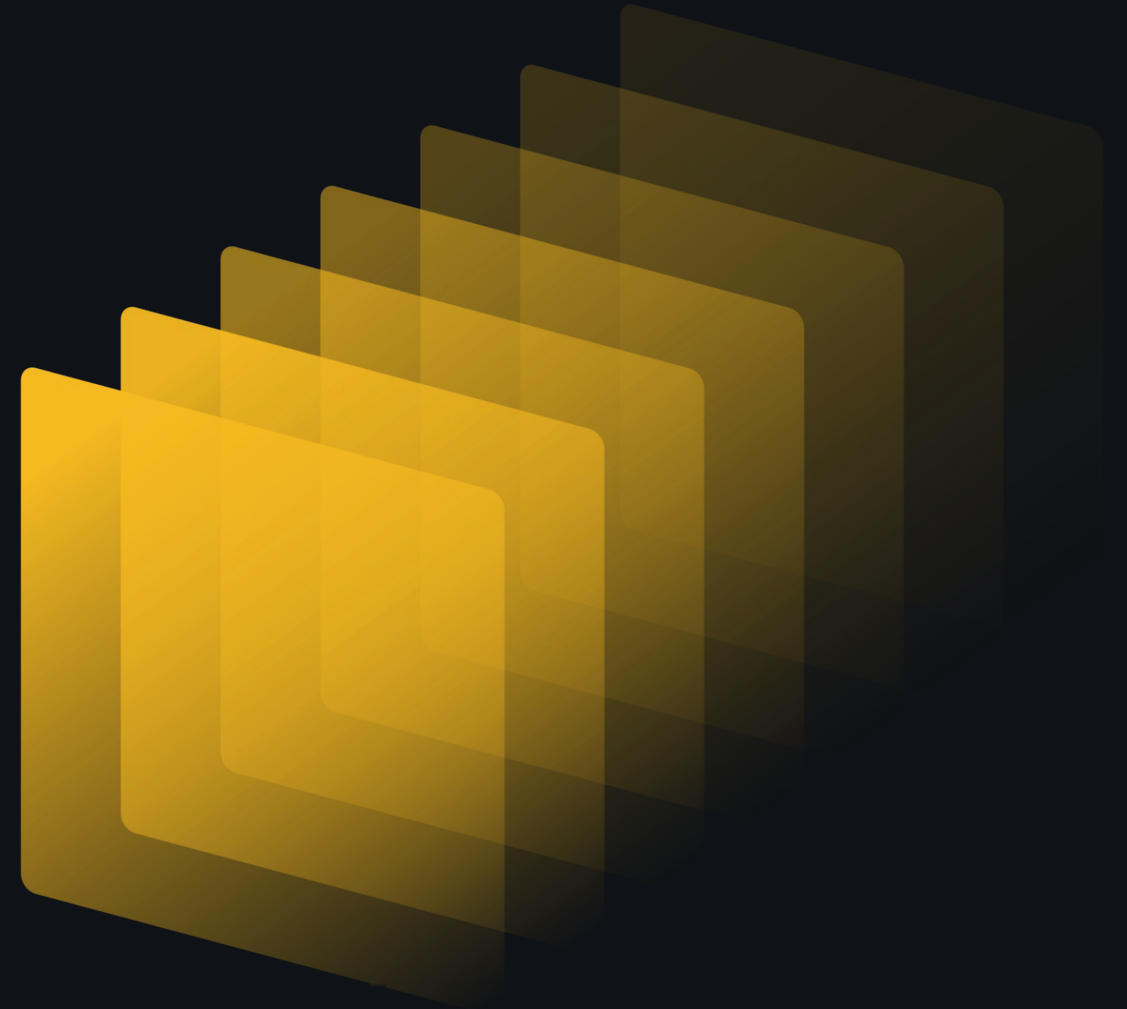


PRÄSENTATION

DevGuard Enterprise

Ihre Developer-Security-Plattform im eigenen Rechenzentrum:
mit vertraglich zugesicherten Service-Levels, geprüften
Updates und einem festen Vertragspartner.



Herausgeberin

L3montree GmbH, Bonn

Klassifizierung

TLP:AMBER

Stand

29. September 2026

Referenzdokument

L3-DG-ENT-2026-02

Was Sie in dieser Präsentation erwartet

Von der regulatorischen Ausgangslage über die Plattform bis zu Paketen, Service-Levels und Preisen für den Betrieb in Ihrem Rechenzentrum.

