ЯL ЯEVERSINGLABS

Exposing Critical Software Supply Chain Security Weaknesses

Katie Norton, Research Analyst, IDC
Dan Petrillo, VP, Product Marketing, RL

November 20, 2024

ReversingLabs At-A-Glance

40B+
Searchable Threat Repository

8X
Larger Than Nearest Competitor

60+
Cybersecurity Companies Trust RL

20M
Files Analyzed Daily

FASTEST
Software/File Deconstruction

3M
Malware Identified Daily

300
Employees Globally

CRN
5 Star Rated Partner Program

Gartner
Recognized for SSCS Solution

Verizon Business
DBIR
Report Contributor

Today's Presenters

Dan Petrillo

VP, Product Marketing
ReversingLabs

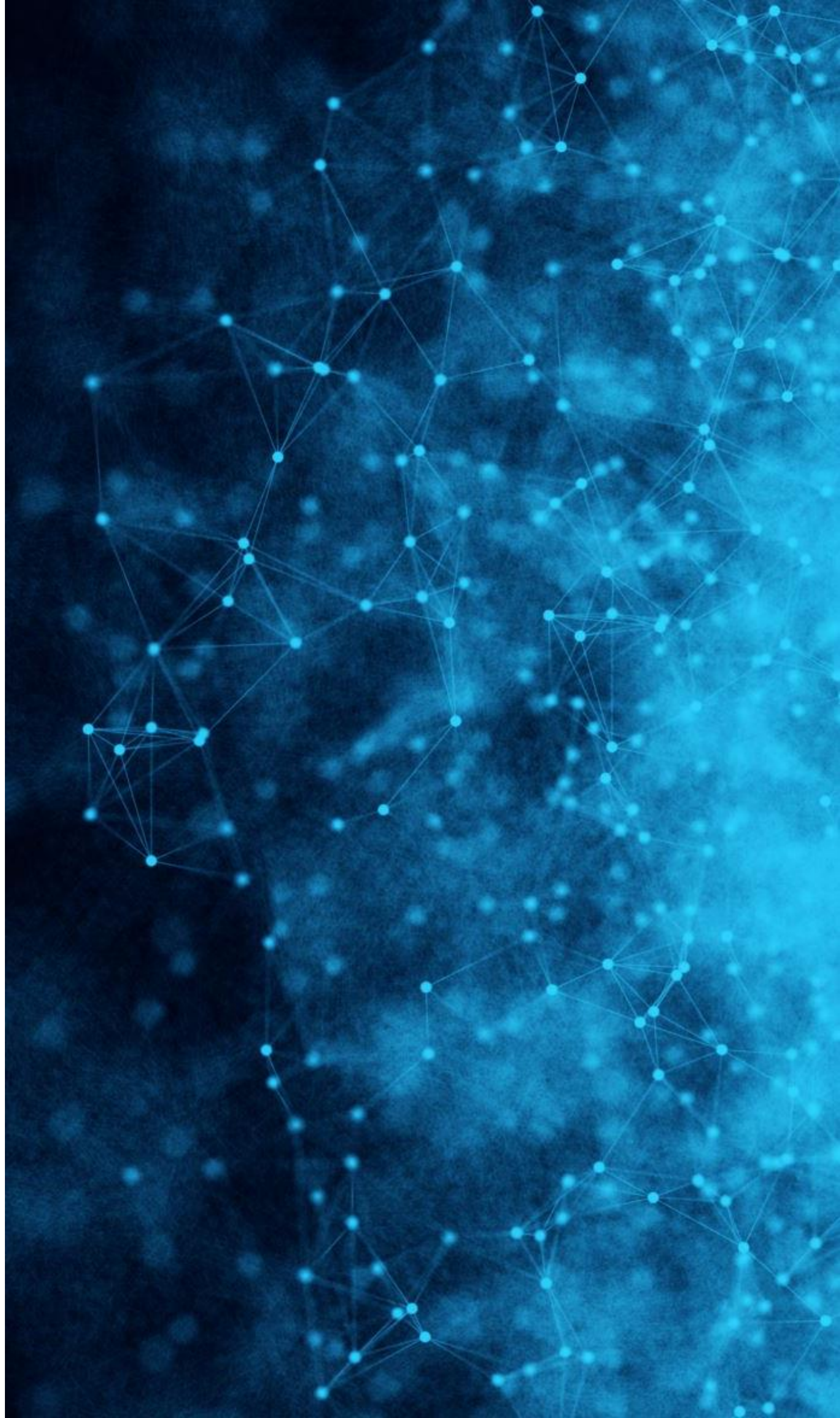
Katie Norton

Research Analyst
IDC

IDC | The Trusted Technology Research Brand

Global provider of market intelligence, insights, and data for nearly 60 years.

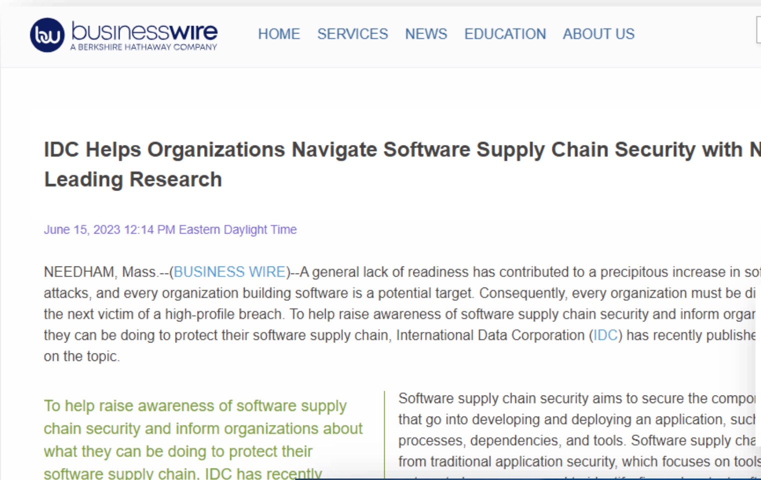
- Innovative products and platforms serving tech suppliers, tech buyers, and tech watchers.
- 5B+ data points helping business leaders at executives make well informed decisions.
- Highly configurable data and research used by customers globally to drive their strategic goals.
- Over 1,300 analysts providing unmatched global and local expertise across hundreds of tech and vertical markets.



