plus de 60 000 vérifications de vulnérabilités
- ✓ Lancement de plus de 700 exploits réels
- ✓ Rapports complets
- ✓ Mobilité aisée grâce à une antenne USB puissante
- ✓ Recherche de SSID et de fournisseurs en mode passif
- ✓ 1 milliard d'entrées de craquage
- ✓ Assistance par chat en direct (7 jours sur 7)

Cloud Penetrator™

Scanner de sécurité des sites web

- ✓ Évaluation de la vulnérabilité et test de pénétration sur des IP publiques
- ✓ Analyse facile de Wordpress, Drupal, Joomla, Magento, Shopify, Umbraco, Custom Apache, PHP et plus encore.
- ✓ Aucune installation requise, fonctionne à partir de n'importe quel navigateur
- ✓ Le Crawler avancé parcourt chaque page web
- ✓ Vérifie le code empoisonné SEO, l'exécution de commandes
- ✓ Vérifie la présence de Cross Site Scripting, SQL Injection
- ✓ Google Black Hat Scanning, Google Hack DB Scanning
- ✓ Rapports complets au format PDF/HTMLScans illimités
- ✓ Assistance par chat en direct (7 jours sur 7)

CLOUD PENETRATOR (SUITE 1)



SECPOINT PPENETRATOR APPLIANCE (SUITE 2)

SecPoint® Penetrator™
Dispositif complet de Pen-Testing

- ✓ Test de pénétration pour les adresses IP publiques et locales
- ✓ Plus de 60 000 vérifications de vulnérabilités
- ✓ Audit des serveurs Web, des serveurs de messagerie, audit à travers le pare-feu
- ✓ Lancement de plus de 700 exploits réels
- ✓ Analyse distribuée
- ✓ Audit Wi-Fi (WEP/WPA/WPA2/WPS)
- ✓ Rapports complets au format PDF/HTML
- ✓ Interface conviviale, support multi-utilisateurs
- ✓ Trouver des SSID, des fournisseurs en mode passif
- ✓ Hébergement en tant que solution cloud pour vos clients
- ✓ Support Live Chat (7 jours par semaine)