GRUNDLAGE

Informationsblatt DevGuard Enterprise (L3-DG-ENT-2026-02), Stand 29. September 2026

01

Ausgangslage

Warum Schwachstellenmanagement heute eine Nachweispflicht ist

02

Die Plattform

Was DevGuard entlang des Softwarelebenszyklus leistet

03

Betrieb im eigenen Rechenzentrum

Betriebsmodelle und Leistungen im Enterprise-Vertrag

04

Pakete

Service-Level, Kontingente und Konditionen

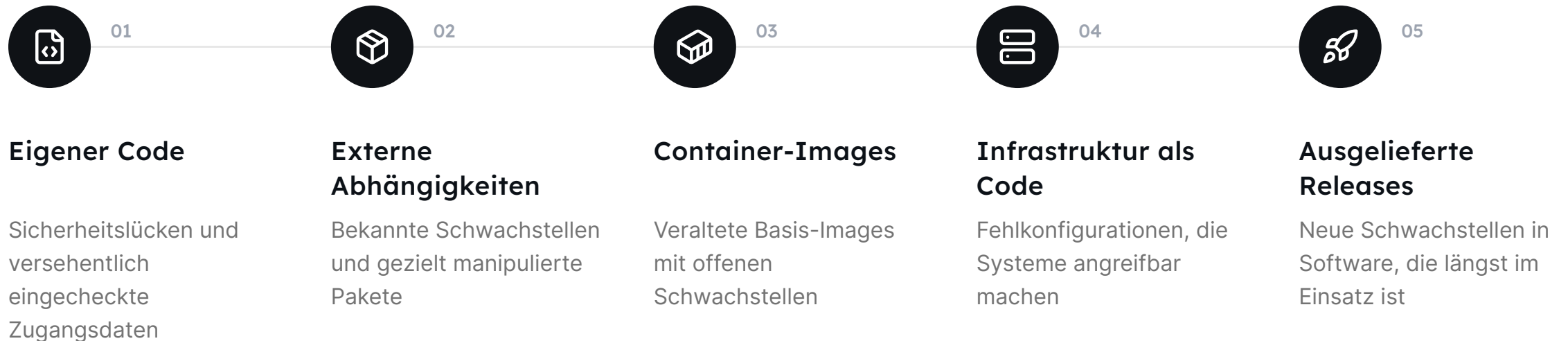
05

Nächste Schritte

Wie wir gemeinsam starten

Sicherheitsrisiken entstehen an jeder Stelle der Softwarelieferkette

Moderne Software besteht zum größten Teil aus Komponenten, die nicht im eigenen Haus entstanden sind. Verantwortlich für sie ist dennoch, wer die Software ausliefert.



Das Problem: Klassische Werkzeuge prüfen jeweils nur einen Ausschnitt – mit eigenen Oberflächen, eigenen Listen und ohne gemeinsamen Prozess.

Aus Sorgfalt wird eine Nachweispflicht

Der Cyber Resilience Act und die NIS-2-Umsetzung verlangen, bekannte Schwachstellen zu erkennen, zu bewerten, zu beheben – und den Vorgang zu belegen.

01

Erkennen

Schwachstellen in eigenem Code und in allen eingesetzten Komponenten kennen.

RELEVANTE REGELWERKE

Cyber Resilience Act (EU)

02

Bewerten

Einschätzen, ob und wie stark eine Schwachstelle Ihr Produkt tatsächlich betrifft.

NIS-2 / BSIG

03

Beheben

Betroffene Komponenten aktualisieren oder Risiken nachvollziehbar mindern.

ISO 27001

04

Belegen

Jeden Schritt so dokumentieren, dass Aufsicht, Auditoren und Kunden ihn prüfen können.

BSI IT-Grundschutz

Angaben zu Rechtsnormen dienen der Orientierung und ersetzen keine Rechtsberatung.

Dieselbe Schwachstelle wird in jeder Organisation neu bewertet

Ohne einen Weg, Bewertungen effizient zu teilen, wird dieselbe Triage-Arbeit tausendfach wiederholt. Für einen Qualitätsanspruch, der dauerhaft gilt und gesetzlich eingefordert wird, ist das die falsche Grundlage.

WAS ES IST

Triage ist die fachliche Prüfung, ob eine gemeldete Schwachstelle im eigenen Produkt tatsächlich ausnutzbar ist.

WAS ES FÜR SIE BEDEUTET

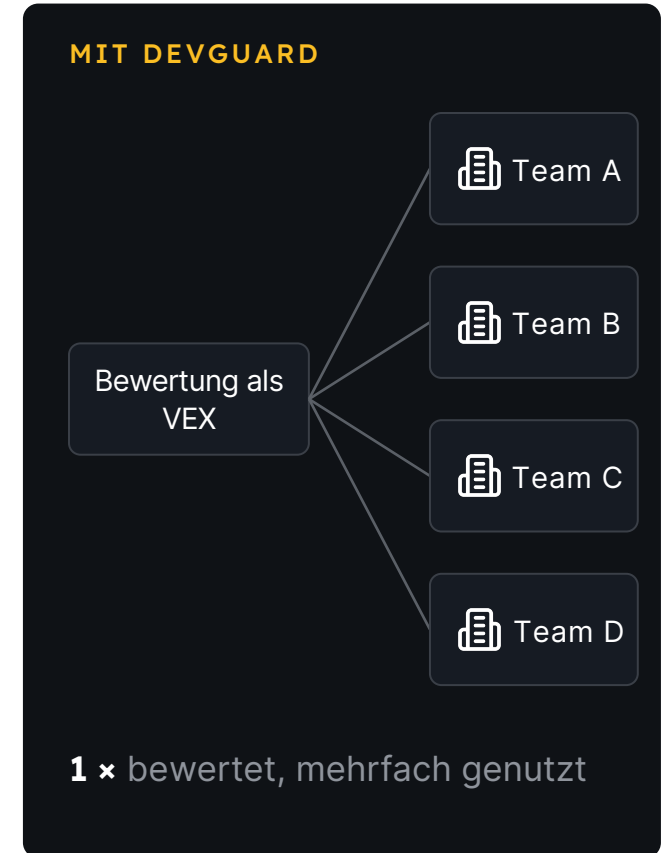
Hochqualifizierte Arbeitszeit, die heute in jeder Organisation und deren Entwicklungsteams für dieselbe Frage aufgewendet wird.

