TÉMOIGNAGE CLIENT AKAMAI

# Une entreprise de résolution des violations tire parti d'Akamai et de son modèle de règles de récupération et de réponse aux ransomwares

Visibilité complète du réseau

Segmentation des infrastructures informatiques

Réponse aux menaces de ransomware

## Le client

Une société de services de résolution des violations basée aux États-Unis a été engagée par un fabricant mondial d'équipements après un incident de sécurité majeur.

## L'enjeu

### Ransomware à propagation rapide

Après avoir réussi à propager une attaque malveillante qui a eu un impact sur les opérations commerciales, le fabricant mondial a commencé à travailler avec la société de services de résolution des violations pour restaurer et améliorer la sécurité de son environnement. L'attaque, lancée à partir de l'ordinateur portable d'un employé, s'était rapidement propagée et avait touché la plupart des sites d'exploitation, en plus d'avoir pénétré les serveurs de sauvegarde de l'organisation.

## Choix d'une solution

Les méthodes initiales de confinement, telles que l'application de règles de restriction d'accès à Internet à travers les pare-feu, ont mis du temps à contenir la violation qui s'est rapidement aggravée. La complexité de l'environnement et la réalité de la mise en réseau dans une entreprise distribuée ont ralenti la mise en œuvre et l'application des règles de restriction avec pare-feu, ce qui a rendu ce processus inefficace.

En outre, la visibilité des machines héritées constituait un problème important pour les intervenants chargés d'enquêter sur la violation et de la contenir. Constatant l'urgence et la nécessité d'accélérer la segmentation avant que la dispersion latérale n'affecte encore plus d'actifs, le fournisseur de services de résolution des violations a recommandé Akamai Guardicore Segmentation.

Breach Remediation Company

**Secteur**
Technologie de l'information

**Solution**
Akamai Guardicore Segmentation

**Impacts majeurs**

- Empêche les ransomwares de se propager via des mouvements latéraux
- Offre une visibilité granulaire des flux réseau
- Sécurise les machines récentes et héritées
- Assure une réponse rapide aux incidents

Akamai

## Avantages d'Akamai Guardicore Segmentation

### Visibilité instantanée

En l'espace de trois heures, les services de résolution des violations ont rapidement déployé des agents Akamai sur plus de 3 000 serveurs de l'entreprise. Et quelques minutes après le déploiement, une visibilité granulaire des flux de communication et de réseau a commencé à émerger, donnant à l'équipe de réponse aux incidents le contexte et les données précises dont elle avait besoin pour enquêter sur la violation et valider le confinement.

### Mise en œuvre rapide des règles

Peu de temps après avoir obtenu cette visibilité indispensable, les équipes ont pris des mesures pour isoler les actifs critiques de l'environnement global. Deux applications de production cruciales, responsables de la seule chaîne de fabrication en activité, ont été rapidement identifiées et sécurisées. Grâce à Akamai Guardicore Segmentation, des règles ont été immédiatement introduites pour restreindre les connexions entre les sous-réseaux et les parties du centre de données infectés et les applications, une tâche qui aurait pris des semaines avec les pare-feu hérités.

Une simple requête a également révélé que les machines héritées connectées à Internet, contournant les pare-feu hérités, tentaient de restreindre le confinement. Après avoir découvert une communication non conforme, l'équipe a créé des règles qui restreignaient efficacement l'accès à Internet pour tous les serveurs, y compris les machines héritées, en quelques minutes.

### Prévention des mouvements latéraux pendant la récupération

Au cours de la partie suivante du processus de récupération, l'équipe a recréé les clusters d'applications du fabricant, en intégrant des agents Akamai. Elle a configuré une règle initiale qui bloquait toutes les connexions entrantes, et a utilisé Akamai Guardicore Segmentation pour identifier les dépendances. Ensuite, les communications ont été autorisées selon les besoins, seulement après validation des exigences et compréhension du contexte. Cette approche a permis à l'équipe de récupérer et de remettre en ligne les applications impactées par l'attaque par ransomware sans risque de réinfection.

### Protection future

Akamai Guardicore Segmentation a permis à l'entreprise de résolution des violations de démontrer une vraie valeur ajoutée pour son client, le fabricant, tout en l'aidant à se remettre de l'attaque par ransomware. Cela a donné la possibilité à cette entreprise d'augmenter ses revenus, d'étendre sa présence et de mieux aider ses clients à atteindre leurs objectifs en matière d'informatique et de sécurité.

La segmentation du centre de données interne introduite lors de la récupération progressive a considérablement réduit la surface d'attaque. Aujourd'hui, la posture de sécurité de l'organisation s'est améliorée et l'impact de toute violation future a été considérablement réduit.

Pour plus d'informations, consultez le site akamai.com/guardicore.

> En quatre heures, [Akamai] nous a permis d'une part d'empêcher l'attaque de se propager, et d'autre part de restaurer les lignes de production en baisse dans un segment de réseau « stérile » sans modifier aucun réseau sous-jacent. Tout cela en parallèle de l'enquête de réponse aux incidents et du confinement.
>
> RSSI de l'entreprise de résolution des violations