Livre blanc

Conformité à la directive NIS2 à l'ère de l'IA

Les quatre principaux défis pour les entreprises, et comment la segmentation permet de tous les relever

Akamai Security

Table des matières

Synthèse 3

Confinement rapide des violations de sécurité 5

Atténuation des risques liés à la chaîne d'approvisionnement 7

Continuité opérationnelle et réduction des perturbations 8

Simplification des audits, de la conformité et de la génération de rapports 10

Les points clés en un coup d'œil 12

Synthèse

La directive NIS2 a élevé la cybersécurité au rang de priorité stratégique pour les conseils d'administration européens et instauré une responsabilité personnelle des dirigeants ainsi qu'un délai strict de 24 heures pour signaler les incidents. À l'heure où les attaques basées sur l'IA réduisent les délais d'exploitation des vulnérabilités de plusieurs jours à quelques minutes, les défenses périmétriques et les approches statiques de la conformité ne suffisent plus.

Nous vivons dans un monde hyperconnecté, où empêcher toutes les attaques est devenu irréaliste. Les entreprises ont désormais besoin d'un véritable filet de sécurité dynamique, capable de contenir activement les menaces et de fournir instantanément une visibilité démontrable sur le rayon d'impact réel d'une compromission, afin d'éviter d'éventuelles mises en cause de la responsabilité des dirigeants.

Dans ce livre blanc, nous étudions quatre domaines que les entreprises jugent particulièrement complexes dans leur démarche pour se conformer à la directive NIS2.

1. Démontrer leur capacité à limiter les conséquences d'une violation de la sécurité
2. Garantir la sécurité de la chaîne d'approvisionnement
3. Assurer la continuité des activités
4. En cas d'attaque, communiquer rapidement les détails et les conséquences de celle-ci

Le présent document vise à expliquer comment une segmentation correctement mise en œuvre permet de répondre à l'ensemble de ces défis, notamment grâce à un confinement rapide et automatisé des menaces, au maintien de la continuité des activités et à une mise en conformité facilitée avec la directive NIS2.

Fournir les preuves nécessaires à la conformité et à la responsabilité des dirigeants

L'entrée en vigueur de la directive NIS2 a conduit davantage de conseils d'administration européens à placer la cybersécurité au rang de leurs priorités, une étape majeure pour préserver la continuité des services critiques. Dans un contexte où les menaces progressent à la vitesse des machines et dépassent les capacités de réaction humaines, les stratégies de sécurité fondées sur le périmètre et le respect formel des normes ne suffisent plus.

À présent, la véritable question pour les entreprises concernées est la suivante : comment *prouver* que vos mécanismes de défense internes sont réellement efficaces ?

Lorsque la responsabilité personnelle des dirigeants est engagée et que les incidents majeurs doivent être signalés dans les 24 heures, une conformité évaluée à un instant donné constitue davantage un risque qu'une protection. Une véritable résilience opérationnelle repose sur des dispositifs dynamiques de confinement des menaces, adaptés à une époque où le délai nécessaire pour exploiter une vulnérabilité en combinant IA et ransomware est passé de plusieurs jours à quelques minutes seulement.

La solution à tous ces défis ? Une segmentation de pointe. La segmentation traditionnelle reposait sur des infrastructures complexes et statiques fonctionnant à un rythme humain. Elles ne répondent plus aux besoins actuels des entreprises, qui requièrent notamment :

- un filet de sécurité capable non seulement de détecter les menaces, mais aussi de les contenir activement avant qu'elles ne se transforment en crises ;
- un cadre adaptatif et automatisé de confinement des risques ;
- une analyse continue de la surface d'exposition.

Une étude révèle que la région EMEA présente le taux d'incidence des attaques par ransomware le plus élevé au monde, ainsi que le niveau de maturité le plus faible en matière de segmentation. Les attaquants exploitent les vulnérabilités plus rapidement que les équipes ne peuvent les corriger. À cela s'ajoutent les difficultés rencontrées par les entreprises pour intégrer leurs systèmes hérités dans des environnements hybrides et pour gérer des infrastructures en pleine expansion sous l'effet de l'IA.