Disponible en tant que

- Appliance Rack 1U / SFF
- Machine virtuelle VMware/Hyper-V

MODELES DE PENETRATOR

Penetrator Scanner de vulnérabilité

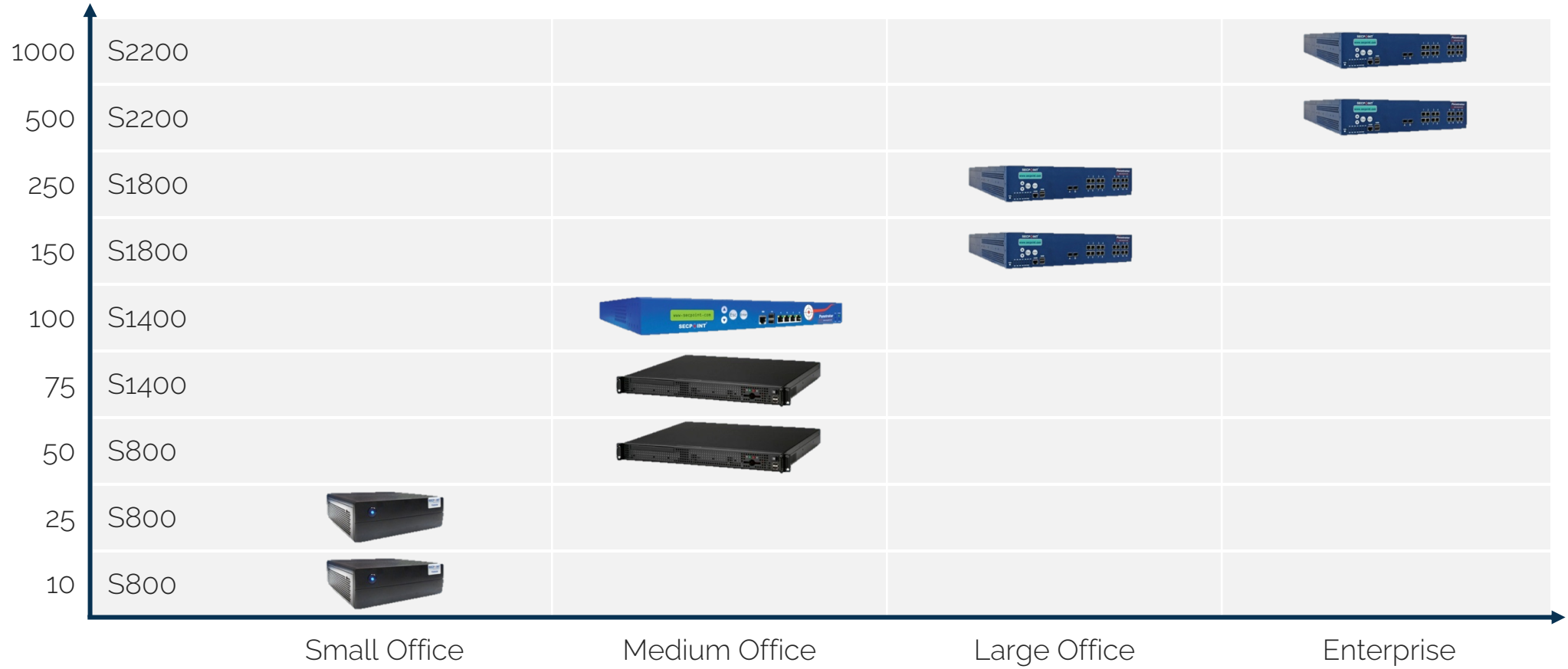
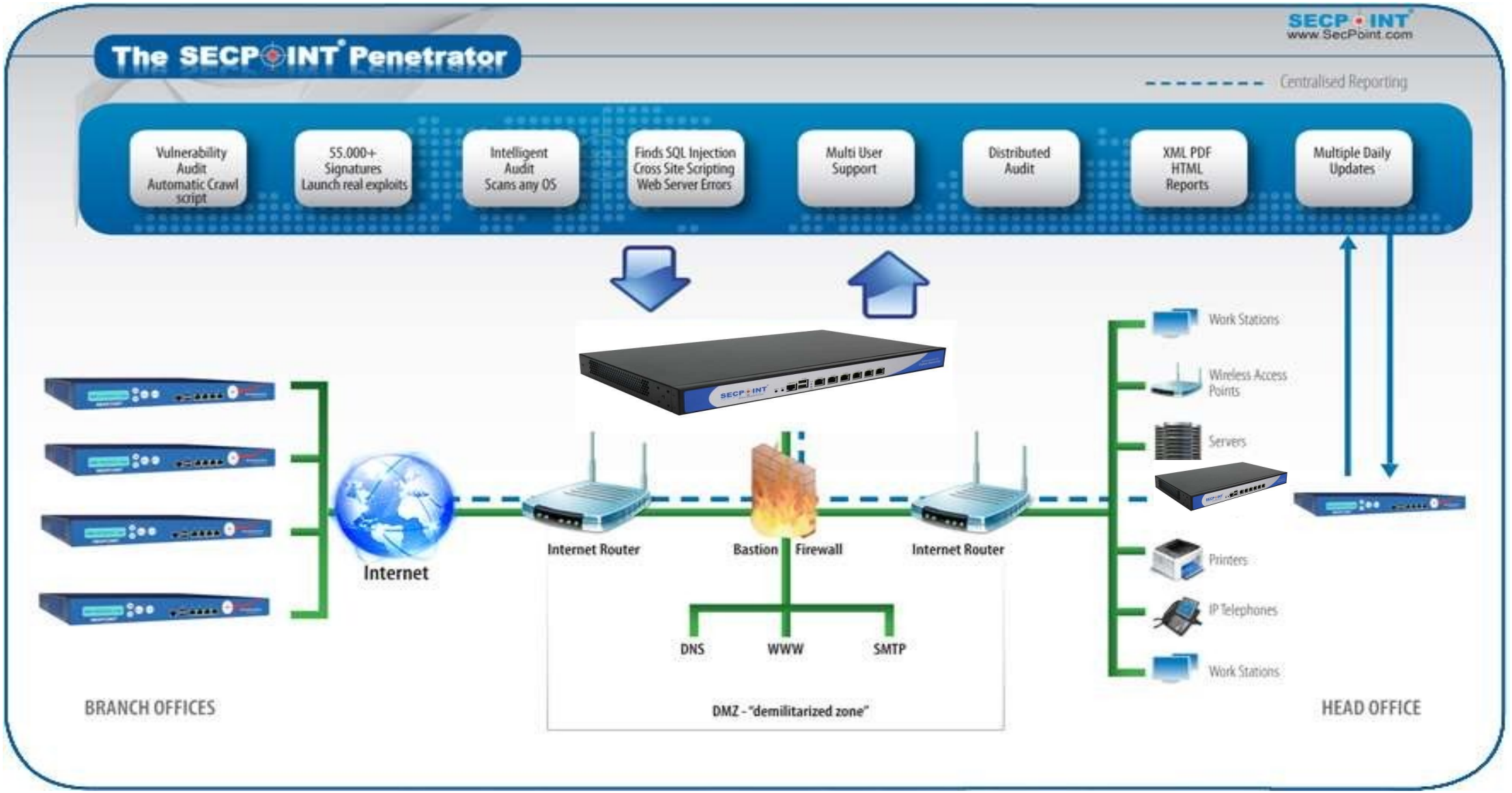


DIAGRAMME DU PENETRATOR



SECPOINT PENETRATOR - SÉLECTION DU PROFIL D'ANALYSE DES VULNÉRABILITÉS

Découvrez facilement les vulnérabilités de votre réseau et choisissez le bon profil pour l'analyse.

Choisir parmi les profils d'évaluation de l'analyse de vulnérabilité

Analyse rapide - Analyse Web rapide - Analyse normale - Analyse complète - Analyse complète du pare-feu - Analyse agressive - OWASP Top 10 - Préparation PCI-DSS pour les applications Web - HIPAA - SCADA ICS PLC.

Le profil peut vous aider à effectuer des analyses rapides qui vous donneront un bref aperçu des vulnérabilités. Vous pouvez également effectuer l'analyse normale recommandée ou l'analyse complète du pare-feu plus intensive, qui peuvent être exécutées en toute sécurité dans les environnements de production. Si vous souhaitez tester la solidité de votre pare-feu et de vos systèmes, le profil d'analyse agressive peut vous aider. Nous disposons également de plusieurs profils d'analyse de conformité qui peuvent être déployés.

