COMMUNIQUE DE PRESSE

Websense étend la protection évoluée du réseau ThreatSeeker à des fournisseurs de solutions tiers au travers d'une infrastructure de Cloud Computing

Une API Web permet d'offrir une connaissance hors pair de la sécurité à de nouveaux marchés et utilisateurs finaux

Paris, le 2 Novembre 2009. Websense, Inc. (NASDAQ : WBSN), le leader des solutions de sécurité des contenus, présente Websense® ThreatSeeker® Cloud, un service de sécurité de type Cloud Computing permettant aux fournisseurs de solutions tiers d'intégrer une protection dynamique et à forte valeur ajoutée à leurs produits et services. Le service ThreatSeeker Cloud assure la sécurité du Web, des données et du courrier électronique via l'infrastructure éprouvée de type cloud qui constitue le cœur des produits de sécurité du contenu Websense, notamment les offres de sécurité en mode SaaS et l'appliance V10000 Web Security Gateway.

« ThreatSeeker Cloud est essentiellement un service, de classe opérateur, d'abonnement à notre infrastructure d'identification et d'analyse du contenu. Cette infrastructure de type cloud s'adresse aux fournisseurs de solutions tiers », déclare Devin Redmond, Vice-président Développement commercial et Gestion des produits de Websense. « Il permet d'offrir les avantages de la technologie Websense à un ensemble élargi d'utilisateurs sur des marchés que nous ne couvrions pas auparavant. Cette nouvelle offre répond à différents besoins : les fournisseurs d'infrastructure peuvent renforcer les atouts de leurs produits et services alors que les utilisateurs finaux bénéficient d'une protection en temps réel et d'un meilleur environnement ».

Le service ThreatSeeker Cloud offre l'accès à l'analyse des contenus la plus évoluée du marché. Cette connaissance repose sur les données rassemblées par les 50 millions de points de collecte en temps réel du réseau Websense ThreatSeeker. Ce dernier traite plus de 1,5 milliard de demandes de sécurité utilisateur par jour et analyse plus de 40 millions de sites Web et 10 millions de messages chaque heure à la recherche de nouvelles menaces. Grâce à une API Web, les fournisseurs de solutions tiers peuvent tirer parti de ThreatSeeker Cloud pour intégrer la connaissance du réseau ThreatSeeker Incluant la classification en temps réel des

contenus et des sites web, la réputation, l'analyse comportementale, l'analyse des fichiers et des données et le filtrage de sécurité) à leurs propres produits et services pour protéger les utilisateurs contre les contenus Web malveillants, la fraude et les attaques de phishing.

Plus de 3,5 millions d'utilisateurs bénéficient actuellement d'une protection contre les menaces Internet grâce aux fournisseurs de solutions tiers faisant appel au service ThreatSeeker Cloud. Voici quelques exemples d'applications tierces utilisant ThreatSeeker Cloud :

- **Services de sécurité Web 2.0 –** Les sites de réseaux sociaux ou d'autres sites Web 2.0 peuvent utiliser ThreatSeeker Cloud pour analyser et classifier les liens hypertexte et les contenus publiés par les utilisateurs en temps réel, évitant la propagation de liens, de spams ou de contenus malveillants sur le site.
- **Passerelles de sécurité réseau –** Les fournisseurs de passerelles de sécurité réseau, de type pare-feu, boîtier UTM ou autres périphériques, peuvent tirer parti de l'API Web de ThreatSeeker Cloud en tant que couche d'extension de service permettant des fonctions de sécurité du contenu complémentaires sans nécessiter de nouvelle capacité matérielle ou puissance de traitement coûteuse sur le périphérique réseau.
- **Services FAI grand public –** Les fournisseurs d'accès Internet (FAI, ou ISP en anglais) peuvent utiliser ThreatSeeker Cloud pour classifier dynamiquement les sites Web et leur contenu afin de proposer des outils de contrôle parental et de navigation sécurisée à leurs clients.
- **Services de sécurité nomade –** Les opérateurs de téléphonie mobile peuvent protéger leurs usagers contre les contenus Web malveillants et le spam sur les périphériques mobiles connectés au Web.

Contrairement aux autres services de sécurité qui ne vérifient que la réputation de l'adresse IP d'origine, ThreatSeeker Cloud est le seul service de sécurité de type

cloud qui offre une analyse complète du contenu et une classification en plus de neuf points de réputation (notamment, type de propriété, catégorie d'URL, réputation lexicale, historique, âge, région ou propriétés de voisinage) pour les adresses IP d'origine, les sites Web et leur contenu. En exploitant les différents moteurs d'analyse du réseau ThreatSeeker, ainsi que les informations réunies à partir des 44 millions de postes abonnés aux solutions de sécurité hébergées ou locales de Websense pour le Web, les données et le courrier électronique, ThreatSeeker Cloud assure une sécurité en temps réel pour protéger contre les menaces combinées actuelles qui impliquent plusieurs vecteurs de menace de type e-mail et Web.

Tous les produits Websense de sécurité Web, des données et du courrier électronique reposent sur la connaissance des menaces collectées par le réseau ThreatSeeker. Websense met désormais cette connaissance à la disposition des fournisseurs d'applications, de services et de solutions tiers grâce à ThreatSeeker Cloud dans la lignée de sa stratégie visant à offrir une sécurité de type cloud dans sa gamme intégrée de solutions de sécurité de contenu et développer ses offres de sécurité Web en mode SaaS.

###

A propos de Websense, Inc.

Websense, Inc. (NASDAQ : WBSN), leader mondial des technologies intégrées de sécurité Web et de protection des courriels et des données, offre l'Essential Information Protection™ à plus de 44 millions de salariés du monde entier. Distribués au travers d'un réseau mondial de partenaires, les logiciels et les solutions de sécurité hébergées Websense aident les entreprises à bloquer les codes malveillants, à prévenir la perte d'informations confidentielles et à appliquer des règles de sécurité et d'accès Internet. Pour en savoir plus, consultez **www.websense.com**.

Suivez Websense sur Twitter: www.twitter.com/websense.

This news release contains forward-looking statements that involve risks, uncertainties, assumptions and other factors which, if they do not materialize or prove correct, could cause Websense results to differ materially from historical results or those expressed or implied by such forward-looking statements. All statements, other than statements of historical fact, are statements that could be deemed forward-looking statements, including statements about our technology and product leadership, growth trends and expense management, and statements containing the words "planned," "expects," "believes," "strategy," "opportunity," "anticipates" and similar words. The potential risks and uncertainties which contribute to the uncertain nature of these statements include, among others, risks associated with launching new product offerings, customer acceptance of the company's services, products and fee structures in a changing market; the success of Websense brand development efforts; the volatile and competitive nature of the Internet and security industries; changes in domestic and international market conditions, risks relating to currency exchange rates and impacts of macro-economic conditions on our customers, risks relating to the required use of cash for debt servicing, the risks of ongoing compliance with the covenants in the senior secured credit facility, risks related to changes in accounting interpretations and the other risks and uncertainties described in Websense public filings with the Securities and Exchange Commission, available at www.websense.com/investors. Websense assumes no obligation to update any forward-looking statement to reflect events or circumstances arising after the date on which it was made.