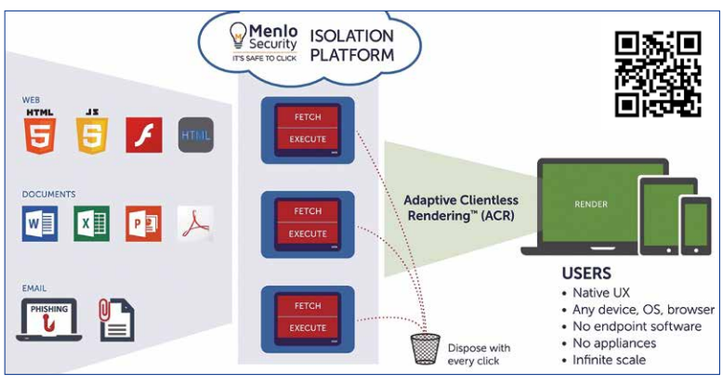
0 % de logiciels malveillants grâce à l'isolement

Les cybermenaces, toujours croissantes, sont de plus en plus difficiles à contrer. Une nouvelle approche technique veille à ce que les attaques de codes malveillants et le hameçonnage n'atteignent plus l'utilisateur: elle consiste à isoler le navigateur, les documents et les e-mails.



La plate-forme d'isolement de Menlo Security garantit que les logiciels malveillants n'atteignent en aucun cas l'utilisateur.

Le problème de la cybercriminalité se pose de plus en plus, comme le constate le rapport de KPMG «Clarity on Cyber Security» de mai 2017. Ainsi, au cours des douze derniers mois, 88% des entreprises suisses interrogées ont subi une cyberattaque, tandis que ce taux était de 54% l'année précédente. A cet égard, les menaces inconnues jusqu'alors et les points faibles non encore identifiés jouent un rôle déterminant. Les principaux vecteurs d'attaque sont les sites contenant des codes malveillants, les documents Office et PDF ou encore les e-mails de hameçonnage. Les contenus Web nocifs et le hameçonnage représentent environ 85% des cyber-risques.

Les solutions conventionnelles de riposte aux cyberattaques se basent le plus souvent sur l'identification de signatures préalablement connues de logiciels malveillants et de caractéristiques déduites. Dès lors, les menaces qui utilisent de nouveaux mécanismes ne sont pas interceptées. Une autre méthode consiste à contrôler l'intégralité du contenu entrant par l'exécution de code potentiellement malveillant dans un environnement protégé (sandboxing), technique qui nécessite beaucoup de temps, de calculs et qui se base elle aussi sur le principe de la détection de code malveillant.

Nouvelle approche

En 2013, l'entreprise californienne spécialisée dans la sécurité Menlo Security a mis au point une toute nouvelle façon de procéder. L'objectif est d'éviter que les logiciels malveillants ne parviennent à l'utilisateur. La plate-forme d'isolement de Menlo Security isole chaque contenu entrant (sites Web, documents, e-mails) dans un conteneur – un environnement virtuel sécurisé – où elle exécute le code embarqué (JavaScript, Flash, Java). S'il s'agit de code malveillant, celui-ci s'exécute à l'intérieur du conteneur et aucun dommage n'est causé, le conteneur étant immédiatement éliminé après l'analyse.

Le contenu inoffensif est quant à lui retransmis à l'utilisateur comme information de rendu ne comportant aucun élément exécutable, sur la base du «Document object model» (DOM) pour HTML, (Adaptive Clientless Rendering). Ceci garantit que le client est isolé de tout code malveillant, le véritable traitement des données de navigation se faisant sur la plate-forme d'isolement. Il en va de même pour les e-mails et les documents; aucun logiciel supplémentaire ne doit être installé sur le terminal, seule la définition d'un serveur proxy est nécessaire. L'utilisateur travaille comme d'habitude avec son navigateur, la suite Office, son lecteur PDF et son client de messagerie.

Sécurité sans détection

Simultanément, la méthode d'analyse incertaine consistant à distinguer un «bon» contenu d'un «mauvais» disparaît. La solution de Menlo Security intervient sans la moindre détection. Ceci présente l'avantage d'éliminer complètement les innombrables alertes de sécurité produites par les solutions à base de détection et de soulager l'équipe de sécurité. Cependant, si vous le souhaitez, la plate-forme d'isolement peut également être combinée à une protection conventionnelle contre les logiciels malveillants.

Autre effet positif: puisque le client ne reçoit que du contenu purgé de tout code exécutable, le chargement de sites Web est beaucoup plus rapide. Le code source des pages rendues est allégé par rapport à l'original et transmis plus rapidement, le navigateur ne devant plus fournir de calculs.

Loin du cloaque

Avec sa solution, Menlo Security se tient très exactement sur la ligne décrite par l'analyste Neil MacDonald de chez Gartner: «Il est temps d'isoler vos utilisateurs du cloaque d'Internet grâce à la navigation à distance.» Sur la base d'une plate-forme d'isolement, le fabricant propose trois services combinables ou utilisables séparément: service d'isolement Web, service d'isolement de documents et service d'isolement du hameçonnage. La plate-forme d'isolement est disponible en tant que service cloud ou comme appliance virtuelle pour l'exploitation sur site. Le fabricant ne propose pas de solution matérielle.

Menlo Security Isolation Platform: les points forts

- Isolement complet des utilisateurs de tout logiciel malveillant
- Agentless: aucun logiciel nécessaire sur le client
- Elimine les contenus malveillants en JavaScript, Flash et Java
- Fiabilité de l'isolement de 100%: les images et les polices sont aussi interceptées
- Protection contre le hameçonnage par des e-mails en lecture seule
- Protection contre la publicité malveillante (Malvertising) et les ransomwares
- Disponible en tant que service cloud ou sous forme d'appliance virtuelle
- Licence par utilisateur et par an

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
vente@boll.ch
www.boll.ch/info/menlo-fr