Symantec by Broadcom | Carbon Black. by Broadcom | Arrow

GUIDE

Guide pratique

Sécurité et résilience avec Symantec ZTNA

Votre VPN est censé offrir un accès distant sécurisé, mais en réalité, il peut devenir une porte ouverte sur votre réseau. Les VPN traditionnels reposent sur l'idée que toute personne à l'intérieur du périmètre réseau est digne de confiance, ce qui constitue un risque. Chaque sous-traitant, partenaire ou fournisseur tiers devient ainsi une porte d'entrée potentielle pour une intrusion.

Lorsqu'un pirate compromet les identifiants d'un seul sous-traitant, il ne se limite pas à une application : il peut circuler librement dans l'ensemble de votre réseau. Les récentes cyberattaques médiatisées ont révélé que l'accès des tiers constitue désormais le maillon faible de la sécurité des entreprises.

Symantec Zero Trust Network Access (ZTNA) révolutionne la sécurité en remplaçant la confiance implicite par une vérification continue et en substituant l'accès global au réseau par des connexions ciblées, limitées à chaque application.

Pourquoi est-il urgent de résoudre la crise liée à l'accès des tiers ?

Les VPN traditionnels donnent par défaut un accès complet au réseau, car ils ne peuvent anticiper les applications dont les utilisateurs auront besoin. Cette approche « tout ou rien » implique qu'un employé, consultant ou sous-traitant à distance, engagé pour mettre à jour votre site web, pourrait également accéder à vos systèmes financiers, à vos bases de données clients et à votre propriété intellectuelle. Les analyses de vulnérabilité et les techniques de cartographie exposent toute la topologie de votre réseau à quiconque dispose d'identifiants basiques.

Le manque de visibilité accentue ce risque. Les données essentielles à la conformité et à la gestion des incidents sont éparpillées sur plusieurs serveurs, appareils et emplacements, sous des formats variés. Les équipes de sécurité peinent à obtenir des informations lors de la réponse aux incidents, car les activités des utilisateurs sont réparties sur des systèmes isolés. Sans visibilité, la défense est impossible.

L'accès BYOD (Bring Your Own Device) soulève un autre défi. Les sous-traitants et partenaires utilisent souvent leurs propres appareils. Les règles de leur entreprise peuvent interdire l'utilisation de votre VPN sur ces appareils, ou votre VPN peut ne pas être compatible.

La gestion des VPN nécessite la mise en place de configurations DMZ complexes ainsi que de règles de pare-feu rigoureuses, ce qui mobilise fortement les ressources informatiques. Cela contraint également le trafic à transiter par des centres de données centralisés, ce qui engendre des goulots d'étranglement susceptibles de freiner l'efficacité du travail à distance.

Améliorer la résilience des systèmes grâce au ZTNA

Le Zero Trust révolutionne les standards de la sécurité des réseaux. Plutôt que de considérer les utilisateurs à l'intérieur du périmètre comme fiables par défaut, le modèle Zero Trust repose sur un principe fondamental : ne jamais accorder de confiance sans vérification systématique.

Dans le cadre du ZTNA, chaque requête d'accès est soumise à une vérification rigoureuse. Les systèmes analysent plusieurs critères lors d'une demande d'accès, notamment l'identité de l'utilisateur, l'état du terminal, sa localisation, le mode d'authentification utilisé, ainsi que l'URI spécifique de l'application sollicitée.

Cette approche de périmètre défini par logiciel permet de sécuriser chaque application individuellement, en les rendant totalement invisibles aux utilisateurs non autorisés. Elle repose sur un modèle d'accès à privilèges minimaux, n'autorisant l'utilisateur qu'à accéder aux seules applications pour lesquelles il dispose d'une autorisation explicite.

