Cloud NGFW : sécurité d'exception, simplicité inégalée sur AWS

Donnez une longueur d'avance à votre cybersécurité avec un pare-feu piloté par ML, géré par Palo Alto Networks et fourni sous forme de service cloud-native sur AWS

paloalto® NETWORKS | aws

Sommaire

L'avènement du cloud redessine les contours de la cybersécurité

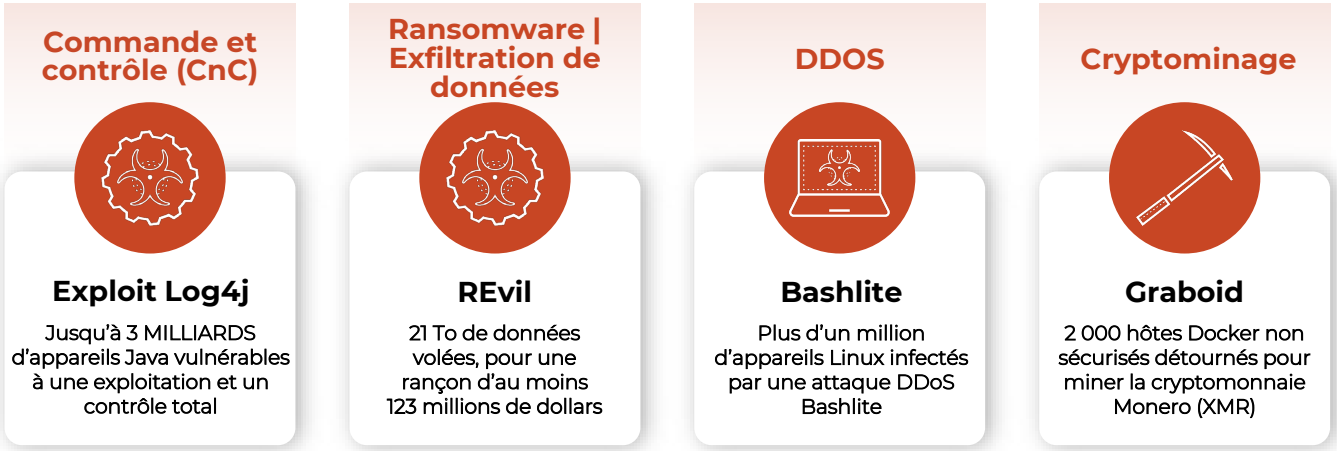
Le cloud public a connu un essor époustouflant ces dernières années. Et la pandémie n'a fait qu'amplifier le phénomène dans les entreprises. Aujourd'hui, 69 % d'entre elles hébergent plus de la moitié de leurs workloads dans le cloud, soit une augmentation de 123 % par rapport à 2020.

Or, qui dit plus de cloud dit aussi plus de sécurité. Les fournisseurs de cloud public comme Amazon Web Services (AWS) permettent aux organisations de gagner en agilité, réduire leurs coûts et simplifier la gestion de leurs infrastructures. Quant à la sécurité, elle est régie par un modèle de responsabilité partagée dans lequel AWS protège l'infrastructure cloud, tandis que les clients se chargent de sécuriser leurs données. En s'associant à un partenaire de sécurité comme Palo Alto Networks, les organisations peuvent se concentrer sur leur cœur de métier tout en bénéficiant d'une protection avancée. Le modèle de responsabilité partagée est le pivot de la lutte contre les cybercriminels et d'une meilleure préparation face aux menaces de demain.

La bonne nouvelle, c'est que les entreprises peuvent désormais compter sur une cybersécurité à la hauteur des enjeux. Les pare-feu nouvelle génération (NGFW) forment aujourd'hui la pierre angulaire de la sécurité réseau. Ils bloquent les menaces qui tentent d'infiltrer le trafic entrant, sortant et est-ouest dans les environnements physiques, virtuels et containerisés.

Les équipes de sécurité veulent conjuguer protection du réseau et simplicité du cloud

Toutefois, un déploiement dans le cloud n'est pas sans risque compte tenu de l'augmentation exponentielle des menaces : émergence récente de la tristement célèbre vulnérabilité Log4j, ransomware, attaques par déni de service distribué (DDoS), vers de cryptojacking, etc.