IDC

The Software Supply Chain

By the Numbers



IDC Helps Organizations Navigate Software Supply Chain Security with New Industry-Leading Research

June 15, 2023 12:14 PM Eastern Daylight Time

NEEDHAM, Mass.--(BUSINESS WIRE)--A general lack of readiness has contributed to a precipitous increase in software supply chain attacks, and every organization building software is a potential target. Consequently, every organization must be di
the next victim of a high-profile breach. To help raise awareness of software supply chain security and inform orgar
they can be doing to protect their software supply chain, International Data Corporation (IDC) has recently publishe
on the topic.

To help raise awareness of software supply chain security and inform organizations about what they can be doing to protect their software supply chain, IDC has recently published a series of reports on the

Tweet this

Software supply chain security aims to secure the compo
that go into developing and deploying an application, such
processes, dependencies, and tools. Software supply cha
from traditional application security, which focuses on tools, technologies, and

survey, IDC found that less than 30% of
exposures, and 23% indicated that they

Bad actors now recognize that the softw
growing more patient and subtle, and tak
states or rogue hackers with criminal or
application software supply chain.

IDC PERSPECTIVE

Operationalizing SBOMs to Secure Your Software Supply Chain

Katie Norton Jim Mercer

EXECUTIVE SNAPSHOT

Operationalizing SBOMs to Secure Your Software Supply Chain

…und operationalizing software bill of materials (SBOMs) … SBOM adoption. It highlights frameworks, open … organizations with solutions to these

Recommended Actions

- As the dust settles on SBOMs, organizations must be attuned … initiatives that may require changes in tooling or workflow.
- In order to prepare for the next Log4j and future regulatory changes, organizations … working on an adaptable and flexible SBOM strategy as soon as possible.
- Align strategy with tooling that enables actionable decision making based on SBOM data, such as Dynamic SBOMs, VEX artifacts, and SBOM management solutions.
- SBOMs are not a cure-all and should be part of a comprehensive software supply chain strategy.

Source: IDC, 2023

IDC PERSPECTIVE

Future of Digital Innovation and DevSecOps: Understanding and Securing the Attack Vectors of the Modern Software Supply Chain

Jim Mercer

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: The Software Supply Chain

Digitally innovative organizations presumably know that bad actors are increasingly targeting their application software supply chains. Therefore, organizations must understand what makes up the software supply chain, how it can be targeted, and what approaches and tools can be used to harden it.

…eryone that touches an organization's code in the … ication software supply chains, with attackers … software supply chain attack, and they need to … security breach. … into their software supply chains.

…users of your software supply chains to have a clearer picture of risk and … be enhanced. … enforward protections, such as removing unused accounts, restricting access to … and enforcing least privileged access via role-based access controls. … your software supply chain as if you were already a victim of a security breach … supply chain security is a top priority for those who have been breached.

- **Prediction 5**: Securing the software supply chain will be a core competency embraced by 75% of large digital innovators by 2023.

