

1. Prezentare generală

Modulul VOGO eBS API Security asigură guvernanta și protecția proactivă a ecosistemului API al organizației: descoperă și cartografiază automat suprafața de atac, clasifică și maschează datele sensibile pentru a menține confidențialitatea și neutralizează precis actorii rău intenționați, nu anomalii izolate.

VOGO eBS API Security este un produs comercial integrat, dezvoltat, licențiat și susținut de VOGO Technology: descoperirea și inventarul API-urilor, clasificarea datelor sensibile, guvernanta posturii, detecția și blocarea atacatorilor, fluxurile de răspuns și consola funcționează ca un singur produs, cu o singură licență și un singur contract de suport. Produsul folosește ca biblioteci open source mature: Akto și OpenSearch.

- ▶ **Inventar complet:** numărul total de API-uri și structura fiecărui endpoint, descoperite automat.
- ▶ **Date sensibile:** identificate în cerere și răspuns, cu mascare pentru analiști.
- ▶ **Postură:** reguli de bune practici și reguli proprii, monitorizate continuu.
- ▶ **Atacatori:** identificați ca persoane, corelați peste adrese, token-uri și dispozitive, cu răspuns automat.

2. Arhitectură, instalare și licențiere

Modulul VOGO eBS API Security se instalează în infrastructura beneficiarului, pe mașini virtuale, astfel încât traficul API și datele analizate nu ies din organizație.

- ▶ **Instalare on-premise:** colectorul de trafic, motoarele de analiză, motorul de fluxuri de lucru, consola și depozitul intern, pe mașini virtuale, în cluster activ-activ. Sistemul de operare recomandat: Red Hat Enterprise Linux 9 (Linux de tip enterprise pe 64 de biți).
- ▶ **Colectarea traficului:** oglindirea traficului de la gateway, load balancer sau proxy, fără modificarea aplicațiilor.
- ▶ **Licențiere:** perpetuă sau pe subscripție, dimensionată pe volumul de apeluri, de la cel puțin 80.000 de apeluri API pe lună, cu toate funcțiile de descoperire, clasificare, detecție și răspuns incluse. Licența acoperă toate mediile logice (producție, dezvoltare și testare) și funcționarea în centrul de date de rezervă, pe durata activării lui, și se ajustează la volumul de apeluri măsurat, fără cost suplimentar.
- ▶ **Implementare prin configurare:** funcțiile se obțin prin configurarea produsului, fără dezvoltări.

3. Descoperirea și inventarul API-urilor

Modulul VOGO eBS API Security construiește și ține la zi inventarul API-urilor din traficul observat și din descoperirea activă.

- ▶ **Numărul total de API-uri:** determinat cu precizie, pentru tot sistemul.
- ▶ **Structura endpoint-urilor:** metode, parametri de sarcină, parametri de interogare și tipul lor de date, documentate automat, fără configurare manuală; documentația se exportă ca specificație OpenAPI, iar abaterile față de specificațiile declarate se marchează în inventar.
- ▶ **Descoperire activă:** tehnici care imită tacticile de recunoaștere ale atacatorilor, pentru a identifica și valida punctele finale expuse.
- ▶ **API-uri zombie:** endpoint-urile al căror volum de trafic a scăzut semnificativ sau versiunile vechi cu trafic rar.
- ▶ **Grupare:** API-urile similare se personalizează și se grupează pentru vizibilitate și raportare.
- ▶ **Etichetare:** etichete personalizate pe endpoint-uri și gruparea după proprietar, funcție sau versiune; un API pentru gestionarea etichetelor, folosit în fluxurile de securitate și în automatizare.
- ▶ **Export:** API public pentru exportul periodic al inventarului către platforma centralizată de gestionare a activelor.
- ▶ **Notificări:** la descoperirea unor active API noi și a unor puncte finale noi, pe e-mail, către SIEM și prin webhook.
- ▶ **Filtrare:** filtrare complexă și filtre avansate salvate pentru părțile interesate (Arhitect, SecOps, AppSec).

4. Datele sensibile

Modulul VOGO eBS API Security identifică datele sensibile din trafic și le protejează în propria consolă.

- ▶ **Identificare automată:** toate datele sensibile și datele personale (PII) din endpoint-uri, cu locațiile lor, inclusiv în cerere și în răspuns — de exemplu CNP, e-mail, telefon.

- ▶ **Clasificări personalizate:** utilizatorii administrativi adaugă categorii proprii de date sensibile, aplicate automat la învătarea API-urilor.
- ▶ **Hash unidirecțional:** valorile sensibile se înlocuiesc înainte de persistare cu un hash unidirecțional cu cheie secretă proprie instalării; valoarea brută nu se persistă, iar tabloul de bord afișează numai amprenta, astfel încât analiștii SOC nu văd informațiile brute în timpul investigațiilor.