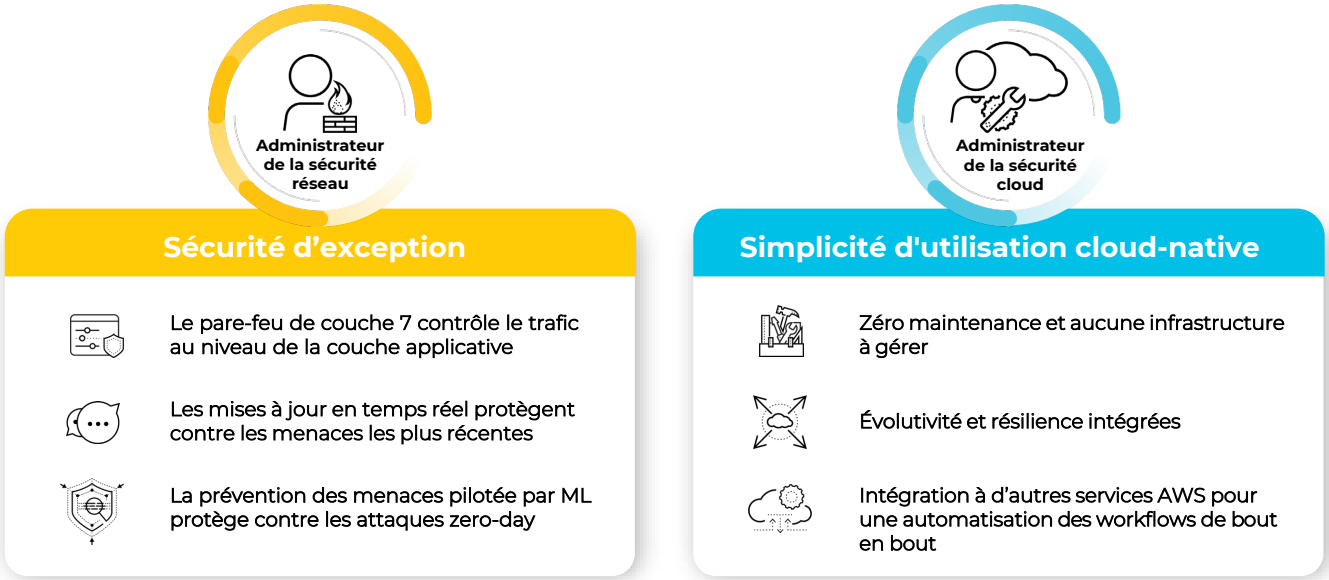


Toute compromission peut non seulement perturber les activités d'une entreprise, mais aussi nuire considérablement à sa réputation. Au final, ce que les clients AWS recherchent, c'est un moyen simple de déployer une sécurité réseau de pointe pour protéger leur volume croissant de workloads exécutés dans le cloud public. Leurs environnements nécessitent une visibilité et une sécurité de couche 7 pour bloquer les cyberattaques, tout en limitant les dépenses opérationnelles pour les équipes DevOps et de sécurité. Aujourd'hui, toute la question pour les RSSI est donc de savoir comment bénéficier du meilleur des deux mondes : la protection d'un NGFW et la facilité d'utilisation du cloud.

Cloud NGFW, une solution signée Palo Alto Networks

Cloud NGFW est le tout premier NGFW intégré à AWS Firewall Manager. Piloté par Palo Alto Networks, Cloud NGFW combine une protection de pointe à une simplicité incomparable pour neutraliser en temps réel même les menaces les plus sophistiquées. Cloud NGFW fonctionne comme n'importe quel autre service AWS natif, à la différence près qu'il permet aux clients AWS de sécuriser facilement leurs workloads cloud grâce à la protection hors-pair qui a fait la réputation de Palo Alto Networks.

Avec cette protection réseau native fournie sous forme de service sur AWS, vous pouvez enfin conjuguer sécurité et simplicité.



Les entreprises ont besoin de la force d'une sécurité d'exception *et* de la facilité d'utilisation du cloud

Une sécurité réseau cloud-native, garante de la protection de votre environnement AWS

Cloud NGFW offre une protection réseau pilotée par ML pour vos clouds privés virtuels (VPC) Amazon. Au menu : App-ID, Threat Prevention, Advanced URL Filtering et autres fonction Palo Alto Networks conçues pour bloquer les menaces connues et zero-day.

