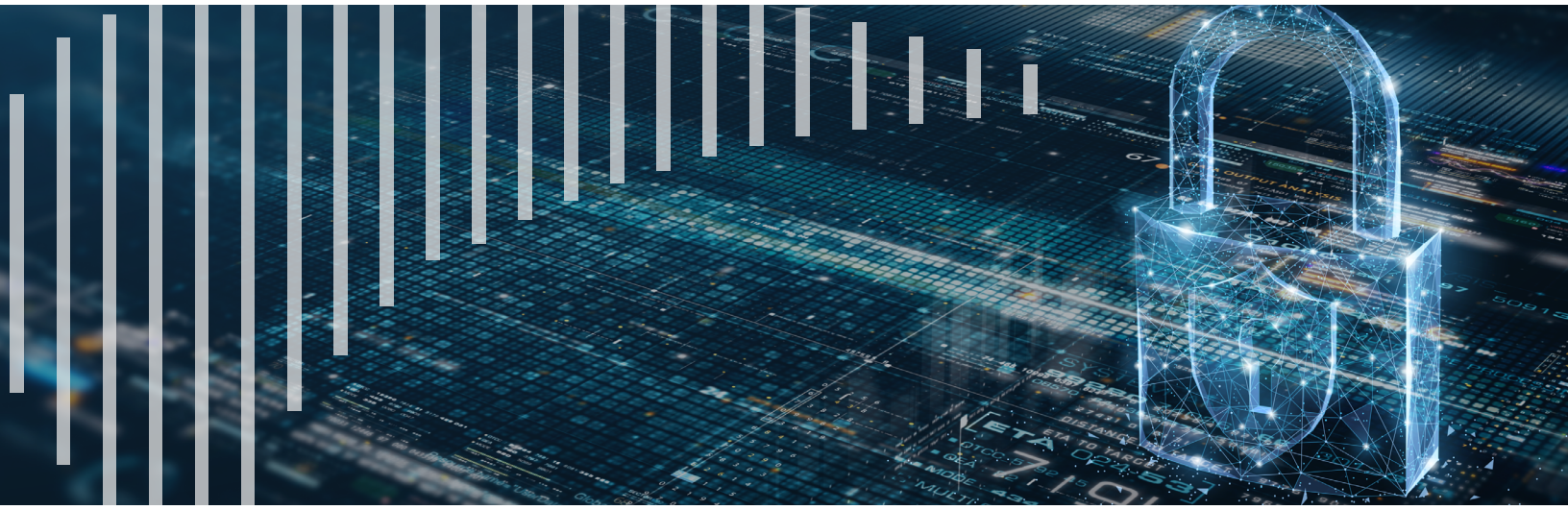


PRÉSENTATION

Évolution des menaces, évolution des stratégies

Intro

Le paysage de la cybersécurité évolue rapidement, et les entreprises doivent évoluer avec lui.

Le développement massif de l'informatique distribuée entraîne une explosion sans précédent des points d'exposition que les cybercriminels et les auteurs de menaces avertis peuvent exploiter.

Avec la généralisation des environnements hybrides et entièrement distants, les vecteurs de cyberattaques se multiplient aussi avec un afflux de nouveaux points d'exposition. Les menaces courantes et les attaques en plusieurs temps sont de plus en plus difficiles à détecter. De nombreuses entreprises sont à la recherche de moyens pour renforcer leur cybersécurité et devancer les pirates. Il existe de nombreuses stratégies et technologies que les entreprises peuvent exploiter pour renforcer leur système de sécurité et se protéger.

Mettez en œuvre une authentification multifacteurs

L'authentification multifacteurs (MFA) est une nécessité absolue, tant pour les entreprises que pour les particuliers. C'est une barrière supplémentaire entre les réseaux et les cybercriminels L'activation de l'authentification multifacteurs peut compliquer les attaques et même rendre leur coût prohibitif pour les auteurs de menaces. L'authentification multifcateurs peut mettre fin aux attaques courantes comme le phishing, les enregistreurs de frappe, la force brute et les attaques de type « man in the middle » (MITM). Il existe différents types d'authentifications multifcateurs :

- Basée sur un dispositif personnel : comme un SMS ou une application d'authentification.
- Basée sur le matériel : une clé USB, une carte à puce ou un jeton RSA, par exemple.
- Biologique : une empreinte digitale ou un scan de la rétine.