5. Scorul de risc și guvernanta posturii

Modulul VOGO eBS API Security evaluează postura de securitate a tuturor API-urilor organizației și semnalează abaterile.

- ▶ **Scor de risc pe endpoint:** calculat după protocol, autentificare și expunerea datelor sensibile, personalizabil; scorurile se reglează prin severitatea regulilor de decalaj de postură; endpoint-urile cele mai critice se identifică automat, pentru prioritizarea remediilor.
- ▶ **Motor de guvernanta:** reguli de bune practici gata de utilizare și standarde de securitate proprii ale organizației.
- ▶ **Reguli compuse:** reguli complexe care aderă la cadrele PCI, PSD2, NIST și altele.
- ▶ **Reguli predefinite și personalizate:** de exemplu JWT fără expirare sau format UserID ghicit.
- ▶ **OAuth:** reguli care identifică uzurparea identității OAuth, injecția de cod OAuth și vulnerabilitățile implementărilor OAuth 2.0 și OpenID Connect: redirect_uri, PKCE, parametrul state, durata de viață a token-urilor, algoritmi de semnare, audiența și emitentul.
- ▶ **Reguli Posture Gap:** identifică riscurile din inventar, monitorizează API-urile riscante și se aplică și API-urilor de pre-producție, înainte de producție, inclusiv specificațiilor OpenAPI transmise de pipeline-ul de livrare.
- ▶ **Clasificare și filtrare:** regulile se filtrează pe utilizator; vulnerabilitățile descoperite au severitate pe patru niveluri: critică, ridicată, medie și scăzută.
- ▶ **Monitorizare continuă:** alerte la orice abatere de la regulile de postură.
- ▶ **Remediere automată:** fluxuri de lucru legate de Jira, ServiceNow, Splunk și alte sisteme.
- ▶ **Centru de bune practici:** îndrumări de securitate actualizate continuu, de exemplu protecția autentificării.

6. Detecția atacatorilor

Modulul VOGO eBS API Security identifică persoana din spatele traficului rău intenționat, nu anomalii individuale disperate.

- ▶ **Identificare și blocare:** atacatorul este identificat și blocat ca persoană.
- ▶ **Caracteristicile atacatorului:** IP, token, identificator de utilizator, chei API și locație geografică, plus agentul de utilizator și amprenta clientului, în tabloul de bord.
- ▶ **Corelare:** activitățile dispersate se asociază unui singur utilizator, chiar dacă atacatorul folosește ID-uri, adrese IP și dispozitive diferite; amenințările se corelează într-o singură vizualizare.
- ▶ **Alerte pe utilizatori rău intenționați:** nu pentru toate anomaliile care pot apărea.
- ▶ **Alerte în timp real:** identificatorul atacatorului (IP, token), endpoint-urile API, tipul de atac, cronologia atacului, solicitarea completă și răspunsul, numărul de încercări, data și ora exactă și contextul.
- ▶ **Rezumate ale atacatorilor:** pentru triere rapidă, cu originile, metodele, țintele și motivațiile potențiale.
- ▶ **Profil de comportament:** atributele, comportamentul trecut și interacțiunile fiecărui utilizator cu toate API-urile; contextul fiecărui apel API: istoricul utilizatorului, API-ul accesat, datele transmise și modelele de trafic.
- ▶ **Anomalii benigne:** distinse de acțiunile dăunătoare, de exemplu o modificare de preferințe față de exploatarea unei vulnerabilități.
- ▶ **Remediere continuă:** informațiile de remediere prezentate împreună cu activitatea normală.

7. Atacurile detectate

Modulul VOGO eBS API Security detectează atacurile asupra API-urilor din clasificarea OWASP API Security Top 10.

- ▶ **Autorizare:** un singur ID BOLA (enumerarea identificatorilor), Double ID BOLA (pierderea corelației dintre doi parametri), apeluri către endpoint-uri neautorizate, legarea automată a intrării clientului în obiecte interne (mass assignment).
- ▶ **Autentificare:** forță brută și umplerea credențialelor pe autentificare, schimbarea parolei, resetarea parolei și 2FA; manipularea JWT (algoritm de downgrade, escaladarea privilegiilor); redirectionarea OAuth; token-uri și parole în URL.

