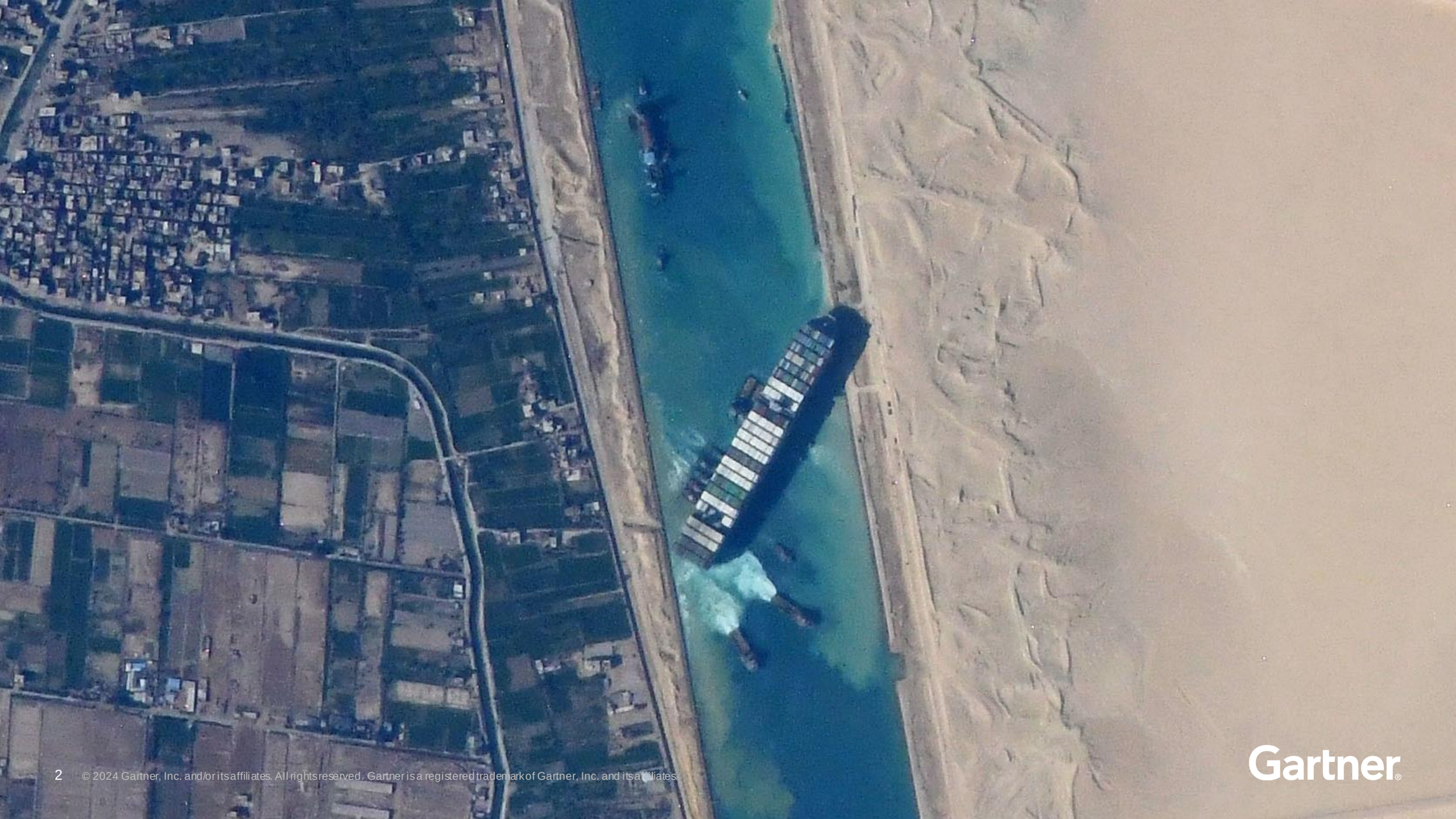
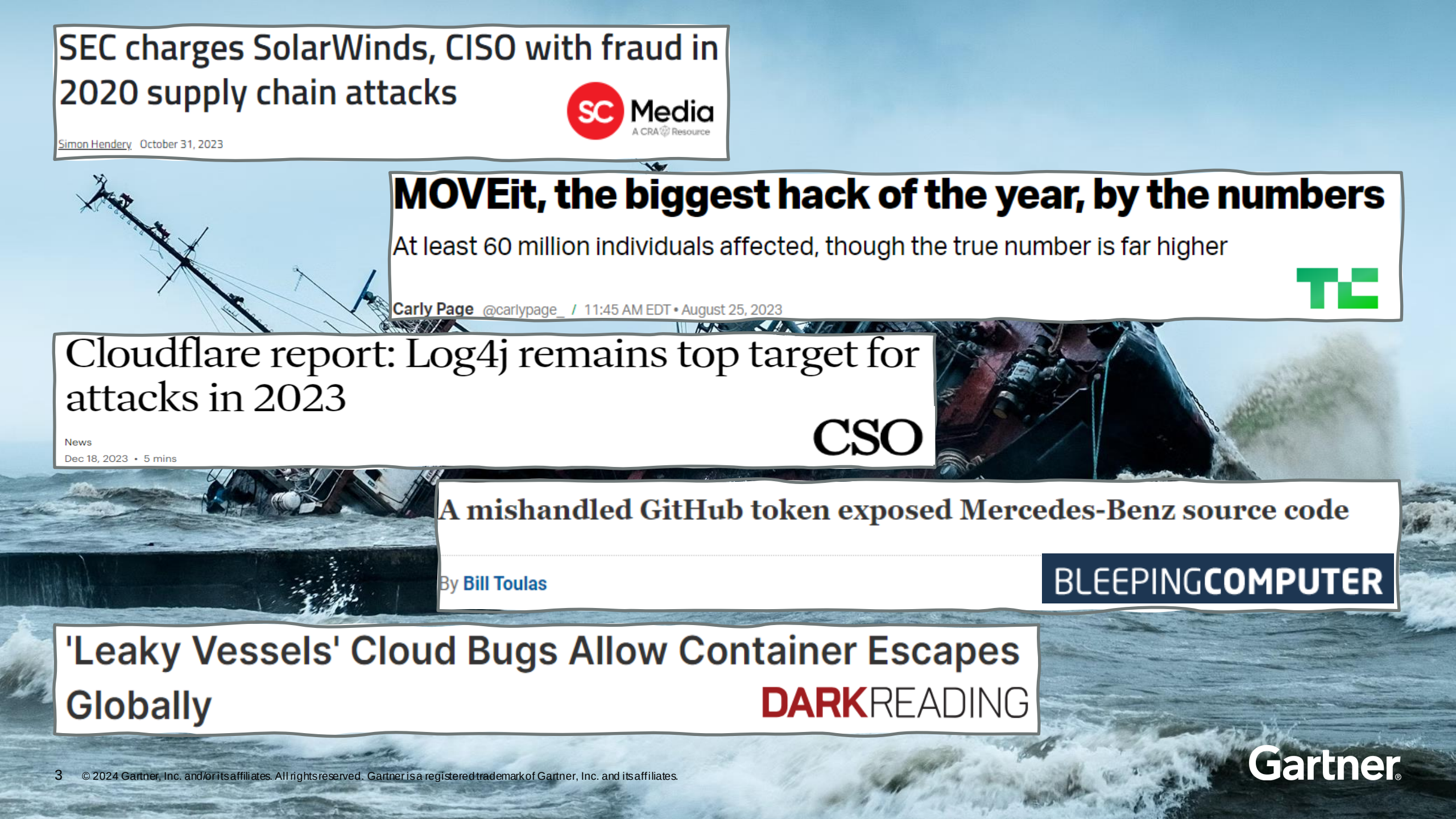
Technical Insights: The 3 Components of Trust in Software Supply Chain Security