Akamai Guardicore Segmentation transforme cette approche. En effet, la solution permet de délimiter rapidement le périmètre d'impact d'une compromission dans le délai de signalement de 24 heures imposé par la directive NIS2. Elle aide également les dirigeants à satisfaire leurs obligations en matière de conformité et de responsabilité en fournissant des données probantes.

Les quatre principaux défis de la conformité à la directive NIS2 à l'ère de l'IA

1. Contenir rapidement les violations de sécurité
2. Atténuer les risques liés à la chaîne d'approvisionnement
3. Assurer la continuité des activités
4. Simplifier les audits et la génération de rapports

Ce livre blanc aborde chacun de ces défis et montre comment la segmentation favorise le maintien de la conformité, tout en protégeant les dirigeants et les services essentiels.

1. Confinement rapide des violations de sécurité

Le défi

En vertu de la directive NIS2, les entreprises doivent démontrer leur capacité à contenir une violation de sécurité afin d'éviter toute répercussion sociétale ou économique, au moyen de « mesures techniques appropriées et proportionnées ».

Parmi les obstacles les plus fréquents à la conformité avec la directive NIS2 figurent :

- des équipes de sécurité qui travaillent en silos et utilisent des outils distincts pour les ressources cloud natives et les centres de données sur site, ce qui crée des angles morts ;
- la difficulté à prioriser les menaces lorsque les outils de sécurité génèrent un grand volume d'alertes sans contexte métier ;
- les mouvements latéraux rapides caractéristiques des attaques accélérées par l'IA, qui se propagent avant que les équipes internes aient le temps de les détecter et d'y répondre ;
- des points de passage réseau statiques, incapables de segmenter efficacement les charges de travail dynamiques, les environnements Kubernetes ou le trafic cloud est-ouest ;
- des capacités d'analyse de l'exposition et de réponse (ExAR) fonctionnant indépendamment des mécanismes d'application des contrôles, ce qui empêche l'automatisation du confinement des risques ;
- des règles de sécurité qui deviennent obsolètes au fil des évolutions de l'infrastructure sous-jacente, ce qui entraîne l'apparition de voies d'exposition non cartographiées.

Alors que les employés font de plus en plus appel à l'IA pour effectuer des tâches à forte valeur ajoutée, il n'a jamais été aussi important pour les organisations d'adopter un modèle de sécurité axé sur le confinement, afin qu'aucune compromission ne puisse se propager au-delà du point d'entrée initial. Les équipes ont également besoin d'aide pour établir les priorités et concentrer leurs efforts sur le confinement des actifs réellement à risque, plutôt que sur l'analyse de scores de gravité.

La solution apportée par la segmentation

Les attaques renforcées par l'IA peuvent être maîtrisées plus rapidement grâce à un confinement lui-même renforcé par l'IA. C'est dans cette optique que nous avons développé Akamai Guardicore Segmentation, une plateforme définie par logiciel et centrée sur les actifs. Conçue pour les infrastructures hybrides, elle peut être déployée dans les environnements cloud, les centres de données, les environnements Kubernetes, les systèmes de technologie opérationnelle (OT) ainsi que les charges de travail d'IA. En collectant des données de télémétrie complètes, des paquets réseau aux processus du système d'exploitation et aux requêtes DNS, la plateforme garantit une segmentation fondée sur les comportements réels et continuellement validée face aux nouvelles voies d'exposition.

Les alertes de sécurité sont classées en fonction du rayon d'impact mesuré et des conséquences métier potentielles, ce qui réduit la lassitude liée aux alertes. Akamai Guardicore Segmentation intègre directement ses résultats dans des règles automatisées pour contenir les menaces avant qu'elles ne puissent se propager. Cette automatisation basée sur l'IA accélère la cartographie des dépendances, souvent responsable des retards observés dans les projets de segmentation traditionnels.

L'objectif n'est plus d'empêcher chaque attaque, mais de limiter la propagation des attaques. En cas de compromission, Akamai Guardicore Segmentation permet de confiner la menace conformément à la stratégie de segmentation définie. Les mesures d'atténuation adéquates peuvent ensuite être mises en œuvre, et l'incident peut être signalé dans le délai prévu par la directive NIS2.