Comme pour n'importe quels technologies ou logiciels, les entreprises doivent conduire des recherches et protocoles de test appropriés pour mettre en œuvre la règle d'authentification multifcateurs adaptée à leurs besoins de sécurité.

Apprenez à mieux évaluer les risques

Pour élaborer une stratégie de sécurité efficace, les entreprises doivent savoir comment évaluer précisément les risques, et cela diffère d'une entreprise à l'autre. Une administration publique peut sauvegarder des ressources mondiales et des informations secret-défense. Une petite entreprise peut développer la réputation de sa marque et verrouiller ses actifs financiers. Quelle que soit la taille de votre entreprise, de nombreux professionnels de la sécurité se tournent vers le NIST (National Institute of Standards and Technology) pour garantir le respect des normes et des bonnes pratiques réglementaires. Si les cadres peuvent constituer une base solide, les entreprises doivent évaluer les risques propres à leurs environnements. Elles doivent avoir une vue d'ensemble et des informations nuancées sur leurs propres risques. Les responsables de services transverses peuvent apporter leur point de vue. Les professionnels de la cybersécurité peuvent constater que les autres départements ont des points de vue différents et valables sur le risque. Une fois que l'entreprise a une connaissance approfondie des risques dans l'ensemble de son écosystème, les professionnels de la sécurité peuvent tracer la voie à suivre pour mettre en œuvre un système de sécurité plus solide.

Comblez les lacunes

Les entreprises ont besoin de professionnels qualifiés pour défendre leur infrastructure contre les cyberattaques. Plus la complexité du réseau augmente, plus il devient nécessaire de pouvoir s'appuyer sur un personnel de support compétent. La plupart des entreprises découvrent qu'elles ont besoin de personnes hautement qualifiées pour protéger efficacement leurs équipements, logiciels et réseaux contre les cybercriminels. Il est impératif pour les entreprises d'attirer les meilleurs talents, mais nombre d'entre elles peuvent être

confrontées à des problèmes de recrutement. Embaucher et retenir des professionnels de la cybersécurité se révèle être une tâche ardue. SonicWall dispose d'un vaste réseau de partenaires auxquels les entreprises de toute taille peuvent faire appel pour atteindre leurs buts et objectifs en matière de sécurité.

Choisissez la bonne technologie

Les mécanismes de sécurité ont progressé, renforçant ainsi la capacité des équipes de gestion informatique à sauvegarder leurs ressources et à assurer la sécurité des réseaux. Une bonne stratégie comprend une protection multicouche et une couverture sans faille de toutes les surfaces d'attaque.

Les auteurs de menaces tentent de cibler votre entreprise en se servant de l'empreinte croissante des applications, dispositifs, réseaux et infrastructures. Ils utilisent toutes sortes de techniques, du phishing aux variantes inédites de malwares, en passant par les ransomwares, les attaques par canal auxiliaire, les attaques de malwares IoT et bien d'autres encore, toutes particulièrement difficiles à détecter.

SonicWall vous aide à éliminer les angles morts et à sécuriser un personnel « sans limites » dans tous les environnements. Vous pouvez tout voir, partout, et agir rapidement sur les événements qui comptent.

Notre Capture Security Center élimine la visibilité en silo. Grâce à un point de contrôle unifié à écran unique, vous pouvez voir chaque surface d'attaque sur plusieurs générations d'infrastructures informatiques (sur site, cloud, terminaux et NaaS).

Une connaissance des menaces en temps réel 24 heures sur 24 révèle les vulnérabilités du paysage au fur et à mesure qu'elles apparaissent et indique toujours ce qu'elles sont et ce qu'elles tentent de violer. Des compteurs de risques personnalisés permettent de minimiser encore l'exposition et de prioriser les actions en fonction du profil de risque, tandis que les analyses et les rapports exploitables accélèrent les temps de réponse et aident à définir votre stratégie.

La technologie brevetée Real-Time Deep Memory Inspection™ (RTDMI) de SonicWall bloque les menaces zero-day et inconnues au niveau de la passerelle, même celles qui se cachent derrière un chiffrement ou n'affichent pas de comportement malveillant. Elle est conçue pour comprendre comment les auteurs de menaces opèrent. Les menaces zero-day n'auront une signature d'attaque qu'après leur première utilisation, ce qui rend les entreprises vulnérables. La technologie RTDMI détecte ces menaces et offre un niveau de visibilité qui vous permet de constater ces changements dans le comportement des attaquants.