The Software Supply Chain Demystified

Industry Insights to Understanding and Securing Your Software Factory

Katie Norton
…are Supply Chain Security
March 2024

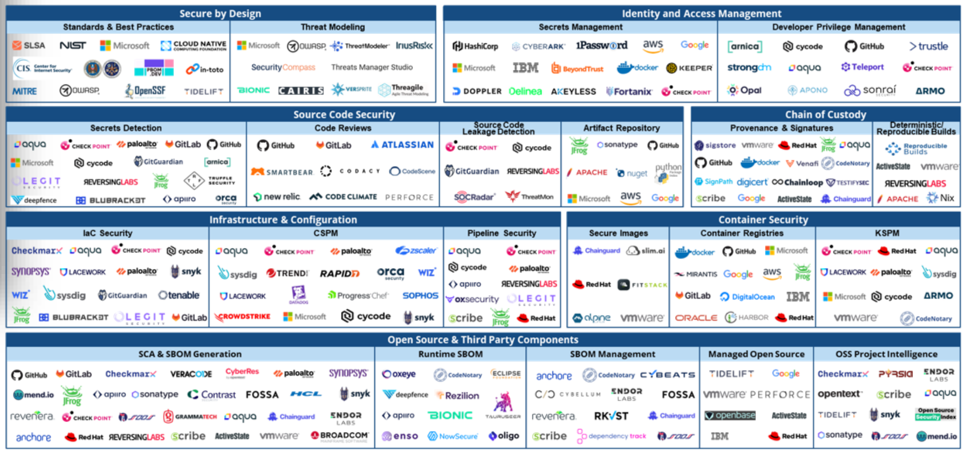
IDC LINK

Real-time IDC Research® opinion on industry news, trends and events

The xz Utils Backdoor and Securing the Open Source Software Supply Chain

April 12, 2024

IDC Market Glance: Software Supply Chain Security

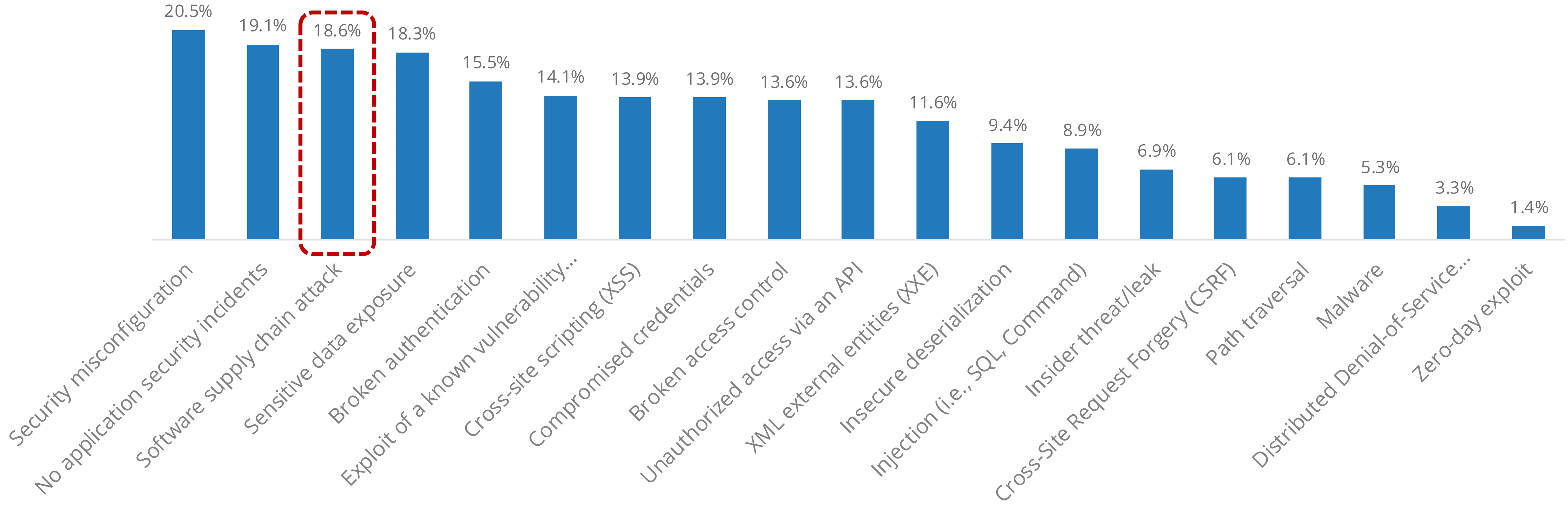

Secure by Design
Standards & Best Practices: SLSA, NIST, Microsoft, Cloud Native Computing Foundation, CIS Center for Internet Security, PBOM.DEV, in-toto, MITRE, OWASP, OpenSSF, Tidelift
Threat Modeling: Microsoft, OWASP, ThreatModeler, IriusRisk, Security Compass, Threats Manager Studio, Bionic, CAIRIS, VerSprite, Threagile
Identity and Access Management
Secrets Management: HashiCorp, CyberArk, 1Password, aws, Google, Microsoft, IBM, BeyondTrust, docker, Keeper, Doppler, Delinea, Akeyless, Fortanix, Check Point
Developer Privilege Management: arnica, cycode, GitHub, trustle, strongdm, aqua, Teleport, Check Point, Opal, Apono, sonrai, ARMO
Source Code Security
Secrets Detection: aqua, Check Point, paloalto, GitLab, GitHub, Microsoft, cycode, GitGuardian, arnica, Legit Security, ReversingLabs, JFrog, Truffle Security, deepfence, BluBracket, apiiro, orca security
Code Reviews: GitHub, GitLab, Atlassian, SmartBear, Codacy, CodeScene, new relic, Code Climate, Perforce
Source Code Leakage Detection: Check Point, cycode, GitGuardian, ReversingLabs, SOCRadar, ThreatMon
Artifact Repository: JFrog, sonatype, GitHub, Apache, nuget, python Package Index, Microsoft, aws, Google
Chain of Custody
Provenance & Signatures: sigstore, vmware, Red Hat, JFrog, aqua, GitHub, docker, Venafi, CodeNotary, SignPath, digicert, Chainloop, TestifySec, scribe, Google, ActiveState, Chainguard
Deterministic/Reproducible Builds: Reproducible Builds, ActiveState, vmware, ReversingLabs, Apache, Nix
Infrastructure & Configuration
IaC Security: Checkmarx, aqua, Check Point, cycode, Synopsys, Lacework, paloalto, snyk, wiz, sysdig, GitGuardian, tenable, JFrog, BluBracket, Legit Security, GitLab
CSPM: aqua, Check Point, paloalto, zscaler, sysdig, Trend, Rapid7, orca security, wiz, Lacework, Datadog, Progress Chef, Sophos, CrowdStrike, Microsoft, cycode, snyk
Pipeline Security: aqua, Check Point, cycode, paloalto, apiiro, ReversingLabs, oxsecurity, Legit Security, scribe, JFrog, Red Hat
Container Security
Secure Images: Chainguard, slim.ai, Red Hat, Fitstack, alpine, vmware
Container Registries: docker, GitHub, Microsoft, Mirantis, Google, aws, JFrog, GitLab, DigitalOcean, IBM, Oracle, Harbor, Red Hat
KSPM: Check Point, Red Hat, aqua, Lacework, paloalto, sysdig, Microsoft, cycode, ARMO, vmware, CodeNotary
Open Source & Third Party Components
SCA & SBOM Generation: GitHub, GitLab, Checkmarx, Veracode, CyberRes, paloalto, Synopsys, mend.io, JFrog, apiiro, sonatype, Contrast, FOSSA, HCL, snyk, revenera, Check Point, Rezilion, GrammaTech, aqua, Chainguard, Endor Labs, anchore, Red Hat, ReversingLabs, scribe, ActiveState, vmware, Broadcom
Runtime SBOM: oxeye, CodeNotary, Eclipse Foundation, deepfence, Rezilion, TauruSeer, apiiro, Bionic, enso, NowSecure, oligo
SBOM Management: anchore, CodeNotary, Cybeats, Cybellum, Endor Labs, FOSSA, revenera, RKVST, Chainguard, scribe, dependency track
Managed Open Source: Tidelift, Google, vmware, Perforce, openbase, ActiveState, IBM, Red Hat
OSS Project Intelligence: Checkmarx, Phylum, Endor Labs, opentext, scribe, aqua, Tidelift, snyk, Open Source Security Index, sonatype, mend.io

