

ABOX

TOUT POUR LES SOLUTIONS DE SECURITE INFORMATIQUE

<mailto:abox@abox.com> - www.abox.com - ☎ +33(0)5.65.68.85.76

>> Historique de ABOX

Abox fut fondée en 1994 en tant que société intégratrice de solutions pour environnements UNIX. Au cours de ces années, l'activité s'est centrée sur la distribution et le support des produits que nous vendions. En 1998 s'est développée l'activité de fournisseur de solutions de sécurité, avec des accords de distribution de solutions de sécurité de fabricants leaders dans leurs activités. Actuellement, nous disposons d'un catalogue restreint de produits dans le domaine de la sécurité informatique et nous poursuivons la recherche de nouveaux produits. Nous disposons d'une politique de canal pour revendeurs et intégrateurs, auxquels nous offrons des solutions gagnantes dans le marché technologique et concrètement dans l'environnement de la sécurité informatique.

>> Nos Valeurs:

Focalisation sur le client final avec l'appui de notre canal :

- Actions de marketing dirigées au client final pour générer une demande à tout niveau.
- Appui sur la Prévente et Postvente.
- Fidélisation de l'utilisateur final.
- Propositions de solutions alternatives aux standards du marché.
- Solutions les plus compétitives et qui conviennent tant à la PME qu'au Grand Compte.
- Options d'acquisition via un renting (approbation préalable bancaire). A partir de 3 000,00 € tant les équipements que les services.

>> Pourquoi Abox?

Distributeur spécialisé dans le marché de la sécurité étant capable de donner le meilleur support prévente et postvente.

- Appui au canal grâce à une formation qualifiée, actions de marketing.
- Rapidité et souplesse pour tout ce que nous demandent nos revendeurs

ABOX

>> Antispam:



>> Passerelles de sécurité Antivirus:



>> Monitoring de Contenus:



>> Blocage de Contenus:



>> Firewall:



>>: Cryptage de disques et données



>> Authentification d'utilisateurs et contrôle d'accès:



>> Antispam:

BorderWare™ Unified Threat Protection and Content Security

Borderware: Solution étendue de sécurité pour le courrier électronique, une solution qui augmente la protection des données et facilite le travail des organisations en prévenant l'entrée de menaces anti-spams, contrôle le contenu de sortie et centralise l'administration de l'infrastructure du courrier électronique.

BorderWare Security Network (BSN) est le premier et unique service pour analyser la réputation et le comportement d'adresses IP, domaines et émetteurs de courrier électronique, web, FTP, IM et VoIP en fournissant une protection sans précédent. Le BSN comprend la réputation au niveau du domaine et de l'utilisateur, une nouvelle technologie qui examine et trace le contenu du trafic pour déterminer les risques potentiels, et représente une importante avancée dans la lutte contre les menaces comme le spam, phishing et flooding.

BorderWare Email Security Gateway : fournit des proxies certifiés sûrs pour Microsoft OWA et Lotus iNotes. Cette caractéristique est idéale pour les utilisateurs qui désirent l'accès à d'autres outils comme des calendriers et dossiers privés, sans exposer directement Microsoft Exchange ou Lotus Notes à Internet. Le Borderware Email Security Gateway fournit aussi un accès de courrier électronique sûr au moyen de BorderPost™, le client WebMail intégré. Le BorderPost se connecte à vos serveurs de courrier électronique internes pour assurer un webmail sûr qui utilise IMAP ainsi qu'un accès SSL crypté de 128-bits aux mailbox des utilisateurs au travers de n'importe quel navigateur web.

>> Antispam:



Commtouch offre une incomparable combinaison quasi parfaite de détection de spams et malwares, ne génère pratiquement pas de faux positifs et représente une solution exceptionnelle facile à intégrer dans n'importe quel réseau d'entreprise. Commtouch 5.0 apporte une solution globale qui filtre le trafic de spam et les programmes malicieux, permet d'utiliser les règles de l'environnement, facilitant l'administration au département IT ainsi que l'utilisation de la part des utilisateurs.

Le plus important est la communication avec le Centre de Détection de Commtouch en temps réel, qui permet de classifier les messages en utilisant l'information d'autres dispositifs, ce qui se traduit par un des réseaux de réputation le plus étendu du marché.

Antivirus:



Norman virus control

Antivirus de première ligne et de qualité résistante NVC v5.8 inclue la nouvelle technologie SandBox, qui étend plus encore la détection de virus nouveaux et inconnus. NVC v5.8 insère tout fichier suspect dans un ordinateur virtuel, le SandBox, et surveille les actions du fichier en temps réel. Si un comportement de virus est détecté, il réalise les actions nécessaires pour prévenir des dommages de celui-ci. Pourquoi choisir Norman Virus Control ?

De nouveaux virus apparaissent quotidiennement et votre négoce pourrait être la prochaine victime. Soyez préparé à contrer ces menaces malware de façon professionnelle avec un partenaire professionnel.