Si vous ne savez pas quel profil d'analyse est le mieux adapté à votre environnement de sécurité réseau, n'hésitez pas à nous contacter pour obtenir de l'aide.

Best Scan- Popular Ports

SSL & CMS Web San - Wordpress, Joomla
Quick Scan - Ports les plus courants
Large Scan - Tous les 65.535 ports
Analyse de pare-feu - Analyse furtive
Analyse agressive - Exploits et attaques DoS
Scan OWASP Top 10 - Vérifications OWASP
Préparation PCI-DSS pour les applications Web
Conformité à la politique HIPAA
SCADA ICS PLC

NOUVELLE ANALYSE DE VULNÉRABILITÉ - PROFILS

Profile 1 - Best Scan - Popular Ports

Profile 10 – SCADA ICS PLC

Profile 2 - CMS Web Scan

Profile 9 - HIPAA Policy Scan for Compliance

Profile 3 - Quick Scan

Profile 8 – PCI-DSS Preparation for Web Applications

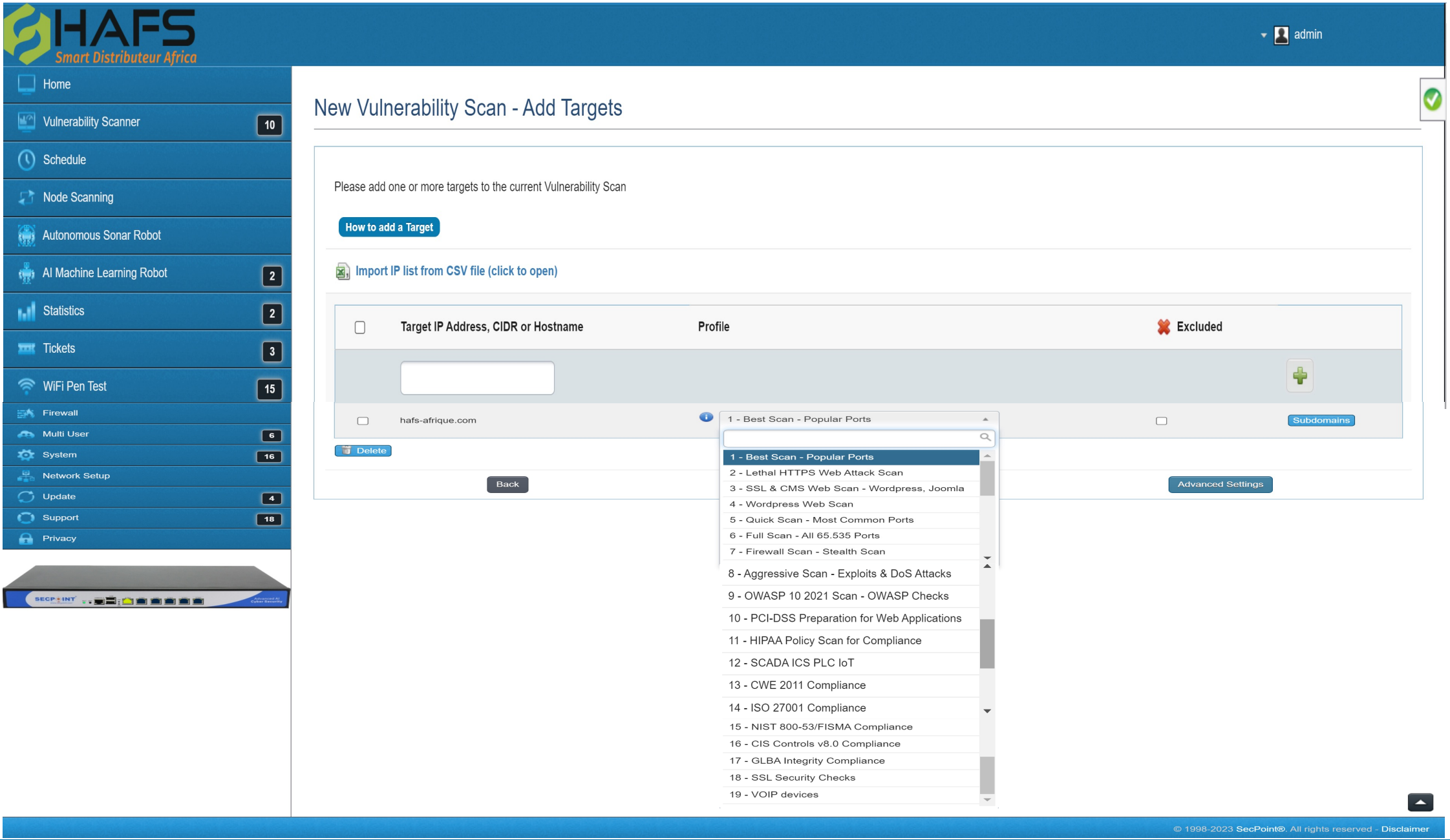
Profile 4 – Large Scan – All 65.535 Ports