- ▶ **Resurse:** utilizarea excesivă, parametri anormal de lungi și răspunsuri supradimensionate care pot duce la refuzul serviciului.
- ▶ **Server:** prevenirea SSRF (Server Side Request Forgery), inclusiv manipularea intrării; preluarea resursei la distanță fără validarea URL-ului.
- ▶ **Configurare:** configurații greșite de securitate, de exemplu mesaje de eroare care expun date ale utilizatorilor și detalii de sistem.
- ▶ **Injectii:** SQL Injection, Remote Code Execution, Cross site scripting, Path Traversal.
- ▶ **Gestionare:** lipsa inventarului și a strategiilor de retragere, comunicarea pe canale nesecurizate și abuzul care profită de lipsa înregistrării și a monitorizării.

8. Răspuns automat și fluxuri de lucru

Modulul VOGO eBS API Security răspunde automat la evenimentele de securitate.

- ▶ **Acțiuni automate de urmărire:** trimiterea IP-urilor, a token-urilor și a cheilor API spre blocare într-un WAF, cu durată de expirare, trimiterea evenimentelor către SIEM, webhook către sistemele interne.
- ▶ **Fluxuri de lucru:** bazate pe criterii complexe și specifice, dincolo de simplii declanșatori de evenimente, și fluxuri automatizate în mai mulți pași.

9. Administrare, acces și medii

Modulul VOGO eBS API Security separă vizibilitatea și accesul pe roluri și pe medii.

- ▶ **Vizualizare agregată:** toate mediile, în panoul de administrare, cu jurnale de audit globale (configurarea rolurilor, aplicarea SSO și altele).
- ▶ **Control granular:** vizibilitatea și accesul utilizatorilor în tabloul de bord; roluri personalizate cu permisiuni precise.
- ▶ **Directorul furnizorului de identitate:** autentificare SSO prin OpenID Connect sau SAML, cu Microsoft Active Directory sau Keycloak; roluri pe persoană sau grup aliniate cu directorul și reguli pentru fiecare mediu, pentru acces segregat.
- ▶ **Separarea în mai multe medii:** după domeniul API, departamente, responsabilități ale utilizatorilor sau seturi de API-uri.

10. Suport și servicii

Modulul VOGO eBS API Security este susținut de VOGO pe toată durata contractului.

- ▶ **Suport:** actualizările produsului, ale regulilor predefinite și ale centrului de bune practici.
- ▶ **Instalare și configurare:** prin VOGO sau prin partenerii certificați VOGO.

11. Capturi de ecran din VOGO eBS API Security Console

Capturile de mai jos sunt făcute în VOGO eBS API Security Console, pe date reale.



Fig. 1 VOGO eBS API Security Console: indicatorii, atacatorii identificați și inventarul API

Atacatori identificați					
Riscul	Identitatea	Adresele suspecte	Motivele	Primul apel	Ultimul apel
Risc 80	ana.ionescu	203.0.113.10, 203.0.113.11, 203.0.113.9	16 autentificări eșuate (forță brută), urmate de autentificare reușită - enumerare de identificatori pe /api/v1/solicitant/{id}: 2 obiecte din afara profilului (BOLA) - aceeași identitate din 3 adrese noi	20:28:22	20:28:27
Risc 70	mihai.pop	198.51.100.77	- enumerare de identificatori pe /api/v1/solicitant/{id}: 4 obiecte din afara profilului (BOLA) 6 apeluri către endpoint-uri neautorizate 8 încercări de injecție	20:28:23	20:28:28

Fig. 2 Atacatori corelați peste adrese și token-uri: forță brută urmată de autentificare reușită, enumerare BOLA, injecții

Inventarul API						
Metoda	Endpoint	Apeluri	Autentificare	Date sensibile	Riscul	Starea
GET	/api/v1/admin/utilizatori	6	Da	—	Risc 30	Activ
POST	/api/v1/auth/login	24	Da	—	Risc 10	Activ
POST	/api/v1/documente	24	Da	—	Risc 10	Activ
GET	/api/v1/dosare	32	Da	—	Risc 10	Activ
GET	/api/v1/dosare/{id}	24	Da	—	Risc 20	Activ
GET	/api/v1/rapoarte/export	4	Da	—	Risc 10	Activ
GET	/api/v1/solicitant/{id}	52	Da	CNP, e-mail, telefon	Risc 60	Activ
GET	/api/v2/avize	1	Nu	—	Risc 30	Zombie

Inventarul motorului de descoperire: VOGO Portal API – 8 endpoint-uri

VOGO® eBS ECM
Enterprise Business Solutions

© 2026 VOGO — Toate drepturile rezervate. Confidențialitate Termeni și condiții

Fig. 3 Inventarul API cu datele sensibile și scorul de risc; abaterile de postură