WHITEPAPER

Weniger Schwachstellen, weniger Meldelast

Container-Härtung als praktischer Hebel für CRA, NIS2 und DORA. Warum KI-gestützte Schwachstellenentdeckung die Uhr beschleunigt, das Patchen allein nicht mehr genügt und was Ihre Container-Teams jetzt tun können.

CONTAINER-SICHERHEIT | EU-COMPLIANCE | KI-BEDROHUNGSLAGE

11.09.2026
CRA-Meldepflicht (Art. 14)
Volle Anwendung ab 11.12.2027

06.12.2025
NIS2 in Deutschland in Kraft
NIS2UmsuCG, keine Übergangsfrist

17.01.2025
DORA anwendbar
Finanzsektor

Für Security-Verantwortliche, CISOs, DevSecOps-Teams und Compliance-Officer

INHALT

AUF EINEN BLICK

Regelwerke	CRA (VO (EU) 2024/2847), NIS2 (in DE: NIS2UmsuCG, BSIG), DORA (VO (EU) 2022/2554)
Scharf für DACH ab	NIS2 seit 06.12.2025, DORA seit 17.01.2025, CRA-Meldepflicht ab 11.09.2026, volle CRA-Anwendung ab 11.12.2027
Gemeinsamer Nenner	Schwachstellenbehandlung, schnelle Vorfallmeldung, Kontrolle von Lieferkette und Drittanbietern
Betroffen	Produkthersteller, wesentliche und wichtige Einrichtungen, Finanzunternehmen und ihre IKT-Dienstleister
Kern der Antwort	Angriffsfläche an der Quelle reduzieren, ohne Änderungen an Code, Betriebssystem oder Pipeline

FÜR WEN DIESES WHITEPAPER GEDACHT IST

Geschrieben für Security- und Engineering-Verantwortliche: CISOs, DevSecOps-Teams, Platform-Engineers und Compliance-Officer, die Cloud-native-Workloads mit EU-Bezug verantworten.

RAPIDFORT IN ZAHLEN

Bis zu 99,9%
weniger CVEs
Automatisch, in Stunden statt Monaten

Bis zu 90%
kleinere Angriffsfläche
Ohne Änderung an Code oder Pipeline

7/10
führende KI-Unternehmen
Im Einsatz über Kundenumgebungen hinweg

01 Einleitung

Der Cyber Resilience Act (CRA), die NIS2-Richtlinie und der Digital Operational Resilience Act (DORA) werden oft als drei getrennte Compliance-Projekte behandelt. Für Container- und Cloud-native-Teams laufen sie auf dieselbe operative Anforderung hinaus.

Sie müssen Ihre Komponenten kennen, die Zahl der ausnutzbaren Schwachstellen niedrig halten und schnell melden, sobald etwas aktiv ausgenutzt wird. Die rechtliche Verpackung unterscheidet sich, die technische Arbeit darunter ist dieselbe. Alle drei Regelwerke sind für den DACH-Raum bereits konkret. NIS2 gilt in Deutschland seit dem 6. Dezember 2025 ohne Übergangsfrist. DORA ist im Finanzsektor seit dem 17. Januar 2025 anwendbar. Die CRA-Meldepflichten greifen ab dem 11. September 2026, die volle Anwendung folgt am 11. Dezember 2027.

Dieses Whitepaper zeigt, warum die Reduktion der Software-Angriffsfläche, und nicht allein das Patchen, der direkteste Hebel für alle drei Rahmen ist. Und wie RapidFort das ohne Änderungen an Code, Betriebssystem oder Pipeline erreicht.