2. Atténuation des risques liés à la chaîne d'approvisionnement

Le défi

Par le passé, les incidents de sécurité provenant d'un sous-traitant, d'un prestataire de maintenance ou d'un fournisseur de services cloud étaient considérés comme des problèmes externes et gérés au moyen de cadres juridiques et de polices d'assurance. Avec la directive NIS2, cela n'est plus possible. La direction doit veiller à ce que l'entreprise respecte les exigences de la directive NIS2, notamment en matière de gestion de la sécurité de la chaîne d'approvisionnement, et peut être tenue responsable en cas de manquement à ces obligations.

La solution apportée par la segmentation

Une segmentation adéquate permet d'assurer le bon déroulement des opérations, même en cas de compromission d'un partenaire commercial tiers. Plutôt que de s'appuyer sur des contrôles d'accès en bordure du réseau, tels que les VPN, qui ont tendance à accorder un accès étendu fondé sur une confiance implicite une fois compromis, les entreprises doivent restreindre l'accès des fournisseurs aux seuls serveurs ou applications nécessaires à l'exécution de leurs missions contractuelles.

Akamai Guardicore Segmentation simplifie cette démarche grâce à une microsegmentation centrée sur les actifs et axée sur l'identité. Les équipes de sécurité peuvent créer des règles granulaires fondées sur l'identité des utilisateurs et les étiquettes applicatives. Ainsi, même si les identifiants d'un fournisseur sont compromis, ils ne permettent d'accéder qu'à la charge de travail qui leur est attribuée sur un port précis, ce qui limite considérablement les possibilités de mouvement latéral vers des infrastructures critiques.

Surtout, la cartographie visuelle en temps réel de la plateforme fournit aux organismes de réglementation et aux auditeurs des preuves claires que les connexions de tiers respectent le principe du moindre privilège et demeurent effectivement isolées. Pour les connexions de fournisseurs présentant un niveau de risque plus élevé, la fonctionnalité de segmentation multifactorielle (MFS) d'Akamai Guardicore Segmentation va encore plus loin en intégrant directement l'authentification multifactorielle (MFA) dans la règle de segmentation elle-même. Au lieu d'authentifier une identité une seule fois au niveau du périmètre réseau, l'identité du fournisseur est soumise à une authentification au niveau de la connexion, pour le service ou le port précis auquel elle tente d'accéder.

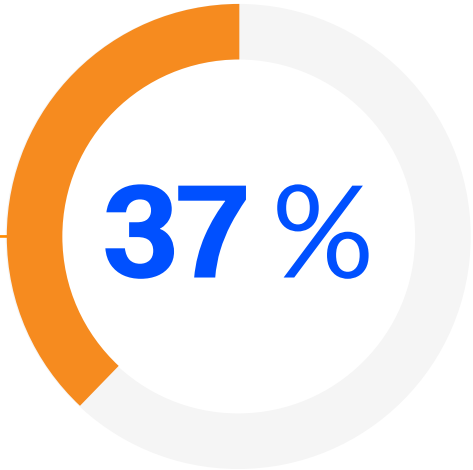
3. Continuité opérationnelle et réduction des perturbations

Le défi

La directive NIS2 ne porte pas uniquement sur la protection des données. Son objectif est également de préserver les services critiques fournis par des secteurs tels que les services financiers, l'énergie, l'eau ou les transports, qui ont tous été victimes de cyberattaques ces dernières années. Ces événements représentent une menace majeure pour l'économie dans son ensemble, les infrastructures essentielles et la sécurité publique. Ils ont également, de toute évidence, des répercussions notables sur le fonctionnement interne des organisations touchées. Bien souvent, c'est le temps nécessaire pour détecter un incident et y répondre qui prolonge les perturbations opérationnelles auxquelles l'entreprise est confrontée.

La microsegmentation constitue un moyen efficace d'accélérer les délais de réponse tout en contribuant à la conformité à la directive NIS2. Cependant, nous savons que la crainte de *perturber l'activité* reste le principal frein à son adoption. Sachant que seulement 37 % des entreprises déclarent partager la responsabilité de la segmentation entre les équipes de sécurité et les équipes d'infrastructure, il est évident que cette pratique est généralement gérée en silos, ce qui conduit à une forme d'inaction.

