Étude de Cas
Secteur des Entreprises

Protégez Votre IP Adresse - Défendez Votre Identité

Contexte

Les entreprises sont aujourd'hui confrontées à un paysage de menaces complexe :

- De multiples API exposées dans le cloud, sur site et via des systèmes hérités.
- Une intégration avec des partenaires, fournisseurs et plateformes SaaS qui élargit la surface d'attaque.
- Des exigences réglementaires (RGPD, ISO 27001, SOC 2, etc.) imposant une protection stricte des données.

Rien qu'en 2024, les violations liées aux API ont coûté en moyenne 5,1 M$ aux entreprises (rapport IBM). Pour beaucoup, une seule vulnérabilité API peut perturber les opérations, entraîner la fuite de données sensibles et causer des dommages réputationnels irréparables.

Le Défi

L'un de nos clients (un groupe régional de services financiers) faisait face à :

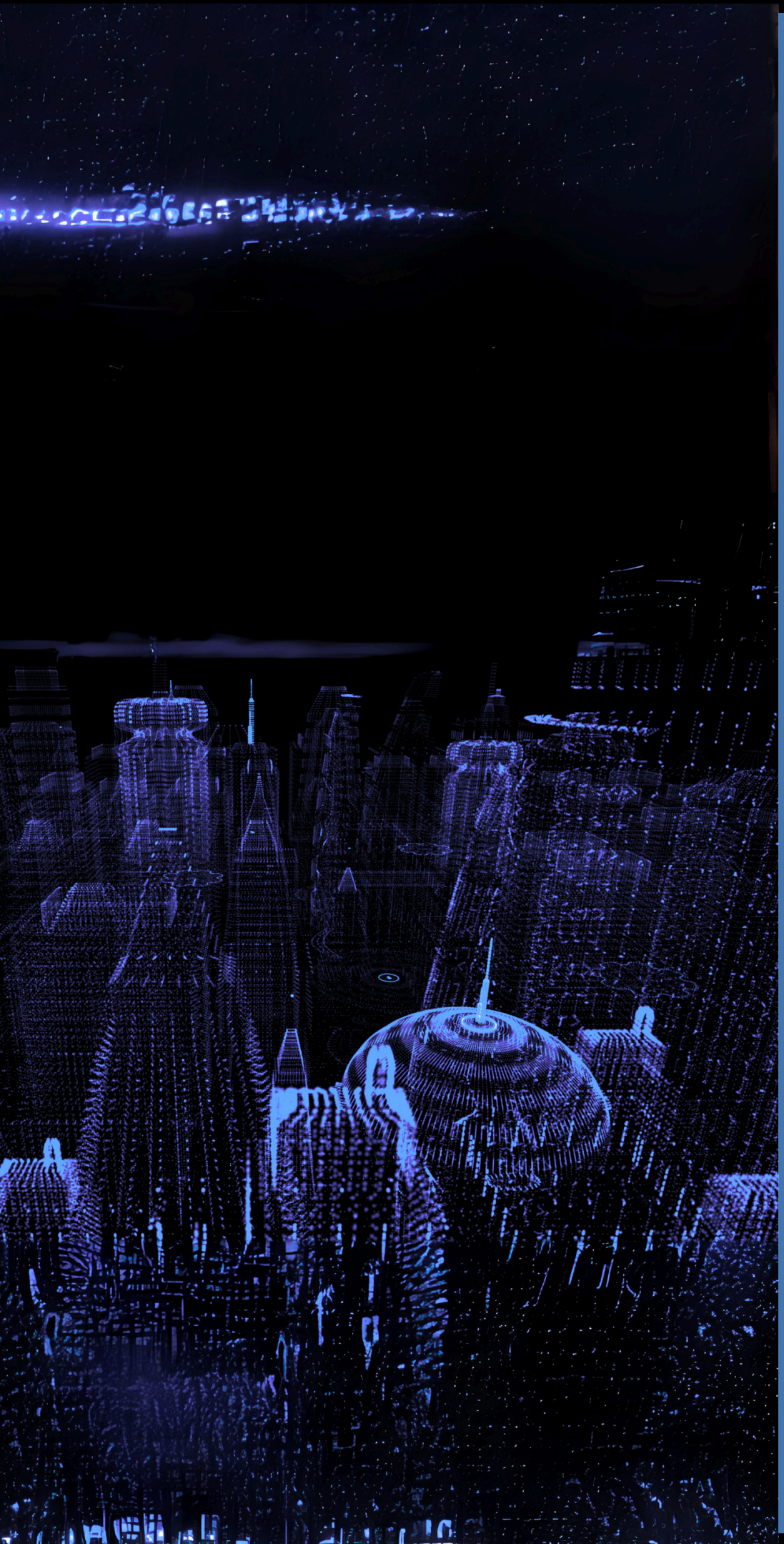
- Une forte exposition : plus de 120 API reliant les systèmes internes aux applications clients.
- Des attaques croissantes : tentatives de DDoS et credential stuffing sur les API de paiement.
- Une visibilité limitée : les pare-feu traditionnels et WAF n'offraient aucun suivi au niveau des API.
- Une pression réglementaire : des audits à venir exigeaient un renforcement des contrôles de sécurité des données.

La solution RitAPI

Le client a déployé RitAPI Advanced avec les fonctionnalités suivantes :

- **Défense en temps réel par IA** : Détection d'anomalies dans les schémas de requêtes et blocage instantané du trafic malveillant.
- **Bouclier anti-DDoS et abus** : Limitation de débit, détection des bots et atténuation automatisée des attaques volumétriques.
- **Visibilité approfondie** : Tableau de bord en temps réel, exportation de journaux et rapports de conformité pour les auditeurs.
- **Souveraineté & contrôl**e : Déploiement local, sans dépendance à des clouds étrangers — conforme aux exigences de résidence des données.

La mise en œuvre a pris moins de 48 heures, s'est intégrée facilement à l'infrastructure existante et a nécessité un minimum de formation pour l'équipe IT.



Résultats

Dans les 30 premiers jours, RitAPI a produit des résultats mesurables :

- Interception de 3 attaques DDoS majeures sur la passerelle de paiement.
- Blocage de 4 200+ tentatives de connexion suspectes (credential stuffing).
- Réduction de 95 % du risque d'indisponibilité des API, garantissant un service continu pour plus de 20 000 utilisateurs quotidiens.
- Simplification des audits de conformité grâce à des journaux prêts à l'export.

Témoignage Client (Paraphrasé pour Confidentialité)

«Avant RitAPI, notre couche API représentait un angle mort. Aujourd'hui, nous voyons les attaques en temps réel et nous pouvons démontrer notre conformité en toute confiance. Le déploiement a été rapide, et l'aspect souveraineté nous a apporté une véritable tranquillité d'esprit.»
— CTO, Groupe de Services Financiers

Enseignements clés pour les entreprises

- Les API sont le nouveau périmètre : leur sécurisation nécessite des outils dédiés.
- RitAPI offre non seulement de la protection, mais aussi de la visibilité et une préparation à la conformité.
- Les entreprises peuvent renforcer leur résilience tout en respectant les normes réglementaires, sans complexifier leurs opérations.

RitAPI

À Propos de RitAPI

RitAPI est une solution de cybersécurité alimentée par l'IA, conçue pour protéger les adresses IP et les points de terminaison API contre les requêtes malveillantes, l'usurpation d'identité et les attaques de la chaîne d'approvisionnement. Grâce à une défense en temps réel et une inspection approfondie, RitAPI assure la continuité opérationnelle et la conformité.

Contact: info@ritapi.io | www.ritapi.io