LIVRE BLANC

Transformer la conformité en avantage concurrentiel grâce à la sécurité d'Akamai

Une approche à quatre piliers pour renforcer la sécurité et se préparer aux audits

Concentrez-vous sur quatre piliers de la sécurité pour ouvrir la voie à la conformité

Aujourd'hui, les entreprises du monde entier sont confrontées à un dédale de réglementations de plus en plus complexe, du RGPD et de l'HIPAA à la norme PCI DSS et à un nombre croissant d'obligations régionales. Mais démontrer son niveau de préparation à la conformité ne se résume pas à satisfaire les organismes de réglementation : il est devenu essentiel de maintenir la confiance avec les clients et les parties prenantes internes, comme les cadres supérieurs et le conseil d'administration.

En effet, en cas de non conformité, les conséquences dépassent nettement les simples pénalités réglementaires. Les coûts liés à la non-conformité comprennent les interruptions d'activité au cours des étapes d'enquête et de résolution, les atteintes à la réputation et l'augmentation de l'exposition juridique. Si une entreprise entre en conflit avec les exigences de conformité, cela peut conduire à une perte de revenus due à la perte de clients, ainsi qu'à des coûts opérationnels élevés, car les ressources sont consacrées à la résolution des problèmes plutôt qu'à l'innovation. En 2024, selon Forrester, les 35 plus grandes violations dans le monde ont entraîné des sanctions s'élevant à 3 milliards de dollars, et 23 d'entre elles étaient liées au Règlement général sur la protection des données (RGPD) de l'Union européenne

Par le passé, les équipes de sécurité ne s'intéressaient généralement à la conformité que pour faire face à l'émergence des réglementations. Mais aujourd'hui, face à l'évolution rapide de la technologie et à des attaques de plus en plus importantes et puissantes, la conformité est un élément à prendre en compte lorsqu'elles évaluent les outils et les modèles de maturité. Les équipes doivent se poser les questions suivantes : « Comment mes choix actuels en matière de sécurité vont-ils m'aider à répondre aux exigences de conformité, aujourd'hui et à l'avenir ? »

Chez Akamai, nous aidons les clients à répondre à cette question en axant la conversation sur les quatre piliers des meilleures pratiques en matière de sécurité, qui contribuent également à améliorer les domaines clés de la préparation à la conformité. Ces piliers sont les suivants :

- Acquérir une visibilité sur l'ensemble du parc informatique
- Bloquer les mouvements latéraux (à travers les réseaux, les applications et les API)
- Empêcher les accès non autorisés
- Protéger les données sensibles des clients et les informations sur les comptes

Le résultat donne un avantage concurrentiel évident. En plus d'être davantage sécurisées, les entreprises sont également mieux préparées à surmonter les obstacles réglementaires. En étant plus sécurisés et conformes, elles sont également plus à même de gagner la confiance des clients et de leur direction.

Pilier 1

Acquérir une visibilité sur l'ensemble du parc informatique

Pour bien se préparer à la conformité, il faut d'abord avoir une visibilité complète sur l'ensemble des ressources digitales. Les entreprises ne peuvent pas protéger ce qu'elles ne peuvent pas voir, et les organismes de réglementation exigent de plus en plus de preuves d'inventaire complet des ressources, de surveillance continue et de sensibilisation aux menaces.

Ce n'est pas si facile. Une étude menée récemment par Forrester révèle que plus de la moitié (52 %) des sociétés financières sont d'accord ou tout à fait d'accord pour reconnaître qu'elles n'ont pas une visibilité suffisante sur leur parc informatique. Malheureusement, la non-conformité implique des enjeux élevés, quel que soit le secteur d'activité. Entre 2023 et 2024, le nombre d'entreprises ayant payé des amendes réglementaires de plus de 100 000 USD a bondi de près de 20 %.