Profile 7 - OWASP Top 10 Scan - OWASP Checks

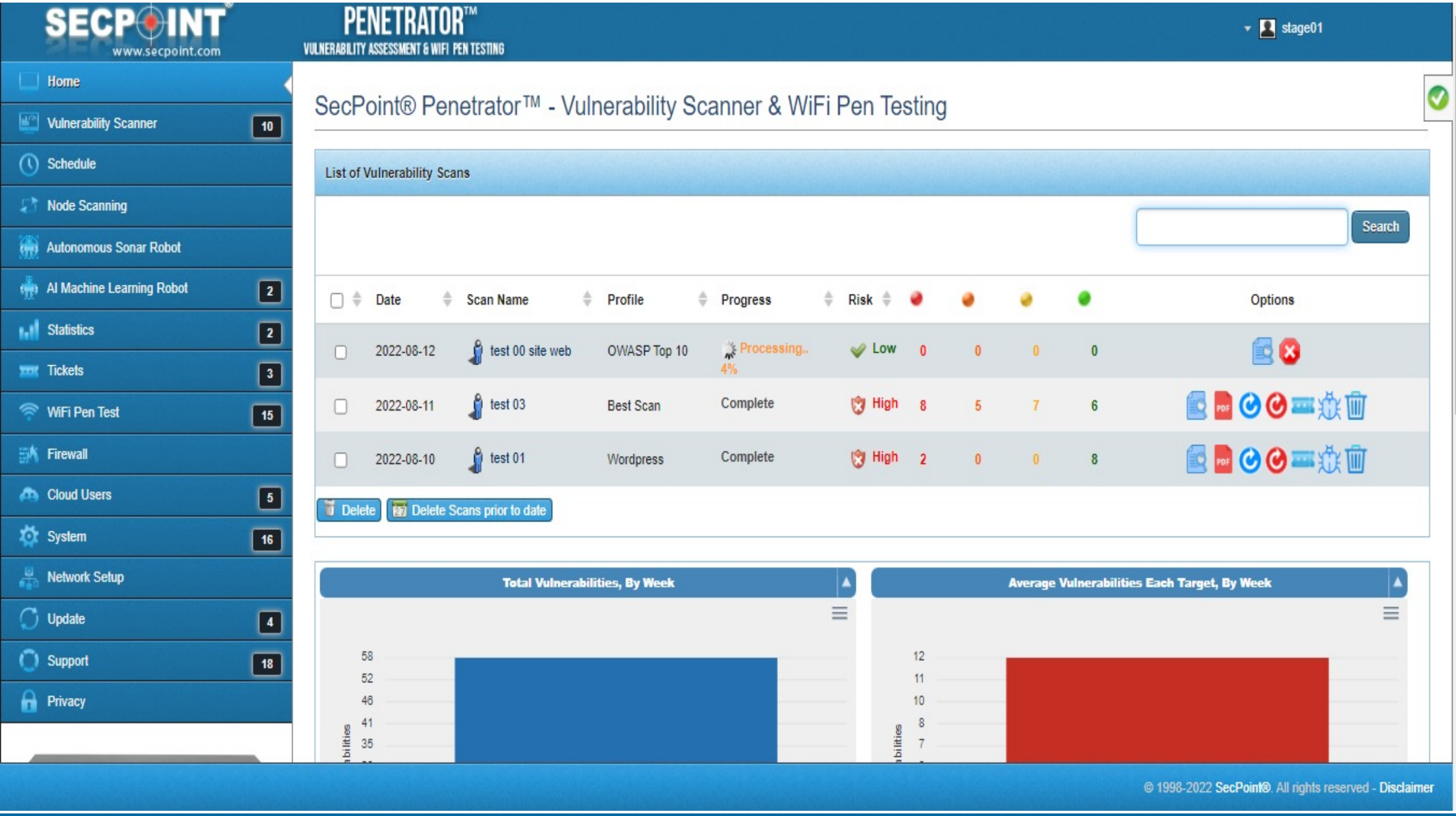
Profile 5 - Firewall Scan - Stealth Scan