37 % des entreprises déclarent partager la responsabilité de la segmentation entre les équipes de sécurité et les équipes d'infrastructure



La solution apportée par la segmentation

Les risques métier peuvent être réduits en combinant la segmentation avec des capacités automatisées de détection, de réponse ainsi que d'analyse et de gestion de l'exposition. En observant le comportement des applications, la plateforme de segmentation est capable de comprendre les véritables flux de communication et d'identifier ce qui est réellement accessible et exploitable. Elle peut ensuite automatiser les mesures d'application des règles qui nécessitent habituellement une intervention manuelle lors d'un incident en cours.

Akamai Guardicore Segmentation est la première plateforme à offrir cette possibilité. Conscient des craintes que suscite le risque de dysfonctionnement des applications, Akamai s'appuie sur un modèle de déploiement qui privilégie la simulation. Les règles de sécurité sont exécutées en mode brouillon à partir du trafic réel, ce qui permet aux équipes de vérifier mathématiquement qu'une règle ne perturbera pas les applications avant d'activer un blocage. Ainsi, Akamai Guardicore Segmentation permet aux équipes de consacrer moins de temps à la rédaction de règles et d'appliquer leurs contrôles en toute confiance, ce qui favorise une adoption plus rapide du modèle Zero Trust tout en réduisant les coûts.

La plateforme comprend un portail dédié aux propriétaires d'applications, qui permet aux responsables des unités métier de consulter et de valider des règles de connexion spécifiques. Cette validation transversale facilite la mise en œuvre des mesures strictes de confinement imposées par la directive NIS2, sans interrompre les opérations.

Akamai Guardicore Segmentation simplifie également l'adoption sécurisée de l'IA, en garantissant que les modèles à forte valeur et les ensembles de données sensibles ne sont pas exposés à des accès latéraux superflus, même lorsque les infrastructures GPU montent en charge. La solution empêche ainsi la phase de propagation des attaques et réduit considérablement l'impact des incidents de sécurité.

Le système est conçu pour assimiler en continu le comportement des applications, cartographier les dépendances et générer des règles de segmentation précises, soumises à approbation humaine. Cette application cohérente des règles s'étend aux environnements sur site, cloud et conteneurisés à partir d'un plan de contrôle unifié, ce qui élimine les failles de sécurité engendrées par les silos architecturaux.

4. Simplification des audits, de la conformité et de la génération de rapports

Le défi

Les membres de la direction sont désormais tenus d'assurer la conformité à la directive NIS2, sous peine d'engager leur responsabilité personnelle, et les entreprises doivent déclarer tout incident significatif dans les 24 heures suivant sa détection. Les auditeurs comme les dirigeants souhaitent avoir en permanence la garantie que les mesures de sécurité en place sont réellement efficaces face aux véritables menaces.

Les rapports de cybersécurité destinés aux dirigeants se concentrent traditionnellement sur les alertes et les vulnérabilités. Pourtant, une longue liste de vulnérabilités non corrigées n'indique pas au conseil d'administration ce qui représente vraiment un danger pour les fonctions critiques de l'entreprise. Les outils traditionnels de protection des points de terminaison peuvent isoler une machine individuelle, mais ils ne disposent pas du contexte réseau et applicatif nécessaire pour contenir instantanément le rayon d'impact d'une violation à l'échelle d'une infrastructure hybride, qu'elle soit hébergée dans le cloud ou dans un centre de données.

Les cartographies statiques et les flux bruts fournis par les outils hérités ne reflètent pas le niveau de risque réel. Plus que la preuve que des outils ont été déployés, les dirigeants exigent une visibilité claire sur les expositions et les chemins d'attaque, ainsi que la preuve que les contrôles de sécurité réduisent activement et continuellement les risques opérationnels.

> **Lorsque l'ANSSI [Agence nationale de la sécurité des systèmes d'information] exige un rapport d'incident sous 24 heures, vous ne pouvez pas vous permettre de passer trois jours à analyser manuellement le réseau pour identifier les ressources affectées. Vous devez disposer instantanément d'une visibilité démontrable sur votre rayon d'impact.**
>
> Yann Fralo, Regional Sales Manager, Akamai

La solution apportée par la segmentation

À l'heure actuelle, les entreprises ont besoin d'une plateforme de segmentation capable de transformer les données de télémétrie techniques en rapports de risque compréhensibles pour les dirigeants. Cette approche permet à la fois de satisfaire aux principaux critères d'évaluation des auditeurs de la NIS2 et de démontrer une réduction mesurable des risques métier.