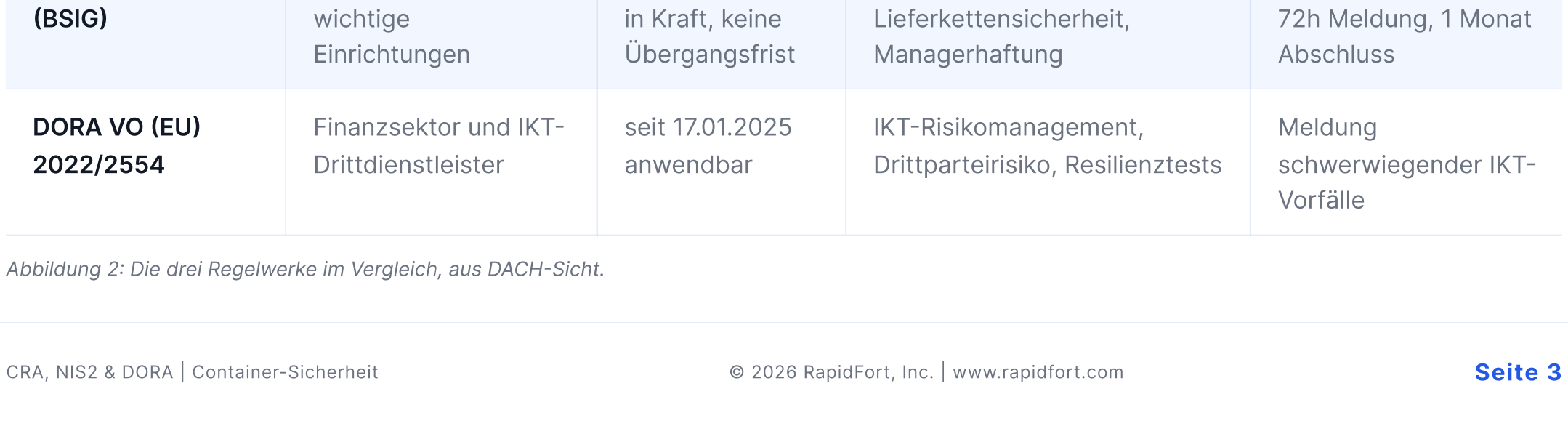

Abbildung 1: Der regulatorische Zeitstrahl für DACH-Teams.

02 Drei Regelwerke, ein gemeinsamer Nenner

CRA, NIS2 und DORA adressieren unterschiedliche Adressaten, verlangen aber im Kern dasselbe: Schwachstellen behandeln, Vorfälle schnell melden und die Lieferkette kontrollieren. Wer die Angriffsfläche seiner Container niedrig hält, arbeitet an allen drei gleichzeitig.

Regelwerk	Geltung für DACH	Scharf ab	Kernpflicht	Meldefenster
CRA VO (EU) 2024/2847	Produkte mit digitalen Elementen am EU-Markt	Meldepflicht ab 11.09.2026, volle Anw. ab 11.12.2027	Security by Design, Schwachstellenbehandlung, SBOM, fünf Jahre Support	24h Frühwarnung, 72h Meldung, 14 Tage Abschluss (Art. 14)
NIS2 NIS2UmsuCG (BSIG)	Wesentliche und wichtige Einrichtungen	seit 06.12.2025 in Kraft, keine Übergangsfrist	Risikomanagement, Lieferkettensicherheit, Managerhaftung	24h Frühwarnung, 72h Meldung, 1 Monat Abschluss
DORA VO (EU) 2022/2554	Finanzsektor und IKT-Drittdienstleister	seit 17.01.2025 anwendbar	IKT-Risikomanagement, Drittparteirisiko, Resilienztests	Meldung schwerwiegender IKT-Vorfälle

Abbildung 2: Die drei Regelwerke im Vergleich, aus DACH-Sicht.

DER GEMEINSAME NENNER

CRA verlangt Schwachstellenbehandlung und Lieferkettensorgfalt (Anhang I). NIS2 verlangt Risikomanagement inklusive Lieferkettensicherheit (§ 30 BSIG). DORA verlangt IKT-Risikomanagement und die Steuerung des Drittparteirisikos (Kapitel V). In allen drei Fällen ist die praktische Arbeit dieselbe: die Angriffsfläche reduzieren und dokumentieren.

OPEN SOURCE IM CRA

Open-Source-Software fällt erst dann unter den CRA, wenn sie kommerziell bereitgestellt wird. Nicht-kommerzielle Projekte sind ausgenommen. Organisationen, die solche Projekte systematisch monetarisieren, können jedoch als Software-Steward nach Artikel 24 in die Pflicht kommen.

03 Die Meldeuhr

Die Meldelast entsteht aus knappen Fristen. Jede aktiv ausgenutzte Schwachstelle kann eine Uhr starten. Je weniger ausnutzbare Schwachstellen Sie tragen, desto seltener beginnt sie zu laufen.

CRA, ARTIKEL 14

24h
FRÜHWARNUNG
Erstmeldung an den CSIRT-Koordinator und ENISA über die Single Reporting Platform

72h
MELDUNG
Detaillierte Angaben zu Produkt, Ausnutzung und Gegenmaßnahmen

14 T
ABSCHLUSS
Abschlussbericht nach verfügbarer Gegenmaßnahme, bei schweren Vorfällen ein Monat

Die Meldepflicht gilt auch für Bestandsprodukte, die bereits am EU-Markt sind.