App-ID : cette technologie Palo Alto Networks brevetée de classification sur la couche 7 vous permet de contrôler le trafic pour mieux réduire le risque d'attaque. App-ID identifie les applications qui circulent sur votre réseau par un système de classification granulaire du trafic qui définit la nature de l'application, indépendamment du port, du protocole, du chiffrement (SSH ou SSL) ou de toute tactique de contournement. Une fois l'application identifiée, App-ID vérifie la politique applicable pour décider de la mesure à prendre : blocage, analyse, inspection ou modelage.

Threat Prevention : misez sur la solution de prévention des menaces leader du marché pour bloquer automatiquement les malwares connus, les exploits de vulnérabilités et les activités CnC. Chaque jour, la Threat Intelligence est automatiquement passée à la loupe, puis transmise à Cloud NGFW pour éliminer toutes les menaces. Quant à son système de prévention des intrusions (IPS), il intègre des fonctionnalités comme l'architecture « single-pass » et la gestion des politiques pour prévenir les menaces sans compromis sur les performances.

Advanced URL Filtering : bloquez les attaques web inconnues en temps réel pour éviter le scénario du patient zéro. Advanced URL Filtering analyse le trafic web, catégorise les URL et bloque les menaces en quelques secondes. Grâce à ses multiples catégories standard et personnalisées, il permet d'ajouter différentes couches de protection supplémentaires, comme le déchiffrement SSL ciblé et la journalisation avancée. En plus de ses propres données d'analyse, Advanced URL Filtering exploite la Threat Intelligence de WildFire®, le service de prévention anti-malware de Palo Alto Networks, et d'autres sources afin d'actualiser automatiquement sa base de sites web malveillants et de renforcer la protection.

Une sécurité évolutive et simple à gérer sur AWS

Cloud NGFW intègre la sécurité à vos workflows existants sur AWS. En réduisant la complexité, il permet à votre équipe de protéger facilement les données, les applications et les workloads, tout en bénéficiant de l'agilité du cloud.

Simplification de la gestion et des opérations : utilisez AWS Firewall Manager pour les environnements plus vastes et bénéficiez d'une gestion cohérente des politiques de pare-feu sur plusieurs comptes AWS et VPC Amazon. Cloud NGFW s'intègre en natif à AWS Firewall Manager pour simplifier la sécurité de votre réseau cloud. Par ailleurs, vous sécurisez facilement vos workflows automatisés et exploitez les fonctionnalités d'équilibrage de charges et de chargement automatique d'AWS à grande échelle.

Ce n'est pas tout : Cloud NGFW répond aux besoins de débit imprévisibles grâce à la puissance d'AWS Gateway Load Balancer (GWLB), un équilibreur de charges conçu pour fournir une haute disponibilité et une évolutivité élastique à la demande.

Zéro maintenance : tirez un trait sur la gestion de l'infrastructure grâce à un service cloud résilient qui évolue au rythme de votre trafic réseau. Cloud NGFW supprime les lourdeurs liées à la conception et à la gestion d'une architecture de pare-feu haute disponibilité, tout en éliminant les déploiements et configurations manuels. Misez sur un pare-feu spécialement conçu pour AWS pour parvenir à une sécurité du réseau à la fois performante et résiliente.

Visibilité contextuelle : bénéficiez d'une visibilité complète sur les applications, les contenus et le trafic, indépendamment des ports, des protocoles et des tactiques de contournement.

Une conception cloud-native pour tirer un trait sur la complexité opérationnelle

Grâce aux infrastructures IaC et à l'intégration aux pipelines CI/CD (intégration continue/livraison continue), Cloud NGFW simplifie le quotidien des équipes de sécurité du cloud.