Pour de nombreuses entreprises, le défi de la visibilité réside dans la surveillance du trafic réseau et des API. Voici quelques réglementations et normes qui exigent une vision claire des risques :

- La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) contient des conseils pour s'assurer que les logiciels d'une entreprise utilisent en toute sécurité les fonctions de composants externes, tels que les API qui transmettent les données de paiement d'une application mobile au système d'une banque.
- Des normes telles que la norme ISO/CEI 27001 de l'Organisation internationale de normalisation (ISO) exigent la séparation des données et des installations de traitement des données pour le cas où un attaquant pénètre dans le réseau.
- La loi sur la sécurité des données de la République populaire de Chine exige des mesures de sécurité strictes pour protéger l'accès aux informations personnelles des clients par le biais de technologies qui échangent des données sensibles entre différents systèmes informatiques.

De nombreuses entreprises disposent d'outils ou de processus capables de répondre à certaines de ces exigences. Cependant, à mesure qu'elles s'étendent dans des environnements informatiques hybrides et dans d'autres zones géographiques, la surveillance devient beaucoup plus difficile. C'est particulièrement vrai pour les API. Selon l'étude d'Akamai, seuls 27 % des professionnels de la sécurité ayant réalisé un inventaire complet de leurs API savent exactement quelles API renvoient des données sensibles, contre 40 % en 2023.

En fin de compte, les entreprises doivent savoir où se trouvent leurs données sensibles et ce qui y accède afin de savoir où concentrer leurs efforts en matière de sécurité. Cela nécessite une visibilité sur :

- les ressources qui communiquent avec le réseau (avec des vues historiques et en temps réel), y compris les processus de couche 7 et le trafic en bordure de l'Internet, dans les environnements cloud hybrides et sur site ;
- l'inventaire des API, y compris les API fantômes et zombies, et la manière dont elles s'intègrent aux sources de trafic et au code ;
- le JavaScript côté client, particulièrement important pour respecter les dernières exigences PCI DSS.

Le portefeuille d'Akamai peut aider les équipes de sécurité à obtenir la visibilité dont elles ont besoin.

Akamai Guardicore Segmentation permet d'identifier et de visualiser les ressources communiquant au sein du réseau dans l'ensemble du parc informatique, ainsi que les processus de couche 7, le hachage et les informations de ligne de commande. La solution offre également un historique pour prouver la non compromission des ressources pendant les audits de conformité. Des visualisations du trafic nord-sud et est-ouest indiquent également les accès.

API Security fournit un inventaire en temps réel des API dont les entreprises ont besoin pour la conformité et aide à identifier le lieu et le moment où des données non chiffrées peuvent circuler dans les API.

App & API Protector offre une visibilité au niveau des applications, notamment l'inventaire des API, la détection de l'exposition des données sensibles et l'analyse du trafic en temps réel.

Client-Side Protection and Compliance offre une visibilité sur les scripts côté client qu'exige la norme PCI DSS v4.

Un organisme de santé a mis en œuvre Akamai Guardicore Segmentation afin de répondre aux exigences de conformité HIPAA et SOC 2. La solution lui a fourni des informations précieuses sur les flux de trafic entre différentes applications. L'équipe de sécurité a pu inspecter des détails granulaires au-delà des journaux de couche 4 : identifiants utilisateur, entrées de ligne de commande et même corrélations de service.

Pilier 2

Empêcher les mouvements latéraux

À l'instar des équipes de sécurité elles-mêmes, de nombreux organismes de réglementation acceptent que même avec une stratégie de sécurité robuste, une violation peut avoir lieu. Ils veillent donc à s'assurer que les entreprises sont en mesure de limiter les dégâts lorsque cela se produit. Par exemple :

- L'article 32 du RGPD exige « la capacité à garantir la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et services de traitement » et « la capacité à restaurer la disponibilité et l'accès aux données à caractère personnel en temps opportun en cas d'incident physique ou technique ».
- De même, la norme PCI DSS v4 demande aux entreprises de « mettre en œuvre des pare-feux pour protéger les données des titulaires de carte de crédit et s'assurer que les pare-feux sont configurés de manière à restreindre les connexions entre les réseaux de confiance et non fiables.
- **L'Organisation internationale de normalisation/la Commission électrotechnique internationale (ISO/CEI) 27001** impose l'isolation des installations de traitement des informations et des données afin de protéger la confidentialité, l'intégrité et la disponibilité des informations.

