

Sophos UTM 9 : la sécurité unifiée et complète jusqu'aux systèmes

L'approche UTM (Unified Threat Management) consiste à gérer un ensemble de solutions de sécurité, distribuées via une appliance, un serveur ou en mode virtuel, et administrées à partir d'une interface utilisateur unique. Dans cette vision globale, **UTM 9** du Britannique **Sophos** se veut la première solution à assurer une protection complète, jusque sur les mobiles.

Le principe de l'UTM est de réunir et gérer un ensemble de produits de sécurité en un seul et même endroit, et sans se soucier des problématiques de compatibilité. Chez Sophos, cela se traduit aujourd'hui par le pare-feu et l'IPS ; le pare-feu pour les applications web ; la sécurité des messageries ; la sécurité web et le filtrage ; l'administration sans fil et la sécurité ; des solutions pour les succursales ; l'accès VPN sécurisé pour les utilisateurs itinérants ; et, désormais, la protection des systèmes d'extrémité.

UTM, approche globale... et politique

La concentration des solutions simplifie l'administration de la sécurité de l'infrastructure avec une protection intégrée et qui se veut complète. En réalité, il manque des composants à la majorité des solutions d'UTM, la plupart d'entre elles se révélant incomplètes. Chez Sophos, par exemple, il manquait la brique protection des systèmes. Un domaine sensible, car il couvre les utilisateurs mobiles et le BYOD (Bring Your Own Device), la vague de fond de l'usage par les employés de leur propre matériel électronique, de l'ordinateur portable au smartphone, en passant par la tablette.

Cette introduction forcée des systèmes dans les domaines de la sécurité et de l'UTM devient essentielle aujourd'hui. En revanche, elle complexifie singulièrement la tâche des administrateurs, comme des responsables sécurité. La couverture fonctionnelle des UTM doit donc s'élargir afin d'en simplifier la gestion. Sophos l'a bien compris en intégrant également dans son offre la gestion des politiques pour l'ensemble des systèmes.

Hotspots, VPN, cloud

Parmi les nouvelles fonctionnalités apportées par UTM 9, Sophos a étendu les fonctions de sa passerelle de sécurité vers les périphériques via son service dans le cloud **LiveConnect** qui protège les systèmes connectés. Le portail VPN en HTML5 sécurise les applications distantes sans nécessiter l'installation d'une brique logicielle sur le poste distant, tout en s'appuyant sur VNC, SSH, etc. Enfin, les fonctionnalités de sécurité sans fil permettent de configurer les hotspots d'accès WiFi à destination des visiteurs ou des employés BYOD, avec par exemple des quotas d'accès en fonction de l'heure ou de la bande passante.