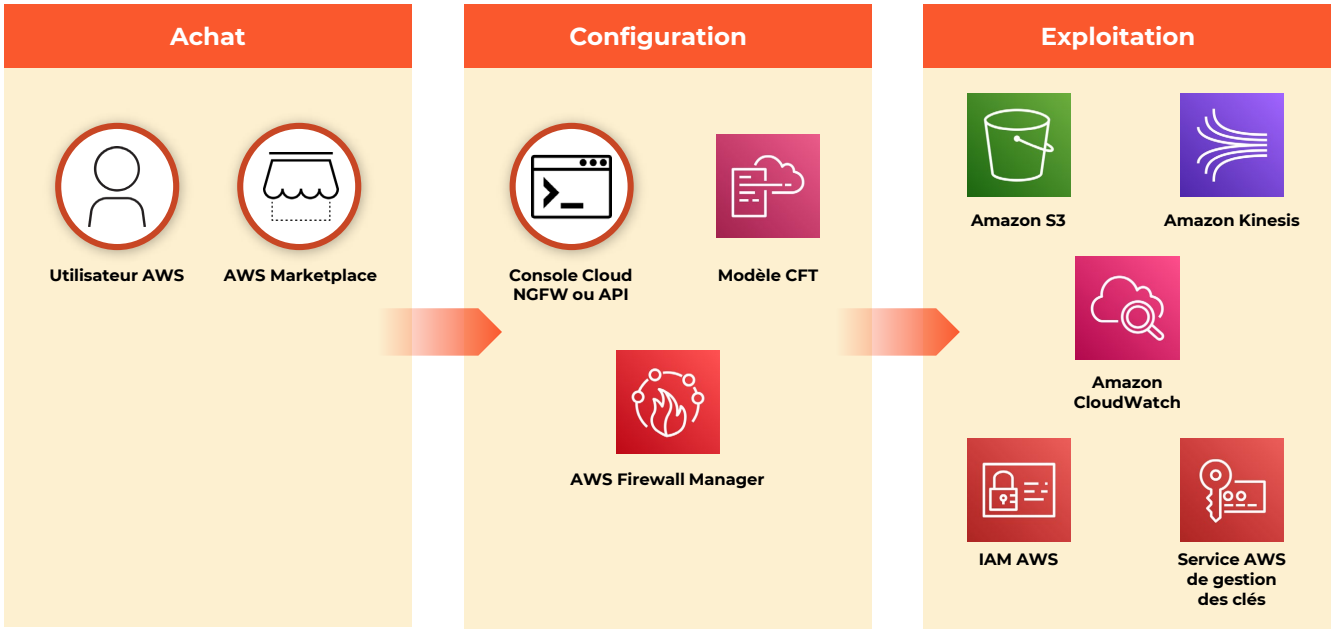
L'IaC pour automatiser les bonnes pratiques de sécurité : fournissez aux équipes DevSecOps des outils IaC qu'elles maîtrisent pour leur permettre de déployer des pare-feu nouvelle génération de façon simple et rapide.

Politiques déclaratives dans le cadre de pipelines CI/CD : déployez les fonctionnalités Cloud NGFW en créant des politiques déclaratives avec les modèles Terraform et CloudFormation. Intégrer la création de politiques à votre pipeline CI/CD permet d'homogénéiser vos workflows et facilite l'ajout ou la suppression d'étiquettes de politiques.

Fonctionnalités d'automatisation : que vous utilisiez Cloud NGFW ou AWS Firewall Manager pour gérer vos déploiements Cloud NGFW, exploitez les fonctionnalités d'automatisation pour simplifier les workflows, éliminer les tâches répétitives et gagner du temps. Cloud NGFW est compatible avec les modèles AWS CloudFormation, le provider Terraform et les API. AWS Firewall Manager intègre les mêmes fonctionnalités d'automatisation, ainsi qu'une interface de ligne de commande (CLI) et des kits de développement logiciel (SDK).

Installation en un clic : soyez opérationnel en cinq minutes. Téléchargez Cloud NGFW via AWS Marketplace et configurez-le en un seul clic.

Journalisation native : intégrez des services AWS natifs en toute simplicité, notamment Amazon Simple Storage Service (Amazon S3), Amazon CloudWatch et Amazon Kinesis, pour répondre aux exigences de conformité d'une journalisation centralisée.



