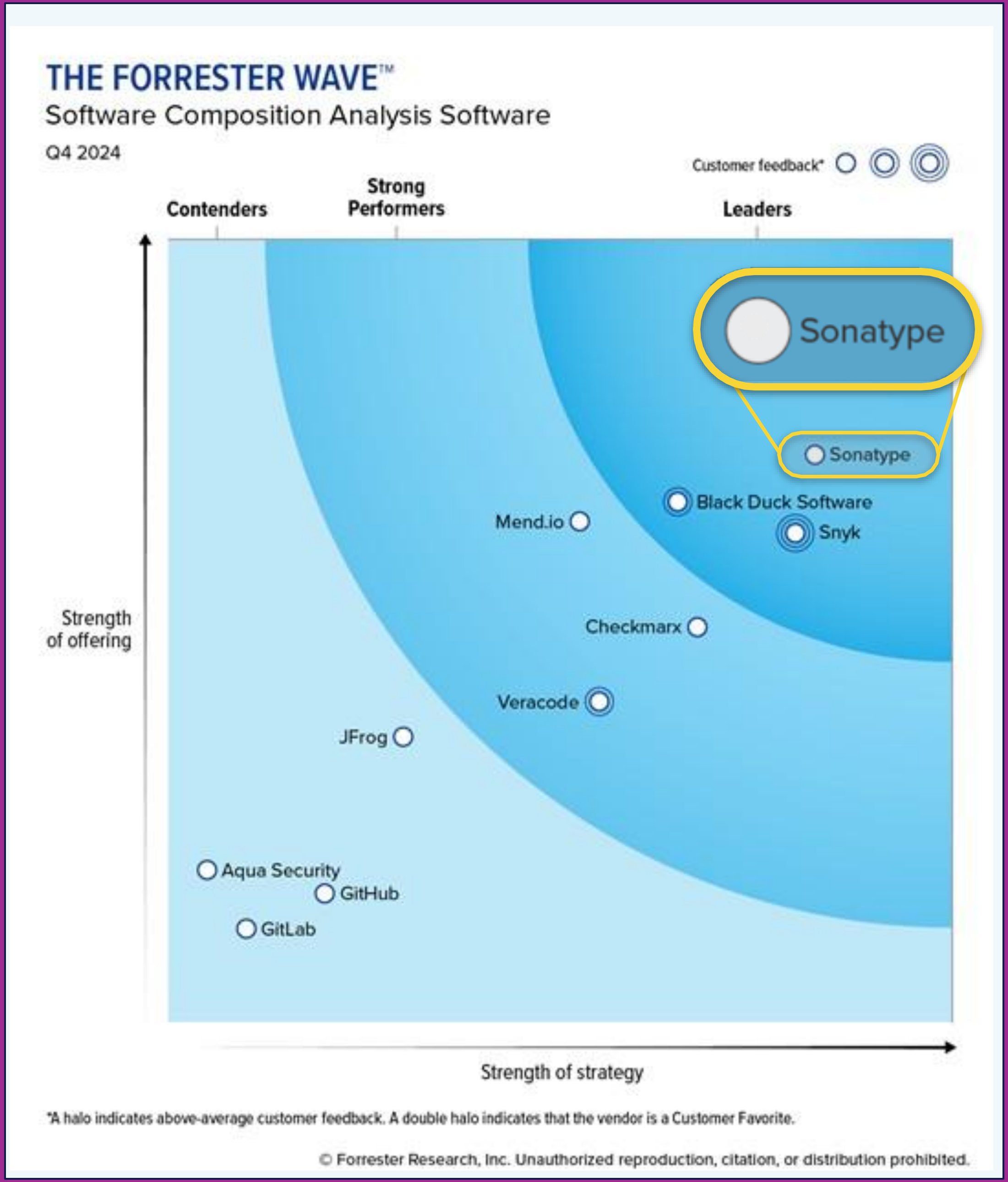
sonatype

The Evolution of Enterprise AI: Navigating New Trends and Challenges

Cameron Townshend
Principle Solutions Architect APJ
Sonatype



THE FORRESTER WAVE™
Software Composition Analysis Software
Q4 2024

*A halo indicates above-average customer feedback. A double halo indicates that the vendor is a Customer Favorite.

Sonatype recognized as a **LEADER** on the The Forrester Wave™ for Software Composition Analysis in Q4, 2024.

Sonatype is **TOP RANKED** for both Current Offering and Strategy.