Norman Virus Control v5.9 (NVC v5.9) est un programme antivirus qui protège vos stations et vos serveurs contre le software malicieux, appelé aussi malware. Lorsque sont détectés des fichiers infectés, NVC les isole ou les élimine immédiatement avant que ne s'active le code destructeur.

La tâche simple la plus importante pour une application antivirus est de conserver les ordinateurs libres de tout virus. Cette dernière version étend le renommé moteur de scannage de Norman en incorporant la révolutionnaire technologie SandBox, pour un plus grand accroissement d'habileté de NVC pour détecter tant les virus connus que les inconnus, y compris les troyens et les vers.

ABOX

LA NOUVELLE GENERATION DE SOLUTIONS

POUR LA SECURITE INFORMATIQUE ET LES COMMUNICATIONS

Monitoring de contenus:



Webspy

Analysez quelles pages web visitent vos employés. WebSpy est un outil de monitoring Internet et/ou email, qui vous permet de réduire les menaces de sécurité et d'instaurer une politique de "bon usage" d'Internet, en informant les employés sur les exigences de sécurité, les problèmes de bande passante, et en leur enseignant que leurs comportements individuels peuvent avoir un effet important sur l'entreprise, ou sur la morale (en naviguant sur des sites pornographiques, pédophiles, d'incitation au racisme, etc).

WebSpy est un produit adapté à chaque type d'organisation, en fonction de l'entreprise, du type de réseau, et du niveau d'informations que vous désirez.

Blocage de contenus:



Inspecteur de contenu pour monitoriser et contrôler l'utilisation d'Internet.

ContentKeeper Technologies est spécialisé dans la construction de produits et de softwares d'avant-garde pour aider les diverses corporations, gouvernements et clients ISP à obtenir une meilleure utilisation de l'accès à leurs ressources Internet.

ContentKeeper surveille la navigation à des sites qui ne sont pas en relation avec les intérêts de l'entreprise.

ContentKeeper administre l'accès et le téléchargement de documents.

ContentKeeper contrôle l'utilisation d'Internet dans le travail en identifiant, bloquant et envoyant des messages d'alerte lorsqu'il y a accès à des sites pornographiques ou illégaux.

ContentKeeper utilise sa propre technologie, leader sur le marché, Close-Loop Collaborative Fintering Technology™ qui assure que la base de données des sites, dont le contenu n'est pas en relation avec l'entreprise, soit de la meilleure qualité et avec la meilleure couverture.

ContentKeeper aide les diverses organisations à surveiller, administrer et contrôler l'utilisation et l'accès d'Internet.

ContentKeeper est une application qui intègre les dernières technologies pour assurer le blocage effectif de pages de manière simple, transparente, et adaptable pour différentes configurations de réseaux d'ordinateurs.

ContentKeeper permet que les entreprises développent et implémentent leurs propres politiques d'accès à Internet.

ABOX

LA NOUVELLE GENERATION DE SOLUTIONS

POUR LA SECURITE INFORMATIQUE ET LES COMMUNICATIONS

Blocage de contenus:

CLAVISTER



Clavister Security Gateway, probablement le Firewall le plus rapide du monde.

L'énorme fonctionnalité du Software Clavister permet d'adapter les solutions aux rapides changements que les environnements de sécurité demandent.

Clavister Security Gateway a été conçu pour ces utilisateurs qui demandent la technologie de sécurité maximale sur le hardware de leur choix.

Les raisons de choisir une solution software peuvent être dues à des recommandations fonctionnelles spécifiques, la conception de plateformes ou simplement parce qu'il y a un hardware disponible.

Son rendement, sécurité et faible coût de propriété, combinés avec la technologie de firewall hautement efficace de Clavister, rendent cette solution idéale pour garantir la sécurité de réseaux tant externes qu'internes.

Ne requiert aucun système d'exploitation de support, et n'est dérivé d'aucun d'entre eux.

Utilise l'inspection d'état, le standard de fait des solutions firewalls avancées, qui permet de travailler plus rapidement et efficacement.

Supporte des taux de transfert supérieurs à 500 Mbps avec une inspection complète d'état et de multiples interfaces.

Firewall:



SnapGear offre une gamme de produits pensés pour la petite et moyenne entreprise, avec des prix réellement compétitifs. C'est une famille Low Cost de sécurité avec des prestations qui permettent de donner un service à des entreprises qui possèdent depuis 2 ou 3 utilisateurs dans une officine jusqu'à une PME avec des centaines d'employés.

C'est une plateforme stable avec plus de 300.000 unités vendues, possédant une console d'administration web centralisée, réellement facile à utiliser et qui permet d'obtenir de nombreuses informations sur le trafic que gère le dispositif, et détient également la possibilité d'ajouter les services de Filtrage de Contenus Web, Anti-Spam, etc.