HEUTE



4 × dieselbe Arbeit

MIT DEVGUARD



1 × bewertet, mehrfach genutzt

DevGuard bündelt Schwachstellen- und Lieferkettenmanagement in einer Plattform

Vom Abwehren schädlicher Pakete vor dem Download über Prüfungen in der Pipeline bis zum fortlaufenden Monitoring ausgelieferter Releases – dort, wo Software entsteht, und ohne Spezialwissen in den Entwicklungsteams.

AGPL-3.0

Quelloffen, ohne Lizenzkosten und ohne Lock-in

Aus Deutschland

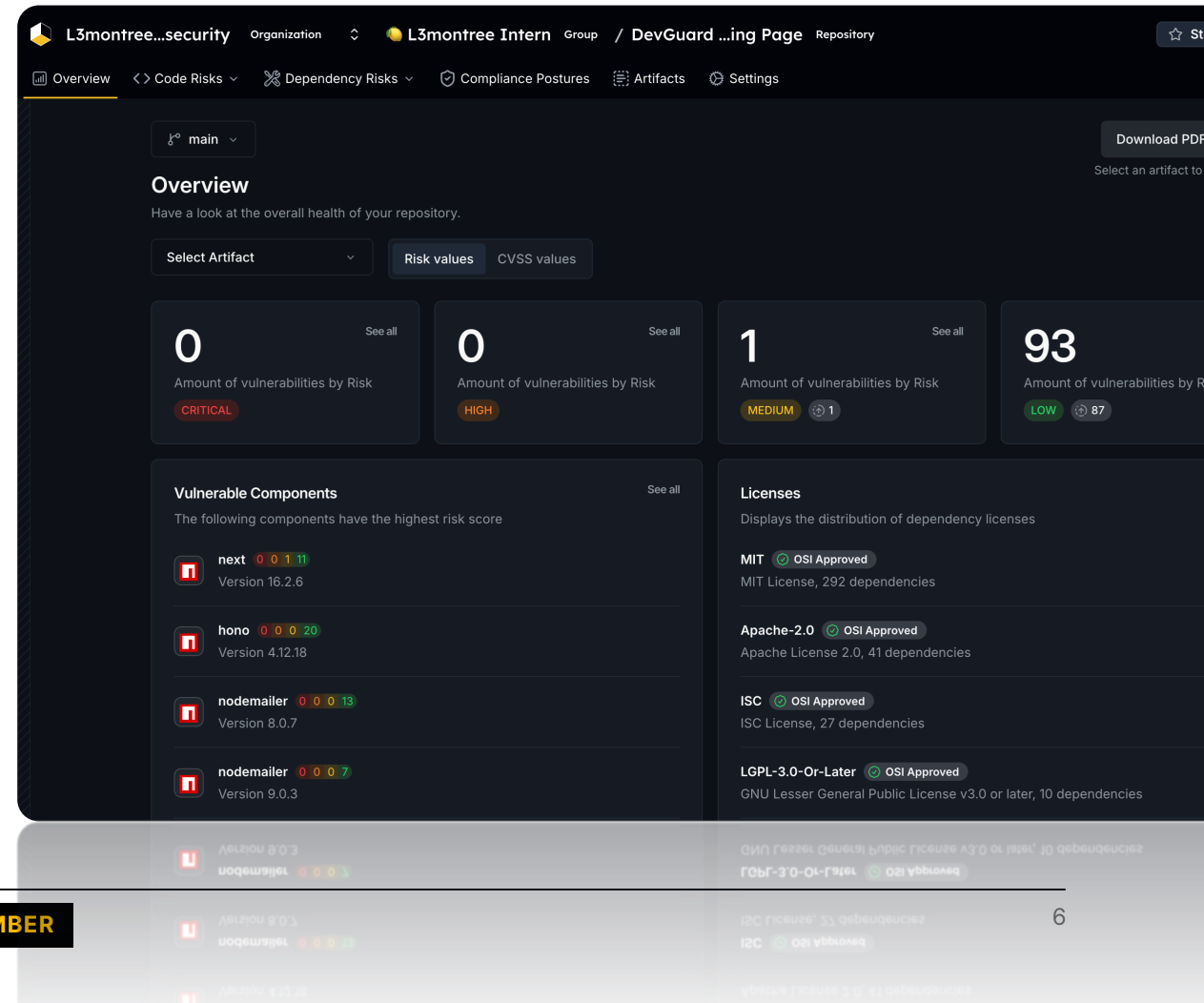
Entwickelt von der L3montree GmbH in Bonn, mit dem openCode-Team des ZenDiS