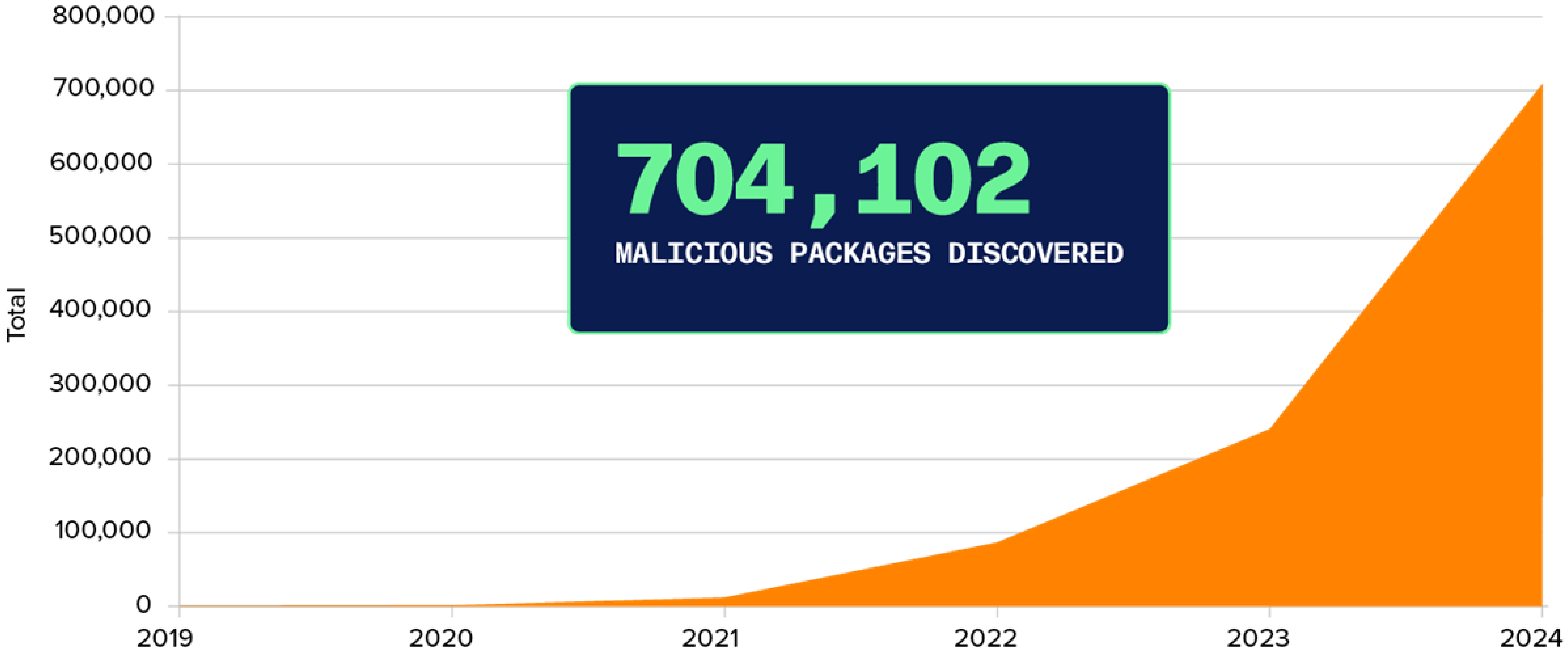
The Forrester Wave ™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave ™ are trademarks of Forrester Research, Inc. The Forrester Wave ™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave ™. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change.

Open source adoption is skyrocketing

2024	6.5 TRILLION	6,500,000,000,000
2023	4.5 TRILLION	3,100,000,000,000
2022	3.5 TRILLION	3,500,000,000,000
2021	2.2 TRILLION	1,500,000,000,000

sonatype

Sonatype Proprietary
Estimated request volume for the 4 largest open source ecosystems
Maven Central (java), NPM (js) , PyPI (python), NuGet Gallery (C# .NET



704,102

MALICIOUS PACKAGES DISCOVERED

Sonatype 10th Annual State of the Software Supply Chain

Evolution of Software Supply Chain Exploits

EARLY YEARS:
Struts, Heartbleed, and Shellshock (2014–2016)