Source: IDC, 2Q23

For areas on which IDC publishes market share data, the top 3-5 market share leaders are represented.
For areas on which IDC does not publish market share data, vendor selection is up to analyst discretion.

Almost 1 in 5 organizations indicated they experienced a software supply chain attack in the last 12 months.

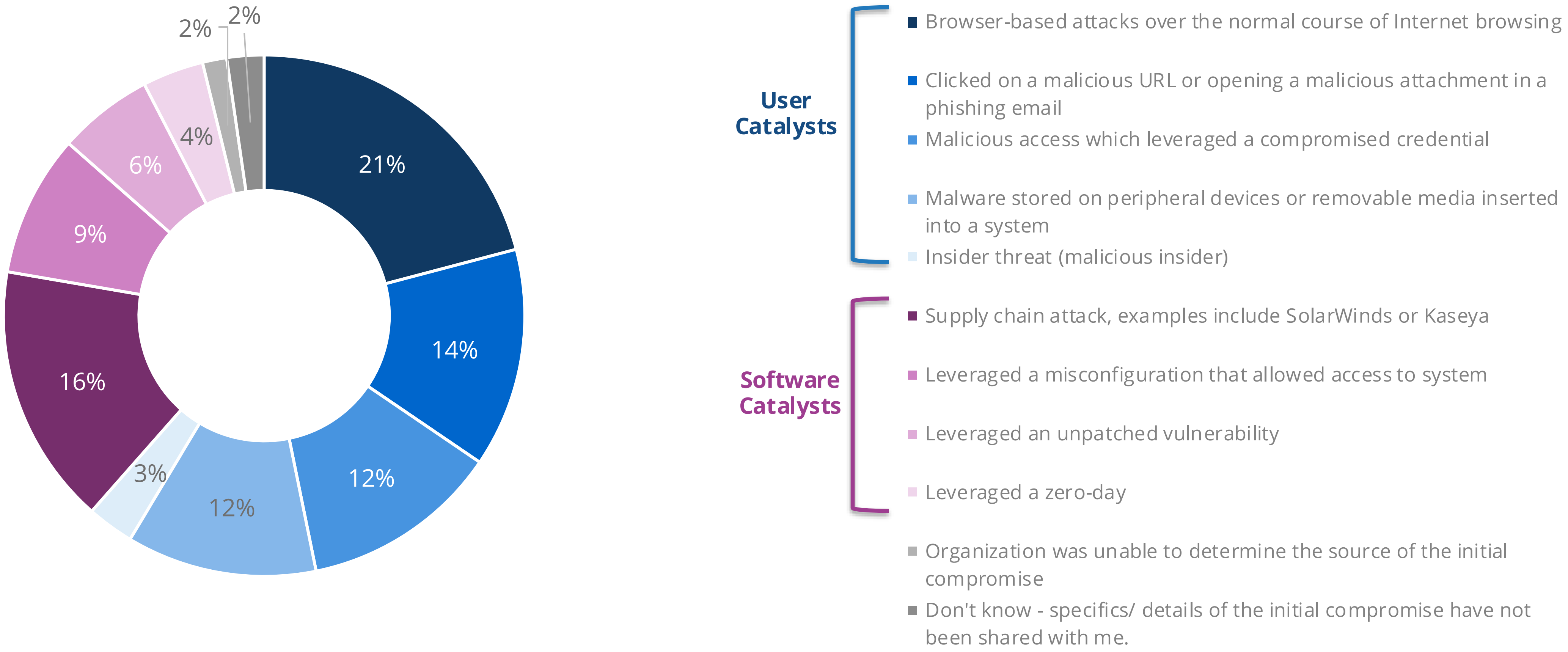
Q: What types of application security incidents have you experienced within the last 12-months?



Source: DevSecOps and Software Supply Chain Security, IDC, July 2024, n = 361

Software supply chain attacks lead to ransomware incidents.

Q: For your most recent ransomware incident that blocked access to systems or data, what was the most significant source of the initial compromise?