OWASP

Anerkannt als Incubation Project der OWASP Foundation

Offene Standards

CycloneDX, VEX, CSAF, SARIF, SLSA und OSCAL

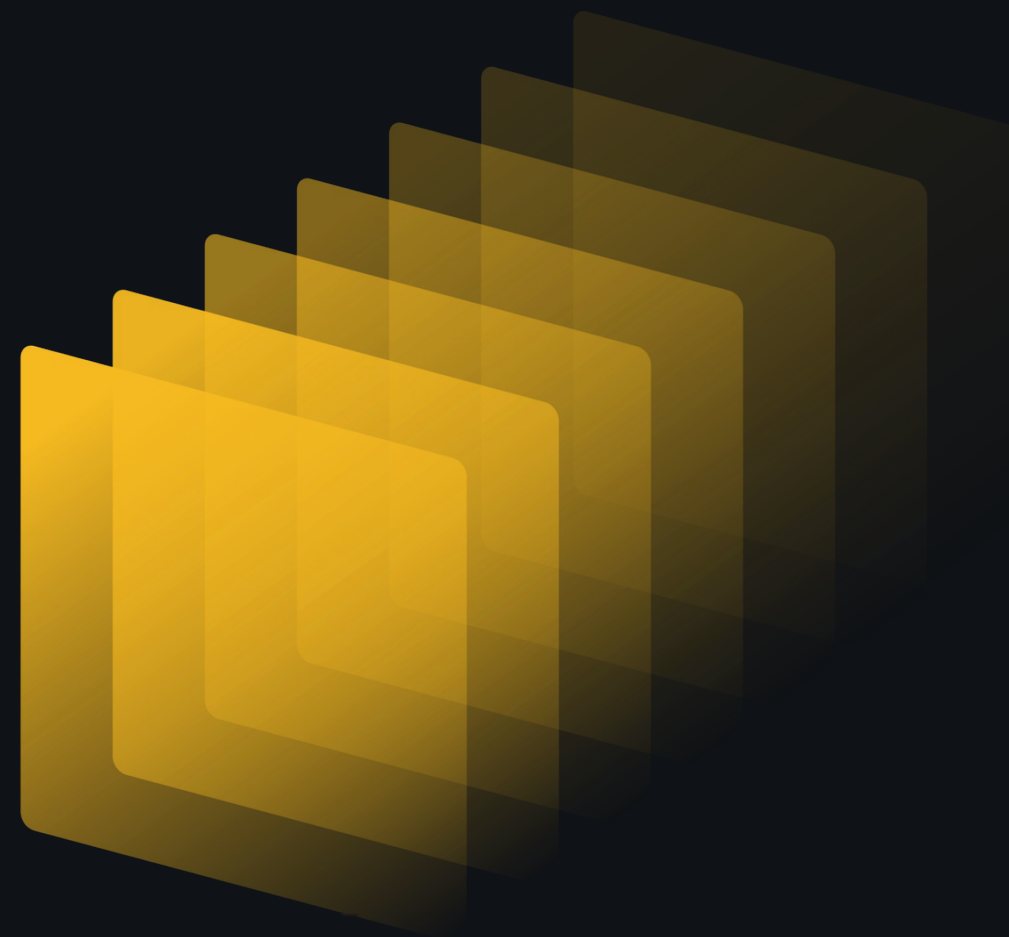
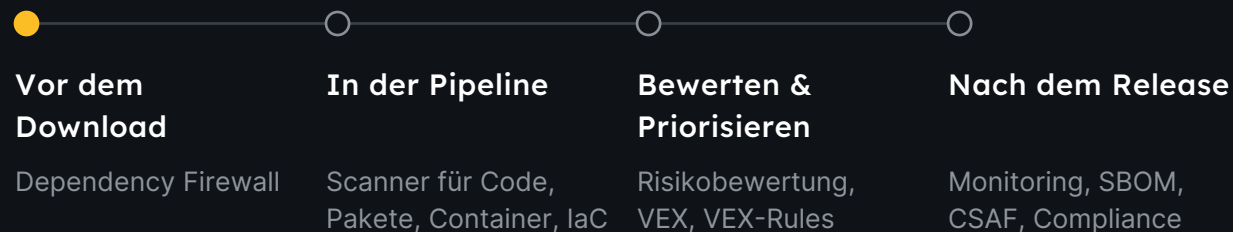


02

ABSCHNITT 02

Die Plattform

Was DevGuard entlang des Softwarelebenszyklus leistet – und was das für Ihre Organisation bedeutet.



Schädliche Pakete werden blockiert, bevor sie Ihren Code erreichen

Dependency Firewall

WAS ES IST

Eine Kontrollstelle zwischen Ihren Builds und den öffentlichen Paketquellen. Jede Anfrage wird zuerst gegen eine Datenbank bekannter Schadpakete geprüft.

WAS ES FÜR SIE BEDEUTET

Manipulierte Pakete gelangen gar nicht erst in Ihre Software, statt im Nachhinein gemeldet zu werden.