STRUTS

2017:
The Rise of Targeted Supply Chain attacks

EQUIFAX

2020:
The Expansion of Supply Chain Attacks

solarwinds

2021–2022:
The Vulnerability that Set the Internet on Fire

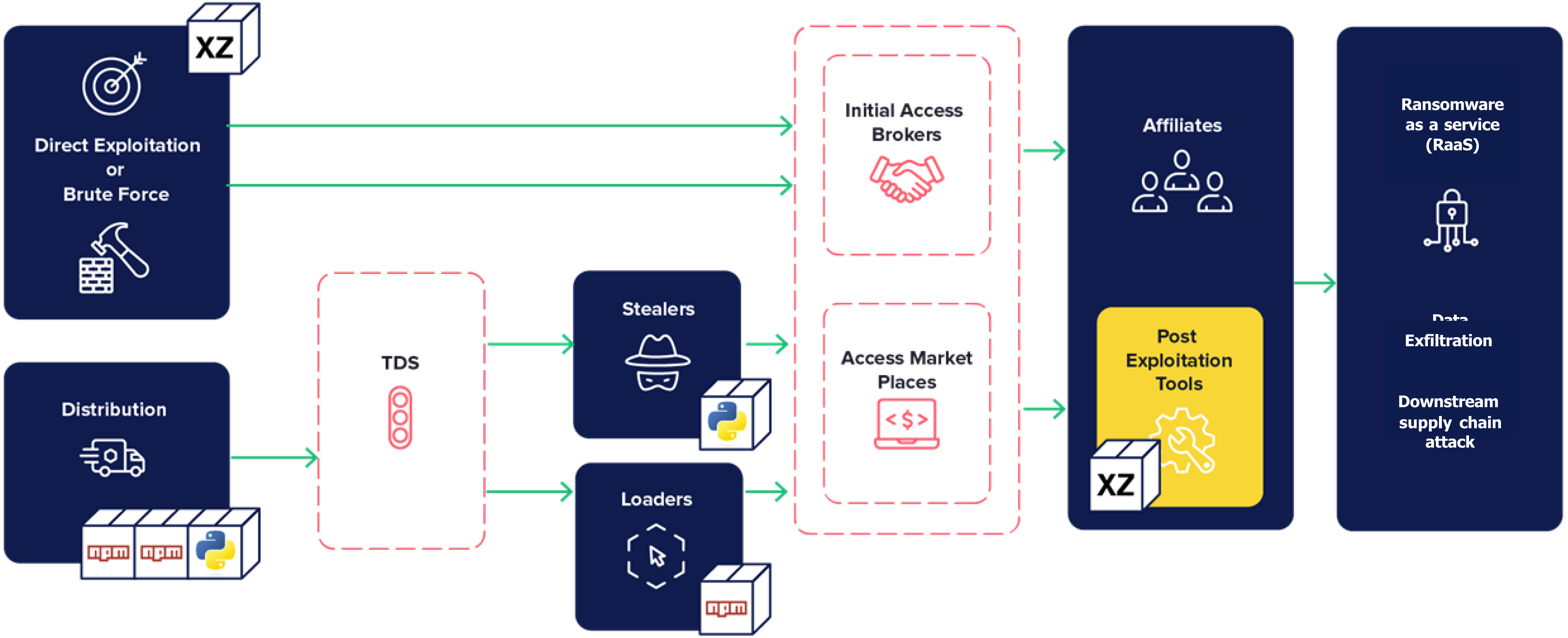
LOG4J

2024:
The Attempted XZ-Utils Supply Chain Attack

XZ Utils

Sonatype 10th Annual State of the Software Supply Chain

Cybercrime Ecosystem



Modified from Original Source: NCSC-UK

180 Dependencies (avg Java project)

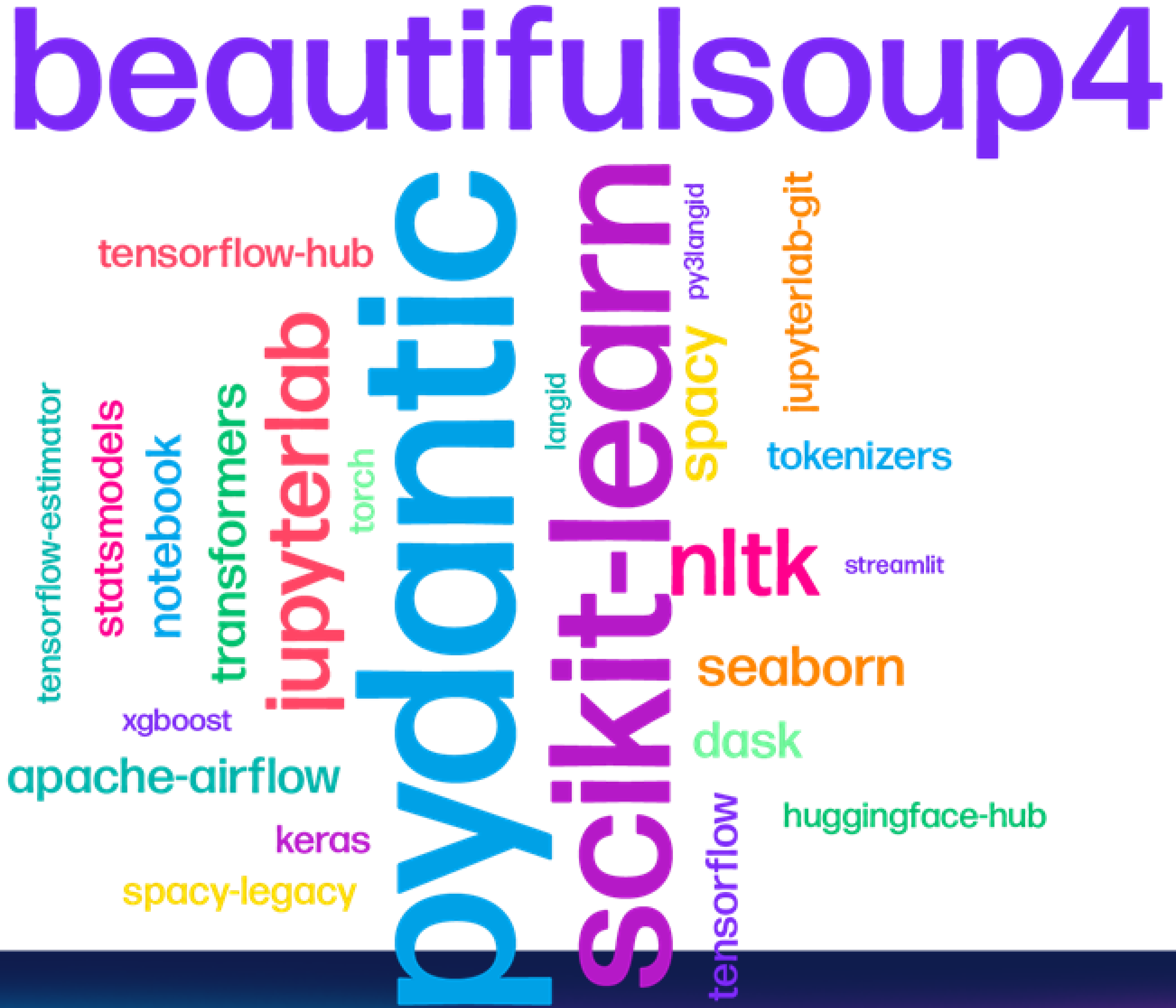
x 10 Releases Per Year (avg per dependency)

