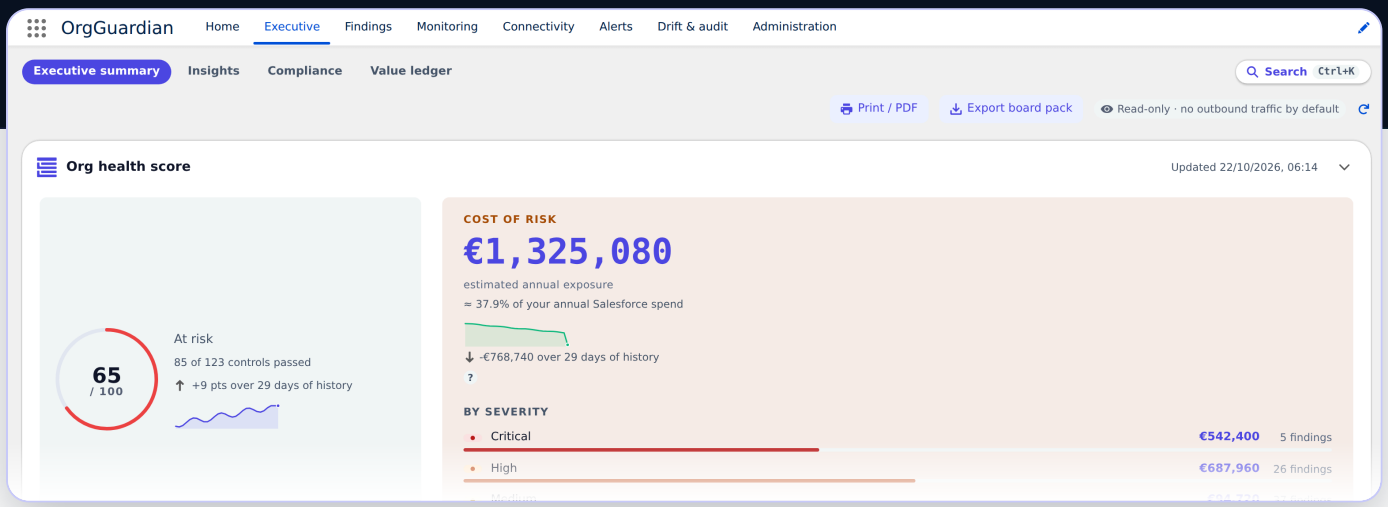
MANAGED PACKAGE FOR SALESFORCE · APPEXCHANGE

Security posture and compliance evidence for Salesforce, computed inside your org.

OrgGuardian scans your org on a schedule and stores what it finds as records in your own org. Read-only, it detects and advises, and never writes to your business data, your security configuration or your code. No connector, no vendor-held OAuth token, no egress by default.



Executive summary in Lightning: the risk your org carries, priced from the risk weights you set, next to the 0–100 org health score. Illustrative demo data.

Counted in the package source

90+
Detection types
Across 7 domains, plan-gated

8
Frameworks mapped
DORA, NIS2, SOC 2, ISO 27001… · paid plan

55+
Controls with evidence
Paid plan, refreshed by each scan

140+
Remediation playbooks
Shipped in the package, every plan

22
Outbound features
All off at install, opt-in one by one

0
Remote Site Settings
0 CSP Trusted Sites, 1 self-org credential

What it covers

Security posture

Over-privilege, dormant users, OAuth apps and grants left dormant, guest-user exposure, configuration blast radius, field exposure, data export and API exfiltration signals, and opt-in permission sprawl.

Monitoring and observability

Org limits and governor headroom; a 0–100 org health score; failed logins; async and Apex performance; API version drift; callout posture; in-org alerting.

Compliance evidence

Article-level mapping to DORA, NIS2, ISO 27001, SOC 2, NIST CSF and SOX; attestations with an owner and a due date; dated reports; evidence snapshots chained by hash, so an auditor can check that a report has not changed since it was written. The chain lives in your org, under your administrators' rights.

Code quality and intelligence

Apex and Lightning Web Components code quality; configuration drift and its opt-in export; opt-in in-org intelligence — baselines, anomalies, trends and breach forecasts for rising limits; an opt-in cost of risk in euros on the Executive screen, from risk weights you set.

Monitoring and a security baseline are in both plans; the full security posture pack, compliance evidence, code quality, in-org intelligence and the cost of risk come with the paid plan.

Where your data goes

Inside your org.

Apex and Lightning Web Components, running on your org's own platform. Every finding, score and attestation is a record in your org, under your retention schedule and your sharing rules. History and evidence snapshots are Big Objects, governed by object and field permissions only: check that your backup covers them.