NIS2 (BSIG)

Wesentliche und wichtige Einrichtungen melden an das BSI: eine Erstmeldung binnen 24 Stunden, eine Bewertung binnen 72 Stunden und eine Abschlussmeldung binnen eines Monats. Hinzu kommt die Registrierungspflicht der Einrichtung über das MUK-Portal des BSI.

DORA

Finanzunternehmen melden schwerwiegende IKT-bezogene Vorfälle an die zuständige Behörde nach festgelegten Fristen und können erhebliche Cyberbedrohungen freiwillig melden. Die Meldung an eine Stelle ersetzt parallele Pflichten aus NIS2 oder branchenspezifischen Regimen nicht.

KOSTEN DES NICHTHANDELNS

CRA sieht Bußgelder von bis zu 15 Mio. Euro oder 2,5% des weltweiten Jahresumsatzes vor. NIS2 in Deutschland bis zu 10 Mio. Euro oder 2% (besonders wichtige Einrichtungen) bzw. 7 Mio. Euro oder 1,4% (wichtige Einrichtungen), zusätzlich persönliche Haftung der Geschäftsleitung nach § 38 BSIG. DORA bis zu 2% des weltweiten Jahresumsatzes. Eventuelle Reputationsschäden sind unkalkulierbar.

04 Warum KI die Uhr beschleunigt

Die Meldeuhr wird nicht durch die Regulierung schneller, sondern durch die Angreiferseite. KI-gestützte Werkzeuge entdecken Schwachstellen schneller und über größere Codebestände hinweg, als klassische Patch-Zyklen es vorsehen.

Anthropics Red-Team berichtet, dass das Modell Claude Mythos Preview Schwachstellen in den meisten großen Betriebssystemen und Browsern eigenständig gefunden und ausgenutzt hat. Nach Angaben von Anthropic wurden mehr als 23.000 potenzielle Schwachstellen über mehr als 1.000 Open-Source-Projekte hinweg identifiziert, wobei der Zugang auf etwa 50 Organisationen im Rahmen von Project Glasswing beschränkt ist. Über 99% dieser Funde sind bislang nicht gepatcht. Das britische AI Security Institute bestätigt unabhängig einen deutlichen Kapazitätssprung.

Entdeckung skaliert

KI findet Schwachstellen schneller und über weit größere Codebestände als menschliche Teams, in einem Tempo, für das kein klassischer Patch-Zyklus ausgelegt war.

Behebung nicht

Patchen, Validieren und Ausrollen laufen weiterhin in Menschengeschwindigkeit. Die Lücke zwischen bekannten und behobenen Schwachstellen wächst.

Ehrliche Einordnung

Unabhängige Tests zeigen, dass auch deutlich günstigere, offen verfügbare Modelle viele derselben Fehler finden. Die Bedrohung ist struktureller Natur: KI-beschleunigte Entdeckung ist gekommen und reproduzierbar, sie hängt nicht an einem einzelnen, beschränkten Modell. Für Ihre Planung ist das der wichtigere Punkt.

Was das für Container bedeutet

Basis-Images, Systembibliotheken und Open-Source-Abhängigkeiten in Kubernetes-Clustern sind genau die langlebige, breit verteilte Art von Code, die solche Werkzeuge zuerst ins Visier nehmen. In der Praxis liegt die Zeit bis zum Patch je nach Umgebung zwischen 30 und 90 Tagen, oft länger. Das Alan Turing Institute (CETAS) berichtet, dass über 45% der in großen Organisationen entdeckten Schwachstellen auch nach zwölf Monaten ungepatcht bleiben. Auf jede Schwachstelle einzeln zu reagieren, ist damit keine belastbare Haltung mehr.

Ist Ihre Umgebung darauf vorbereitet?

Das RapidFort Readiness Assessment gibt Ihnen eine klare, priorisierte Sicht auf Ihre tatsächliche Exposition, ohne Code-Änderungen und mit Ergebnissen innerhalb von Minuten.