User Catalysts

- ■ Browser-based attacks over the normal course of Internet browsing
- ■ Clicked on a malicious URL or opening a malicious attachment in a phishing email
- ■ Malicious access which leveraged a compromised credential
- ■ Malware stored on peripheral devices or removable media inserted into a system
- ■ Insider threat (malicious insider)

Software Catalysts

- ■ Supply chain attack, examples include SolarWinds or Kaseya
- ■ Leveraged a misconfiguration that allowed access to system
- ■ Leveraged an unpatched vulnerability
- ■ Leveraged a zero-day

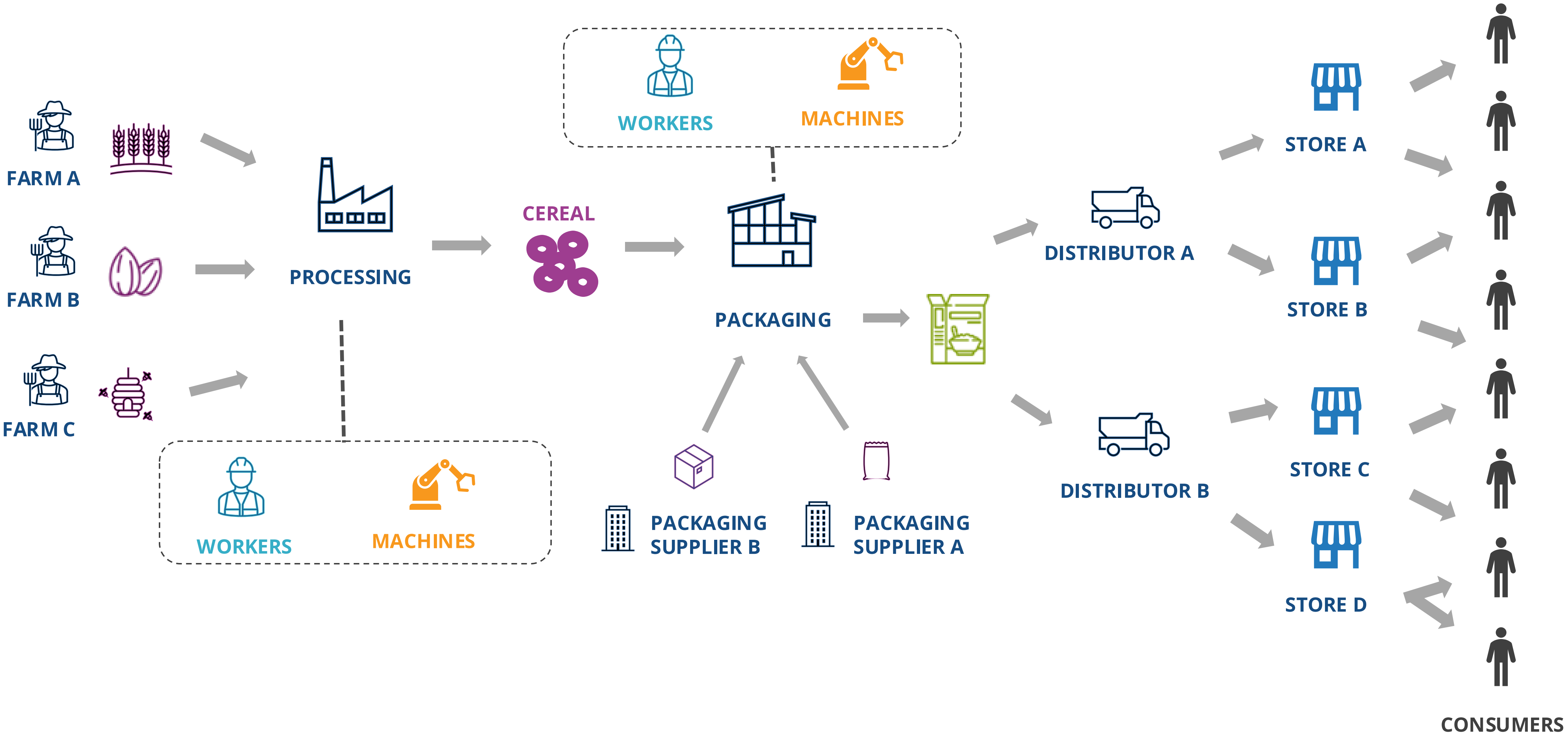
- ■ Organization was unable to determine the source of the initial compromise
- ■ Don't know - specifics/ details of the initial compromise have not been shared with me.

Source: Future Enterprise Resiliency & Spending Survey Wave 6, IDC, June 2024, n = 479

