PRÉSENTATION DE LA SOLUTION AKAMAI

Deloitte renforce ses offres de réponse aux incidents et d'atténuation des ransomwares en tirant parti d'Akamai Guardicore Segmentation

Défis des clients

Les catégories de produits de sécurité solidement établies promettent des niveaux de protection croissants contre les dernières menaces pesant sur les réseaux d'entreprise. Cependant, peu de solutions sont en mesure d'offrir une méthode complète et unique de réduction de la surface d'attaque en protégeant contre les mouvements latéraux malveillants, que ces mouvements se produisent vers ou depuis du matériel sur site, des charges de travail hébergées dans le cloud, des terminaux des utilisateurs finaux ou des conteneurs. En outre, la mise en place des initiatives initiales de segmentation Zero Trust a toujours pris des mois, voire des années, pour les clients de type grande entreprise, en raison des contraintes technologiques et de l'expertise humaine limitée pour exécuter des projets visant à stopper les attaques si elles contournent les produits de sécurité établis tels que les pare-feux existants, les EDR, etc.

Lorsqu'ils abordent des projets de segmentation, les clients de type grande entreprise sont généralement confrontés aux défis suivants :

- manque de visibilité sur tous les actifs, flux réseau, utilisateurs et connexions dans tous les environnements ;
- contrôles de sécurité limités sur des technologies et des infrastructures disparates, telles que l'infrastructure de cloud hybride, les systèmes d'exploitation anciens et OT/IoT ;
- nécessité d'assurer la continuité de l'activité en évitant les temps d'arrêt qui vont souvent de pair avec les techniques de segmentation traditionnelles ;
- manque de ressources de sécurité et de talents pour créer, déployer et gérer des initiatives qui prennent en charge le Zero Trust.

Points forts de la solution

Akamai Guardicore Segmentation est une solution de microsegmentation basée sur l'hôte, conçue pour vous aider à appliquer les principes Zero Trust dans le réseau de la manière la plus simple, la plus rapide et la plus intuitive qu'il soit. En alliant des capteurs basés sur des agents, des collecteurs de données basés sur le réseau et des journaux de flux de cloud privé virtuel pour mapper votre réseau, la solution Akamai Guardicore Segmentation vous offre une vue unique de toutes vos ressources et de votre infrastructure (systèmes d'exploitation anciens et actuels, technologie opérationnelle et terminaux IoT inclus). Elle a donc été conçue pour la création et la mise en application de règles destinées à limiter les communications indésirables, en réduisant votre surface d'attaque et en assurant la continuité des activités.

Principaux cas d'utilisation

- **Contrôles du trafic est-ouest**
  Environnements, applications, utilisateurs et infrastructures distincts qui n'ont pas besoin de communiquer
- **Atténuation des ransomwares**
  Déploiement de modèles de règles avec AI/ML afin de bloquer les chemins d'attaque connus pour être utilisés lors de différents types d'attaques par ransomware
- **Cloisonnement des applications**
  Concentration sur les dépendances spécifiques de vos applications stratégiques pour créer des contrôles de sécurité stricts

- **Segmentation basée sur l'utilisateur**
  Blocage de l'accès des utilisateurs aux applications, environnements et terminaux qui ne sont pas essentiels à leur travail
- **Isolation des terminaux infectés**
  Limitation de la propagation d'une violation si un ou plusieurs terminaux sont compromis
- **Conformité**
  Soyez prêt à prouver votre conformité à tout moment grâce à une compréhension contextuelle approfondie de votre réseau, de vos terminaux et des chemins d'attaque potentiels

Avantages pour les clients

- Résolution des problèmes de visibilité grâce à une visibilité unique sur l'ensemble de votre réseau et de vos connexions, y compris les serveurs, les terminaux, les clouds, les conteneurs, les utilisateurs et bien plus encore
- Application des politiques Zero Trust pour limiter la possibilité d'attaques réussies de ransomwares
- Réduction du temps de réponse aux incidents grâce à des informations sur les menaces et à des fonctionnalités complètes de détection des violations et de pare-feu
- Simplification de l'analyse des réseaux et des projets de conformité à l'aide de fonctionnalités historiques et en temps réel

Expertise de Deloitte

1. **Conseil**
   L'expérience de Deloitte en matière d'aide à la décision relative à la cybersécurité, d'analyse des lacunes en matière de sécurité et de création de feuilles de route de mise en œuvre des procédures permet aux clients de type grande entreprise de prendre des décisions éclairées en cas de violations de données et lors de la planification de leur avenir
2. **Services professionnels**
   Découvrez des services de mise en œuvre des procédures entièrement gérés ainsi que des intégrations personnalisées dans vos solutions de sécurité, ITSM et cloud existantes
3. **Services gérés de réponse aux incidents**
   En cas d'incident, recevez une assistance instantanée de pointe par les experts en tactique d'intervention de Deloitte pour contenir la violation et prévenir de futurs incidents
4. **Abonnements de licence**
   Deloitte propose à l'achat une large gamme d'abonnements de licence