Symantec ZTNA remplace l'accès réseau étendu par des connexions directes et sécurisées, établissant des tunnels chiffrés entre des utilisateurs identifiés et des applications précises. **Cela offre trois principaux avantages :**

Rendimiento

La connectivité directe entre les points supprime les goulots d'étranglement et améliore la réactivité en réduisant la latence. Les tests menés par Symantec ont révélé que les temps de transaction étaient en moyenne 62 % plus rapides qu'avec les connexions VPN classiques. Grâce à son intégration avec Google Cloud, Symantec ZTNA offre des performances accrues et une évolutivité renforcée, permettant de répondre efficacement à l'ensemble des besoins des utilisateurs.

Securidad

ZTNA réduit l'impact d'une compromission en rendant invisibles les segments du réseau non autorisés pour l'utilisateur. En cas de compromission d'identifiants, un attaquant ne pourra accéder qu'à une seule application, sans possibilité d'explorer davantage le réseau. Le déplacement latéral devient impossible en l'absence d'un réseau accessible pour s'y propager.

Resiliencia

Les solutions Symantec s'appuient sur l'infrastructure de Google Cloud pour proposer trois zones de disponibilité par point de présence, ainsi qu'un basculement en un clic en cas de panne, disponible dans toutes les régions du monde. Cela garantit leur disponibilité, même en cas de catastrophe naturelle.

Sécurité et résilience avec Symantec ZTNA

Votre plan d'action étape par étape pour déployer le ZTNA

Le déploiement du ZTNA peut s'effectuer sans perturber les opérations existantes Symantec préconise une approche en trois étapes afin de maximiser les bénéfices du ZTNA et d'offrir des fonctionnalités que les VPN traditionnels ne proposent pas.

Étape 1 : accorder aux utilisateurs distants un accès strictement limité, basé sur le principe du moindre privilège.

Le modèle d'accès à privilèges minimaux de Symantec ZTNA garantit que chaque utilisateur ne peut accéder qu'aux applications pour lesquelles il dispose d'une autorisation explicite. Ces applications sont isolées du reste du réseau, ce qui empêche tout accès non autorisé, qu'il soit malveillant ou accidentel, aux données et ressources sensibles.

Commencez par les collaborateurs à distance — qu'ils travaillent depuis leur domicile, soient en déplacement commercial ou fassent partie d'équipes décentralisées — qui ont besoin d'un accès sécurisé aux applications. Ces utilisateurs constituent la principale surface d'exposition aux risques et ont une influence majeure sur la productivité. Activez l'accès avec agent pour les appareils administrés, et privilégiez l'accès sans agent pour les environnements BYOD. Symantec ZTNA prend en charge divers protocoles, notamment les applications Web, SSH pour les équipes DevOps, RDP pour l'accès aux postes de travail à distance, ainsi que TCP pour les applications existantes.

Une fois que les employés bénéficient d'un accès sécurisé, il est essentiel d'étendre cette protection aux sous-traitants, partenaires et fournisseurs. Cette démarche démontre rapidement sa valeur auprès de vos utilisateurs clés, tout en maîtrisant les risques liés aux partenaires externes. Cette solution s'avère également particulièrement pertinente dans le cadre de fusions et acquisitions, où la nouvelle entité doit souvent accéder aux ressources de l'entreprise mère tout au long du processus d'intégration.

Votre VPN actuel peut rester opérationnel durant la phase de transition, ce qui permet d'éviter toute interruption pendant la validation du modèle Zero Trust.

Étape 2 : consolidation des mesures de sécurité par l'intégration de protections avancées contre les menaces et de dispositifs de sécurisation des données.

Cette étape intègre les dispositifs de protection contre les menaces ainsi que les mécanismes de sécurisation des données. Les VPN peuvent introduire des vulnérabilités dans le système de sécurité. Ils sont incapables d'analyser le trafic pour détecter les menaces ou d'appliquer des politiques de protection des données. Symantec ZTNA apporte une rupture avec les approches traditionnelles. Chaque accès à une application privée est désormais soumis aux mêmes contrôles de sécurité que le reste du trafic réseau. Symantec ZTNA s'intègre nativement au service Symantec Threat Intelligence, qui inspecte tous les fichiers pour détecter les logiciels et contenus malveillants, ainsi qu'à Web Isolation, qui protège automatiquement les utilisateurs contre les sites inconnus ou potentiellement dangereux. Symantec ZTNA s'aligne également avec Symantec Data Loss Prevention (DLP), permettant l'application des politiques existantes de prévention des pertes de données au trafic ZTNA, et assurant ainsi une cohérence des protections et des restrictions.