Profile 6 - Aggressive Scan - Full Scan, Exploits & DoS Attacks

COMMENT NUMÉRISER CORRECTEMENT AVEC DES PROFILS



PAGE D'ACCUEIL SECPOINT

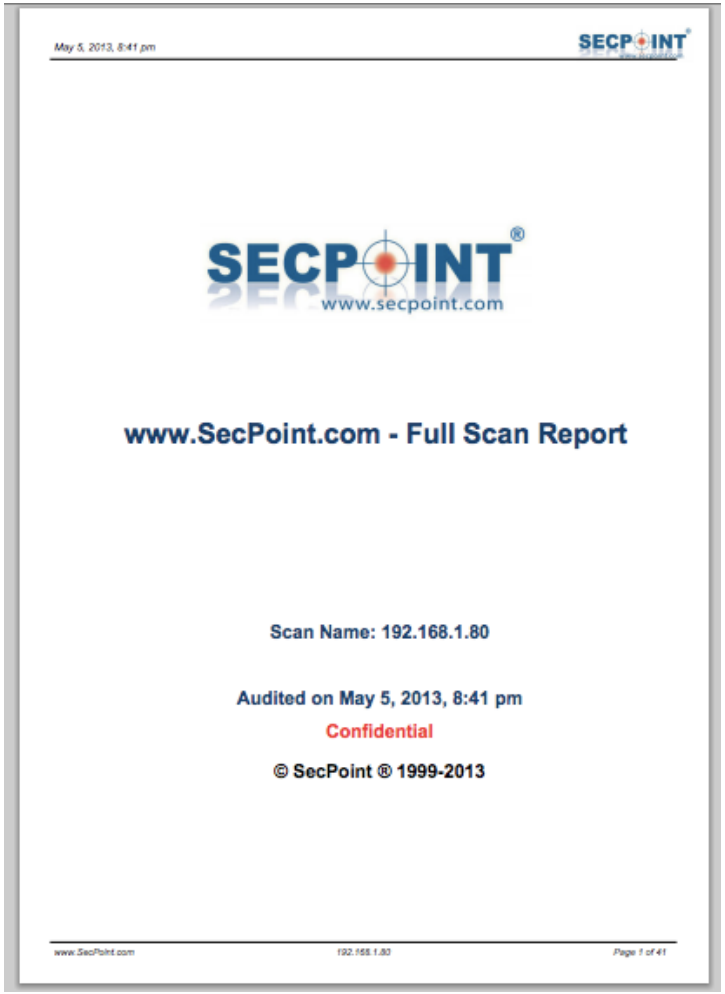


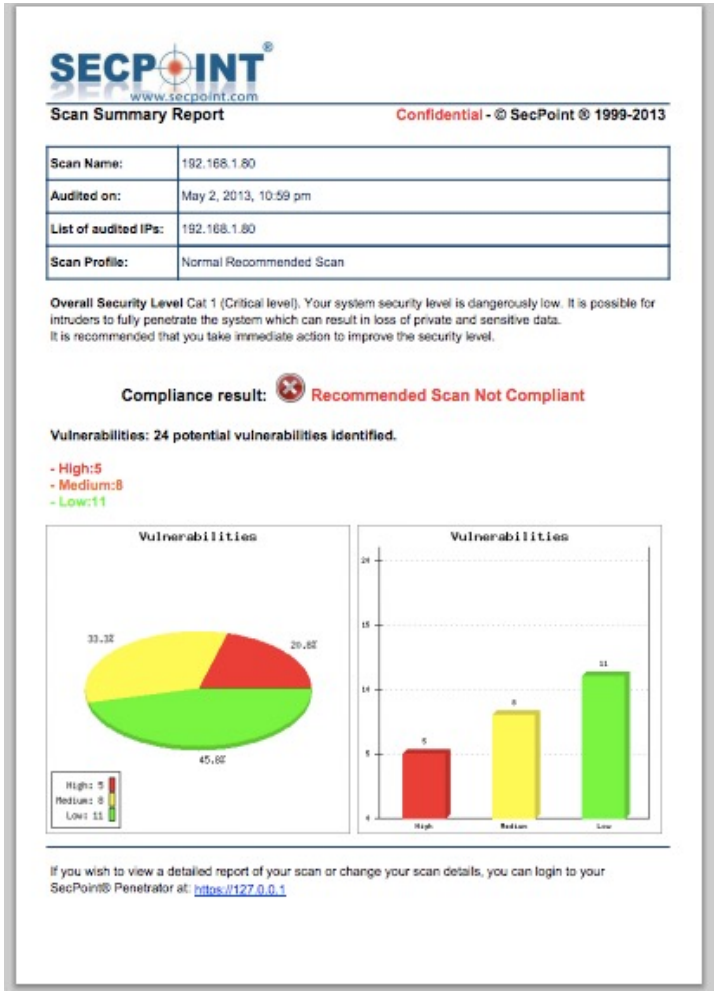
EXEMPLE DE RAPPORT

ÉCHANTILLON DE VULNÉRABILITÉ

Rapport complet

http://www.secpoint.com/manual/Penetrator_Example_Audit.pdf





COMMENT VENDRE FACE À LA CONCURRENCE & PRINCIPAUX POINTS CLÉS DU PÉNÉTRATEUR SECPOINT

Quels sont les principaux arguments de vente face à un concurrent ? Veuillez consulter la matrice ci-dessous pour une comparaison complète des concurrents.

- Les principaux arguments en faveur de l'utilisation du Penetrator par rapport à ses concurrents sont les suivants :
- Il n'y a pas de portes dérobées gouvernementales comme celles que de nombreuses entreprises basées aux États-Unis sont obligées d'avoir.
- Aucune donnée n'est envoyée, toutes les données se trouvent chez le client.
- Vous ne payez pas par scan mais vous êtes autorisé à changer d'IP et vous pouvez faire tous les scans que vous voulez.
- Le Penetrator prend en charge plusieurs utilisateurs, de sorte que plusieurs utilisateurs peuvent se connecter avec des autorisations différentes.
- Il est possible de créer son propre service Cloud avec le Penetrator et d'y faire accéder différents utilisateurs.
- Il est possible de renommer les rapports et de les personnaliser en fonction du client ou du revendeur.
- Support 24/7 inclus dans les prix, vous n'avez pas à payer de supplément pour le support.
- Les produits sont pris en charge pendant au moins 5 ans.
- Les produits sont supportés pendant au moins 5 ans - avec de nombreux concurrents, après 2 ans, vous devez acheter un nouveau produit.
- La capacité d'audit WiFi complète récupère les clés WEP, WPA, WPA2 et WPS.
- Option de crash DoS sur les systèmes IP lors d'un pentest, si vous le souhaitez.
- Option pour les crashs DoS ciblant les points d'accès Wifi lors du Pentest si vous le souhaitez.
- Convivialité pour les consultants - possibilité de revendre les rapports avec le logo de l'entreprise.
- Preuves complètes dans les rapports pour les vulnérabilités trouvées.
- Système de ticket puissant pour prendre facilement des mesures sur les vulnérabilités trouvées.
- Assistance récompensée par 5 étoiles sur Trustpilot - Produit récompensé par 5 étoiles sur SC Magazine.