- ✓ npm, Go, PyPI und Container-Images an einem Kontrollpunkt
- ✓ Eigene Regeln je Organisation, Projekt oder Repository
- ✓ Wartefrist für neue Paketversionen für npm, PyPI, Go, Java, PHP & Debian
- ✓ Betrieb samt Paket-Cache vollständig bei Ihnen

```
ci-runner — build

$ npm install @ctrl/tinycolor
npm error 403 Forbidden
npm error X-Malicious-Package: blocked

reason: Package @ctrl/tinycolor is flagged
as malicious (ID: MAL-2025-47141)
```

237.726

Schadpaket-Meldungen, gegen die jede Anfrage geprüft wird (Stand September 2026)

6

Paket-Ökosysteme über einen einzigen Zugangspunkt: npm, Go, PyPI, Java, PHP und OCI

Alle zentralen Sicherheitsprüfungen laufen in Ihrer bestehenden Pipeline

Eine Kommandozeile bündelt etablierte Open-Source-Scanner. Fertige Bausteine für GitHub Actions und GitLab CI – die Integration dauert weniger als zehn Minuten.



Abhängigkeitsanalyse

Prüft eingebundene Fremdkomponenten auf bekannte Schwachstellen.

SCA Basis: Trivy



Statische Codeanalyse

Findet Sicherheitslücken im Code Ihrer Teams, bevor er ausgeliefert wird.

SAST Basis: Semgrep



Secret Scanning

Erkennt versehentlich eingetragene Passwörter, Schlüssel und Tokens.

SECRETS Basis: Gitleaks



Container-Scanning

Prüft Container-Images samt Basis-Image auf bekannte Schwachstellen.

CONTAINER Basis: Trivy



Infrastruktur als Code

Findet Fehlkonfigurationen in Infrastrukturbeschreibungen.

IAC Basis: Checkov



Lizenzprüfung

Zeigt, welche Lizenzen Ihre Abhängigkeiten mitbringen.

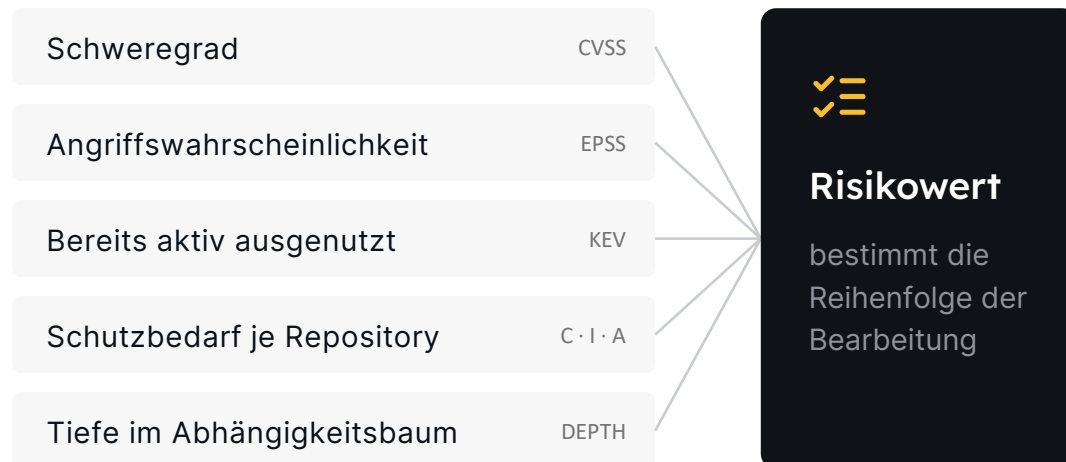
LICENSE License Compliance

Vorhandene Scanner weiter nutzen: Ergebnisse anderer Werkzeuge lassen sich als Stückliste (CycloneDX-SBOM) oder Scan-Bericht (SARIF) übernehmen.

Ihr Team bearbeitet zuerst, was tatsächlich riskant ist

Risikobasierte Priorisierung

DevGuard bewertet jede Schwachstelle nicht nur nach ihrem Schweregrad, sondern auch danach, wie wahrscheinlich ein Angriff ist und wie tief die Komponente in Ihrer Software steckt.



VEX und wiederverwendbare Bewertungen

WAS ES IST

Eine maschinenlesbare Aussage, ob eine Schwachstelle Ihr Produkt tatsächlich betrifft, samt Begründung.

WAS ES FÜR SIE BEDEUTET

Nicht relevante Meldungen werden nachvollziehbar abgeschlossen, statt immer wieder aufzutauchen.



VEX-Rules

Bewertungen einmal treffen und projektübergreifend als Regel nutzen.



Instanzübergreifender Austausch (optional)

Fremde Bewertungen als Empfehlung; Ihre Regeln haben Vorrang.



Import und Export

Bewertungen von Zulieferern übernehmen, an Abnehmer weitergeben.

Nachweise entstehen nebenbei und bleiben aktuell

Die Nachweise, die Aufsicht, Auditoren, Marktüberwachung und Kunden verlangen, entstehen als Nebenprodukt der Entwicklung – nicht als nachgelagerte Dokumentationsaufgabe.



Fortlaufendes Monitoring

Neue Schwachstellen werden auch in bereits ausgelieferten Releases erkannt.



Security Advisories (CSAF)

Eigene Sicherheitshinweise maschinenlesbar im offenen Standard CSAF veröffentlichen.



Attestierung

Herkunft und Bauprozess Ihrer Artefakte signiert belegen: SLSA-Provenance, in-toto, cosign.