C'est précisément ce que propose Akamai. Les entreprises peuvent facilement démontrer leur capacité à contrôler les environnements hybrides et réglementés sans avoir à produire une documentation manuelle ni à gérer des ensembles de règles fragiles. Au lieu de présenter à un auditeur des milliers de lignes de code de pare-feu, Akamai Guardicore Segmentation fournit une cartographie visuelle intuitive et en temps réel qui atteste de l'isolement des ressources et de l'application du principe de moindre privilège.

Par ailleurs, la fonctionnalité Insight Query, associée à ExAR, permet aux équipes d'effectuer des recherches en langage naturel afin d'évaluer instantanément le rayon d'impact d'un incident. Elle apporte les informations nécessaires pour respecter le délai strict de signalement de 24 heures imposé par la directive NIS2, sans avoir à consacrer plusieurs jours à des analyses manuelles approfondies.

Elle accélère également considérablement l'adoption de la microsegmentation. Alors que les projets de segmentation traditionnels peuvent s'étendre sur plusieurs années, Akamai Guardicore Segmentation s'appuie sur l'étiquetage automatisé et des modèles alimentés par l'IA pour atteindre un niveau de segmentation compatible avec les exigences de la directive NIS2, en quelques semaines seulement. Cela réduit ainsi la période d'exposition réglementaire du conseil d'administration.

Enfin, la plateforme offre l'infrastructure de confinement requise pour les clusters d'entraînement de modèles d'IA à forte valeur afin de limiter les risques, notamment l'élargissement du rayon d'impact d'une attaque, l'exfiltration non autorisée de données ou l'accès illicite aux modèles.

Les points clés en un coup d'œil

Défis liés à la NIS2	Article de la NIS2	Approche traditionnelle	Akamai Guardicore Segmentation
Confinement des violations de sécurité	Articles 21(1) et 21(2)(f)	Les défenses périmétriques et les points de passage réseau statiques ne prennent pas en compte le trafic cloud/Kubernetes est-ouest	Une microsegmentation définie par logiciel et centrée sur les actifs qui empêche les mouvements latéraux
Sécurité de la chaîne d'approvisionnement	Article 21(2)(d)	Les vulnérabilités des fournisseurs sont traitées comme un risque juridique ou lié à l'assurance	Un contrôle d'accès Zero Trust défini par logiciel et fondé sur le principe du moindre privilège, qui limite strictement l'accès des fournisseurs tiers aux ressources de serveur qui leur sont attribuées Une authentification MFA appliquée au niveau de la connexion, de sorte que des identifiants compromis ne puissent pas être utilisés pour obtenir un accès
Continuité opérationnelle	Article 21(2)(c)	L'inaction est souvent dictée par la crainte de mettre à mal l'activité	Un moteur de déploiement fondé sur la simulation qui permet de tester les règles en mode brouillon à partir du trafic réel
Responsabilité	Article 23	Les opérations manuelles de détection peuvent prendre plusieurs jours pour identifier les actifs compromis	Une évaluation instantanée du rayon d'impact d'une violation de sécurité grâce à des requêtes en langage naturel, associée à une application rapide des règles pour répondre aux obligations de signalement sous 24 heures Une cartographie visuelle en temps réel pour remplacer l'analyse des lignes de code

La microsegmentation pour contenir les violations de sécurité grâce à l'IA

La directive NIS2 a introduit la responsabilité individuelle au sein des conseils d'administration. Parallèlement, l'IA a profondément transformé la donne en matière de cybersécurité. Les vulnérabilités peuvent être identifiées, exploitées à des fins malveillantes puis attaquées en quelques minutes seulement, ce qui supprime le délai de réaction dont les entreprises dépendaient autrefois. Dans notre économie mondiale hyperconnectée, l'empreinte digitale d'une entreprise s'étend à sa chaîne d'approvisionnement, à ses environnements cloud, à ses réseaux OT ainsi qu'à ses infrastructures d'entraînement de modèles d'IA à forte valeur. Tout est étroitement interconnecté.