Étude de cas client - Comment Akamai et Deloitte résolvent les problèmes des clients liés aux ransomwares

Certaines attaques majeures par ransomware ont poussé les clients à rechercher des conseils et des solutions pouvant les aider immédiatement à un moment critique. Les capacités combinées des équipes de sécurité et de réponse aux incidents de Deloitte, qui exploitent la visibilité du réseau, l'analyse des violations et les mesures ultérieures de réduction significative de la surface d'attaque fournies par Akamai Guardicore Segmentation, se sont avérées être la combinaison gagnante pour les clients.

Contexte

Une grande entreprise était confrontée à une attaque importante de ransomware ayant mis hors service ses activités principales, et elle ne savait pas comment y remédier. L'intégralité de son centre de données, composé de milliers de serveurs, avait été détournée, et la violation devait être contenue immédiatement et en toute sécurité. Se fiant aux conseils de Deloitte, le client a appelé pour s'enquérir de la procédure à suivre. L'équipe de Deloitte étant déjà prête à proposer et à déployer Akamai Guardicore Segmentation, le client a pu avoir rapidement une visibilité sur l'ampleur de l'attaque, comprendre quels actifs et applications avaient été touchés et voir quelles étaient les dépendances des applications concernées.

Solution

En cartographiant l'ensemble de l'environnement du client jusqu'au niveau des processus, la solution Akamai Guardicore Segmentation a permis de révéler toutes les routes pouvant être empruntées par le logiciel malveillant à partir de l'infrastructure compromise. L'équipe de Deloitte a ainsi pu se concentrer sur des parties spécifiques du réseau pour effectuer une analyse supplémentaire. Après le rétablissement par le client de ses activités et de l'accès à son centre de données, il ne restait plus aucun terminal compromis.

Résultat

Une fois que l'attaque par ransomware a été résolue, que le centre de données a été remis en service et que les opérations commerciales ont repris, des mesures ont été prises pour réduire le risque qu'une telle attaque se reproduise. Comme de nombreux clients de type grande entreprise, ce client utilisait une approche de sécurité multidimensionnelle intégrant plusieurs solutions de pointe pour protéger les terminaux, les applications, les utilisateurs, etc. Cependant, comme un simple e-mail d'hameçonnage peut constituer la porte d'entrée d'un attaquant, ces solutions n'ont pas suffi à intercepter l'attaque. Grâce à une visibilité totale sur le réseau, aux dépendances des applications et aux utilisateurs ayant accès au centre de données, le client a pu mettre en œuvre des contrôles de microsegmentation précis afin de réduire considérablement les routes pouvant être empruntées lors d'une future attaque par ransomware.

Le client ayant pu expérimenter la valeur de la solution, et sa confiance en l'expertise de Deloitte ayant été renforcée, il a décidé de conserver la solution pour continuer à fournir une segmentation Zero Trust et a demandé à Deloitte d'assurer la gestion de la technologie au quotidien.

En résumé

L'expertise technique approfondie et l'expérience de Deloitte dans l'exécution de projets Zero Trust pour le compte de ses clients en font un partenaire idéal pour le déploiement et la gestion d'Akamai Guardicore Segmentation. Les clients peuvent compter sur Deloitte pour recourir à cette technologie dans le cadre de toute initiative de sécurité incluant la réduction de la surface d'attaque, le contrôle des mouvements latéraux, le cloisonnement des applications ou l'atténuation des ransomwares.

À propos de Deloitte

Deloitte fournit des services d'audit, de conseil et de fiscalité de pointe à bon nombre des marques les plus admirées au monde, dont près de 90 % des entreprises du classement Fortune 500® et plus de 7 000 sociétés privées. Nos collaborateurs s'associent dans l'intérêt général et travaillent dans les secteurs qui animent et façonnent le marché d'aujourd'hui. Ils produisent des résultats mesurables et durables qui permettent de renforcer la confiance du public dans nos marchés de capitaux, qui incitent les clients à considérer les défis comme des occasions de se transformer et de prospérer, et qui ouvrent la voie à une économie plus forte et à une société en meilleure santé. Deloitte est fière de faire partie du plus grand réseau mondial de services professionnels à destination de ses clients sur les marchés les plus importants pour eux. Fort de plus de 175 ans de service, notre réseau d'entreprises membres couvre plus de 150 pays et territoires. Visitez le site deloitte.com pour découvrir comment les quelque 415 000 collaborateurs de Deloitte s'associent dans le monde entier pour faire la différence.

Contact

Ola Sergatchov
Head of Global Strategic Alliances, Akamai
osergatc@akamai.com