Kostenloses Assessment Anfordern ↗

05 Der eigentliche Hebel: Angriffsfläche reduzieren

Die meisten CVEs in einem Container stecken in Code, den die Anwendung nie ausführt. Entfernt man diesen Code vor der Produktion, verschwindet die Schwachstelle und die Meldepflicht zugleich. Das ist der Unterschied zwischen Reduzieren und immer nur Patchen. RapidFort entfernt ungenutzte Komponenten automatisch aus Basis-Images und Abhängigkeiten. Das Ergebnis: bis zu 99,9% weniger CVEs und eine bis zu 90% kleinere Angriffsfläche, ohne Änderungen an Code, Betriebssystem oder Pipeline. Der kuratierte Katalog umfasst mehr als 35.000 gehärtete, near-zero-CVE Basis-Images. Betrieb im Air-Gap und vollständig on-premises wird unterstützt, was für digitale Souveränität im DACH-Raum relevant ist.

Bis zu 99,9%
weniger CVEs
Automatisch, in Stunden statt Monaten

Bis zu 90%
kleinere Angriffsfläche
Ohne Änderung an Code oder Pipeline

35.000+
gehärtete Basis-Images
Near-zero-CVE, kontinuierlich gepatcht

Ererbte statt selbst geschriebene Schwachstellen

Der Großteil des Risikos in einem Container stammt nicht aus Ihrem Code, sondern wird aus dem Basis-Image geerbt. Minimierung setzt genau an diesem ererbten Ballast an.

KI- und ML-Workloads (CUDA)

Wer eigene KI-, ML- oder Quant-Workloads baut, trägt besonders große Images. RapidFort entfernt ungenutzte Build-Werkzeuge, CUDA- und Interpreter-Bibliotheken sowie reine Trainingsabhängigkeiten und verkleinert Images um bis zu 80%, ohne Änderungen an Modell oder Code.

Der Nutzen ist doppelt. Kleinere Images senken Registry-Speicher, verkürzen Pull-Zeiten und beschleunigen Kaltstarts sowie die Wiederherstellung beim Autoscaling. Und jede entfernte Bibliothek ist eine Bibliothek, die keine meldepflichtige Schwachstelle mehr tragen kann. Unter CRA, NIS2 und DORA zählt genau das.

EFFIZIENZ

Bis zu 80% kleinere KI-/ML-Images — ohne Änderungen an Modell oder Code. Kürzere Pull-Zeiten, schnellere Kaltstarts.

COMPLIANCE

Jede entfernte Bibliothek ist eine Bibliothek, die keine meldepflichtige Schwachstelle mehr tragen kann. Unter CRA, NIS2 und DORA zählt genau das.

06 In der Praxis: von SBOM zu RBOM®

Vier Bereiche geben jedem Cloud-native-Team einen belastbaren Startpunkt.

01. Minimal-Container

Von gehärteten, near-zero-CVE Basis-Images ausgehen. Ungenutzte Software vor der Produktion entfernen und so die Angriffsfläche senken.

02. SBOM um RBOM® ergänzen

Laufzeitprofiling zeigt, welche Komponenten tatsächlich erreichbar sind. Das priorisiert die Behebung und dokumentiert risikobasierte Schwachstellenbehandlung, mit bis zu 25% weniger Rauschen.

03. Verteilungsstrategie

Konsistente Registry-Standards über alle Umgebungen. Sicherheitsupdates nachvollziehbar an Kunden ausliefern, passend zum Fünf-Jahres-Support des CRA.

04. Lieferkette absichern

Herkunft und Reaktionsgeschwindigkeit der genutzten Images kennen. Unabhängige Prüfung auf Manipulation und Malware über ReversingLabs Spectra Assure.

SBOM
zeigt, was **installiert** ist.

RBOM®
zeigt, was **läuft**.

Eine statische Stückliste allein senkt kein Risiko. Erst der Abgleich mit der Laufzeit-Erreichbarkeit trennt die Schwachstellen, die zählen, von denen, die nie ausgeführt werden. Die ReversingLabs-Integration (Spectra Assure) ist für Python und Java allgemein verfügbar, JavaScript befindet sich in geschlossener Beta.

07 Wie RapidFort CRA, NIS2 und DORA adressiert

RapidFort beseitigt Schwachstellen an der Quelle und unterstützt so die Anforderungen aller drei Regelwerke. RapidFort erfüllt keine Compliance stellvertretend, sondern liefert den technischen Beitrag, auf dem Ihre Nachweise aufsetzen.

