# Blue Coat veut casser la sécurité en silo

Fort de ses **récentes acquisitions** (technologie SSL de Netronome et Solera Networks en mai 2013, Crossbeam Systems en décembre 2012), l'éditeur américain Blue Coat a récemment fait évoluer ses solutions de protection réseau pour les entreprises. Le spécialiste de la 'Business Assurance Technology' lance, dans le courant de ce mois de décembre, **Advanced Threat Protection** (ATP), une solution globale visant à lutter contre les menaces connues et inconnues, et pourvue de services de résilience ou remédiation.

Avec ATP, Blue Coat entend créer un cercle vertueux de protection à contre-courant des approches en silo où l'absence de synchronisation entre les technologies de sécurité exploitées contre chaque type de menace, mais aussi le manque d'échange entre les équipes chargées de la sécurité au quotidien et celles dédiées à la résolution des incidents, crée des effets de bords. *« Les approches en silo ne sont plus en mesure de répondre aux besoins des entreprises »*, souligne **Dominique Loiselet**, responsable de la branche française de l'éditeur.

## Trois solutions

ATP est construit autour de trois solutions principalement : Secure Web Gateway, Content Analysis System et Security Analytics Platform.

La première est une **appliance chargée de lutter contre les menaces connues** qui transitent sur le réseau en s'appuyant sur la base mondiale Global Intelligence Network (GIN), alimentée par 90% des quelque 80 millions d'utilisateurs de Blue Coat (ceux qui acceptent de partager ces informations). Cette première couche de protection s'installe n'importe où sur le réseau de l'entreprise, ou bien en mode Cloud ou hybride. Blue Coat vient de faire évoluer son offre avec la SSL Visibility Appliance capable de **déchiffrer les communications SSL** (tous protocoles confondus sauf en VPN) **jusqu'à 20 Gbit/s** et permet de gérer les listes blanches.

## Faire vieillir le code

Content Analysis System remonte pour sa part **les événements et menaces inconnus**. Elle s'appuie pour ce faire sur des listes blanches et un antivirus à double moteur en parallèle (dont les fournisseurs restent à préciser). Les codes inconnus sont filtrés et traités à partir de technologies de bac à sable (sandboxing) qui se chargent de « faire vieillir » le code suspect pour en vérifier le comportement et l'intégrité avant de, soit le réinjecter dans le réseau en cas d'absence avérée de menace, soit l'envoyer enrichir le réseau de l'entreprise et le GIN en cas de menace déterminée. Autrement dit, *« rendre connu ce qui était inconnu quelques instants auparavant »*, résume Dominique Loiselet.

Le **sandboxing s'exécute sur la Malware Analysis Appliance** (MAA) de Blue Coat, à partir de technologies IntelliVM et SandBox fournies par Norman Shark. L'offre du spécialiste du sandboxing entend se distinguer en permettant aux responsables de la sécurité de personnaliser l'environnement d'exécution pour **le rapprocher de l'environnement réel de l'entreprise**. Cibler

les besoins permet ainsi d'optimiser les ressources et améliorer l'efficacité des détections.

## Remonter dans le passé

En cas de code malicieux détecté commence alors la difficile quête pour en vérifier les éventuelles conséquences (à quand remonte l'attaque, qui est l'attaquant, quels systèmes sont compromis, etc.) et le travail pour retrouver un environnement sain et se protéger à l'avenir. Pour Dominique Loiselet, il n'y a, pour ce faire, qu'une seule méthode : ***« Remonter dans le passé ».***

C'est tout l'objet de l'offre **Security Analytics Platform by Solera**, ex-Solera Platform racheté par Blue Coat en mai dernier. Le rôle de ces appliances est simple : enregistrer tout le trafic qui a circulé sur le réseau (selon les critères définis par la politique de l'entreprise). Cette montagne de données permettra, à coup de sandboxing et de technologies Big Data, de *« recréer l'histoire du réseau »* (cessions e-mail, web, transfert de fichiers…) pour repérer à quel moment à eu lieu l'infection et comment elle s'est développée. Un travail titanesque manuellement (à l'image de l'aiguille dans la botte de foin), mais une technologie par défaut gourmande en ressources de stockage.

## Technologies tierces

Notons que Content Analysis System peut s'intégrer aux environnements de sécurité existant, mais aussi accueillir des technologies de bac à sable tierces comme FireEye, une offre de nouvelle génération pour lutter contre les failles Zero Day, les attaques ciblées et le malwares avancés. Autant de nouvelles couches qui viennent s'ajouter aux méthodes historiques de protection (parefeu, antivirus, inspection de packets…) et que Blue Coat entend automatiser en positionnant ses solutions de prévention et détection à chaque étape du cycle de vie des menaces pour l'entreprise.

Crédit photo : © Sergej Khackimullin – Fotolia.com

---

**Lire également**

Blue Coat Systems résume le Byod dans une infographie
Reporters sans frontières s'attaque aux éditeurs d'outils de filtrage