1800 Updates To Consider

😱

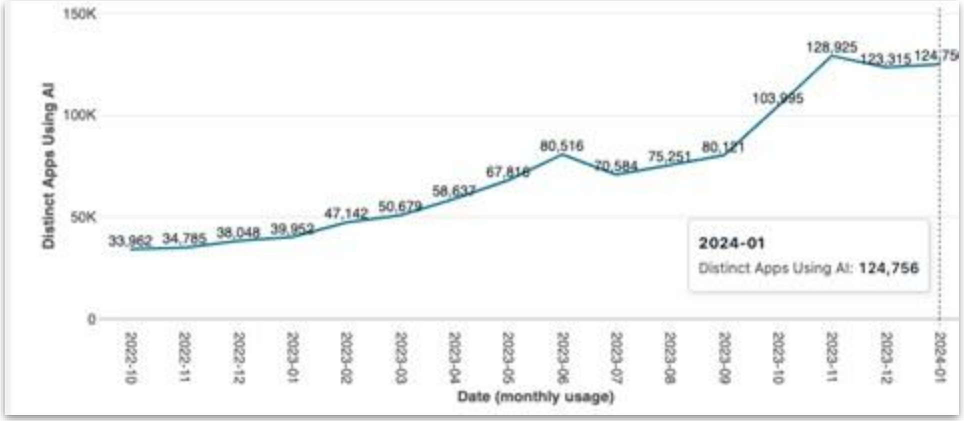
The software supply chain is overwhelming engineering and security teams.

