GIDS

De complete gids voor container security

Image scanning, runtime bescherming, Kubernetes beveiliging, kosten, NIS2 en trends. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Container-adoptie groeit explosief, maar de beveiliging blijft achter. Dit zijn de feiten.

82%
van containergebruikers draait Kubernetes in productie (was 66% in 2023)
CNCF Annual Survey 2025 [1]

100%
van ondervraagde Nederlandse organisaties is bezig met containerisatie
Nutanix ECI 2024 [2]

98%
van container CVE's zit buiten de top 20 populaire images -- de long tail is het probleem
Chainguard/InfoQ 2026 [3]

40%
van organisaties heeft misconfiguraties gedetecteerd in container/Kubernetes-omgevingen
Checkmarx 2025 [4]

USD 3,05B
Marktomvang container security in 2025 -- groeit naar USD 9,01B in 2030 (CAGR 24%)
Mordor Intelligence [5]

72%
van organisaties noemt security als grootste container-uitdaging
CNCF Voice of K8s Experts 2025 [6]

21.500+
nieuwe CVE's gepubliceerd in H1 2025 -- een recordaantal
DeepStrike 2025 [7]

38%
van Nederlandse bedrijven containeriseert alle nieuwe applicaties (NL loopt voorop)
Nutanix ECI 2024 [2]

1. Wat is container security?

Container security omvat alle maatregelen, tools en processen om gecontaineriseerde applicaties te beschermen -- van het bouwen van images tot het draaien in productie.

Containers zijn lichtgewicht, geïsoleerde omgevingen waarin applicaties draaien. Ze delen de kernel van het hostsysteem, wat ze efficiënt maakt maar ook kwetsbaar als de beveiliging niet op orde is. Een container escape -- waarbij een aanvaller uit de container breekt naar het hostsysteem -- kan het hele cluster compromitteren [8].

Container security gaat verder dan alleen het scannen van images. Het omvat de volledige levenscyclus: de broncode, het buildproces, de container registry, de deployment en de runtime-omgeving. Dit wordt ook wel "shift-left security" genoemd: beveiliging begint al bij de eerste regel code [9].

DRIE LAGEN VAN CONTAINER SECURITY

- **Build-time** -- image scanning, SBOM-generatie, base image verificatie, secrets detectie in Dockerfiles
- **Deploy-time** -- admission control, configuratievalidatie, policy enforcement, RBAC-controle
- **Runtime** -- anomaliedetectie, network policies, gedragsmonitoring, container isolatie

Nederlandse context

Nederland loopt voorop in containerisatie: 100% van ondervraagde Nederlandse organisaties is ermee bezig, en 38% containeriseert alle nieuwe applicaties -- significant hoger dan het wereldwijde gemiddelde van 27% [2]. Maar 68% worstelt met inzicht in kosten en ROI van containerisatie [2].

2. Waarom containers beveiligen?

Containers bieden flexibiliteit en snelheid, maar zonder beveiliging zijn ze een open deur voor aanvallers.

DE RISICO'S ZONDER CONTAINER SECURITY

RISICO	IMPACT
Kwetsbare base images	98% van container CVE's zit in images buiten de top 20 -- de "long tail" wordt zelden gescand [3]
Container escape	Drie high-severity runc-kwetsbaarheden in 2025 maakten directe host-compromittering mogelijk [8]
Misconfiguraties	40% van organisaties detecteert misconfiguraties in Kubernetes -- vaak te brede permissies of open API's [4]
Supply chain aanvallen	Malafide code in base images of CI/CD-scripts kan ongemerkt in productie terechtkomen [10]
Secrets exposure	API-keys en wachtwoorden hardcoded in images zijn voor aanvallers direct bruikbaar [9]
Laterale beweging	Zonder netwerksegmentatie kan een gecompromitteerde container het hele cluster bereiken

DE BUSINESS IMPACT

De gemiddelde kosten van een datalek bedragen wereldwijd USD 4,44 miljoen [11]. Voor Nederlandse MKB-bedrijven liggen de directe kosten bij EUR 75.000--150.000 per incident [12]. Container-gerelateerde incidenten zijn bijzonder duur omdat ze vaak meerdere services tegelijk treffen.

