La solution FireAMP de Sourcefire délivre une protection innovante contre les malwares perfectionnés avec une visibilité et un contrôle sans précédent.

Cette nouvelle solution permet aux grands comptes d'identifier, de mieux comprendre puis de bloquer les malwares en utilisant les analyses du Big Data.

Paris, le 23 janvier 2012 – Sourcefire Inc. (Nasdaq : FIRE), acteur majeur sur le marché des solutions de cybersécurité adaptatives (Intelligent Cybersecurity solutions), annonce FireAMP™, sa solution innovante de protection contre les malwares qui identifie, analyse et bloque ces derniers, grâce aux données big data. Conçue pour les grands comptes, FireAMP délivre une visibilité et un contrôle sans précédent nécessaire pour bloquer les attaques non détectées par les autres layers de sécurité. FireAMP est la dernière réalisation issue de la vision Agile Security™ de Sourcefire, pour des solutions de sécurité adaptatives, automatisées et qui prennent en compte le contexte.

« *Les résultats de plusieurs tests montrent que les plateformes de protection du poste de travail (EPPs) actuellement disponibles ne protègent pas efficacement contre les menaces propagées massivement – et leur performance est d'autant plus décevante lorsqu'elles sont face à des attaques ciblées* », précisent **Neil MacDonald, vice président et Peter Firstbrook, directeur de recherche Gartner**[1]. « *De plus, dans certains cas, la durée d'une menace ciblée peut se mesurer en mois ou même en années. Gartner estime que 4 à 7 % des postes de travail en entreprise sont infectés de manière imprévisible et que les scans destinés à détecter les vulnérabilités ne détecteront que 1 % des menaces* ».

Avec le lancement de FireAMP, Sourcefire est le premier acteur du marché à proposer 5 nouvelles fonctionnalités qui renforcent la protection des entreprises contre les malwares perfectionnés :

- FireCloud™ - Infrastructure basée sur le Cloud qui englobe un certain nombre de fonctionnalités de détection avancées qui s'appuie sur l'analyse Big Data pour identifier et mettre en évidence les menaces non détectées par les autres couches de sécurité.
- File Trajectory - Traque le mouvement des données dans l'entreprise permettant d'identifier le point d'entrée du malware et sa propagation.
- File Analysis - Fournit des informations détaillées sur le comportement des malwares, soutenu par l'équipe VRT (Vulnerability Research Team) de Sourcefire et les connaissances collectives en sécurité de la société.

[1] Gartner, "Predicts 2012: Sophisticated Attacks, Complex IT Environments and Increased Risks Demand New Approaches to Infrastructure Protection" November 29, 2011.

- Outbreak Control – La détection de malwares définie par un client entraine le blocage immédiat des malwares sans devoir attendre une mise à jour par l'éditeur.
- Cloud Recall™ - Analyse continue dans le Cloud de l'historique de l'activité afin d'identifier et de remédier aux menaces qui n'auraient pas été détectées précédemment.

FireAMP utilise un agent léger pour communiquer avec un moteur d'analyse basé sur le Cloud et exploite uniquement les metadata pour l'évaluation, nécessitant moins de stockage, de calcul et de mémoire que les autres produits de sécurité. Ceci permettant également de minimiser l'impact sur le système, de faire coexister cette solution avec les autres layers de sécurité existantes sans sacrifier la performance et l'adaptabilité.

« *En développant ce produit, nous avons interrogé plus d'une centaine de grands comptes et nous avons toujours entendu le même discours : les entreprises disposent des dernières technologies de sécurité avec les dernières mises à jour mais constatent toujours des infections de malwares* », précise **Olivier Friedrichs, senior vice président Cloud Technology Group de Sourcefire.** « *Nous avons développé FireAMP avec une technologie de détection sophistiquée, une visibilité et un contrôle spécifiques pour les entreprises dont les principales solutions font défaut. Les fonctionnalités de détection et d'analyse de FireAMP peuvent aider ces entreprises à déterminer rapidement quel système est infecté, comment l'infection s'est produite, voir l'étendue de l'attaque et comprendre comment le malware se comporte afin de l'arrêter et de mettre fin aux dommages subis* ».

FireAMP propose des reporting qui fournissent une visibilité sur l'état des malwares dans l'environnement de l'entreprise. Ces rapports détaillent les ordinateurs à risque et la raison des vulnérabilités, mettent en évidence les applications qui ont permis d'introduire le(s) malware(s) et les attaques persistantes avancées, et font ressortir les malwares qui peuvent être unique à l'environnement du client. FireAMP intègre également des rapports comparatifs, afin que les utilisateurs puissent évaluer l'activité dans leur environnement ou plus largement sur la base installée des clients FireAMP.

Pour plus d'information, merci de consulter le site : http://sourcefire.com/FireAMP

A propos de Sourcefire

Sourcefire, Inc. (Nasdaq : FIRE), l'un des leaders mondiaux sur le marché des solutions de cybersécurité adaptatives, transforme la manière de gérer les réseaux des entreprises (moyennes et grandes) ainsi que des organismes gouvernementaux, tout en minimisant les risques liés à la sécurité, avec des solutions allant des plateformes de sécurité Next-Generation à la protection contre les malwares perfectionnés. Sourcefire, grâce à son concept Agile Security, apporte le dynamisme du monde réel dont les entreprises ont besoin, afin de se protéger et de se défendre contre les attaques des Hackers. Depuis 10 ans, Sourcefire est reconnu pour ses innovations et son leadership avec de nombreux brevets, classements mondiaux et récompenses.

A ce jour, le nom de Sourcefire est synonyme d'innovation, de sécurité adaptatives et agile pour une sécurité en continue.

###

Contacts Presse :

SOURCEfire
164 bis, avenue Charles de Gaulle – 92200 Neuilly sur Seine
Céline Gajnik
Email : celine.gajnik@sourcefire.com
www.sourcefire.com

Agence : CYMBIOZ
31, rue des Petits-Champs – 75001 PARIS
Pauline Moreau / Laëtitia Berché
Tel : 01 42 97 93 32 / 06 14 48 02 95
Email : pauline.moreau@cymbioz.com / laetitia.berche@cymbioz.com