Étape 3 : généralisation du déploiement du ZTNA à l'échelle de l'organisation.

Cette étape marque le déploiement de Symantec ZTNA à l'échelle de l'organisation, au-delà des seuls utilisateurs à distance. Elle propose à l'ensemble des collaborateurs, y compris ceux présents sur site, un accès aux applications et aux ressources via une méthode renforcée en matière de sécurité.

Avec Symantec ZTNA, les règles de conformité appliquées à l'accès au SaaS et au Web s'étendent désormais aux applications internes. Le trafic est inspecté directement dans le cloud, sans recours à un proxy ni redirection via les data centers, assurant une protection homogène, que les utilisateurs accèdent aux ressources sur site ou dans le cloud. Les règles applicatives assurent que chaque utilisateur n'accède qu'aux ressources qui lui sont autorisées, tandis que le reste demeure totalement invisible. Chaque tentative d'accès génère des journaux d'audit centralisés, offrant une visibilité inédite que les VPN ne permettaient pas.

Vous avez également la possibilité de déployer un agent unique, capable de gérer ZTNA en parallèle des solutions Symantec déjà en place, telles que Cloud SWG, Cloud Access Security Broker, DLP et Web Isolation. Cela simplifie grandement le déploiement et la gestion, grâce à l'utilisation d'un agent unique couvrant plusieurs cas d'usage.

Une fois les résultats positifs constatés, vous serez en mesure de retirer progressivement votre infrastructure VPN. Ce n'est pas un hasard si 80 % des projets pilotes aboutissent à une adoption définitive.

Sécurité et résilience avec Symantec ZTNA

Concrétiser les bénéfices du SSE pour les entreprises modernes

La consolidation permet de réduire la multiplication des outils. L'association de ZTNA avec Cloud SWG et DLP/CASB dans le cadre du Security Service Edge (SSE) permet de renforcer, rationaliser et simplifier vos opérations de sécurité.

Les clients de Symantec SWG disposent déjà d'un composant clé d'un cadre Zero Trust. Ils peuvent désormais intégrer cette solution à ZTNA de manière transparente, en s'appuyant sur le même agent, la même console de gestion et le même cadre de politiques.

Les bénéfices opérationnels sont immédiats :

Mise en œuvre accélérée

Mettez en place le système en quelques minutes, plutôt qu'en plusieurs semaines.

Protection totale

Symantec Threat Intelligence Service et Remote Browser Isolation assurent une protection unifiée contre les malwares et les menaces émergentes, quel que soit le service utilisé.

Simplification de la gestion

Simplifiez votre sécurité en centralisant l'infrastructure, plutôt que de gérer plusieurs fournisseurs aux interfaces, licences et processus d'assistance disparates.

Conclusión

Mettre en œuvre le ZTNA permet de réduire efficacement les risques associés à la transformation numérique. Il ne s'agit pas uniquement de réaliser des économies — même si la réduction du nombre de fournisseurs permet effectivement d'alléger le budget. L'objectif est de déployer une architecture de sécurité flexible, conçue pour s'aligner sur les besoins de votre entreprise tout en simplifiant sa gestion.

Continuer à utiliser des VPN jugés « acceptables » expose les organisations à des risques évitables. Une technologie moderne permet désormais de bloquer les mouvements latéraux, de sécuriser les accès tiers, tout en optimisant l'expérience utilisateur et les performances. La vraie question n'est plus de savoir si vous devez adopter le Zero Trust, mais quand vous le ferez.