A whole new AI supply chain has emerged

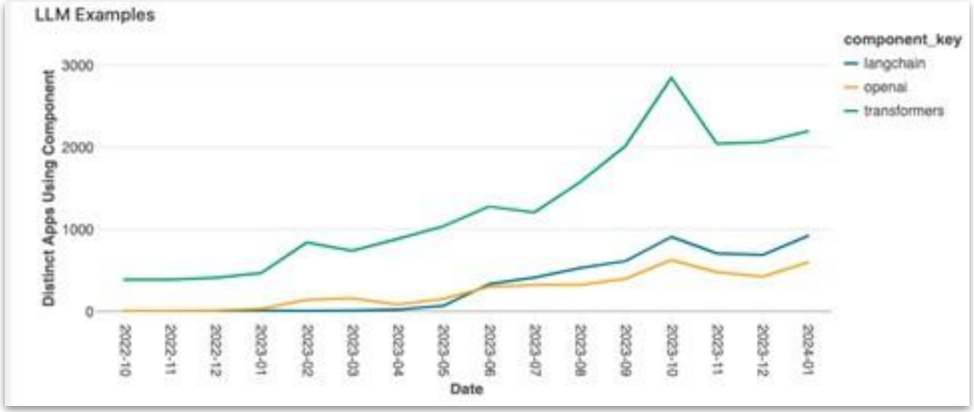


The gold rush of AI/ML: World changing, disruptive technology

AI Usage



LLM (Generative AI) Usage



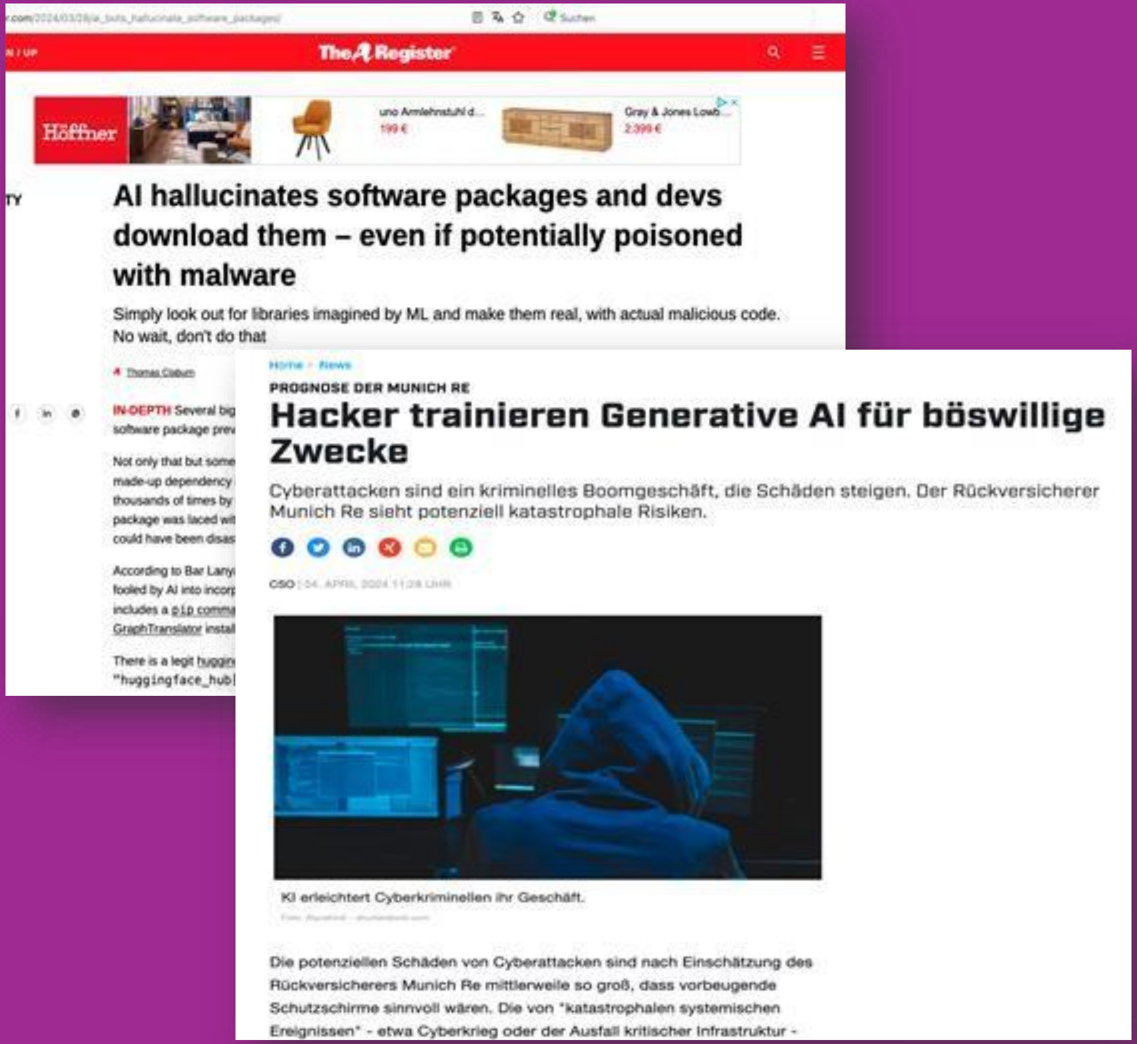
267% growth in traditional AI

870% growth in Generative AI usage over 18 months

sonatype

“

3 out of 5 DevOps Leads expressed concerns regarding impact of GenAI on security vulnerabilities



AI hallucinates software packages and devs download them – even if potentially poisoned with malware

Simply look out for libraries imagined by ML and make them real, with actual malicious code. No wait, don't do that

IN-DEPTH Several big
software package prev

Not only that but some
made-up dependency
thousands of times by
package was laced wit
could have been disas

According to Bar Lany
fooled by AI into incorp
includes a pip comma
GraphTranslator instal

There is a legit huggin
"huggingface_hub[

PROGNOSE DER MUNICH RE

Hacker trainieren Generative AI für böswillige Zwecke

Cyberattacken sind ein kriminelles Boomgeschäft, die Schäden steigen. Der Rückversicherer Munich Re sieht potenziell katastrophale Risiken.