Defining the Supply Chain

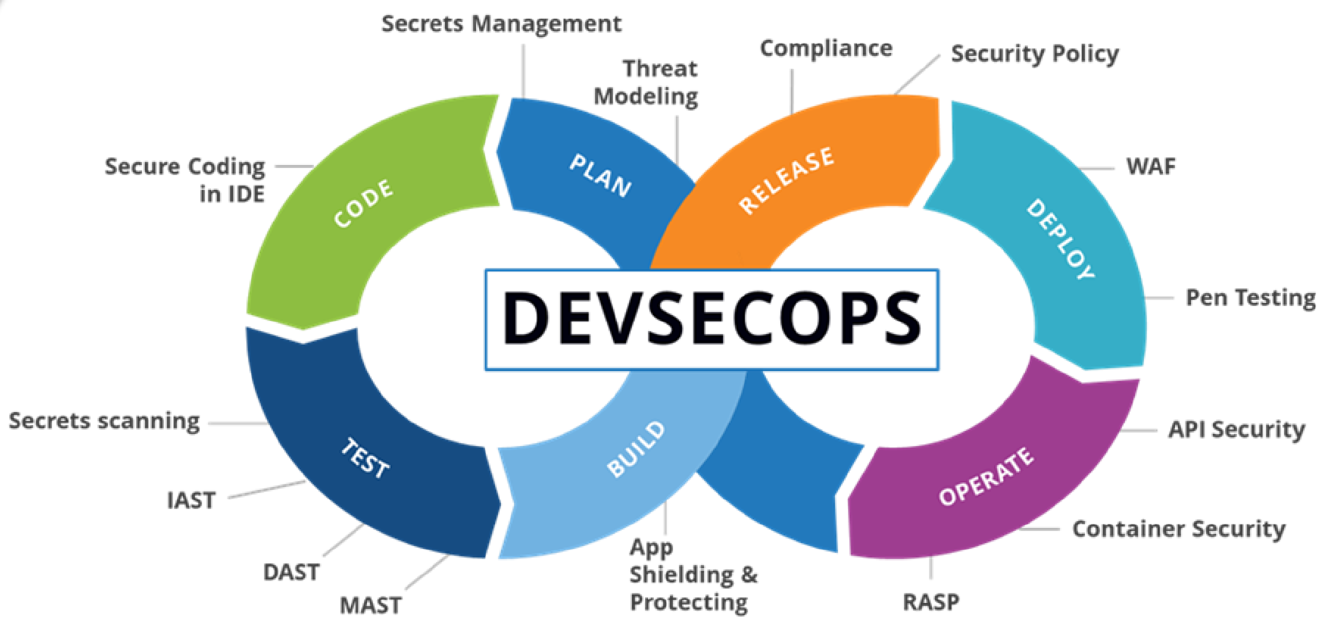
> ***"A supply chain is an entire system of producing and delivering a product or service, from the very beginning stage of sourcing the raw materials to the final delivery of the product or service to end-users."***
>
> **- Corporate Finance Institute (CFI)**

Visualizing A Supply Chain



Misconception #1: DevSecOps/AppSec tools are sufficient to protect the software supply chain.

Software Supply Chain Security



DEVSECOPS

CODE
Secure Coding in IDE

PLAN
Secrets Management
Threat Modeling

RELEASE
Compliance
Security Policy

DEPLOY
WAF
Pen Testing

OPERATE
API Security
Container Security
RASP

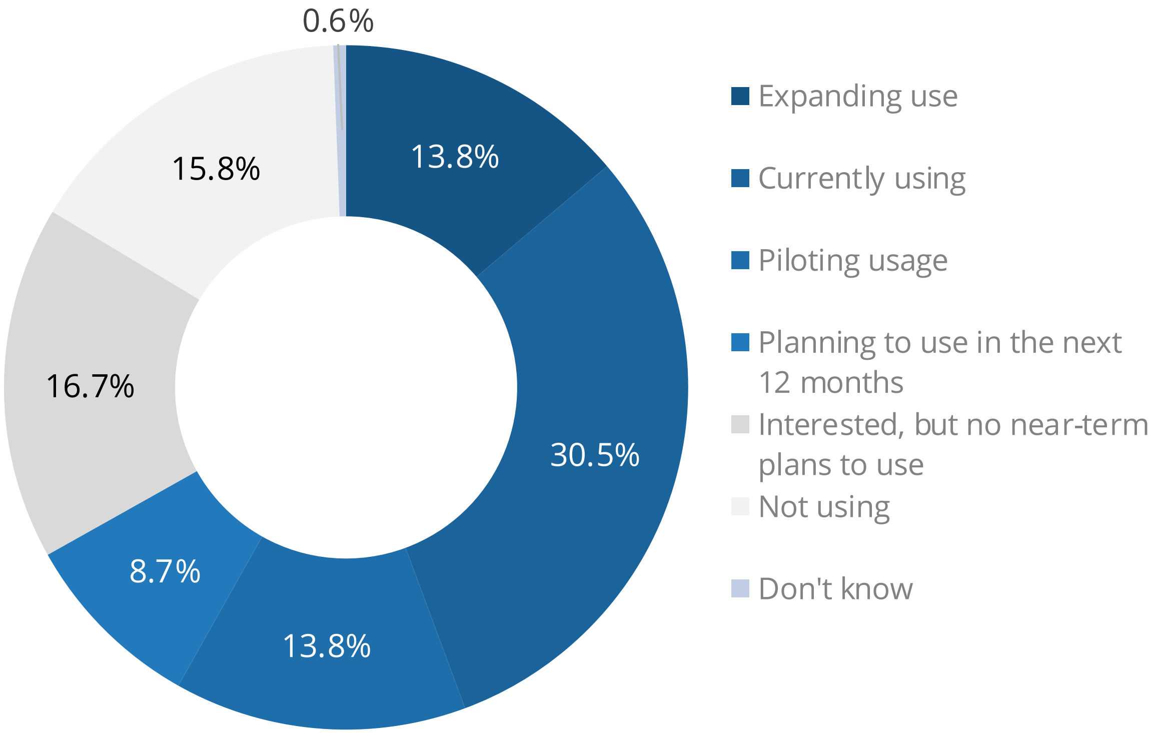
BUILD
App Shielding & Protecting

TEST
Secrets scanning
IAST
DAST
MAST

- ✓ SDLC Identity & Access Management
- ✓ Provenance & Attestation
- ✓ Reproducible Builds
- ✓ Hardened Container Images
- ✓ Open Source Ecosystem Monitoring
- ✓ Managed Open Source
- ✓ SBOMs
- ✓ Pipeline Security
- ✓ Malware Detection

