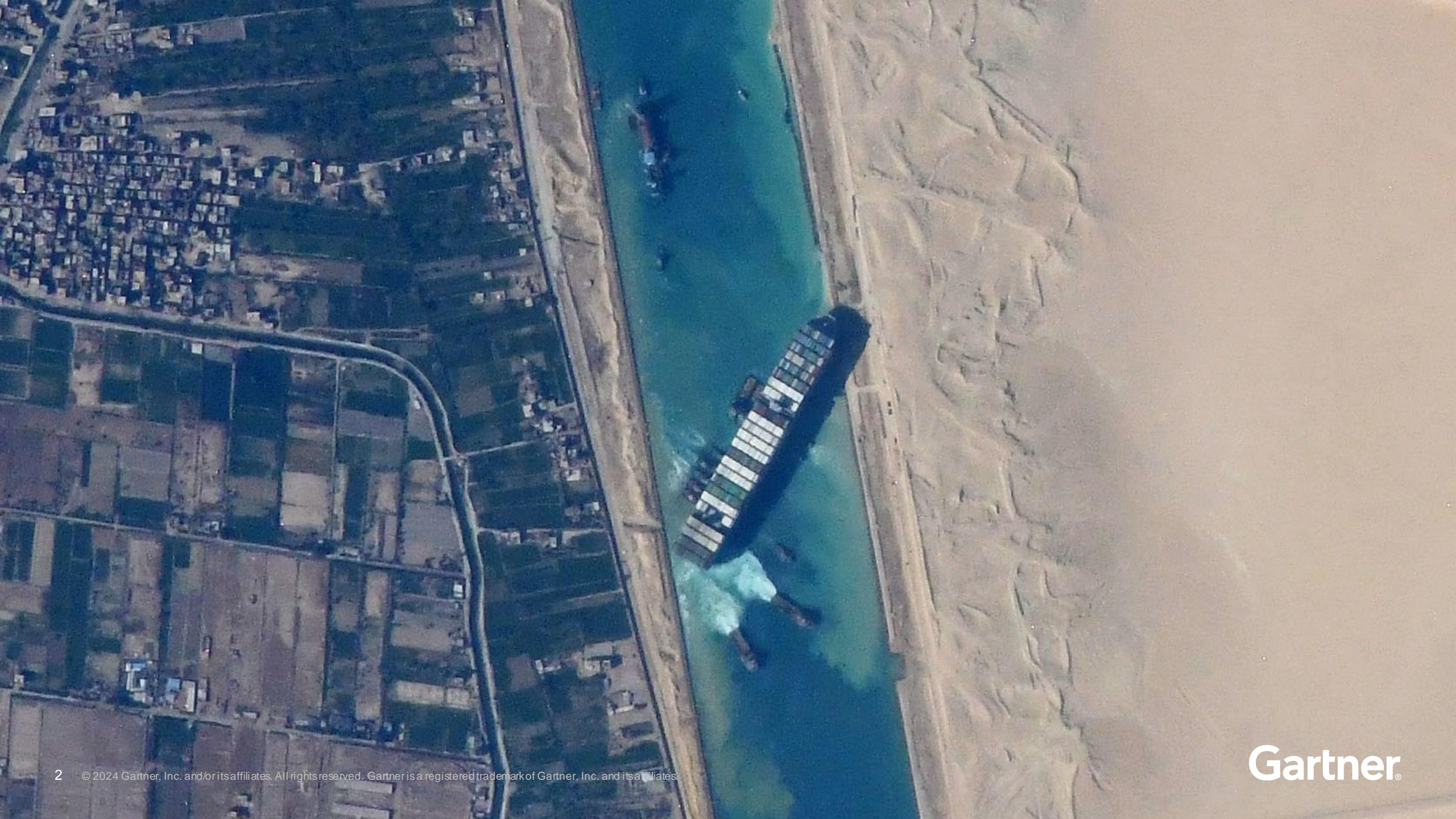


Technical Insights: The 3 Components of Trust in Software Supply Chain Security

William Dupre

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

Gartner®



SEC charges SolarWinds, CISO with fraud in 2020 supply chain attacks



Simon Hendery, October 31, 2023

MOVEit, the biggest hack of the year, by the numbers

At least 60 million individuals affected, though the true number is far higher

Carly Page @carlypage_ / 11:45 AM EDT • August 25, 2023



Cloudflare report: Log4j remains top target for attacks in 2023

News

Dec 18, 2023 • 5 mins

CSO

A mishandled GitHub token exposed Mercedes-Benz source code

By Bill Toulas

BLEEPINGCOMPUTER

'Leaky Vessels' Cloud Bugs Allow Container Escapes Globally

DARKREADING

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