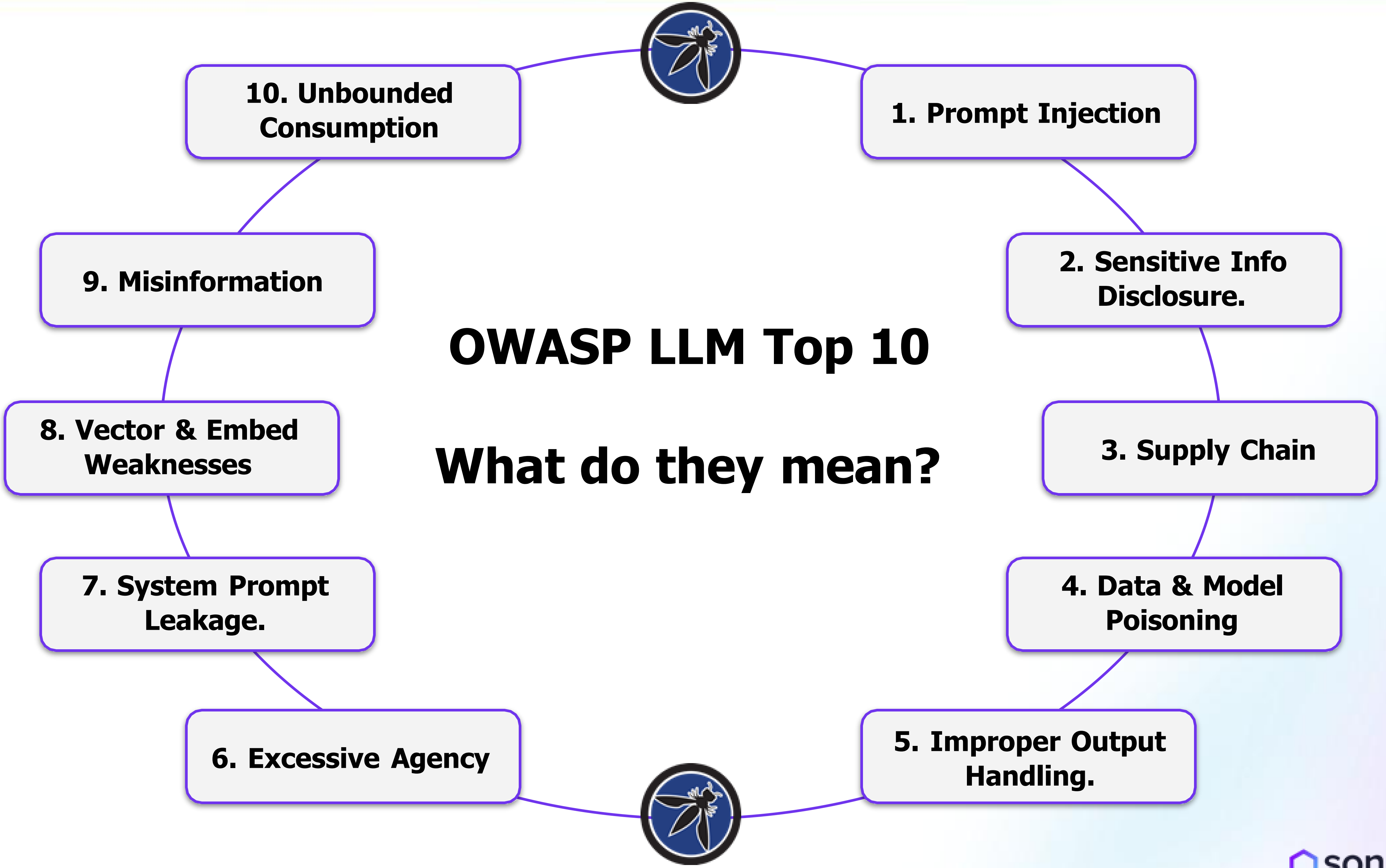
CSO

KI erleichtert Cyberkriminellen ihr Geschäft.

Die potenziellen Schäden von Cyberattacken sind nach Einschätzung des Rückversicherers Munich Re mittlerweile so groß, dass vorbeugende Schutzschirme sinnvoll wären. Die von "katastrophalen systemischen Ereignissen" - etwa Cyberkrieg oder der Ausfall kritischer Infrastruktur -

OWASP LLM Top 10

What do they mean?