Bien que la plupart des entreprises disposent d'un pare-feu, pour limiter les mouvements latéraux lorsqu'un acteur malveillant se trouve à l'intérieur du réseau, il faut un niveau de contrôle plus élevé. C'est pourquoi la microsegmentation, de préférence définie par logiciel, est un outil clé pour assurer la conformité. Akamai dispose des moyens adéquats pour répondre aux préoccupations des auditeurs relatives aux mouvements latéraux.

Akamai Guardicore Segmentation fournit les barrières nécessaires pour bloquer les mouvements latéraux et aider à maintenir la conformité. Les modèles de règles prêts à l'emploi facilitent la mise en place des initiatives liées à la conformité grâce à des contrôles granulaires de couche 7. Et comme il est défini par logiciel, il peut fournir le même niveau de protection granulaire, quel que soit l'emplacement des ressources. En outre, sa capacité à identifier les applications communiquant au sein du réseau et les tentatives de communication entre les zones segmentées renforce votre capacité à atténuer les menaces aux yeux des auditeurs.

Les attaquants trouvent de nouvelles opportunités de se déplacer latéralement grâce à la prolifération des API, notamment via les points de terminaison d'API vulnérables aux défaillances d'autorisation au niveau de l'objet (BOLA). Les acteurs malveillants peuvent manipuler les identifiants d'objet dans les requêtes API pour faciliter les mouvements latéraux dans le réseau. Une fois à l'intérieur, ils peuvent contourner l'autorisation, élever les privilèges et accéder aux données des clients.

Akamai API Security peut signaler les API qui exposent des données sensibles sans méthode d'authentification appropriée et identifier les API dont les contrôles d'accès sont faibles ou mal configurés, ce qui pourrait entraîner un accès non autorisé aux données et des mouvements latéraux. L'intégration d'API Security avec Akamai Web Application Firewall (WAF) permet également à la solution de bloquer les menaces en temps réel.

Cliente d'Akamai, une organisation internationale de services financiers, a mis en œuvre la sécurité des API parce qu'elle rencontrait des difficultés avec des API inconnues dans son environnement. Le déploiement a considérablement réduit la prolifération de ses API et amélioré la conformité, car Akamai API Security classifie les données sensibles afin de satisfaire aux réglementations telles que le RGPD, l'HIPAA, etc. Au cours des audits réglementaires, ces mises en œuvre sont la preuve directe que l'entreprise a pris les mesures techniques appropriées.

Les menaces actuelles liées à l'IA sont les obstacles réglementaires de demain

Aujourd'hui, tout examen des défenses d'une entreprise en matière de cybersécurité doit tenir compte du spectre de l'IA. La prolifération rapide des applications basées sur l'IA, des grands modèles linguistiques (LLMS) et des API génératives liées à l'IA a introduit de nouvelles vulnérabilités dont de nombreuses entreprises n'ont pas encore connaissance. Parmi ces applications, on peut citer les chatbots basés sur l'IA, les moteurs de recommandation de commerce de détail, les outils de diagnostic de santé et les moteurs de décision en matière de risques. Pendant ce temps, les acteurs des menaces tirent parti de l'IA pour lancer des attaques plus sophistiquées.

Et lorsque des menaces visant les opérations commerciales et le public apparaissent, des réglementations sont susceptibles d'être mises en place.