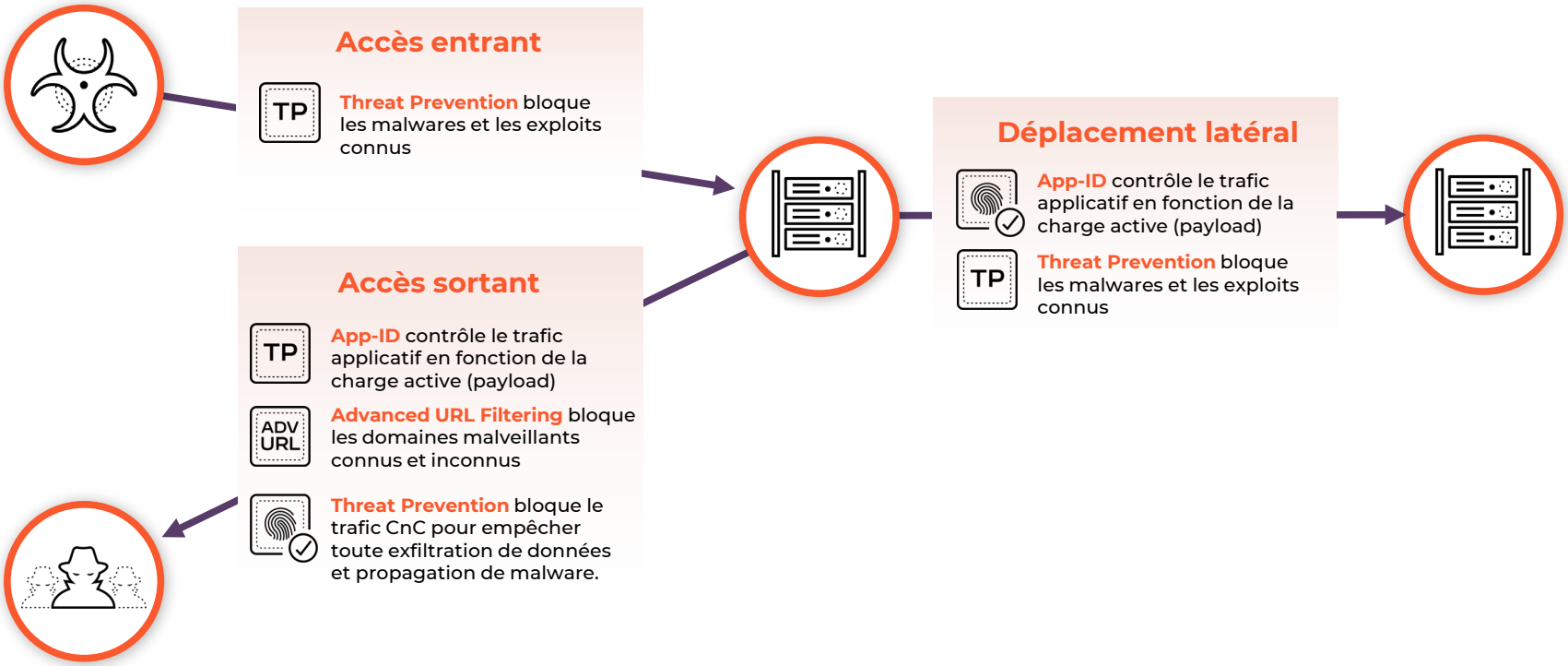
Cloud NGFW s'intègre à vos workflows existants sur AWS

Protection nouvelle génération : un déploiement simple et rapide

Palo Alto Networks et AWS ont facilité le déploiement de Cloud NGFW pour vous permettre de bénéficier rapidement des avantages d'une sécurité réseau pilotée par ML.

1. Recherchez Cloud NGFW sur AWS Marketplace. Quelques clics suffisent pour vous inscrire. À partir de là, intégrez vos comptes AWS et choisissez votre option de paiement (par ex., paiement à l'usage).
2. Créez des ressources Cloud NGFW sans passer par des tâches manuelles comme la conception d'une architecture haute disponibilité et la configuration à grande échelle.
3. Définissez des politiques de sécurité via AWS Firewall Manager ou la console Cloud NGFW, qui se connecte via une API. Les politiques ainsi paramétrées sur App-ID, Threat Prevention et Advanced URL Filtering permettent à Cloud NGFW de prendre automatiquement les mesures nécessaires pour sécuriser vos environnements AWS.
4. Redirigez Cloud NGFW vers Gateway Load Balancer (GWLB) pour inspecter et sécuriser le trafic sortant, entrant, de VPC à VPC, et entre les sous-réseaux d'un VPC Amazon. Vous disposez ainsi d'un cluster hautement disponible qui évolue de façon dynamique avec le trafic et permet des mises à niveau logicielles transparentes. GWLB assure une intégration simple et transparente dans les environnements AWS existants.