SBOM je Release

Eine Stückliste Ihrer Software (CycloneDX): jederzeit belegbar, welche Komponenten in welcher Version stecken – auch als Live-Endpunkt.

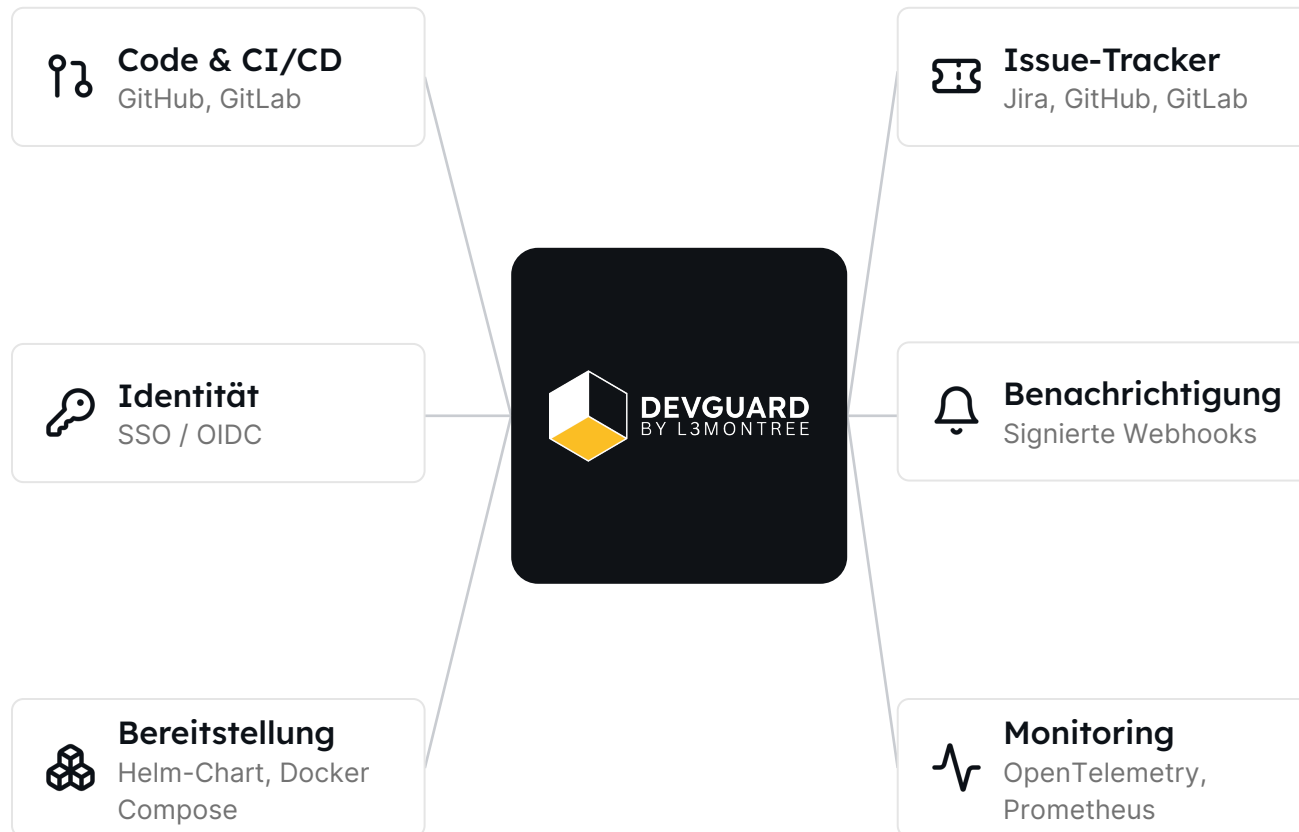


Compliance Posture

Controls aus ISO 27001, BSI IT-Grundschutz u. a. nachverfolgen; Export als maschinenlesbares Sicherheitskonzept (OSCAL).



DevGuard fügt sich in Ihre bestehende Werkzeuglandschaft ein



Kein zusätzliches Portal

Entwickler arbeiten weiter in Pull- und Merge-Requests, in der CI und im Issue-Tracker – ohne Parallelprozess. Die Anbindung an Jira, GitHub und GitLab funktioniert in beide Richtungen.

Betrieb nach Ihren Standards

Bereitstellung über Helm-Chart oder Docker Compose, Access Tokens mit Ablaufdatum und verschlüsselte Integrations-Secrets.

Strukturen übernehmen

Gruppen, Projekte und Berechtigungen lassen sich aus GitLab bzw. openCode synchronisieren.

Drei Betriebsmodelle – eines verbindet Datenhoheit mit vertraglicher Absicherung

1

SaaS

Wir betreiben DevGuard für Sie. Sie benötigen keine eigene Infrastruktur und starten ohne Installationsaufwand.

DATENHALTUNG

Bei L3montree, gehostet in Deutschland

BETRIEB UND UPDATES

Betrieb, Updates und Verfügbarkeit liegen bei uns

2

Self-Hosting

Quelloffen unter AGPL-3.0 und ohne Lizenzkosten in Ihrem Rechenzentrum, zum Beispiel über unser Helm-Chart.