> **21.500+ NIEUWE CVE'S IN H1 2025**
> Het aantal gepubliceerde kwetsbaarheden bereikt recordhoogtes. Zonder geautomatiseerd scannen is het onmogelijk om handmatig bij te houden welke kwetsbaarheden jouw containers treffen [7].

3. De vier pijlers van container security

Effectieve container security rust op vier pijlers die samen de volledige levenscyclus dekken.

1. Image security

Scan elke container image op bekende kwetsbaarheden (CVE's) voor deployment. Gebruik geverifieerde, minimale base images en genereer een Software Bill of Materials (SBOM) voor elke image [3].

2. Configuratie en compliance

Controleer Kubernetes-configuraties tegen CIS Benchmarks. Voorkom dat containers als root draaien, dat API-servers publiek toegankelijk zijn, of dat RBAC te breed is geconfigureerd [4].

3. Runtime bescherming

Monitor draaiende containers op afwijkend gedrag: onverwachte processen, privilege escalatie, verdachte netwerkverbindingen. eBPF-gebaseerde tools bieden kernel-level zichtbaarheid zonder overhead [10].

4. Netwerk en segmentatie

Implementeer Kubernetes network policies om containerverkeer te segmenteren. Beperk communicatie tot alleen wat nodig is -- dit voorkomt laterale beweging bij een compromis.

TIP

Begin met image scanning in je CI/CD-pipeline. Dit is de snelste win: je vangt kwetsbaarheden af voordat ze in productie komen, zonder bestaande processen te verstoren.

4. Container security vs verwante oplossingen

Container security is een specialisatie binnen het bredere cloud security-landschap. Dit is hoe het zich verhoudt tot verwante oplossingen.

KENMERK	CONTAINER SECURITY	CWPP	CSPM	CNAPP
Focus	Containers en images	Alle workloads	Cloudconfiguratie	Volledige lifecycle
Scope	Build + runtime containers	Runtime workloads	Control plane configuratie	CWPP + CSPM + meer
Detectie	CVE-scanning + anomaliedetectie	Gedragsanalyse	Misconfiguratie-detectie	Cross-domain correlatie
Kosten MKB	EUR 150--1.500/maand	EUR 250--2.000/maand	EUR 50--750/maand	EUR 500--4.000/maand
Geschikt voor	Containerworkloads	Hybride omgevingen	Multi-cloud compliance	Grote cloud-native orgs

> **Trend: consolidatie naar CNAPP**
>
> Standalone container security tools worden geïntegreerd in bredere CNAPP-platforms. Google's overname van Wiz voor USD 32 miljard (maart 2025) versnelt deze consolidatie [5]. Voor MKB met beperkt budget is een standalone container security tool vaak de juiste start.

5. Wat kost het?

Container security kent verschillende prijsmodellen. De keuze hangt af van je omgeving en groeiplannen.

PRIJSMODELLEN

MODEL	INDICATIE	GESCHIKT VOOR
Per node	EUR 10--30/node/maand	Stabiele, middelgrote omgevingen
Per cluster	EUR 200--800/cluster/maand	Kleine omgevingen met weinig clusters
Per workload	EUR 3--15/workload/maand	Dynamische omgevingen met veel containers
Per gebruiker	EUR 8--20/gebruiker/maand	Kleine teams, SaaS-modellen

KOSTENOVERZICHT PER BEDRIJFSGROOTTE

SEGMENT	OMVANG	JAARKOSTEN
Klein MKB	3--5 nodes, 1 cluster	EUR 1.800--4.800 [13]
Middelgroot MKB	10--25 nodes, 2--3 clusters	EUR 6.000--18.000
Groot MKB	50--100 nodes, 5+ clusters	EUR 30.000--72.000

VERBORGEN KOSTEN

- **Implementatie:** 40--80 uur initieel (EUR 4.000--12.000 bij een partner)
- **Training:** EUR 1.000--3.000 per persoon voor Kubernetes security
- **Operationele overhead:** 0,5--1 FTE voor beheer bij middelgroot MKB
- **Compliance-rapportage:** vaak extra module of add-on

> **ROI**
>
> Een middelgroot MKB investeert EUR 12.000--18.000/jaar in container security. Bij het voorkomen van een enkel incident (gemiddeld EUR 75.000--150.000 schade) is de ROI 300--600% over drie jaar [11].