FONCTIONNALITÉ UNIQUE DU PÉNÉTRATEUR POUR COMPARAISON - MATRICE DES CONCURRENTS (I/III)

	SecPoint	Qualys	Acunetix	Rapid7	Nessus	GFI	SAINT	NetIQ	Core
Virtual, Appliance, Cloud & Linux G4L	✓	X	X	X	X	X	X	X	X
Pas de portes dérobées de la NSA Confidentialité totale !	✓	-	-	-	-	-	-	-	-
Pas de collecte de données	✓	X	X	X	X	X	X	X	X
Anti-faux positifs grâce à l'IA avancée	✓	-	-	-	-	-	-	-	-
Rétrocompatibilité 5+ ans	✓	-	-	-	-	-	-	-	-
5 étoiles attribuées par Trustpilot	✓	-	-	-	-	-	-	-	-
Google 2FA Authentication	✓	-	-	-	-	-	-	-	-
Chat en direct 24/7 sans frais supplémentaires	✓	-	-	-	-	-	-	-	-
Prix 5 étoiles décerné par le magazine SC	✓	-	-	-	-	-	-	-	-
Interface graphique intuitive et conviviale	✓	-	-	X	X	-	X	-	-
Permet de changer le logo du rapport	✓	X	X	X	X	X	X	X	X
Permet de personnaliser le filigrane du rapport	✓	X	X	X	X	X	X	X	X
WiFi Pen Testing WPA WPA2	✓	-	-	-	-	-	-	-	-
Support inclus dans le prix	✓	-	-	-	-	-	-	-	-
Bugtraq ID / Mitre CVE	✓	-	-	-	-	-	-	-	-
Politique différente pour les utilisateurs de l'informatique en Cloud	✓	X	X	X	X	X	X	X	X
Coût d'entrée compétitif Ne payer que pour les balayages IP simultanés, pas de verrouillage	✓	X	X	X	X	X	X	X	X

FONCTIONNALITÉ UNIQUE DU PÉNÉTRATEUR POUR COMPARAISON - MATRICE DES CONCURRENTS (II/III)

	SecPoint	Qualys	Acunetix	Rapid7	Nessus	GFI	SAINT	NetIQ	Core
Autorisé à changer d'adresse IP	✓	X	-	-	-	-	-	-	-
Grappe d'analyse distribuée	✓	X	X	X	X	X	X	X	X
Point de mise à jour de la numérisation centralisée	✓	-	-	-	-	-	-	-	-
ESXi / Hyper-V / 1U Appliance	✓	-	-	-	-	-	-	-	-
Protection Partenaire principal	✓	X	X	X	X	X	X	X	X
Conformité des analyses de calendrier	✓	-	-	-	-	-	-	-	-
Mise à jour rapide des vulnérabilités	✓	-	-	-	-	-	-	-	-
11 profils d'analyse détaillés	✓	-	-	-	-	-	-	-	-
Google DB Hack - Black Hat SEO	✓	-	-	-	-	-	-	-	-
Un système de tickets pour faciliter la gestion	✓	-	-	-	-	-	-	-	-
Tendances en matière d'analyse de vulnérabilité	✓	-	-	-	-	-	-	-	-
Plate-forme Linux sécurisée	✓	-	-	-	-	-	-	-	-
Système mondial des faux positifs	✓	-	-	-	-	-	-	-	-
Notification automatique des vulnérabilités	✓	-	-	-	-	-	-	-	-
Téléchargement en bloc de tous les rapports	✓	-	-	-	-	-	-	-	-
Soumettre des signatures personnalisées	✓	-	-	-	-	-	-	-	-

FONCTIONNALITÉ UNIQUE DU PÉNÉTRATEUR POUR COMPARAISON - MATRICE DES CONCURRENTS (III/III)

	SecPoint	Qualys	Acunetix	Rapid7	Nessus	GFI	SAINT	NetIQ	Core
Support multi-utilisateurs	✓	-	-	-	-	-	-	-	-
Rapports centralisés	✓	-	-	-	-	-	-	-	-
Option de numérisation distribuée	✓	X	X	X	X	X	X	X	X
Mitre CVE Compatible	✓	-	-	-	-	-	-	-	-
Découverte de dispositifs sans fil	✓	X	X	X	X	X	X	X	X
Test de pénétration complet pour le WiFi	✓	X	X	X	X	X	X	X	X
Point d'accès WiFi DoS	✓	X	X	X	X	X	X	X	X
Lancer des attaques de type DoS	✓	-	-	-	-	-	-	-	-
Lancer des exploits	✓	-	-	-	-	-	-	-	-
Disponible sous forme d'appliance	✓	-	-	-	-	-	-	-	-
Émulation humaine	✓	-	-	-	-	-	-	-	-
Numérisation à sécurité intégrée	✓	-	-	-	-	-	-	-	-
Audits de la plate-forme	Any	-	-	-	-	-	-	-	-
Scanner les systèmes d'exploitation non Windows	✓	-	-	-	-	-	-	-	-
Indépendant du système d'exploit	✓	-	-	-	-	-	-	-	-
Découverte de logiciels P2P	✓	-	-	-	-	-	-	-	-