DATENHALTUNG

In Ihrem Rechenzentrum

BETRIEB UND UPDATES

Vollständig bei Ihnen; Community-Support ohne zugesagte Reaktionszeiten

3

Gegenstand dieser Präsentation

Self-Hosting mit Enterprise-Vertrag

Plattform und Daten bleiben bei Ihnen, abgesichert durch vertragliche Reaktionszeiten, geprüfte Updates und einen festen Vertragspartner.

DATENHALTUNG

In Ihrem Rechenzentrum

BETRIEB UND UPDATES

Bei Ihnen, abgesichert durch Service-Level und Wartung des Herausgebers

Ein Vertrag bündelt Einrichtung, Support und Wartung



01

Initiale Einrichtung

Gemeinsamer Blick auf Zielarchitektur und Entwicklungslandschaft. Bereitstellung über unser Helm-Chart, Anbindung an CI/CD, SSO/OIDC und Issue-Tracker, Best-Practice-Checkup Ihrer Pipelines und begleitetes Onboarding Ihres Teams.



02

Support mit definierten Service-Levels

Festes Kontingent an Support-Stunden, verbindliche Reaktionszeiten und klare Eskalationswege. Sie eskalieren an ein Team, das Ihre Installation kennt – nicht in ein öffentliches Issue-Tracking.



03

Wartung

Geprüfte Updates und, je nach Paket, begleitete Upgrades bei Breaking Changes. In der Stufe Mission Critical sind zusätzlich Security-Backports auf das vorherige Minor-Release möglich.



Geregeltes Lieferantenverhältnis. Der Vertrag begründet ein Lieferantenverhältnis zum Herausgeber – ein Baustein für die Lieferantenbewertung, die NIS-2, viele Regelwerke und interne Richtlinien für Drittkomponenten verlangen.

Service-Level und Kontingente im Detail

Leistung	Enterprise Standard	Enterprise Advanced	Mission Critical / LTS
Servicezeiten ¹	Werktags 9–17 Uhr	Werktags 8–18 Uhr	Werktags 8–20 Uhr
Rufbereitschaft ¹	–	–	Nicht-Werktage 10–17 Uhr (8 h Reaktionszeit)
Reaktionszeit ²	max. 16 h	max. 8 h	max. 4 h
Behebungszeit ³	max. 18 Arbeitstage	max. 10 Arbeitstage	max. 5 Arbeitstage
Kanäle	Dedizierte E-Mail	zzgl. Chat (Matrix) und Telefon	Beliebiger Kanal nach Vereinbarung
Priority Support, Senior Engineers	–	–	Vorrangige Bearbeitung; direkter Zugang in kritischen Fällen
Support-Stunden pro Jahr ⁴	20 h	80 h	160 h
davon benannte Ansprechperson ⁴	–	20 h	50 h
Vor-Ort-Tage pro Jahr (DE) ⁵	–	1	3
Wartung	Latest-stable-Release-Stream, Patches und Sicherheitsfixes im Rahmen der SLA	Wie Standard, zzgl. begleitete Major-Upgrades bei Breaking Changes	Wie Advanced, zzgl. Security-Backports auf das vorherige Minor-Release möglich
Begleitete Upgrade-Fenster	–	In regulären Servicezeiten	Auch außerhalb der Geschäftszeiten (max. 2× pro Jahr)

HINWEISE

- 1 Alle Zeiten MEZ/MESZ. Werktage sind Mo–Fr ohne gesetzliche Feiertage in NRW sowie 24. und 31. Dezember. Rufbereitschaft nur für schwerwiegende Störungen des Produktivbetriebs.
- 2 Vom Eingang einer einordbaren Störungsmeldung über einen vereinbarten Kanal bis zur ersten qualifizierten Rückmeldung einer Person; läuft nur in den Servicezeiten.
- 3 Gilt bei Installation gemäß dokumentierter Referenzarchitektur. Bei schwerwiegenden Störungen ggf. zunächst als Workaround.
- 4 Je Vertragsjahr; nicht genutzte Stunden verfallen zum Ende des Vertragsjahres. Separat gekaufte Stundenpakete sind 24 Monate abrufbar.
- 5 Für gemeinsame Arbeit an Installation und Prozessen. Reisekosten nach Aufwand; weitere Tage zubuchbar.

Sie können jedes DevGuard-Release selbst prüfen, statt uns vertrauen zu müssen

PRÜFEN STATT VERTRAUEN

Herkunft, Komponenten
und
Schwachstellenstatus
jedes Releases sind
dokumentiert.

Das ist die Grundlage dafür, DevGuard selbst
in Ihr Lieferantenmanagement aufzunehmen.



Reproduzierbar gebaute, gehärtete Images

Bit-genau reproduzierbares Container-Image mit minimierter Angriffsfläche. Herkunft und Bauprozess sind über SLSA-Provenance belegt und mit cosign unabhängig prüfbar.



SBOM je Release

Zu jedem Artefakt gehört eine CycloneDX-SBOM als Attestation. Damit ist jederzeit belegbar, aus welchen Komponenten Ihre Installation besteht.



VEX-basierte CVE-Behandlung

Wir bewerten Schwachstellen in DevGuard und seinen Abhängigkeiten und veröffentlichen das Ergebnis als CycloneDX-VEX-Statement: eine Aussage zur Betroffenheit statt einer Rohmeldung Ihres Scanners.