6. Veelgemaakte fouten

Deze zeven valkuilen maken je containeromgeving kwetsbaar -- ook als je security-tools hebt.

1. Containers draaien als root

De meest kritieke fout. Een container die als root draait geeft bij een container escape volledige controle over het hostsysteem. Oplossing: gebruik altijd een non-root user in je Dockerfile [9].

2. Ongecontroleerde base images

Zelfs populaire images bevatten honderden bekende kwetsbaarheden. Veel images worden 2+ jaar niet geüpdatet. Gebruik geverifieerde, minimale base images en scan ze voor elke deployment [3].

3. Secrets hardcoden in images

API-keys, wachtwoorden en encryptiesleutels worden baked in images of Dockerfiles. Gebruik Kubernetes Secrets of een dedicated secrets manager -- mount secrets alleen waar ze nodig zijn [9].

4. De :latest tag gebruiken

De :latest tag trekt mogelijk ongeteste wijzigingen of nieuw ontdekte kwetsbaarheden binnen zonder waarschuwing. Pin altijd specifieke image-versies voor reproduceerbaarheid en veiligheid.

5. Geen scanning in de CI/CD-pipeline

Veel organisaties scannen pas bij deployment, niet tijdens de build. Container images kunnen onzichtbare kwetsbaarheden binnenhalen via dependencies tijdens build time [4].

6. RBAC te breed geconfigureerd

Kubernetes Role-Based Access Control en pod security contexts worden vaak niet of verkeerd geconfigureerd. Dit geeft te brede toegang tot cluster-resources [14].

7. Geen netwerksegmentatie

Zonder Kubernetes network policies communiceren containers vrij met elkaar. Dit maakt laterale beweging bij een compromis triviaal. Implementeer network policies voor alle kritieke workloads.

> **BELANGRIJK**
> Misconfiguraties -- niet ongepatche CVE's -- zijn de grootste oorzaak van container-gerelateerde incidenten. 40% van organisaties heeft misconfiguraties in hun Kubernetes-omgeving [4].

7. NIS2 en DORA

Twee Europese wetten maken container security van een "nice to have" naar een compliance-vereiste.

NIS2 / CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet (NIS2-implementatie) treedt naar verwachting in Q2 2026 in werking. Ongeveer 10.000 Nederlandse organisaties vallen er direct onder [15]. Container security is relevant op meerdere vlakken:

NIS2-EIS	VERBAND MET CONTAINER SECURITY
Risicoanalyse	Container images en orchestrators moeten in de risicoanalyse
Supply chain beheer	SBOM voor container images wordt verwacht
Incidentdetectie	Runtime monitoring voor tijdige detectie
Toegangsbeheer	Kubernetes RBAC moet voldoen aan least-privilege
Kwetsbaarheidsbeheer	Continue scanning op CVE's
Aantoonbaarheid	Audit trails van container-activiteit

DORA

DORA (van kracht sinds januari 2025) raakt container security via ICT-risicomanagement, third-party oversight van cloud providers, resilience testing en incidentrapportage [16].

> **Regulatory als marktdriver**
>
> NIS2, PCI-DSS 4.0 en SBOM-verplichtingen hebben container security van een discretionaire investering naar een compliance-vereiste gemaakt. De container security-markt groeit met 24% CAGR, deels gedreven door deze regulatoire druk [5].

8. Een oplossing kiezen

De juiste container security-oplossing hangt af van je omgeving, team en budget.

