

# Studi Kasus Sektor Perusahaan



**Protect Your IP - Defend Your Identity**

## Latar Belakang

Perusahaan saat ini menghadapi lanskap ancaman yang semakin kompleks:

- Puluhan hingga ratusan API terbuka di cloud, sistem on-premise, maupun aplikasi lama.
- Integrasi dengan partner, vendor, dan platform SaaS yang memperluas permukaan serangan.
- Regulasi ketat (GDPR, ISO 27001, SOC 2, dsb.) yang menuntut perlindungan data tingkat tinggi.

Menurut laporan IBM, sepanjang 2024 rata-rata kerugian akibat pelanggaran terkait API mencapai \$5,1 juta. Satu celah API saja dapat mengganggu operasional, membocorkan data sensitif, dan merusak reputasi perusahaan secara permanen.

## Tantangan

Salah satu klien kami, sebuah grup jasa keuangan regional, merasakan tekanan ini secara langsung:

- Jejak API yang luas: Lebih dari 120 API yang menghubungkan sistem internal dengan aplikasi nasabah.
- Ancaman yang meningkat: DDoS dan credential stuffing yang menargetkan API pembayaran.
- Minim visibilitas: Firewall dan WAF yang mereka gunakan tidak bisa memberikan visibilitas pada level API.
- Tuntutan regulasi: Audit keamanan yang menuntut standar keamanan lebih tinggi.

## Solusi RitAPI

Untuk menjawab tantangan ini, mereka memilih RitAPI Advanced:

- Real-time AI Defense: Machine learning mendeteksi anomali pola permintaan dan langsung memblokir traffic berbahaya.
- DDoS & Abuse Shield: Rate limiting, deteksi bot, dan mitigasi otomatis untuk serangan volumetrik.
- Deep Visibility: Dashboard live, ekspor log, dan laporan kepatuhan untuk auditor.
- Sovereignty & Control: Deployment lokal tanpa ketergantungan cloud asing, sesuai regulasi data residency.

Implementasi selesai dalam kurang dari 48 jam, terintegrasi mulus dengan infrastruktur yang ada, dan tim IT tidak membutuhkan banyak penyesuaian.



## Hasil

Dalam 30 hari pertama, hasilnya terlihat jelas:

- Menghentikan 3 serangan DDoS besar pada gateway pembayaran.
- Memblokir 4.200+ percobaan login mencurigakan (credential stuffing).
- Mengurangi risiko downtime API hingga 95%, menjaga layanan tetap berjalan untuk lebih dari 20.000 pengguna harian.
- Audit keamanan menjadi lebih sederhana berkat log yang siap diekspor.



## Testimoni Klien

(Parafrase untuk menjaga kerahasiaan)

*“Dulu kami merasa buta terhadap apa yang terjadi di API kami. Setelah menggunakan RitAPI, semuanya berubah — kami bisa melihat ancaman langsung saat muncul dan lebih percaya diri menghadapi audit. Proses penerapannya juga mulus, dan yang paling melegakan, data kami tetap sepenuhnya dalam kendali kami.”*

*— CTO, Perusahaan Jasa Keuangan*



## Pelajaran bagi Perusahaan

- API kini menjadi perimeter baru — butuh solusi khusus untuk melindunginya.
- RitAPI memberikan perlindungan, visibilitas, sekaligus kesiapan keamanan.
- Perusahaan dapat memperkuat resiliensi dan memenuhi standar regulasi tanpa menambah kompleksitas operasional.



# RitAPI



## Tentang RitAPI

RitAPI adalah solusi keamanan siber berbasis AI yang dirancang untuk melindungi IP dan endpoint API dari permintaan berbahaya, penyamaran, serta serangan rantai pasokan. Dengan pertahanan real-time dan inspeksi mendalam, RitAPI memastikan kesinambungan operasional serta keamanan data.

Kontak: [info@ritapi.io](mailto:info@ritapi.io) | [www.ritapi.io](http://www.ritapi.io)