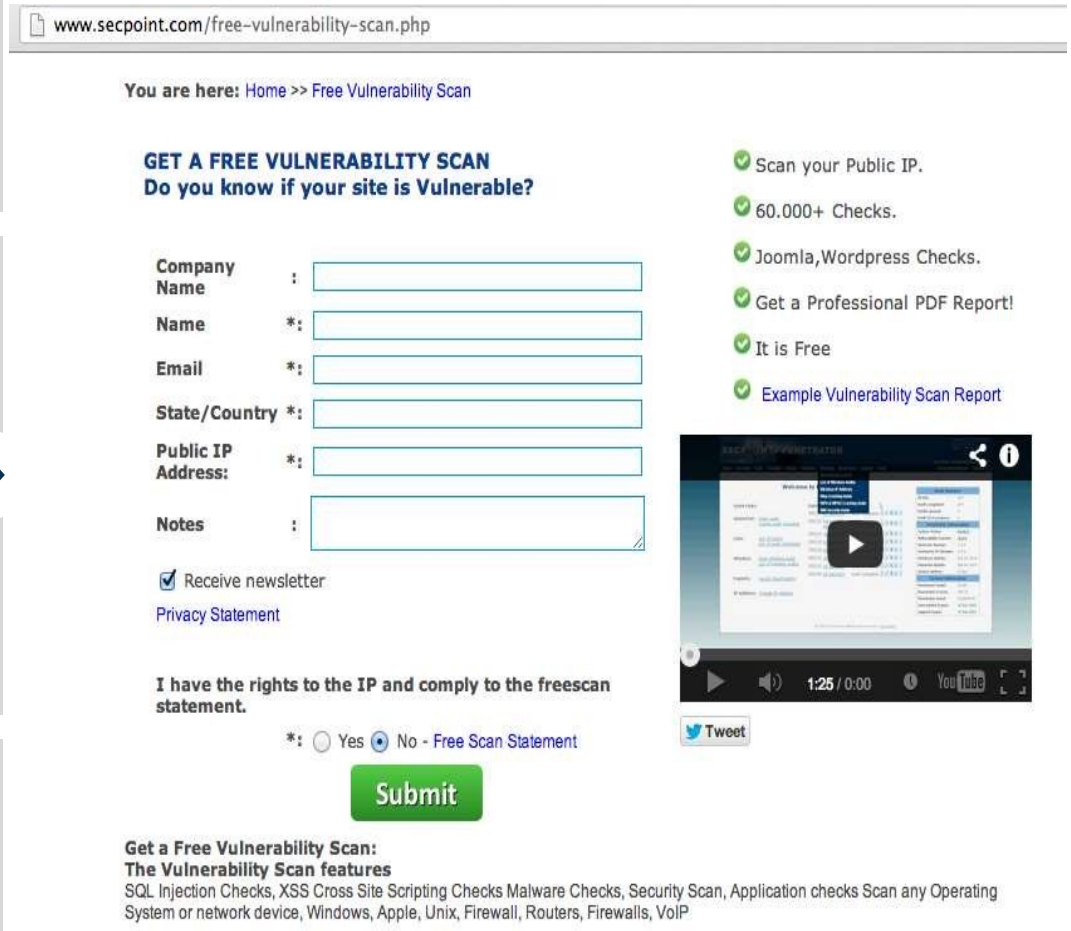
ANALYSE DE VULNÉRABILITÉ GRATUITE

Les nouveaux clients n'achètent pas s'ils n'ont pas de problème

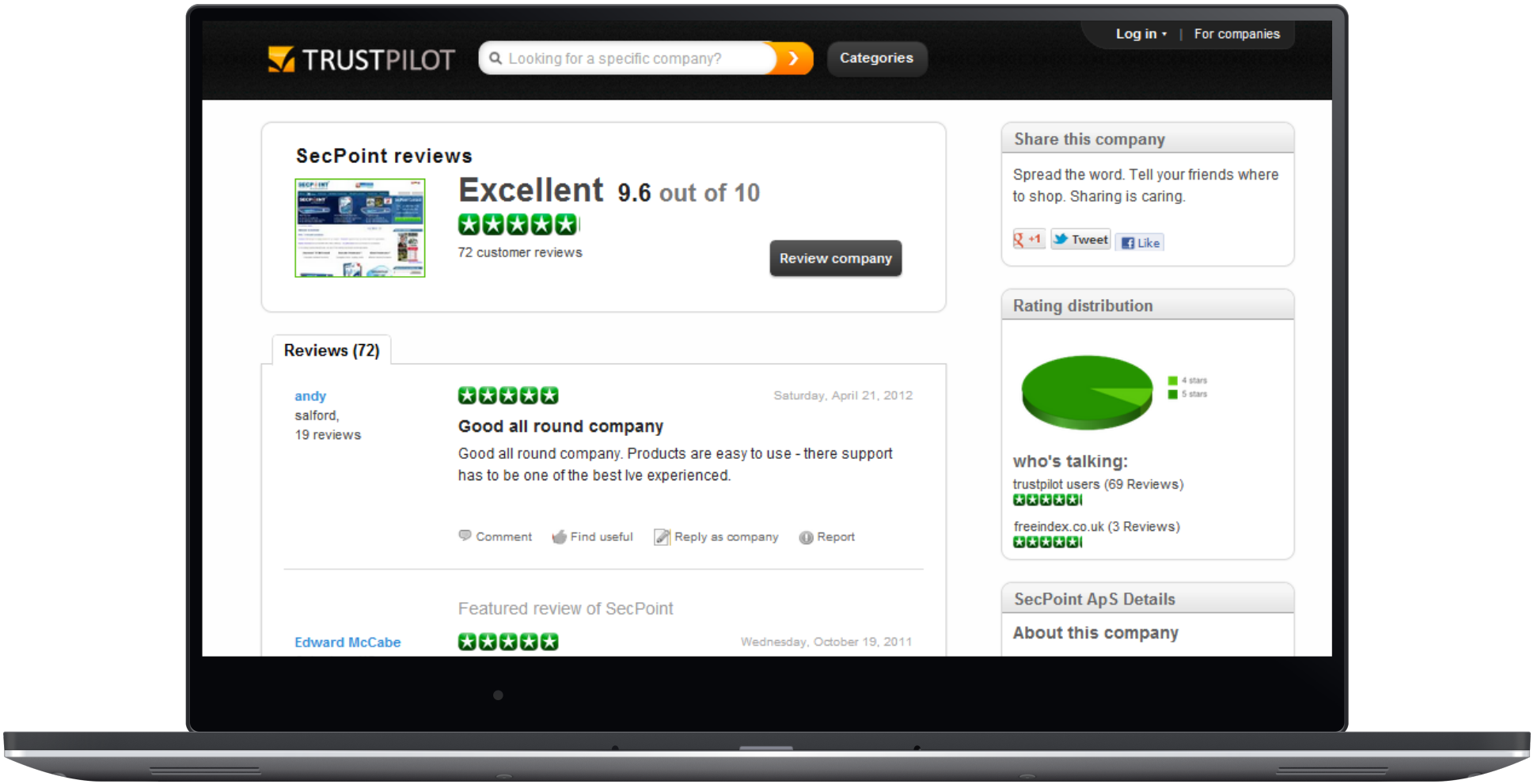
Les nouveaux clients ne veulent pas vous parler jusqu'à ce que vous leur montriez qu'ils ont un problème.

Offrez-leur un audit de sécurité (gratuit) afin qu'ils puissent voir l'état de leur réseau.

http://www.secpoint.com/free-vulnerability-scan.html



LA SATISFACTION DU CLIENT - NOTRE FORCE

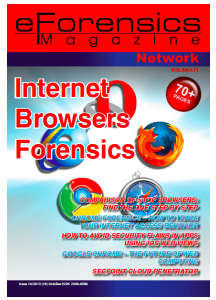


LA SATISFACTION DU CLIENT - NOTRE FORCE (SUITE)

CUSTOMERS

unicef
NEW YORK COLLEGE EUROPEAN & AMERICAN EDUCATION
KING
TradeTracker.com we track your trade
ROCHDALE
ROSCREA credit union limited
TDC NetDesign
CANONICAL
ubuntu
OLYMPIA ODOS
Realtime CONSULTING & SERVICES LTDA
TradeTracker® we track your trade
PARK Developments Group
TROYGROUP
Secure Cyber Communications
PLAMECO® SYSTEMS
BING RESEARCH
Technigro
THANOS hotels and resorts