Les entreprises qui cherchent à protéger leurs investissements dans l'IA, leurs données et leurs clients font appel à Akamai pour obtenir de l'aide. En tant que fournisseur de sécurité ayant fait ses preuves en matière de conformité aux exigences actuelles de visibilité, de mouvement latéral et de contrôle des accès, Akamai investit de manière proactive afin de s'adapter aux exigences futures en matière d'IA. Akamai a développé des capacités d'IA avancées pour renforcer ses solutions de sécurité et a introduit une solution pour aider les entreprises à protéger leurs propres investissements en IA.

Akamai Firewall for AI assure une sécurité complète des applications basées sur l'IA en identifiant et en atténuant les menaces et les attaques spécifiques à l'IA, contrairement aux outils de sécurité traditionnels inadéquats. Firewall for AI inclut des protections spécifiques, telles que :

- **Une défense contre l'injection de prompt** : protège contre les attaquants qui manipulent les modèles d'IA à l'aide de saisies malveillantes.
- **La prévention des pertes de données (DLP)** : détecte et bloque les fuites de données sensibles dans les réponses générées par l'IA et protège contre la réception de données sensibles dans les requêtes.
- **Le filtrage du contenu toxique et nuisible** : signale les propos haineux, les informations erronées et les contenus offensants avant leur diffusion.
- **Une sécurité contre l'IA malveillante** : protège contre l'exécution de code à distance, les portes dérobées de modèles et les attaques par empoisonnement de données.
- **L'atténuation des attaques par déni de service** : atténue les attaques DoS basées sur l'IA en contrôlant l'utilisation excessive des requêtes et la surcharge des modèles.

En outre, Firewall for AI aide les entreprises à se conformer aux directives en matière de protection de la vie privée, de sûreté et de sécurité. En appliquant des politiques de sécurité spécifiques à l'IA, les entreprises peuvent atténuer les risques liés aux réglementations en matière de protection des données, à l'utilisation éthique de l'IA et aux obligations de gouvernance d'entreprise.

Pilier 3

Empêcher les accès non autorisés

Dans pratiquement tous les cadres réglementaires, le contrôle de l'accès aux systèmes et données sensibles constitue une pierre angulaire de la conformité. Les entreprises doivent comprendre leur stratégie de sécurité des applications et des API et empêcher les accès non autorisés et les abus. Cela exige une authentification appropriée des utilisateurs, l'autorisation de l'accès selon les besoins et la tenue à jour d'enregistrements détaillés de toutes les activités d'accès.

Pour bénéficier d'un contrôle d'accès complet répondant aux exigences réglementaires, les entreprises doivent relever trois défis clés. Le portefeuille de solutions de sécurité d'Akamai peut vous fournir des défenses approfondies qui répondent à chacun d'eux :

1. **Obtenir une compréhension complète de leur stratégie de sécurité des applications et des API**

Akamai App & API Protector permet aux entreprises d'appliquer des règles de trafic dans tous les environnements dans lesquels elles sont exécutées, tandis qu'Akamai API Security alerte les entreprises en cas d'activité inhabituelle, d'accès non autorisé aux données ou d'erreur de configuration, autant d'éléments clés pris en compte par les auditeurs. D'autre part, Akamai Guardicore Segmentation suit toutes les applications communiquant au sein du réseau et établit une base de référence de l'activité.

2. **Surveiller le comportement des utilisateurs et limiter l'accès aux informations sensibles**

Akamai Guardicore Segmentation limite l'accès au réseau en fonction de l'identité des utilisateurs, tandis qu'**App & API Protector** applique des règles de trafic avec une détection des menaces basée sur l'IA pour empêcher les violations. Enfin, **Client-Side Protection & Compliance** analyse le comportement d'exécution de JavaScript pour atténuer les attaques côté client.

3. **Détecter et limiter les activités frauduleuses**

API Security peut aider en détectant les comportements anormaux des API et les contrôles d'authentification mal configurés pour bloquer les attaques à haut risque.
Akamai Guardicore Segmentation protège le réseau en signalant et en bloquant les connexions suspectes pouvant indiquer une activité frauduleuse. App & API Protector détecte et atténue les menaces identifiées par l'OWASP afin de réduire davantage le risque de fraude.

