Fortinet présente sa nouvelle solution de contrôle d'accès au réseau dédié à la sécurité de l'IoT

FortiNAC offre visibilité et contrôle sur les objets connectés, une réponse automatisée aux menaces, ainsi qu'un contrôle d'accès à grande échelle au sein des environnements hétérogènes.

« La transformation digitale s'accompagne d'une prolifération d'objets connectés peu ou pas sécurisés qui accèdent au réseau, alimentant ainsi le risque d'un incident de sécurité. FortiNAC permet aux entreprises d'identifier tous les dispositifs présents sur le réseau, et de mettre en œuvre une segmentation qui encadre les accès de ces dispositifs. Cette fonctionnalité est proposée par une solution adaptée aux environnements hétérogènes et sans limite en nombre d'équipements. FortiNAC vient au renfort de la Security Fabric de Fortinet pour sécuriser l'Internet des objets, instituant ainsi une cybersécurité élargie, intégrée et automatisée sur l'ensemble de la surface d'attaque. Dans l'univers de l'IoT, FortiNAC offre une visibilité sur les équipements présents sur le réseau, ainsi que les moyens de les protéger »

John Maddison, SVP of products and solutions at Fortinet

L'essentiel

Fortinet® (NASDAQ: FTNT), leader mondial des solutions de cybersécurité automatisées, intégrales et intégrées, annonce la disponibilité de FortiNAC, une nouvelle gamme de plateformes de contrôle d'accès, avec segmentation du réseau et sécurité automatisée des objets connectés.

- Les objets connectés vulnérables et sans interface de gestion, qui prolifèrent dans les domaines de l'industriel et du médical notamment, exigent de nouveaux outils de sécurité.
- La nouvelle gamme de produits offre un contrôle d'accès réseau pour les environnements IoT, ainsi que des fonctions renforcées de visibilité, de contrôle et de réponse automatisée.
- FortiNAC offre un profilage détaillé de chaque équipement sur le réseau, ainsi qu'une segmentation précise et une réponse automatisée aux changements de statut ou de comportement des équipements. Ainsi, chaque dispositif ne peut accéder qu'aux ressources réseau qui lui sont autorisées.

Les objets connectés non sécurisés sont source de vulnérabilités

L'utilisation d'objets connectés progresse sensiblement, corollaire de la transformation numérique qu'opèrent les entreprises pour gagner en productivité. Selon Gartner, l'Internet des Objets devrait progresser à un taux annuel moyen de 32% entre 2016 et 2021, pour atteindre le chiffre de 25,1 milliards.[1] Le volume important d'équipements (IoT, corporate et BYOD) souhaitant se connecter en filaire ou sans fil au réseau étend la surface d'attaque et augmente les coûts de provisioning, de gestion et de mise en conformité. La connexion et la sécurité des accès imposent un réel défi aux entreprises : les professionnels de la sécurité doivent protéger chaque dispositif en permanence, tandis que les cybercriminels savent qu'ils peuvent commettre leurs exactions en tirant parti d'un seul port ouvert, d'un équipement piraté ou inconnu, ou encore d'un malware furtif.

FortiNAC sécurise les réseaux accueillant les dispositifs non-sécurisés

FortiNAC maîtrise les risques de sécurité liés aux dispositifs non-sécurisés qui accèdent au réseau, offrant ainsi une visibilité totale sur les appareils d'extémité, les utilisateurs, ainsi que les équipements et applications, qu'ils soient de confiance ou inconnus. Une fois cette visibilité établie, FortiNAC active un contrôle en temps réel et s'assure que tous les dispositifs filaires ou sans fil sont authentifiés, légitimes, et conformes aux règles contextuelles définissant les modalités de connexion (quels équipements, quels utilisateurs, plages horaires de connexion et périmètre de connexion). De plus, FortiNAC permet d'appliquer les règles corporate en matière de patching des dispositifs et de version du firmware. FortiNAC propose également des outils d'orchestration du réseau pour une prise en charge automatisée des

menaces identifiées. Celles-ci peuvent être confinées en quelques secondes, soit bien plus rapidement qu'avec un processus manuel chronophage.

Les réseaux fonctionnent en temps réel, avec des équipements qui s'y connectent ou s'en déconnectent. L'intégrité de ces réseaux implique de gérer l'accès de chaque dispositif qui souhaite se connecter. Une telle approche implique d'interdire l'accès aux équipements inconnus de l'infrastructure corporate, de segmenter automatiquement les équipements sur la base de règles et de rôles, et de confiner immédiatement tout équipement transgressant les règles en vigueur. De plus, la solution de contrôle d'accès réseau FortiNAC se veut économique et particulièrement évolutive, ce qui étend la visibilité et la protection à un nombre illimité de dispositifs et élimine le besoin de déployer un outil de contrôle sur chacun des sites d'une entreprise multisite.