1. Prompt Injection

2. Sensitive Info Disclosure.

3. Supply Chain

4. Data & Model Poisoning

5. Improper Output Handling.

6. Excessive Agency

7. System Prompt Leakage.

8. Vector & Embed Weaknesses

9. Misinformation

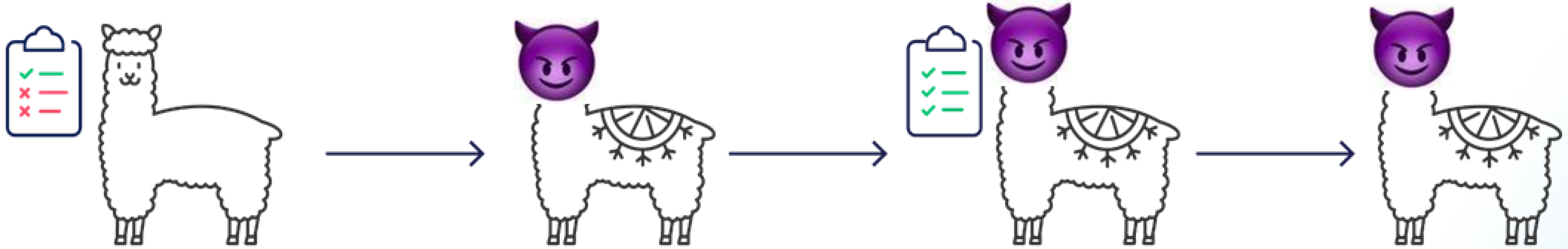
10. Unbounded Consumption

sonatype

The risks of AI/ML in Enterprise

Security	The security risk of using LLMs, security risk in context of the app
Data Exfiltration	Loss of IP and sensitive data
License	LLM and Dataset usage have license obligations
Quality	Not safe for work (NSFW), popularity, determinism, serialization….
Legal	Automated code creation, IP loss
Culture	AI website usage at work
Lineage	Knowing what the foundation “models” are