SELECTIECRITERIA

1. **Lifecycle coverage** -- dekt de oplossing build-time, deploy-time en runtime?
2. **Kubernetes-integratie** -- native integratie met je orchestrator
3. **CI/CD pipeline integratie** -- scanning als onderdeel van je build pipeline
4. **Runtime bescherming** -- detectie en respons op anomalieën
5. **Compliance frameworks** -- CIS Benchmarks, NIS2, SOC 2
6. **SBOM-generatie** -- automatische Software Bill of Materials
7. **Multi-cloud support** -- werkt over AWS, Azure, GCP en on-premises
8. **Prijsmodel** -- past bij je groeimodel

MKB-SPECIFIEKE OVERWEGINGEN

SITUATIE	ADVIES
Budget beperkt	Start met open-source (Trivy voor scanning, Falco voor runtime) en groei naar commercieel
Geen security team	Kies een managed oplossing of CNAPP met geïntegreerde container security
Kleine omgeving (< 10 nodes)	Per-cluster pricing is vaak voordeliger dan per-node
Multi-cloud	Kies een vendor-onafhankelijke oplossing
Compliance-vereisten	Kies oplossing met ingebouwde compliance-rapportage

9. Implementatie-aanpak

Een pragmatisch stappenplan voor MKB-organisaties die container security willen implementeren.

1 Inventarisatie

1--2 WEKEN

Breng alle containerworkloads, images, registries en orchestrators in kaart. Welke applicaties draaien in containers?

2 Risicoanalyse

1--2 WEKEN

Scan bestaande images op CVE's. Beoordeel Kubernetes-configuratie tegen CIS Benchmarks. Identificeer de grootste risico's.

3 Tool selectie

2--4 WEKEN

Evalueer oplossingen op basis van je criteria. Start eventueel met open-source tools als proof of concept.

4 CI/CD integratie

1--2 WEKEN

Implementeer image scanning in je build pipeline. Blokkeer images met kritieke CVE's automatisch.

5 Runtime monitoring

2--4 WEKEN

Activeer runtime bescherming voor productieomgevingen. Configureer alerts voor anomalieën.

6 Policy enforcement

1--2 WEKEN

Stel Kubernetes security policies en network policies in. Dwing least-privilege af.

7 Training en compliance

2--4 WEKEN

Train je team. Configureer compliance-rapportage en audit trails voor NIS2 en interne audits.

QUICK WINS -- EERSTE 30 DAGEN

1. Scan alle productie-images op CVE's. 2. Verwijder containers die als root draaien. 3. Pin image-versies (geen :latest). 4. Implementeer RBAC. 5. Activeer network policies voor kritieke workloads.

10. Trends 2025--2026

Zeven ontwikkelingen die container security de komende jaren vormgeven.

1. Zero-CVE base images

Chainguard (gewaardeerd op USD 3,5 miljard) leidt de beweging naar images met nul bekende kwetsbaarheden. De verantwoordelijkheid verschuift van scannen-en-patchen naar inherent veilige foundations [3].

2. SBOM-verplichtingen

NIS2, de Cyber Resilience Act en PCI-DSS 4.0 vereisen transparantie over software-componenten. SBOM wordt een standaard artefact naast het container image [5].

3. AI/ML workload security

Kubernetes is het de-facto platform voor AI-workloads (82% productiegebruik). Dit brengt nieuwe uitdagingen: model poisoning, data exfiltratie en GPU-resource hijacking [1].

4. eBPF-gebaseerde runtime security

eBPF wordt de standaard voor runtime monitoring: kernel-level visibility zonder overhead van agent-based oplossingen.

5. Platform consolidatie naar CNAPP

Standalone container security tools worden onderdeel van bredere CNAPP-platforms. Google's overname van Wiz (USD 32 miljard) versnelt dit [5].

6. Supply chain security

Verificatie van de volledige software supply chain -- van base image tot deployment -- is een topprioriteit geworden na recente supply chain-aanvallen [10].