Demandez plus

Les entreprises ont besoin de savoir que leurs fournisseurs prennent des mesures de sécurité appropriées lorsqu'ils développent leurs produits. Idéalement, les fournisseurs devraient avoir mis en place des systèmes comme l'analyse de la composition des logiciels et des tests statiques de sécurité des applications. Il est essentiel d'avoir une visibilité sur le pipeline de développement pour comprendre votre exposition au risque de vulnérabilités multiples. Les auteurs de menaces savent que le périmètre sera l'endroit le plus difficile à atteindre au sein de l'entreprise. Ils recherchent les vulnérabilités dans toute l'entreprise, et cela inclut les logiciels et le matériel tiers. Les entreprises peuvent créer des questionnaires à l'intention des fournisseurs qui évaluent les normes que ceux-ci doivent respecter pour être pris en considération. Ces questionnaires permettent d'obtenir des données suffisantes pour décider quel fournisseur convient le mieux à votre entreprise. Le fait d'exiger des fournisseurs plus performants peut aider les entreprises à renforcer leur système global de cybersécurité.



Conclusion

Les auteurs de menaces modifient constamment leurs plans d'attaque pour infiltrer les entreprises et causer le plus de dégâts possible. Dans un monde où les cybercriminels changent en permanence leurs attaques pour prendre les entreprises au dépourvu, ces mêmes entreprises peuvent mettre en œuvre des stratégies qui leur donneront une longueur d'avance.

- Mettez en œuvre une authentification multifacteurs pour compliquer l'infiltration de vos réseaux par les auteurs de menaces.
- Développez de meilleures stratégies d'évaluation des risques pour garantir la protection de tous les points d'entrée potentiels de votre entreprise.
- Embauchez et formez du personnel hautement qualifié pour optimiser et entretenir tous vos systèmes de sécurité.
- Choisissez la meilleure technologie pour vos réseaux, terminaux et points d'accès afin de protéger les données et les utilisateurs.
- Adoptez des exigences strictes envers vos fournisseurs afin de vous assurer que votre entreprise n'importe pas des vulnérabilités provenant de matériels et de logiciels tiers.

En définitive, il incombe à chaque entreprise de déterminer les stratégies de cybersécurité qui lui conviennent le mieux. Pour en savoir plus sur la manière d'élaborer, de faire évoluer et de gérer la sécurité dans les environnements cloud, hybrides et traditionnels, contactez dès aujourd'hui un expert en sécurité SonicWall.



À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution, dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com

© 2023 SonicWall Inc. TOUS DROITS RÉSERVÉS.
SonicWall est une marque commerciale ou déposée de SonicWall Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales et déposées sont la propriété de leurs sociétés respectives. Les informations contenues dans ce document sont fournies en relation avec les produits de SonicWall et/ou ses filiales. Aucune licence, expresse ou implicite, par estoppel ou un autre moyen, quant à un quelconque droit de propriété intellectuelle n'est accordée par le présent document ou en lien avec la vente de produits SonicWall. Sauf disposition contraire dans les conditions du contrat de licence, la société SonicWall et/ou ses filiales déclinent toute responsabilité quelle qu'elle soit et rejettent toute garantie expresse, implicite ou statutaire concernant leurs produits, y compris et sans s'y limiter, les garanties implicites de qualité marchande, d'adéquation à un usage particulier ou de non-contrefaçon. En aucun cas, SonicWall et/ou ses filiales ne seront responsables des dommages directs, indirects, consécutifs, punitifs, spéciaux ou fortuits (y compris, sans limitation, les dommages pour perte de profits, interruption de l'activité ou perte d'informations) provenant de l'utilisation ou l'impossibilité d'utiliser ce document, même si SonicWall et/ou ses filiales ont été informés de l'éventualité de tels dommages. SonicWall et/ou ses filiales ne font aucune déclaration ou ne donnent aucune garantie en ce qui concerne l'exactitude ou l'exhaustivité du contenu de ce document et se réservent le droit d'effectuer des changements quant aux spécifications et descriptions des produits à tout moment sans préavis. SonicWall Inc. et/ou ses filiales ne s'engagent en aucune mesure à mettre à jour les informations contenues dans le présent document.

ExecBrief-EvolvedThreats_EvolvedStrategies-A4-JK-7925