NIS2 et sécurisation des accès

La directive mise à jour sur la sécurité des réseaux et des informations (NIS2) est conçue pour créer un niveau de cybersécurité commun dans les États membres de l'UE. Les récents ajouts à la NIS2 comprennent l'obligation pour les entreprises de mettre en place un système de gestion de la sécurité de l'information qui évalue les personnes, les règles et la technologie afin de protéger les données sensibles et de garantir la résilience opérationnelle. La NIS2 met également l'accent sur la sécurisation des chaînes d'approvisionnement informatiques et des relations avec les fournisseurs tiers.

Pilier 4

Protéger les données sensibles des clients et les informations sur les comptes

Le dernier pilier d'une approche de préparation réglementaire complète exige que les entreprises disposent de plans pour les données sensibles. La sécurisation des données des clients, des patients, des partenaires, etc. est un point essentiel dans la plupart des réglementations axées sur la sécurité.

Par exemple, la loi japonaise sur la protection des informations personnelles exige des évaluations de l'impact sur la protection des données qui peuvent identifier et atténuer les risques pour les technologies traitant de grands volumes de données personnelles ou impliquant des activités de traitement des données à haut risque.

Pour les institutions financières aux États-Unis, le FFIEC (Federal Financial Institutions Examination Council) exige des contrôles qui assurent que les API autorisent uniquement l'accès à des données spécifiques pour les utilisateurs autorisés via une sécurité multicouche (par exemple le suivi, la journalisation et la génération de rapports.

La résolution de ce pilier commence par la détection des menaces. La solution de protection des applications Web et des API d'Akamai, **App & API Protector**, assure la première couche de défense, tandis qu'**Akamai Guardicore Segmentation** surveille et segmente le trafic nord-sud et est-ouest. Le **portefeuille de solutions de protection contre les bots et les abus** d'Akamai ajoute une couche supplémentaire de sécurité contre les menaces automatisées et les attaques humaines.

Cependant, pour identifier correctement les menaces, les entreprises doivent également comprendre le comportement de base au sein de leur réseau. Voici comment les fonctionnalités de sécurité d'Akamai peuvent fournir ces informations essentielles :

- Akamai API Security et Akamai Guardicore Segmentation, respectivement, fournissent une compréhension de base des API et des applications qui communiquent au sein du réseau afin de signaler tout comportement inhabituel.
- Adaptive Security Engine, une des principales technologies d'App & API Protector, apprend les schémas d'attaque en s'appuyant sur les données locales et mondiales pour ajuster les protections en fonction du client, tout en s'adaptant aux futures menaces.
- Akamai Hunt, un service géré de recherche des menaces soutenu par l'équipe de recherche experte d'Akamai, offre aux entreprises une approche plus proactive de la défense.

DORA et sécurité des données

La loi sur la résilience opérationnelle numérique (DORA) vise à aider les entreprises de services financiers des États membres de l'Union européenne à résister aux cyberattaques et à s'en remettre. Avec DORA, le secteur dispose d'un cadre contraignant et complet de gestion des risques pour les technologies de l'information et de la communication (TIC). L'article 3 de la loi DORA exige des entreprises qu'elles utilisent des solutions et des processus TIC qui :

- réduisent au minimum les risques liés aux données, les accès non autorisés et les défauts techniques ;
- empêchent l'indisponibilité des données, la perte de données et les atteintes à l'intégrité et à la confidentialité ;
- assurent la sécurité du transfert des données.

Du silo de la conformité à un avantage concurrentiel

Les programmes de conformité efficaces doivent démontrer un impact commercial au-delà du simple fait de « cocher les cases » des exigences réglementaires. Les entreprises qui mettent en œuvre les solutions de sécurité axées sur la conformité d'Akamai ont signalé des améliorations mesurables dans trois domaines clés.