Des solutions de contrôle d'accès et de sécurité de l'IoT qui renforcent la Security Fabric

Avec cette nouvelle annonce, Fortinet renforce sa Security Fabric qui se rend compatible à des équipements réseau tiers (pare-feux, commutateurs, points d'accès et endpoints) non certifiés dans le cadre du programme partenaire Fabric-Ready. FortiNAC est parfaitement intégré avec les pare-feux Next-Generation FortiGate, FortiSwitch, le contrôleur sans fil FortiWLC, FortiSIEM et les FortiAP, dans l'optique de minimiser les risques associés aux cyber-menaces et d'offrir davantage de visibilité et de sécurité aux environnements complexes.

Verbatims du marché

« Il est tout simplement impossible de surveiller et de protéger des équipements qui vous sont inconnus. FortiNAC nous donne une perspective claire de notre réseau, pour identifier rapidement les ressources et fermer les ports d'accès de manière individuelle lorsque nécessaire. Cette visibilité granulaire prévient les pertes de données et favorise la conformité réglementaire. FortiNAC, c'est un peu comme de disposer de verrous sur les portes et fenêtres de sa maison. Sans cette protection, votre maison devient vulnérable. Aujourd'hui, nous n'avons plus à subir les infections en interne liées à des malwares, puisque nous pouvons déconnecter les ports utilisés pour propager l'infection. Aujourd'hui, seuls les dispositifs légitimes peuvent se connecter à notre réseau et nous pouvons identifier et contrôler l'ensemble de nos ports »

Rob Fountaine, manager of information security, Atrius Health

« Le marché du contrôle d'accès au réseau connaît une croissance à deux chiffres, tirée par ce besoin de disposer d'une visibilité sur le réseau et par des préoccupations vis-à-vis de la sécurité aléatoire des objets connectés. FortiNAC est un atout majeur de la Security Fabric de Fortinet. La solution déploie une solution efficace face aux risques de sécurité liés à l'IoT et est adaptée aux environnements hétérogènes. La détection des menaces et l'application des règles de sécurité gagnent en efficacité, tandis que l'évolutivité est au rendez-vous pour assurer un déploiement économique »

Zeus Kerravala, ZK Research

Ressources complémentaires

- Consultez notre blog pour en savoir davantage sur cette annonce.
- Plus d'informations sur les contrôleurs d'accès réseau FortiNAC.
- Abonnez-vous aux FortiGuard Threat Intelligence Briefs hebdomadaires.
- En savoir davantage sur les programmes Network Security Expert, Network Security Academy et FortiVets.
- Découvrez ce qu'est la Security Fabric de Fortinet et la troisième génération de la sécurité réseau.
- Suivez-nous sur Twitter, LinkedIn, Facebook, YouTube, and Instagram.

[1] Gartner," Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017," Peter Middleton, Tracy Tsai, Masatsune Yamaji, Anurag Gupta, Denise Rueb, 21 décembre 2017.

Gartner ne cautionne aucun fournisseur, produit ou service mentionné dans ses études, ni ne recommande aux utilisateurs technologiques de ne choisir que parmi les solutions des fournisseurs les mieux classés ou distingués de

quelque autre forme que ce soit. Les rapports d'étude de Gartner reflètent les avis des équipes d'analystes de Gartner et ne doivent en aucun cas être considérés comme des déclarations de fait. Gartner exclut toute garantie, expresse ou tacite, concernant ces études, y compris toute garantie de commerciabilité et d'adéquation à un usage particulier.

À propos de Fortinet

Fortinet assure la sécurité des entreprises, fournisseurs de services et administrations parmi les plus grandes au monde. Fortinet apporte à ses clients une protection intelligente et transparente, véritable ligne de défense d'une surface d'attaque qui s'étend. Cette sécurité affiche des performances pérennes, adaptées à des réseaux décloisonnés. Seule l'architecture Security Fabric de Fortinet est capable de déployer une sécurité sans compromis pour relever les défis de sécurité les plus critiques au sein des environnements réseaux, applicatifs, cloud ou mobiles. Plus de 360 000 clients dans le monde font aujourd'hui confiance à Fortinet pour les protéger.
Pour en savoir davantage : http://www.fortinet.com, http://www.fortinet.fr, le blog Fortinet ou FortiGuard Labs.

FTNT-O