Tous ses modèles permettent la création de connexions sûres VPN, avec un double facteur d'Authentification.

Cryptage de disques et données:



Sécurité de documents pour Microsoft Office

L'échange sûr de fichiers transmis légalement est une condition requise de base pour le transfert électronique à caractère professionnel. SECUDE secure file est un outil direct et facile à utiliser avec lequel vous pouvez signer et crypter des documents.

Le cryptage assure que seuls les associés des entreprises puissent lire les documents. La signature électronique vous assure que vos documents envoyés électroniquement sont publiés légalement. Les signatures satisfont diverses conditions requises tant pour la personne qui envoie que pour le destinataire des documents. La personne qui envoie ne peut changer les contenus du document à posteriori. Dans le même sens, le destinataire peut vérifier l'intégrité du document, il peut identifier clairement qui l'envoie, et peut se fier à leurs contenus. Pour votre entreprise, cela signifie:

- Confidentialité : Le cryptage direct de documents dans Microsoft Office garantit la confidentialité des données
- Intégrité : L'intégrité des documents peut être vérifiée sur la base des signatures digitales.
- Identité : Les signatures digitales permettent de différencier l'authenticité par auteur.
- Contrôle d'accès : Les auteurs peuvent prévenir l'accès non désiré à certaines données, en cryptant les documents respectifs pour des utilisateurs spécifiques sélectionnés.
- Acceptation d'utilisateurs : L'intégration transparente avec les produits Microsoft Office fait que son utilisation soit le plus facile possible.

Authentification d'utilisateurs et contrôle d'accès:



Carte intelligente et mémoire flash dans une seule clé USB.

CryptoCombo est un dispositif « tout en un », en format de clé USB, combinant et les fonctions de carte intelligente et son lecteur.

Grâce à la technologie de carte intelligente, CryptoCombo peut enregistrer en mémoire avec une sécurité totale les données de l'utilisateur (profils personnels, certificats digitaux, X.509) ; le composant de la mémoire flash dans la clé vous permet de garder des données et des applications. La clé privée utilisée pour signer les documents électroniques est stockée sûrement et secrètement à l'intérieur d'un composant cryptographique, par conséquent l'accès est protégé par des méthodes de PIN personnalisable : détenir le dispositif hardware CryptoCombo et connaître le PIN sont deux éléments de base de cette authentification au travers de « deux facteurs ».

CryptoCombo vous permet de générer une paire de clés cryptographiques internes et d'appliquer la signature digitale. Elle est équipée de dispositifs de sécurité qui empêchent l'exportation et la copie de la clé privée hors du dispositif qui l'a générée. La large mémoire, tant pour lire que pour écrire, vous permet de transférer des données et des applications.

Authentification d'utilisateurs et contrôle d'accès:



Votre signature digitale sur Internet. La clé USB intelligente.

Cryptoidentity est une clé de sécurité USB de haut rendement compatible avec la technologie PKI.

Cryptoidentity est capable d'exécuter en interne toutes les fonctions de sécurité grâce à son processeur interne, en restant isolé de l'ordinateur et d'autres points susceptibles d'être attaqués.

Compatible avec le standard ISO :

Support complet des standards ISO-IEC 7816, parties 1-4. Permet de stocker et d'administrer des données pour des applications différentes.

Caractéristiques principales : Génération de clé RSA : Cryptoidentity supporte la génération de clés RSA jusqu'à 1024 bits. Génération aléatoire de nombres : ceux-ci sont générés aléatoirement par le processeur de la clé, assurant que toutes les instances temporaires du processus de génération de clés s'exécutent dans un environnement sûr.

Pas besoin de lecteur, et sur n'importe quel système d'exploitation Windows, Cryptoidentity fournit des fonctions avancées de cryptographie utilisant la technologie PKI.

Authentification d'utilisateurs et contrôle d'accès



Protection de software.

Avec le système HARDkey vous pouvez protéger votre software en utilisant deux méthodes distinctes: l'une automatique qui protège les exécutables déjà compilés, et une autre qui invoque les bibliothèques depuis le code source.

Authentification d'utilisateurs

Les clés HARDkey USB peuvent aussi être utilisées pour implémenter une authentification par deux facteurs: quelque chose que je possède (la clé), plus quelque chose que je sais (le PIN). Cela permet de respecter les normes de sécurité comme la ISO 17799/27001 (Hardkey MIO).

Cryptage on-line de données

L'environnement de développement qui permet d'implémenter la protection automatique d'exécutables, vous apporte une option pour spécifier quels sont les fichiers de données associés à ce programme que vous souhaitez manipuler de façon cryptée.

Environnement de gestion.

Avec le nouvel Environnement de Gestion Intégrale pour Protection de Software vous pourrez manipuler de façon centralisée tout le processus productif, pour que votre produit soit réellement protégé, car la sécurité doit débiter déjà au sein de votre entreprise.