William Dupre

Gartner®





Gartner

The software supply chain consists of the components, dependencies and build environment that enable the development, integration and deployment of software artifacts.

Gartner®

Trust = Visibility + Integrity + Posture

Gartner®

Trust = Visibility + Integrity + Posture

Cloudflare report: Log4j remains top target for attacks in 2023

News

Dec 18, 2023 • 5 mins

CSO

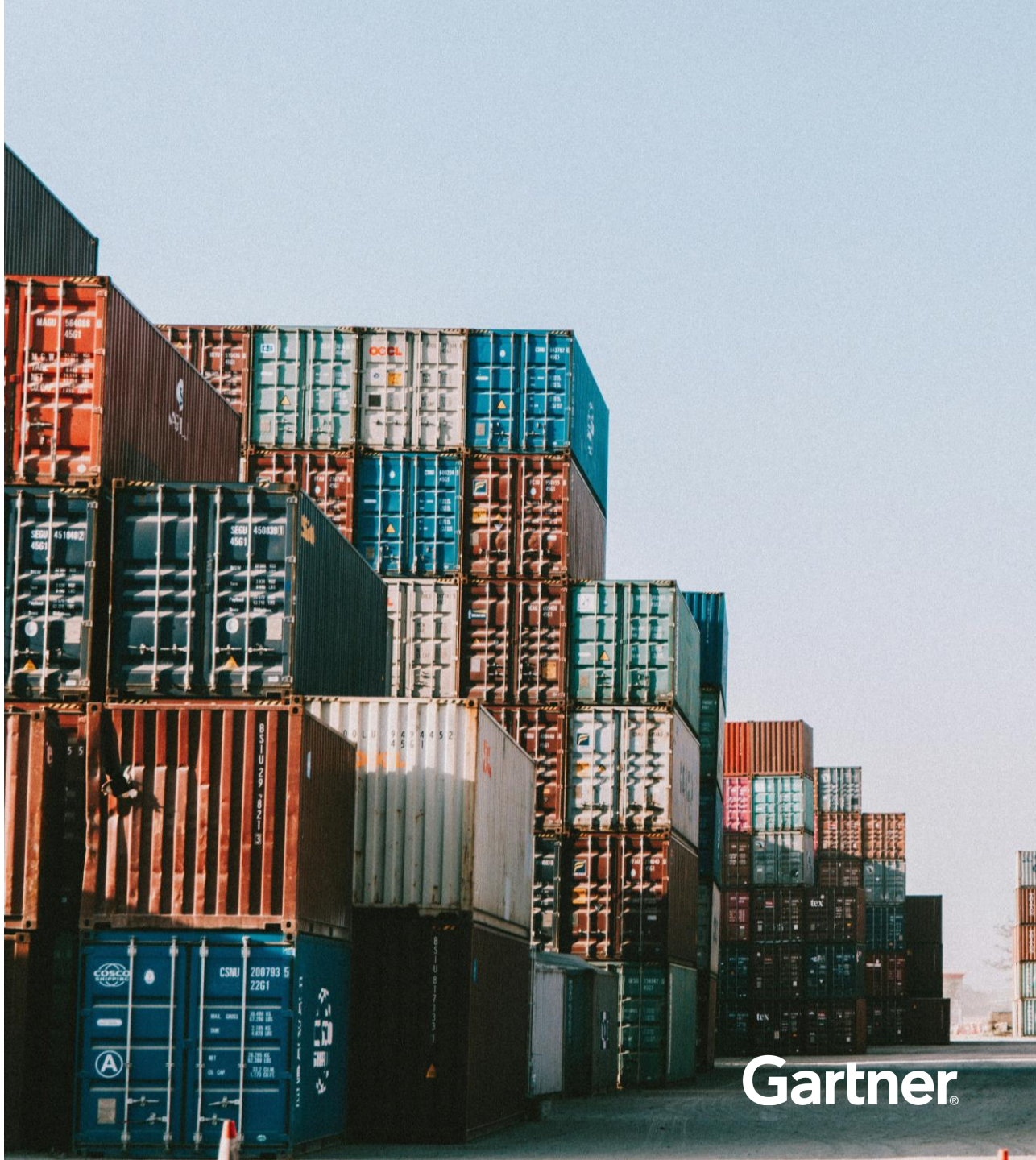
Gartner®

Visibility

Repository

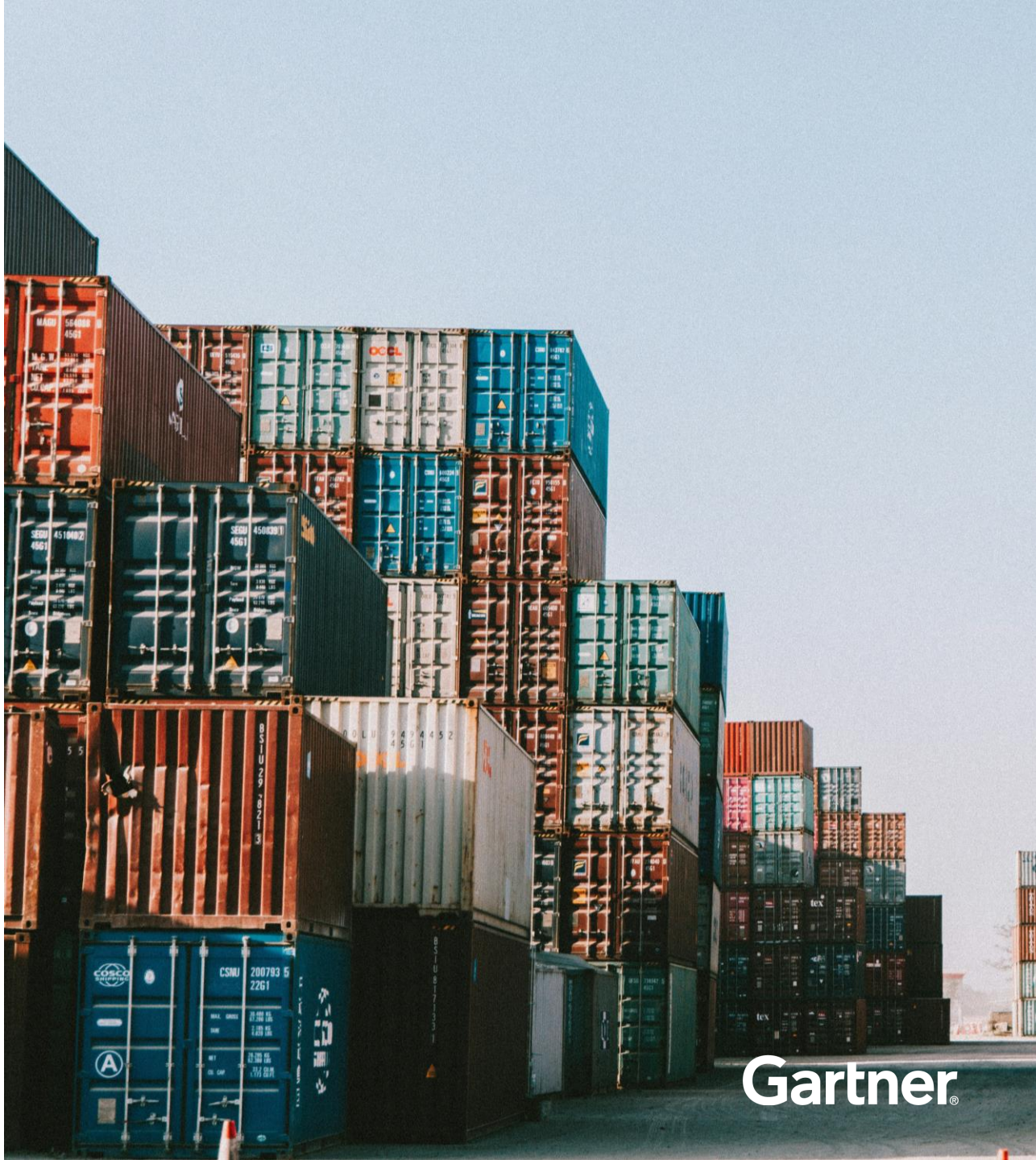
Pipeline

Artifact



Visibility

- ✓ Repository inventory
- ✓ Software composition analysis & application security testing
- ✓ Pipeline activity logging, monitoring & auditing
- ✓ Bills of material



Trust = Visibility + Integrity + Posture

Over 800 npm Packages Found with Discrepancies, 18 Exploitable to 'Manifest Confusion' The Hacker News

Gartner®

Integrity

Component

Pipeline and repository

Artifact

Integrity

- ✓ Private/curated repositories
- ✓ Secrets management
- ✓ Repository controls & policies
- ✓ Signed artifacts