7. Shift-left security

Security schuift verder naar links in de pipeline: van runtime-detectie naar build-time preventie. Container scanning wordt een standaard CI/CD-stap.

Bronnenlijst

[1] **CNCF** -- Kubernetes Production Use Hits 82% in 2025 Annual Survey. cncf.io/announcements/2026/01/20/kubernetes-established-as-the-de-facto-operating-system-for-ai-as-production-use-hits-82-in-2025-cncf-annual-cloud-native-survey/

[2] **Nutanix** -- Nederland loopt voorop in containerisatie en GenAI-adoptie. nutanix.com/nederland/press-releases/nederland-loopt-voorop-in-containerisatie-en-genai-adoptie-maar-worstelt-met-roi-en-use-cases

[3] **Chainguard/InfoQ** -- 98% of Container CVEs Lurking outside Top 20 Images (januari 2026). infoq.com/news/2026/01/chainguard-opensource-vulns/

[4] **Checkmarx** -- 4 Common Container Security Misconceptions. checkmarx.com/blog/4-common-container-security-misconceptions-and-how-to-avoid-them/

[5] **Mordor Intelligence** -- Container Security Market Size 2025--2030 (USD 3,05B--9,01B). mordorintelligence.com/industry-reports/container-security-market

[6] **CNCF** -- Voice of Kubernetes Experts 2025: security 72% top challenge. cncf.io/blog/2025/08/02/what-500-experts-revealed-about-kubernetes-adoption-and-workloads/

[7] **DeepStrike** -- Vulnerabilities Statistics 2025: 21.500+ CVEs in H1. deepstrike.io/blog/vulnerability-statistics-2025

[8] **ARMO** -- High-Severity runc Vulnerabilities (CVE-2025-31133, -52565, -52881). armosec.io/blog/high-severity-runc-vulnerabilities-what-you-need-to-know/

[9] **Aikido** -- 9 Common Docker Container Security Vulnerabilities. aikido.dev/blog/docker-container-security-vulnerabilities

[10] **Red Hat** -- Four container and Kubernetes security risks you should mitigate. redhat.com/en/blog/four-container-and-kubernetes-security-risks-you-should-mitigate

[11] **Auxis** -- How to Calculate Cybersecurity ROI, gemiddeld datalek USD 4,44M. auxis.com/how-to-calculate-cybersecurity-roi-prove-business-value/

[12] **NTNT** -- Wat kost goede cybersecurity voor een MKB? ntnt.nl/wat-kost-goede-cybersecurity-voor-een-mkb/

[13] **ARMO** -- Kubernetes Security Cost and Pricing Methods Comparison. armosec.io/blog/kubernetes-security-cost-comparison/

[14] **OWASP** -- Kubernetes Security Cheat Sheet. cheatsheetseries.owasp.org/cheatsheets/Kubernetes_Security_Cheat_Sheet.html

[15] **MSafe** -- Aantoonbare compliance in 2026: NIS2, DORA, AI Act. msafe.co/nl/blog/aantoonbare-compliance-in-2026-nis2-dora-ai-act/

[16] **Kennedy Van der Laan** -- Cyber in 2026: NIS2 in aantocht. kvdl.com/en/articles/cyber-in-2026-nis2-in-aantocht

[17] **CBS** -- Cybersecuritymonitor 2024, cloudgebruik 71% (10+ pers.). cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[18] **NCSC.GOV.UK** -- Using containerisation: security guidance. ncsc.gov.uk/collection/using-containerisation

[19] **SentinelOne** -- Top 5 Container Security Solutions for 2026. sentinelone.com/cybersecurity-101/cloud-security/container-security-solutions/

[20] **OX Security** -- Top 10 Container Security Tools to Know in 2026. ox.security/blog/container-security-tools-2026/

Deze gids is samengesteld door IBgids.nl op basis van openbare bronnen en marktonderzoek. Alle genoemde prijzen zijn indicatief (peildatum: maart 2026). IBgids.nl is een onafhankelijk platform en geen aanbieder van container security-oplossingen.