Read-only by architecture.

OrgGuardian writes only its own records and scheduled jobs, plus Chatter alert posts once an administrator turns that channel on, and one Files document when an administrator replaces the shipped compliance mapping. Among what it reads but never writes: users, profiles and permission sets, connected apps and credential settings, the Setup Audit Trail, org limits.

Closed at install.

The package ships 22 outbound features in four families, and every one stays off until an administrator turns it on. It ships 0 Remote Site Settings, 0 CSP Trusted Sites and 1 Named Credential, meant for your own org and shipped with a placeholder address: the platform blocks unregistered endpoints.

Two channels reach us; we name them.

The AppExchange licensing channel reports your org ID, instance, licence status and install and uninstall events, and creates a lead (installing user's name, company, e-mail); nothing else from your org. The Heroku option, off by default, sends our EU-hosted service a twelve-key posture summary once an administrator consents, plus external host names if certificate monitoring is on.

Compliance mapping (6 of 8 frameworks)

DORA	Regulation (EU) 2022/2554 — Art. 7, 8, 9, 10, 12, 28
NIS2	Directive (EU) 2022/2555 — Art. 21(2)(b)(c)(d)(e)(h)(i)
ISO/IEC 27001:2022	Annex A — A.5.15, A.5.19, A.5.21, A.8.2, A.8.6, A.8.9, A.8.13, A.8.16, A.8.24, A.8.25
SOC 2	Trust Services Criteria — CC6.1, CC6.3, CC6.6, CC6.7, CC7.1, CC7.2, CC8.1, CC9.2; Availability A1.1, A1.2
NIST CSF 2.0	GV.SC, ID.RA, PR.AA, PR.DS, PR.IR, PR.PS, DE.AE, DE.CM
SOX	IT general controls — access, change management, operations

Evidence on a bounded scope: the configuration, identities, integrations and code of your Salesforce orgs. Certificate controls (NIS2 Art. 21(2)(h), ISO A.8.24, SOC 2 CC6.7, NIST CSF PR.DS) produce evidence only once certificate monitoring is turned on: it is off at install and needs an outbound call. PCI DSS, HIPAA and GLBA are not mapped. OrgGuardian does not certify, and does not make an organisation compliant with any framework.

Outbound features, by family

5 **Alert channels**
Slack, Teams, PagerDuty, webhook, Slack reactions

4 **Exports and integrations**
SIEM, ITSM, automatic ITSM tickets, the Heroku option

7 **External probes**
Connectivity, certificates, endpoint health, fleet reads of linked orgs, outbound resilience

6 **Self-callouts**
To your own org's API

All closed at install; an administrator opens each one. E-mail alerts, off until activated, are not among the 22: like the weekly board report, they use your org's e-mail service, unpseudonymised.

Plans

Free

One production org, unlimited users, 7 days of history: org limits, the org health score, failed logins, async and Apex performance, API version drift, callout posture, in-org alerting, and a security baseline (accounts without MFA, guest users, public file links, connected apps, OAuth tokens, holders of Modify or View All Data). An administrator's first visit starts a 30-day paid-plan trial.

Paid

One plan, a flat fee per production org by band of active user licences, never per seat or summed across orgs. Adds the full Security posture pack, code quality, configuration drift, compliance packs with attestations, in-org intelligence, cost of risk in euros and full e-mail alerting. Sandboxes, scratch and developer orgs are not counted.

Requirements

- Managed 2GP package (orgguardian, API 67.0); Enterprise, Unlimited, Performance or Developer Edition; Lightning Experience on desktop; install in a sandbox first
- Scan account: four read permissions from a permission set you create (View Setup and Configuration, View Roles and Role Hierarchy, View All Users, View All Profiles)
- No add-on licence or Salesforce Shield needed; the paid plan ingests Event Monitoring if you own it

Guides on this listing

Installation · Permissions and Personas · Configuration · Operations · Troubleshooting · Uninstall · Security FAQ · Glossary

contact@orgguardian.com
security@orgguardian.com

OrgGuardian 1.0.0.7 · October 2026. Figures counted in the package source; compliance mapping is indicative, not a certification. Salesforce, AppExchange, Lightning, Apex, Chatter, Heroku and Salesforce Shield are trademarks of Salesforce, Inc.; Slack, Microsoft Teams and PagerDuty are trademarks of their respective owners; all are used for identification only. OrgGuardian and DOPAMINE SAS are not affiliated with, endorsed by or sponsored by Salesforce, Inc.