Regelwerkübergreifende Anforderung	Verankert in	RapidFort-Beitrag
Angriffsfläche und Schwachstellen an der Quelle reduzieren	CRA Anhang I, NIS2 § 30 BSIG, DORA IKT-Risikomanagement	Automatische Entfernung ungenutzten Codes: bis zu 99,9% weniger CVEs und bis zu 90% kleinere Angriffsfläche, ohne Änderung an Code oder Pipeline
Komponenten dokumentieren und priorisieren	CRA Anhang I (SBOM), NIS2 § 30 BSIG, DORA Informationsregister	Automatisierte SBOM plus RBOM® zur Laufzeit-Erreichbarkeit, bis zu 25% weniger Rauschen
Lieferkette und Drittanbieter absichern	CRA Lieferkettenpflichten, NIS2 Lieferkettensicherheit, DORA Drittparteirisiko (Kapitel V)	Gehärtete Basis-Images (35.000+), ReversingLabs Spectra Assure zur unabhängigen Manipulations- und Malware-Prüfung
Meldelast senken	CRA Art. 14, NIS2 Meldepflichten, DORA Vorfallmeldung	Weniger aktiv ausnutzbare Schwachstellen bedeuten weniger meldepflichtige Ereignisse, plus kontinuierliche Baseline-Validierung
Nachweise für Aufsicht und Haftung	CRA technische Dokumentation, NIS2 § 38 Managerhaftung, DORA Nachweispflichten	Audit-fähige Berichte und durchgängiger Evidenztrail
Langfristige Wartung sicherstellen	CRA Fünf-Jahres-Support	Aktive Rebuild-Pipelines und kontinuierlich gepatchte Images
KI- und ML-Workloads verschlanken	Effizienz und Angriffsflächenreduktion	Entfernt ungenutzte CUDA-, Interpreter- und Trainingsbibliotheken: bis zu 80% kleinere Images, ohne Änderung an Modell oder Code

Tabelle 1: Regelwerkübergreifende Anforderungen und der RapidFort-Beitrag.

WARUM RAPIDFORT FÜR DIE COMPLIANCE-BEREITSCHAFT

CVE-Elimination ✓
Bis zu 99,9% der Schwachstellen automatisch entfernt

Gehärtete Images ✓
Near-zero-CVE, kontinuierlich gepatcht und geprüft

SBOM und RBOM® ✓
Bis zu 25% weniger Rauschen, plus Laufzeit-Priorisierung

Audit-Nachweise ✓
Kontinuierliche Baseline-Validierung und Evidenztrail

08 Kernaussagen

☑ **Sicherheit ist Produktanforderung, nicht nur Best Practice**
Eine minimale Angriffsfläche und sichere Voreinstellungen sind über CRA, NIS2 und DORA hinweg rechtlich verankert.

☑ **Weniger ausnutzbare Schwachstellen bedeuten weniger Meldelast**
Wer die Zahl der aktiv ausnutzbaren Schwachstellen senkt, startet die Meldeuhr seltener.

☑ **SBOM und RBOM® in CI/CD verankern**
Statische Stückliste und Laufzeit-Erreichbarkeit zusammen priorisieren die Behebung und dokumentieren risikobasiertes Vorgehen.

☑ **Fünf-Jahres-Horizont einplanen**
Jede an Kunden verteilte Container-Version braucht Rebuild-Pipeline, Update-Pfad und Kompatibilitätsplanung, wie der CRA es verlangt.

☑ **Angriffsfläche reduzieren statt nur patchen**
Im Tempo KI-gestützter Entdeckung ist das Entfernen ungenutzten Codes der einzige tragfähige Weg

ÜBER RAPIDFORT

RapidFort ist eine Software-Supply-Chain-Security-Plattform, die Schwachstellen an der Quelle beseitigt. Gegründet 2020, mit Hauptsitz im Silicon Valley, bedient RapidFort über 100 Unternehmens- und Public-Sector-Kunden, darunter 7 der 10 führenden KI-Unternehmen, mit kuratierten near-zero-CVE Basis-Images, Laufzeitprofiling und durchgängigem Attack-Surface-Management. Ausgezeichnet als Gartner Cool Vendor in Container Management.

Sprechen Sie mit RapidFort

Wenn Sie sich auf CRA, NIS2 und DORA vorbereiten und verstehen wollen, wie RapidFort Schwachstellen beseitigt, EU-Anforderungen unterstützt und KI-beschleunigten Bedrohungen zuvorkommt, sprechen Sie mit unserem Team.

Termin Vereinbaren ↗

IHR ANSPRECHPARTNER IN DACH
Felix D. Panter
Sales Director DACH
✉ felix@rapidfort.com
☎ +49 (0)176 23909690
RAPIDFORT