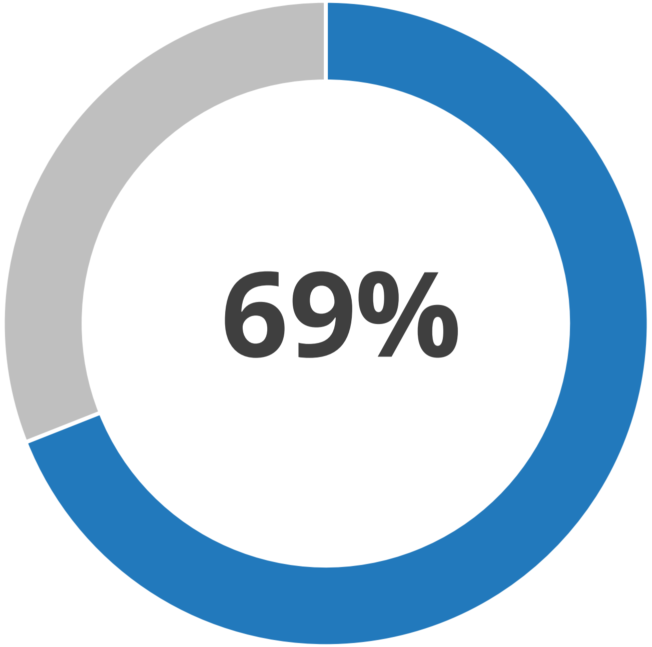
Misconception #2: SBOMs are the software supply chain silver bullet.

Q. Which best describes the current adoption of producing a software bill of materials (SBOM) for the applications your organization develops and deploys?



Source: DevSecOps and Software Supply Chain Security, IDC, July 2024, n=361

Misconception #3: We only need to care about CVEs.

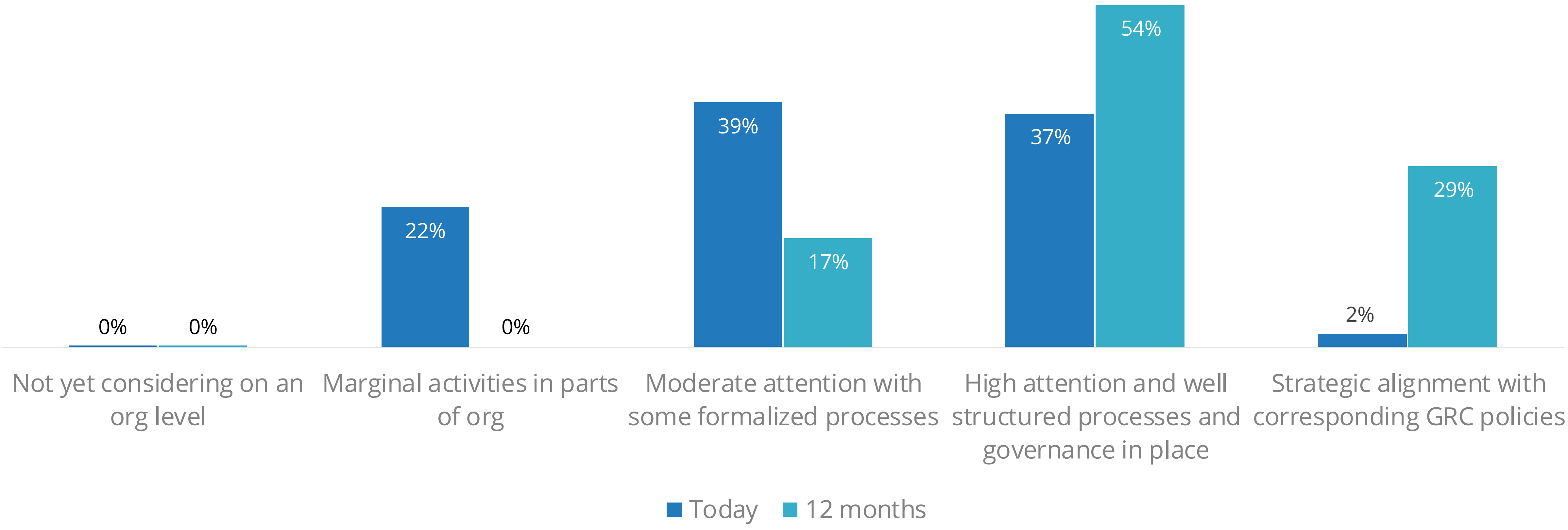


Not scanning their binaries for malware

Source: DevSecOps and Software Supply Chain Security, IDC, July 2024, n=361

Securing your software supply chain weaknesses must be a strategic imperative.