Réduction des coûts de conformité

Les entreprises ayant des programmes de conformité matures dépensent généralement moins dans les activités de conformité que celles ayant des approches ad hoc. L'automatisation de la collecte des preuves par le biais de plateformes de sécurité intégrées peut réduire considérablement le temps de préparation des audits, tout comme la consolidation de solutions ponctuelles sur une plateforme complète.

Amélioration de la stratégie de protection contre les risques

Au-delà de la réduction des coûts, les améliorations de la conformité doivent permettre une diminution mesurable des risques. Les entreprises qui mettent en œuvre les solutions de segmentation d'Akamai peuvent limiter les trajectoires vulnérables aux déplacements latéraux, en répondant directement aux exigences de conformité clés tout en réduisant les risques organisationnels.

Des fonctionnalités de suivi complètes améliorent la visibilité, ce qui se traduit par une réduction des risques en éliminant les zones d'ombre où les violations de conformité pourraient autrement passer inaperçues.

Efficacité opérationnelle

La troisième dimension de l'impact sur la conformité implique des améliorations de l'efficacité opérationnelle. Les contrôles pré-approuvés et les modèles de sécurité cohérents peuvent accélérer considérablement les approbations de sécurité pour les nouvelles applications. Cela améliore la satisfaction des développeurs en réduisant les frictions dans les processus de vérification de la sécurité et en accélérant le délai de mise sur le marché des nouvelles applications.

Ajustement de la conformité

À mesure que les exigences réglementaires continuent d'évoluer et que les entreprises se développent, elles ont besoin d'une approche de conformité qui s'adapte. Le portefeuille de solutions de sécurité intégrées d'Akamai constitue la base d'une stratégie de conformité capable d'anticiper les tendances réglementaires et de s'adapter à la croissance de l'entreprise.

- Les structures de règles configurables s'adaptent aux nouvelles exigences sans avoir à apporter de modifications significatives à l'infrastructure, tandis que les capacités extensibles de génération de rapports s'adaptent aux exigences de preuves émergentes à mesure que les réglementations évoluent.
- Le déploiement automatisé des règles pour les nouvelles ressources garantit que la couverture de conformité s'étend automatiquement à mesure que l'entreprise se développe.
- Les fonctionnalités de gestion centralisée offrent une visibilité complète quelle que soit l'échelle, tandis que la prise en charge complète des API permet l'automatisation des processus de conformité pour gérer la complexité croissante.

En outre, les entreprises doivent être proactives pour établir une cadence régulière de révision des réglementations et de mise à jour de leurs contrôles de conformité en conséquence. Akamai fournit régulièrement des mises à jour de ses solutions de sécurité, spécialement conçues pour répondre à l'évolution des exigences de conformité, afin de garantir aux clients une conformité continue, quelles que soient les modifications réglementaires.

Conclusion : La conformité en tant que facteur de différenciation concurrentiel

Une conformité efficace ne se limite plus à la satisfaction des exigences réglementaires : elle représente un impératif métier stratégique qui a un impact direct sur les performances organisationnelles, la confiance des clients et le positionnement concurrentiel. Quel que soit votre secteur d'activité ou votre région, une approche proactive de la conformité garantit une stratégie de sécurité solide et agile.

En adoptant une approche intégrée de la sécurité qui s'appuie sur les quatre piliers de la préparation à la conformité (visibilité sur l'ensemble du parc informatique, enrayement des mouvements latéraux, enrayement des accès non autorisés et protection des données clients et des informations sur les comptes sensibles), les entreprises peuvent établir une fondation durable pour la conformité, tout en bénéficiant d'une valeur commerciale mesurable au-delà de la satisfaction des réglementations.

Les entreprises qui réussissent le mieux sont celles qui sont parvenues à faire passer la conformité d'un coût nécessaire à la réalisation des activités commerciales à un avantage stratégique, qui permet la transformation digitale tout en protégeant ce qui compte le plus : la confiance des clients, l'intégrité des données et la réputation de l'entreprise.

Contactez-nous pour savoir comment Akamai peut aider votre entreprise.

Contactez-nous