Trust = Visibility + Integrity + Posture

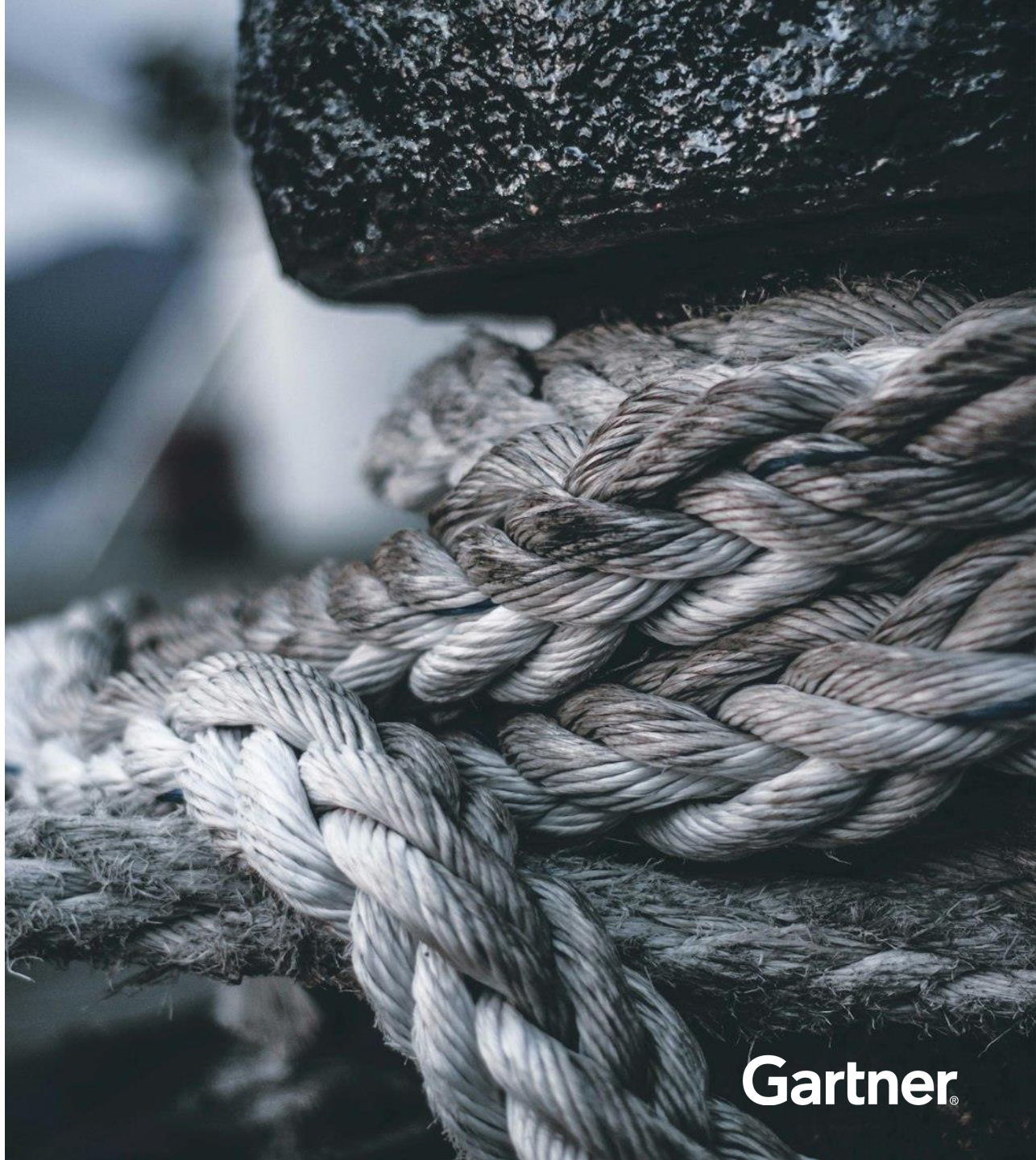
Gartner

Posture

Application and infrastructure

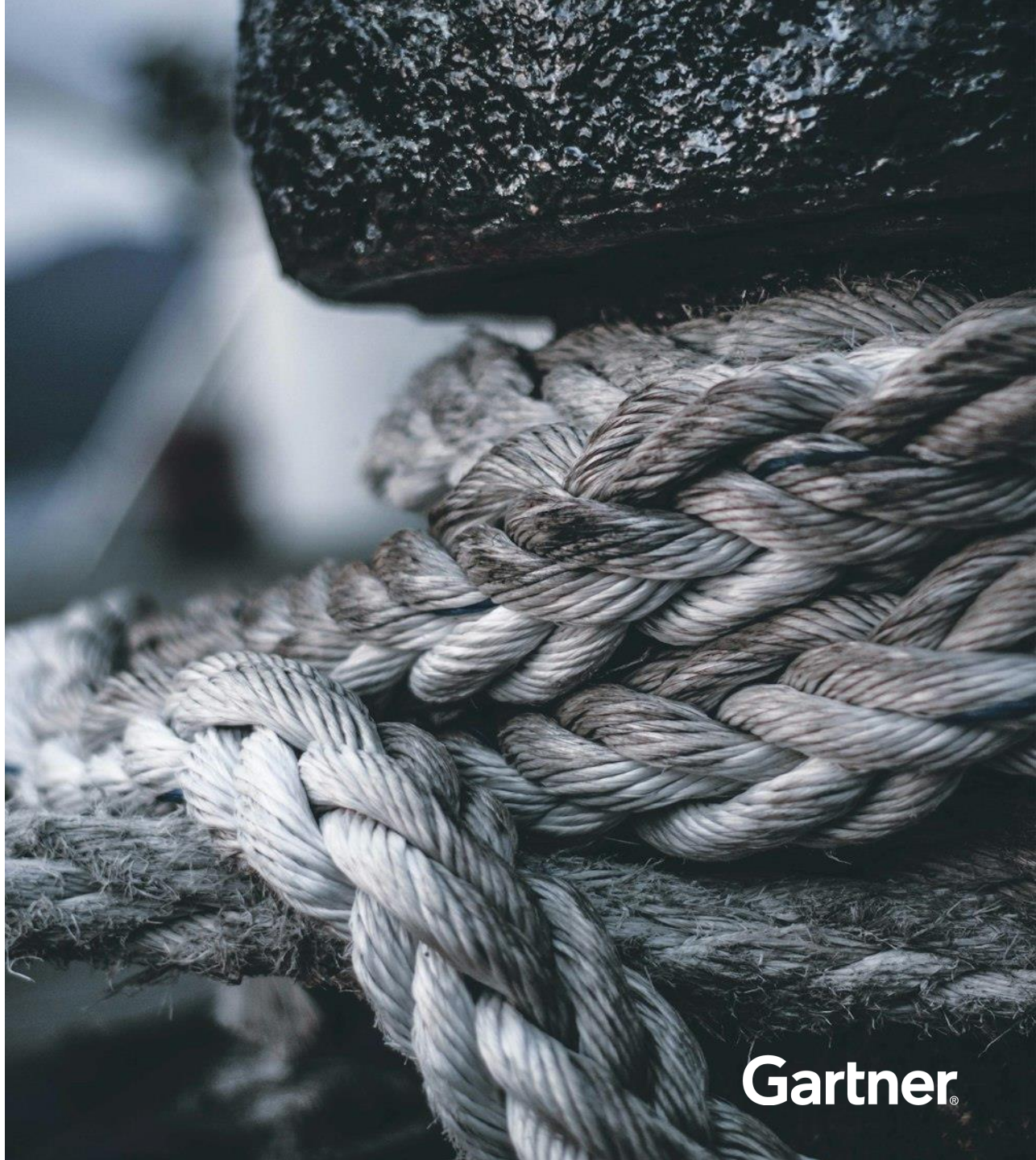
Access control

Continuous risk visibility



Posture

- ✓ Application security posture management (ASPM)
- ✓ Identity & access management (IAM)
- ✓ Runtime context



Trust = Visibility + Integrity + Posture

DevSecOps

MLSecOps

Hugging Face AI Platform Riddled With 100 Malicious Code-Execution Models

DARKREADING

Gartner

Don’t Forget Automation

“Leveraging automation helps to ensure that processes are deterministic, bolstering the attestation and verification mechanisms we rely on for supply chain security.”

Source: CNCF Paper Defines Best Practices for Supply Chain Security, Cloud Native Computing Foundation (CNCF)

Recommendations

- **Get visibility** into all aspects of the software supply chain.
- **Enforce integrity** controls on build process.
- **Improve the posture** of the supply chain infrastructure.
- **Automate!**

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **Guide to Application Security Concepts**
  Greg Harris
- **Innovation Insight for Application Security Posture Management**
  Dale Gardner, Dionisio Zumerle and Manjunath Bhat
- **Mitigate Enterprise Software Supply Chain Security Risks**
  Dale Gardner
- **The CISO’s Guide to Application Security**
  William Dupre
- **A Guidance Framework for Building an Application Security Program**
  William Dupre

Access to Gartner research is subject to individual subscription type and product entitlements.

Gartner