

SonicWall Capture Client powered by SentinelOne

La menace en constante expansion que représentent les ransomwares et autres attaques par logiciels malveillants montre que l'efficacité des solutions de protection client ne se mesure pas à la simple conformité des terminaux. La technologie d'antivirus classique est fondée sur des signatures, une approche depuis longtemps en proie à des difficultés et qui n'est pas parvenue à suivre le rythme des malwares et techniques d'évasion de dernière génération. Ces derniers nécessitent en effet une approche différente de la protection client. De plus, avec la généralisation du télétravail, de la mobilité et du BYOD, il est devenu urgent de fournir une protection cohérente de tous les terminaux, où qu'ils soient.

SonicWall Capture Client est une offre unifiée proposant diverses fonctionnalités de protection à l'intention des terminaux. Doté d'un moteur de protection anti-malware de nouvelle génération propulsé par SentinelOne, Capture Client applique des techniques de protection contre les menaces évoluées, comme l'apprentissage machine ou le rollback du système. Capture Client tire également parti de l'inspection approfondie du trafic TLS chiffré (DPI SSL) sur les pare-feux SonicWall en installant et en gérant des certificats TLS de confiance.

Capture Client coexiste avec SonicWall Content Filtering Client et SonicWall Global VPN Client. Des règles valables pour tous les produits peuvent être gérées d'une seule et même console de gestion basée dans le cloud. SonicWall Capture Client s'ajoute très simplement à tout client déployé, que ce soit via des règles de groupe Microsoft Active Directory ou une autre technique de déploiement de logiciel tiers ; ou encore via la fourniture d'URL personnalisées où les clients peuvent procéder au téléchargement et à

l'auto-installation en toute discrétion, sans aucune intervention supplémentaire. Dans le cas d'une intégration à un pare-feu SonicWall, Capture Client offre également une expérience « zéro intervention » lors du déploiement sur des appareils non protégés.

Fonctionnalités et avantages

Surveillance comportementale en continu des appareils : elle aide à créer un profil complet de l'activité des fichiers, des applications, des processus et du réseau. Cela permet d'assurer une protection contre les logiciels malveillants agissant avec ou sans fichier et offre une vue à 360 degrés des attaques avec des informations exploitables, utiles pour mener l'enquête.

Différentes techniques de protection heuristiques multicouches : veille cloud, analyse statique avancée et protection comportementale dynamique. Elles aident à protéger contre les logiciels malveillants connus et inconnus et à y remédier.

Pas besoin d'analyses régulières ni de mises à jour périodiques : le plus haut niveau de protection est assuré à tout moment sans que la productivité des utilisateurs soit freinée.

Fonctionnalités uniques de rollback : elles prennent en charge des règles qui non seulement suppriment entièrement la menace, mais qui restaurent aussi le client ciblé à l'état précédant le début de l'activité malveillante. Il n'est plus nécessaire d'opérer une restauration manuelle en cas de ransomware ou d'attaques similaires.

Console de gestion cloud : elle réduit l'empreinte et les frais de gestion. Elle améliore également la possibilité de déployer et d'appliquer la protection sur un terminal, où qu'il soit.

Avantages :

- Gestion indépendante dans le cloud
- Synergies avec les pare-feux SonicWall
- Application des règles de sécurité
- Gestion des certificats DPI SSL
- Surveillance comportementale en continu
- Déterminations haute précision grâce à l'apprentissage machine
- Différentes techniques heuristiques multicouches
- Fonctionnalités uniques de rollback

Intégration aux pare-feux de nouvelle génération SonicWall : pour un déploiement zéro intervention et une conformité améliorée des terminaux. Cela permet en outre l'application de l'inspection approfondie des paquets du trafic chiffré (DPI SSL) par le déploiement de certificats de confiance au niveau de chaque terminal.

Gestion centralisée et reporting de la protection client

La console de gestion cloud SonicWall fonctionne comme un seul écran où sont gérées toutes les règles des clients, dont la protection anti-malware de nouvelle génération, la gestion des certificats DPI SSL, le filtrage de contenu et le VPN.

La console de gestion est une plateforme cloud mutualisée, proposée sans frais supplémentaires. Elle fournit des rapports sur la protection des clients et assure la gestion des règles, notamment de contrôle d'accès granulaire. Les fournisseurs

de services gérés (MSP) peuvent ainsi proposer la gestion et le reporting des équipements de plusieurs clients. Parallèlement, chacun de ces clients ne peut gérer et obtenir des rapports que sur ses propres appareils.

C'est aussi une plateforme d'investigation qui aide à identifier la racine des malwares décelés et fournit des informations directement exploitables sur la manière d'empêcher ces menaces de réapparaître. Par exemple, un administrateur peut facilement voir quelles applications sont exécutées sur un appareil, ce qui, en retour, peut aider à identifier les machines sur lesquelles sont installés des logiciels vulnérables ou non autorisés.

Offres et plateformes prises en charge

SonicWall Capture Client est disponible en deux offres :

SonicWall Capture Client Basic intègre toutes les fonctionnalités de protection et de réparation anti-malware de nouvelle

génération SonicWall, ainsi que la prise en charge DPI SSL.

SonicWall Capture Client Advanced intègre toutes les fonctionnalités Basic susmentionnées, auxquelles s'ajoutent des fonctionnalités de rollback avancées.

Les deux offres sont disponibles pour Windows 7 et versions plus récentes, ainsi que pour Mac OSX.

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cybersécurité en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