AI mutation and licensing risk

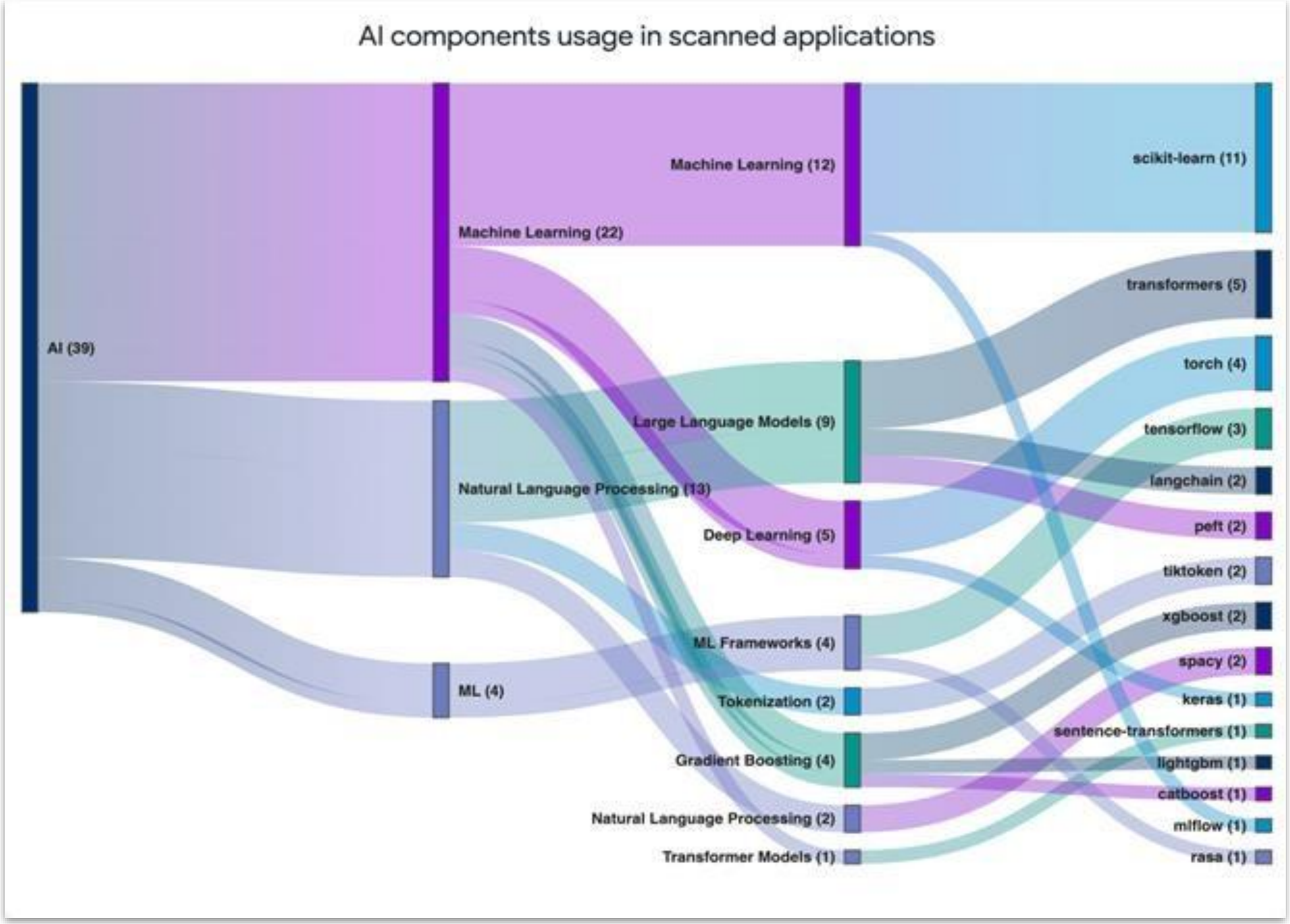


Meta releases LLaMA with specific, non-commercial license

3rd party fine tunes or quantizes the model

3rd party releases it under an incorrect license

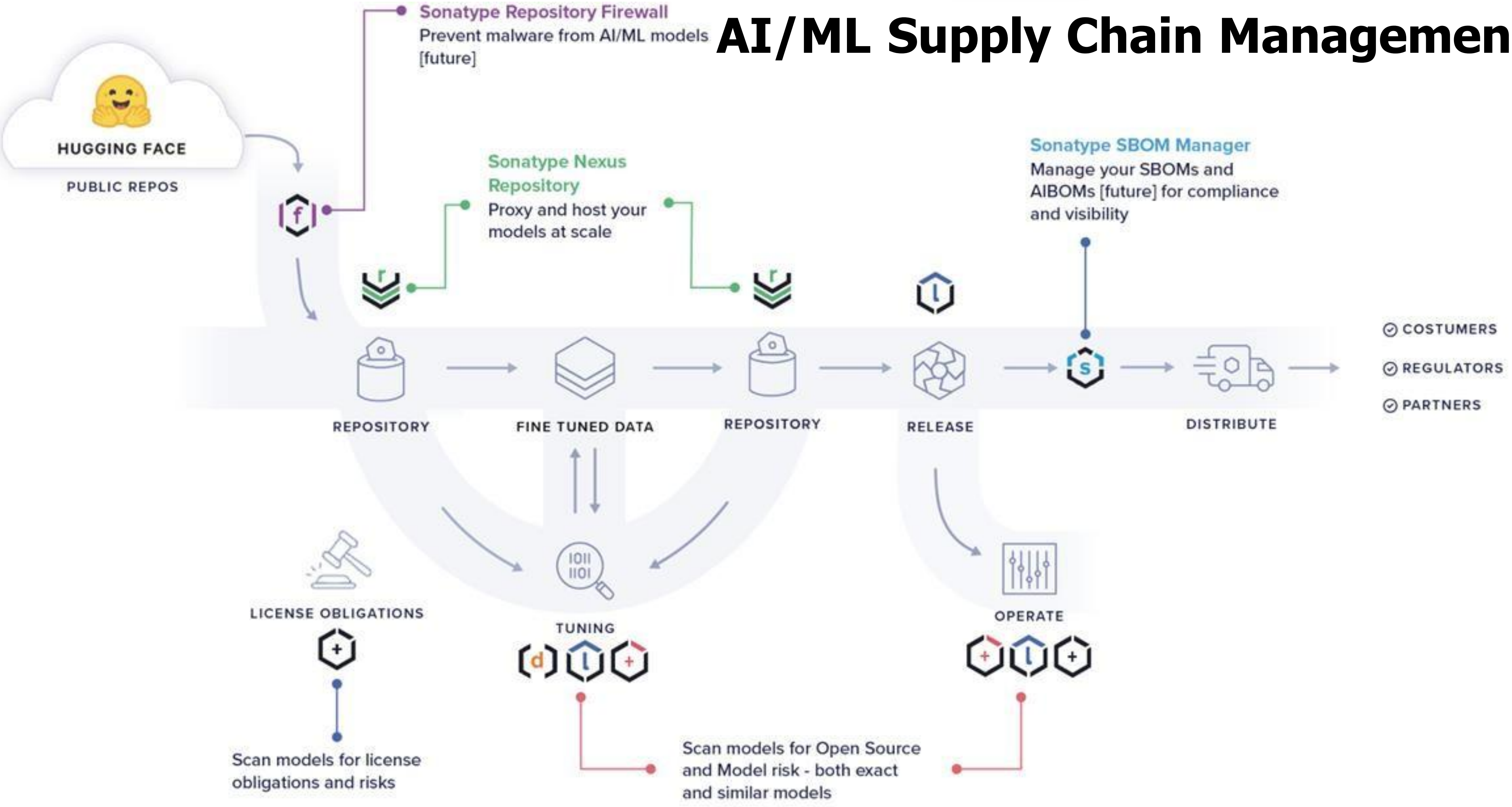
Developer downloads & uses, inadverantly voilating terms of original license



AI components usage in scanned applications

Policies and **Decisions** on usage will vary based on the **type of AI** used throughout the organization

AI/ML Supply Chain Management



Sonatype Repository Firewall
Prevent malware from AI/ML models [future]

Sonatype Nexus Repository
Proxy and host your models at scale

Sonatype SBOM Manager
Manage your SBOMs and AIBOMs [future] for compliance and visibility

Scan models for license obligations and risks

Scan models for Open Source and Model risk - both exact and similar models

sonatype

sonatype