AWARDS, CERTIFICATIONS & REVIEWS



DTL Data TestLab BEST OF THE TESTS 2007
SC MAGAZINE
INNOVATION PC WORLD AWARD
PROTECTSTAR AWARD 2012
TRUSTPILOT TRUSTSCORE 9.7 79 ANMELDELSER
CO2 neutralt website
CVE COMPATIBLE cve.mitre.org
HIPAA COMPLIANCE

PLUS DE CLIENTS SATISFAITS DANS LE MONDE ENTIER

RUSSIA & CIS

- Volga Telecom
- Devon Credit
- FSUE State ATM Corporation
- Rostelecom

EMEA

SECPOINT®

HAFS Smart Distributeur Africa

HAFS NETWORKS | France

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Wi-Fi | Réseaux

Hillstone NETWORKS | SEARCHINFORM RISK AND COMPLIANCE MANAGEMENT | ALTAI Super WiFi | vade | SECPOINT®

Nous Contacter

www.hafs-afrique.com

West Africa | Côte d'Ivoire
+225 07 89 82 56 49 | 07 87 57 64 11
sales@hafs-afrique.com

Maroc
+212 52 24 49 937
sales@hafs-networks.com

North & Central Africa | France
+33 09 73 89 20 39 | 06 24 12 27 05
sales@hafs-networks.com

SECPOINT®

QUESTIONS ET REPONSES

DIAGRAMME DU LAB