Was Organisationen vor einem Enterprise-Vertrag klären möchten

01 Warum ein Servicepaket, wenn DevGuard quelloffen ist?

Die Software ist frei verfügbar. Das Servicepaket sichert ihren Betrieb ab: verbindliche Reaktionszeiten, vom Herausgeber geprüfte Updates und ein Vertragspartner, der im Ernstfall handelt.

02 Was passiert, wenn DevGuard selbst eine Schwachstelle hat?

Wir informieren Sie aktiv über den vereinbarten Kanal, soweit möglich vor der Veröffentlichung – mit Einordnung der betroffenen Versionen, Handlungsempfehlung und geprüfem Fix.

03 Wie unterstützt der Vertrag unsere Lieferantenbewertung nach NIS-2?

Benannte Ansprechpartner, zugesagte Reaktionszeiten und eine nachvollziehbare Update-Versorgung sind Bausteine Ihrer Nachweisführung.

04 Wofür können wir die Support-Stunden einsetzen?

Nicht nur für Störungen: auch für Schulungen, Prozessabstimmung und den Austausch zur Bewertungspraxis. Für Individualentwicklung können die Stunden nicht verwendet werden.

Was Anwender über DevGuard sagen

640+

Projekte auf openCode nutzen DevGuard · Stand August 2026

“

DevGuard schafft es, durch moderne Software-Security-Konzepte unseren Entwicklern und Nutzern auf openCode einen benutzerfreundlichen Einstieg in die Best Practices des Schwachstellenmanagements zu ermöglichen, ohne dabei Abstriche in der Enterprisefähigkeit zu machen.

Julian Schauder

DevSecOps & Development Lead, ZenDiS GmbH



“

Als Hersteller von Security-Lösungen ist eine sichere Softwareentwicklung für uns unerlässlich. Mit DevGuard haben wir ein präzises Tool gefunden, mit dem sich hochsichere Software effizient und zuverlässig entwickeln lässt.

Vincent Breitmoser

CTO & Co-Founder, Heylogin GmbH

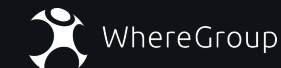


“

Als Hersteller von Open-Source-Geoinformationssystemen muss unsere Software nicht nur genaue Daten liefern, sondern auch besonders sicher sein, um in kritischen Infrastrukturen eingesetzt werden zu können. Daher freuen wir uns sehr über Software-Security-Tools wie DevGuard. Diese erleichtern nicht nur die Entwicklung sicherer Software, sondern sind auch Open Source!

Peter Stamm

Geschäftsführer, WhereGroup GmbH



Wie wir gemeinsam starten

01

Einführungsgespräch

30 Minuten zu Ihrer Ausgangslage, Ihren Anforderungen und der passenden Paketstufe.

02

Zielarchitektur und Angebot

Wir betrachten gemeinsam Ihre Zielarchitektur und erstellen Ihnen ein individuelles Angebot.

03

Einrichtung und Onboarding

Bereitstellung über unser Helm-Chart oder Docker Deployment, Anbindung an Ihre Systeme und begleitetes Onboarding Ihres Teams.

Vorab ausprobieren: DevGuard ist quelloffen und lässt sich jederzeit selbst evaluieren – oder 14 Tage kostenlos als SaaS testen.

IHR KONTAKT



Frédéric Noppe

COO, L3montree GmbH

✉ requests@devguard.org

🌐 devguard.org/enterprise

📅 Termin online buchen

DevGuard Enterprise

Leistungspakete, Service-Level und Preise für den Betrieb von DevGuard in der eigenen Infrastruktur.

Dokumentinformationen

Version	1.0
Stand	29. September 2026
Klassifizierung	TLP:AMBER
Grundlage	Infoblatt L3-DG-ENT-2026-02

Herausgeberin

L3montree GmbH
Markt 3
53111 Bonn
requests@devguard.org
devguard.org

Rechtlicher Hinweis

Diese Präsentation ist als TLP:AMBER eingestuft. Sie ist für die Empfängerorganisation und die dort mit der Bewertung eines möglichen Vertragsverhältnisses befassten Personen bestimmt. Eine Weitergabe an Dritte bedarf der vorherigen schriftlichen Zustimmung der L3montree GmbH.

Urheberrecht

© 2026 L3montree GmbH. Alle Rechte vorbehalten. Die hier beschriebene Software DevGuard steht unter der GNU Affero General Public License (AGPL-3.0); diese Präsentation selbst ist davon nicht erfasst und darf ohne vorherige schriftliche Zustimmung weder vervielfältigt noch verbreitet werden.

Vorbehalt

Die dargestellten Leistungen, Service-Level und Preise dienen der Information und stellen kein bindendes Angebot dar. Maßgeblich ist allein der schriftlich geschlossene Vertrag. Alle Preise verstehen sich netto in Euro zzgl. gesetzlicher Umsatzsteuer. Angaben zu Rechtsnormen geben den Stand bei Drucklegung wieder, dienen der Orientierung und ersetzen keine Rechtsberatung.

PROJEKTPARTNER & ORGANISATIONEN, DIE DEVGUARD EINSETZEN