Les organisations d'aujourd'hui ont besoin d'un filet de sécurité dynamique et automatisé capable de maintenir la continuité des activités même en cas de violation, tout en leur permettant de produire presque instantanément des preuves que celle-ci a été rapidement contenue.

Une segmentation granulaire peut constituer une solution efficace à l'ensemble de ces défis. Toutefois, les plateformes adoptées doivent être conçues pour répondre aux réalités actuelles de la cybersécurité et pour s'adapter à son évolution future.

Akamai Guardicore Segmentation est une plateforme de microsegmentation de premier plan qui protège les entreprises contre la nouvelle génération de cybermenaces sophistiquées, tout en contribuant à leur conformité à la directive NIS2. Elle assure un confinement rapide des violations de sécurité grâce à l'IA, réduit les risques liés à la chaîne d'approvisionnement, offre une mise en œuvre plus rapide que les solutions traditionnelles et favorise activement la continuité des activités au lieu de la compromettre.

Repenser les priorités en matière de sécurité

Akamai Guardicore Segmentation change totalement les règles du jeu en accélérant le déploiement de la microsegmentation et en redéfinissant les priorités en matière de sécurité : il ne s'agit plus d'empêcher chaque attaque, mais d'en maîtriser la propagation.

La solution contribue à la conformité à la directive NIS2 à travers quatre piliers essentiels :

Confinement rapide des violations de sécurité grâce à l'IA
La plateforme, axée sur les actifs, collecte des données de télémétrie complètes sur l'ensemble des charges de travail hybrides. Elle isole automatiquement les menaces en fonction de leur impact métier calculé, empêchant ainsi les mouvements latéraux rapides.

Atténuation des risques liés à la chaîne d'approvisionnement
Akamai Guardicore Segmentation limite l'accès des fournisseurs aux seuls serveurs strictement nécessaires et fournit la cartographie visuelle indispensable pour démontrer l'isolement des infrastructures critiques.

Continuité opérationnelle
Afin d'éliminer l'inaction suscitée par la crainte d'interrompre les opérations, la plateforme propose un modèle qui privilégie la simulation. Les équipes de sécurité peuvent valider mathématiquement les règles en mode brouillon à partir du trafic réel avant leur activation.

Simplification des audits et de la génération de rapports
Akamai Guardicore Segmentation fournit des cartographies visuelles en temps réel qui servent de preuve pour les auditeurs. La plateforme transforme les données de télémétrie techniques en rapports orientés risque et compréhensibles pour les dirigeants, offrant ainsi une assurance continue en matière de conformité.

À l'ère de l'IA, empêcher chaque attaque est impossible. En revanche, vous pouvez en maîtriser les conséquences.

Accélérez votre préparation à la directive NIS2 grâce à la microsegmentation automatisée. Voyez Akamai Guardicore Segmentation à l'œuvre et découvrez comment protéger vos actifs critiques en quelques minutes seulement.

Planifiez une évaluation personnalisée.

Avis : les informations du présent document sont fournies à titre d'information uniquement. Elles ne doivent pas être interprétées comme un conseil juridique et ne créent aucun engagement de la part d'Akamai. Les lois et réglementations peuvent varier et les interprétations juridiques peuvent changer au fil du temps. Aucune garantie n'est donnée quant à l'exactitude, l'exhaustivité ou l'adéquation des informations fournies. Si vous avez besoin de conseils juridiques ou si vous avez des problèmes juridiques spécifiques, veuillez consulter un professionnel qualifié qui pourra vous conseiller en fonction de votre situation et de votre juridiction.

Akamai est l'entreprise de cybersécurité et de Cloud Computing qui soutient et protège l'activité en ligne. Nos solutions de sécurité leaders du marché, nos informations avancées sur les menaces et notre équipe opérationnelle internationale assurent une défense en profondeur pour protéger les données et les applications des entreprises du monde entier. Les solutions de Cloud Computing complètes d'Akamai offrent des performances de pointe à un coût abordable sur la plateforme la plus distribuée au monde. Les grandes entreprises du monde entier font confiance à Akamai pour bénéficier de la fiabilité, de l'évolutivité et de l'expertise de pointe nécessaires pour développer leur activité en toute sécurité. Pour en savoir plus, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 08/26.