Check Point Threat Emulation : Matrix version anti-malware.

En émulant en conditions réelles l'exécution d'un code suspect, la solution Threat Emulation de Check Point Software apporte une réponse efficace aux codes les plus malicieux, les moins repérables.
Antivirus, antibot (bot : agent logiciel interagissant avec des serveurs informatiques à l'insu de l'utilisateur), anti-intrusion… les solutions de protection contre les menaces électroniques savent de mieux en mieux détecter au plus vite des attaques qui se sont déjà produites, en divulguant et recevant au plus tôt les signatures de ces codes dès qu'ils sont repérés (y compris via des mécanismes de collaboration au niveau mondial, et même entre éditeurs concurrents).
Certaines peuvent même détecter des "comportements apparemment suspects".
Néanmoins, la marge de manœuvre des hackers reste importante. D'où la nécessité d'intervenir en amont, et de jouer in vivo les éventuelles menaces pour les écarter. Ainsi, les attaques de type "Zero day" (exploit qui tire parti d'une faille non encore découverte) peuvent être déjouées.

De la détection a posteriori…

La protection des systèmes d'information est majoritairement assurée via des passerelles de sécurité. Tout le trafic de données à analyser est alors redirigé vers ces équipements installés sur le réseau.
La solution Threat Prevention de Check Point Software combinait déjà trois types de protection : l'IPS/IDS contre les intrusions (Intrusion prevention system, Intrusion detection system), un antibot et un antivirus évitant l'infection de codes malveillants. En fait, la solution peut exécuter un ou plusieurs de ces lames (ou blades) logicielles.
Avec le nouveau module Threat Emulation, l'éditeur se propose de s'attaquer aussi aux malware de type "zero day".

… à une réelle prévention.

« En mode traditionnel, il s'agit de détecter au plus tôt des malwares connus,» explique Ben Carmi, responsable produit chez Check Point Software. *« Désormais, il s'agit également de détecter les malwares non connus a priori. D'où la nécessité d'une émulation en conditions réelles.»*
Check Point Threat Emulation détourne les fichiers attachés aux e-mails ou téléchargés de type Microsoft Office ou Adobe PDF vers une sandbox.
Cet environnement reprenant la configuration à laquelle est destinée l'information ouvre les fichiers et le système examine tout ce qui se passe : comportement inhabituel, modification anormale du registre du système, connexion réseau ou processus système suspects, etc.
Si un problème est détecté, les données concernées sont bloquées dès la passerelle.
Les menaces détectées sont automatiquement remontées vers le Threat Cloud de Check Point.
Cela permet ainsi de partager ces informations avec toutes les passerelles déployées chez les clients de l'éditeur. Un processus qui assure une prévention optimale.

Les terreurs du bac à sable

Threat Emulation détourne les données, mais les envoie vers un autre équipement pour réaliser l'émulation dans la sandbox. Ce sas étanche reproduit (émule) l'environnement récepteur des

données, et peut simuler un environnement Windows (XP,7 et bientôt 8) ou encore l'environnement spécifique de l'utilisateur.
« Il est également possible de définir des groupes d'utilisateurs et de simuler alors l'exécution dans un environnement en fonction de la destination des données,» ajoute Ben Carmi.

Boite à émuler ou cloud de simulation

L'éditeur propose deux types de déploiement pour le mécanisme de sandbox.
L'entreprise peut accéder au service cloud en charge de ce type de traitement, ou opter pour une appliance qu'elle installera sur son réseau.
Dans ces deux configurations, l'interface d'administration de la passerelle de Check Point permettra aussi bien de définir les divers paramètres et environnements que d'accéder aux rapports détaillés (avec multiples possibilités d'analyses et recoupements documentés).
« La passerelle détermine les fichiers à examiner, et le service cloud ou l'appliance exécute le traitement,» affirme Ben Carmi. *« Les PME et agences de grandes entreprises seront intéressées par l'offre cloud. Pour des besoins spécifiques ou de temps de latence critique, l'appliance incarne une alternative efficace.»*

Tout système a son talon d'Achille

Point délicat du système : la détermination de ce qui doit être examiné.
Comme le précise Ben Carmi, *« Nous cherchons à nous assurer de ne laisser passer que les fichiers nécessaires à l'émulation. Et le système ne laisse passer que ceux dont il sait qu'ils ne présentent aucun risque.»*
Pourtant, même en ne laissant passer que ce qui est connu, aucun système n'est à l'abri d'un faux positif (qui passerait sans être examiné).
Comme toujours, le juste équilibre entre coût, performance et sécurité sera déterminé selon les exigences de chaque entreprise.

Disponible au second trimestre 2013 auprès des partenaires et revendeurs Check Point, la solution sera facturée sous forme de licence annuelle incluant le service cloud. Ceux qui en ont besoin pourront ajouter le prix d'une appliance.