Cloud NGFW en action



Cloud NGFW sécurise les accès entrants/sortants et empêche les déplacements latéraux

Cloud NGFW en action

Trafic sortant : les workloads cloud avec accès sortant s'exposent au risque d'exfiltration et de comportement malveillant issu du web. En outre, les applications réglementées soumises aux standards PCI (Payment Card Industry) ou aux normes HIPAA doivent appliquer des fonctionnalités IPS sur le trafic sortant.

Cloud NGFW bloque les attaques web émergentes, réduisant ainsi la complexité pour votre équipe de sécurité et le risque global pour votre entreprise. Ses fonctionnalités de prévention des menaces vous permettent de répondre aux exigences IPS réglementaires.

Trafic entrant : les applications exposées à Internet et les applications réglementées nécessitent une protection contre les comportements malveillants.

Cloud NGFW réduit les risques et les tâches manuelles grâce à une prévention automatique des menaces. Il vous permet également de répondre facilement aux exigences IPS imposées par des standards et aux réglementations comme le PCI, HIPAA, etc.

Trafic de VPC à VPC Amazon : pour atteindre une sécurité Zero Trust, empêcher toute latéralisation et répondre aux exigences de conformité, les workloads cloud nécessitent une segmentation et une prévention des menaces avancées.

Cloud NGFW utilise Threat Prevention et App-ID entre les segments de réseau pour empêcher les déplacements latéraux et satisfaire aux exigences de conformité. Il élimine également la complexité liée à l'installation d'équipements IPS d'ancienne génération.

Trafic VPC Amazon vers environnement sur site : pour atteindre une sécurité Zero Trust, empêcher les déplacements latéraux et répondre aux exigences de conformité, le trafic entre les VPC et les environnements sur site doit faire l'objet d'une segmentation et d'une prévention des menaces avancées.

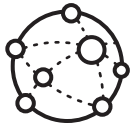
Cloud NGFW utilise Threat Prevention et App-ID entre les segments de réseau pour empêcher les déplacements latéraux et satisfaire aux exigences de conformité. Il élimine également la complexité liée à l'installation d'équipements IPS d'ancienne génération.

Faites confiance à un leader mondial de la cybersécurité

Cloud NGFW s'appuie sur la plus grande plateforme de sécurité réseau du marché et sur l'expérience d'un leader de la cybersécurité. Quels que soient les nouveaux modes opératoires des attaquants, Palo Alto Networks garde toujours une longueur d'avance pour anticiper tous leurs mouvements.

4,3 M
de mises à jour de sécurité par jour

224 MD
de menaces bloquées par jour



15 M
de transactions sécurisées par jour

95 %
d'entreprises du Fortune 100 font confiance à Palo Alto Networks

Nº 1
de la sécurité des entreprises

10 FOIS
leader du Gartner® Magic Quadrant™ des pare-feu réseau

Visibilité continue, mise en conformité, reporting... Palo Alto Networks assure une protection de toutes vos ressources AWS contre les menaces. D'Amazon Elastic Cloud Compute (Amazon EC2) à Amazon Elastic Container Service (Amazon ECS), en passant par AWS Lambda, Palo Alto Networks vous protège en actionnant des services AWS natifs. Ensemble, AWS et Palo Alto Networks fournissent le plus large éventail de fonctionnalités de sécurité intégrées, que votre entreprise entame sa migration ou mène déjà toutes ses opérations dans le cloud.

Passez à l'étape suivante

Inscrivez-vous sur AWS Marketplace pour faire vos premiers pas avec Cloud NGFW et mettre dès aujourd'hui une sécurité d'exception et la simplicité du cloud au service de la protection de vos applications et workloads.

Commencez dans AWS Marketplace >>

cloud-ngfw-ebook-033022-fr