Trust = Visibility + Integrity + Posture

Trust = **Visibility** + Integrity + Posture

Cloudflare report: Log4j remains
top target for attacks in 2023

News

Dec 18, 2023 • 5 mins

CSO

Visibility

Repository

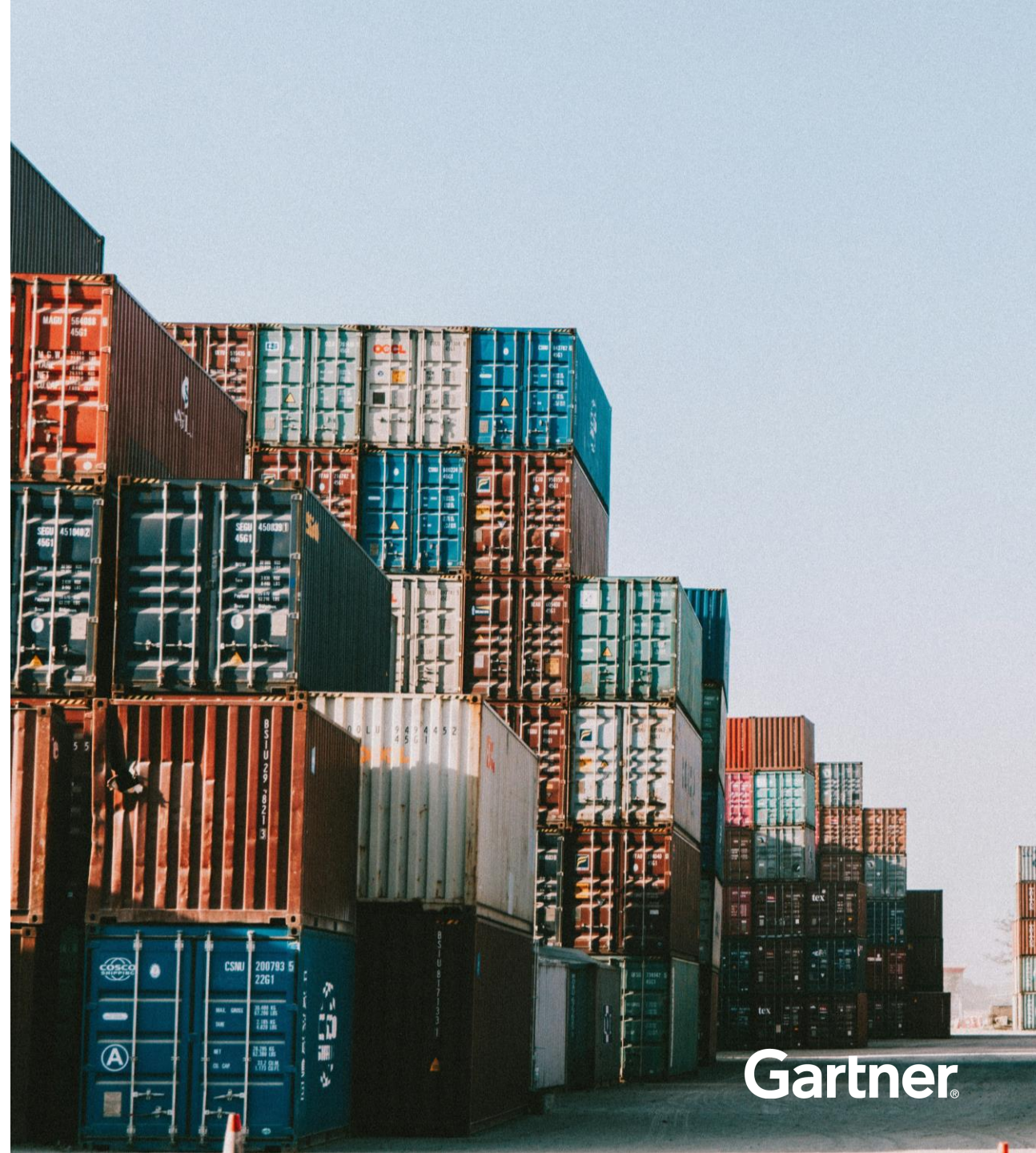
Pipeline

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**

Integrity

Component

Pipeline and repository

Artifact



Integrity

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



Trust = Visibility + Integrity + Posture



Slack GitHub Account Hacked via Stolen Employee API Token



by Ivanwallarm on January 5, 2023



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

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)

16 © 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.



Gartner®

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