Q. Which one statements best describes your organization's approach to securing your software supply chain today?



Source: App Development and Delivery Survey, IDC, Aug 2024, n=720

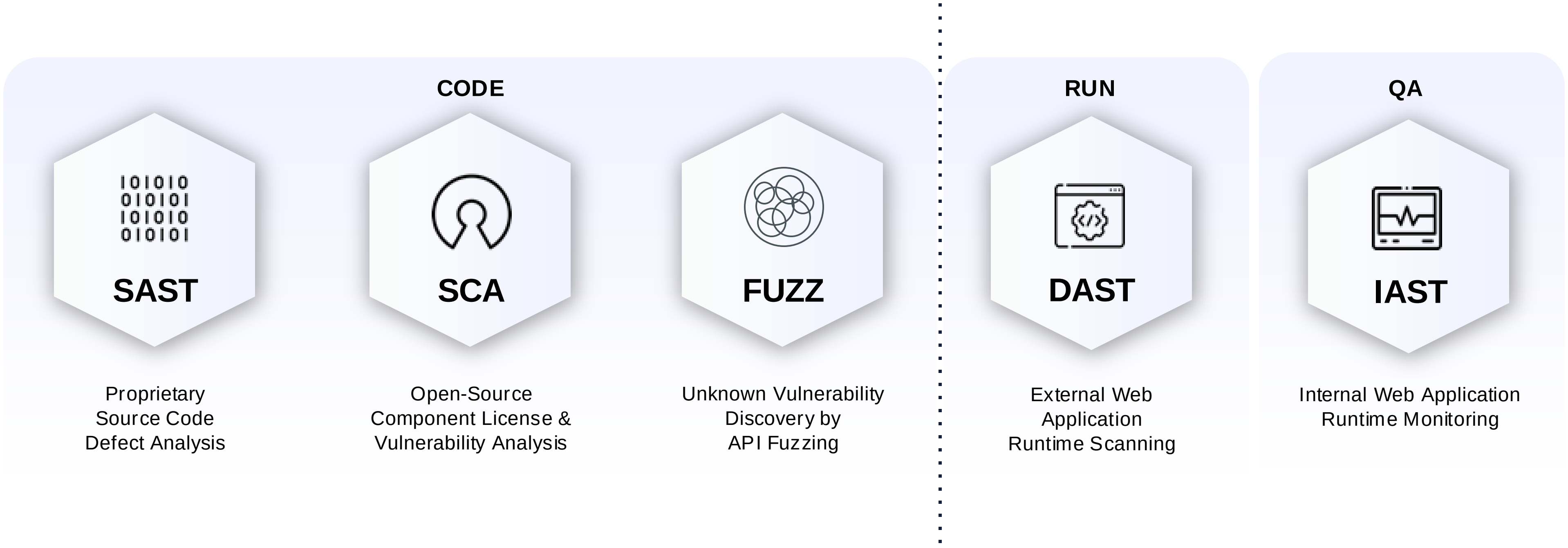
We would love to hear from you.

Which of these statements best describes your organization’s approach to securing your software supply chain today?

Links in the Chain

1: Software Providers

The Legacy Approach



CODE

SAST

Proprietary
Source Code
Defect Analysis

SCA

Open-Source
Component License &
Vulnerability Analysis

FUZZ

Unknown Vulnerability
Discovery by
API Fuzzing

RUN

DAST

External Web
Application
Runtime Scanning

QA

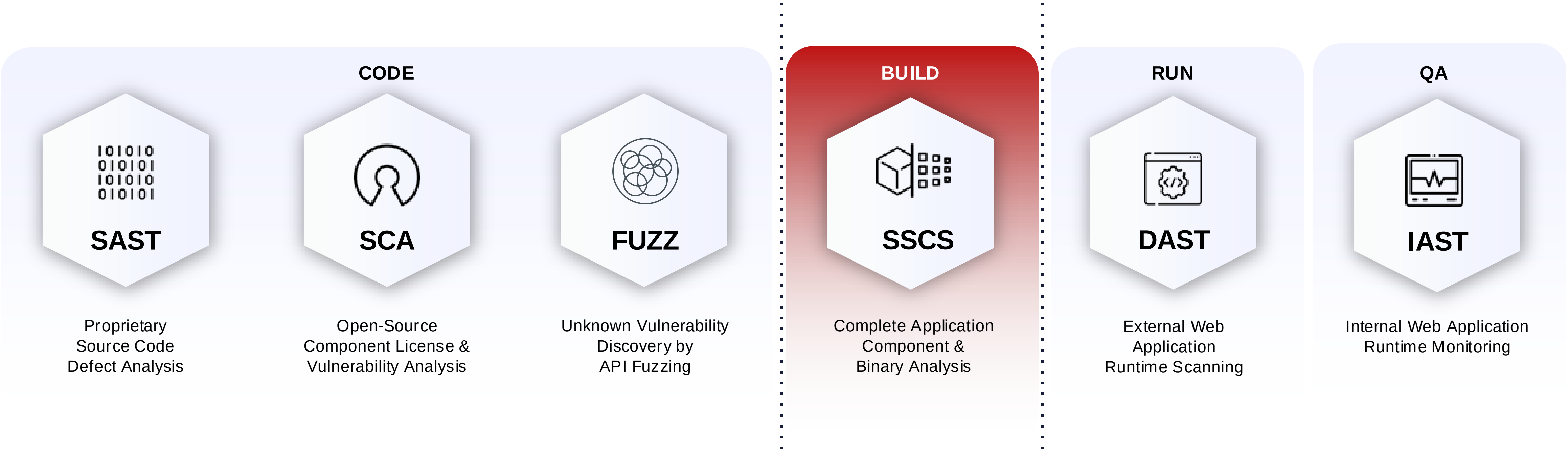
IAST

Internal Web Application
Runtime Monitoring

The legacy methods fail to deliver sufficient and complete security.

There is a reason they crash the whole car.

Modern Approach



CODE

SAST

Proprietary Source Code Defect Analysis

SCA

Open-Source Component License & Vulnerability Analysis

FUZZ

Unknown Vulnerability Discovery by API Fuzzing

BUILD

SSCS

Complete Application Component & Binary Analysis

RUN

DAST

External Web Application Runtime Scanning

QA

IAST

Internal Web Application Runtime Monitoring

A critical build exam delivers the final analysis to close a major gap in the SDLC.

Links in the Chain

2: Software Buyers

Legacy Solutions: **No Primary Control**

Questionnaires

- Rely on truthful & accurate self-attestation
- Based on “inherent trust model”

SBOM

- Essential but basically a list of ingredients
- Doesn’t identify risks and threats

Pentesting

- Fundamental practice to mimic threat actor
- Too expensive to scale to address TPSRM

Security Rating Services

- Convey a vendor’s exposure with a rating
- Doesn’t identify malware, tampering, etc.

Sandbox

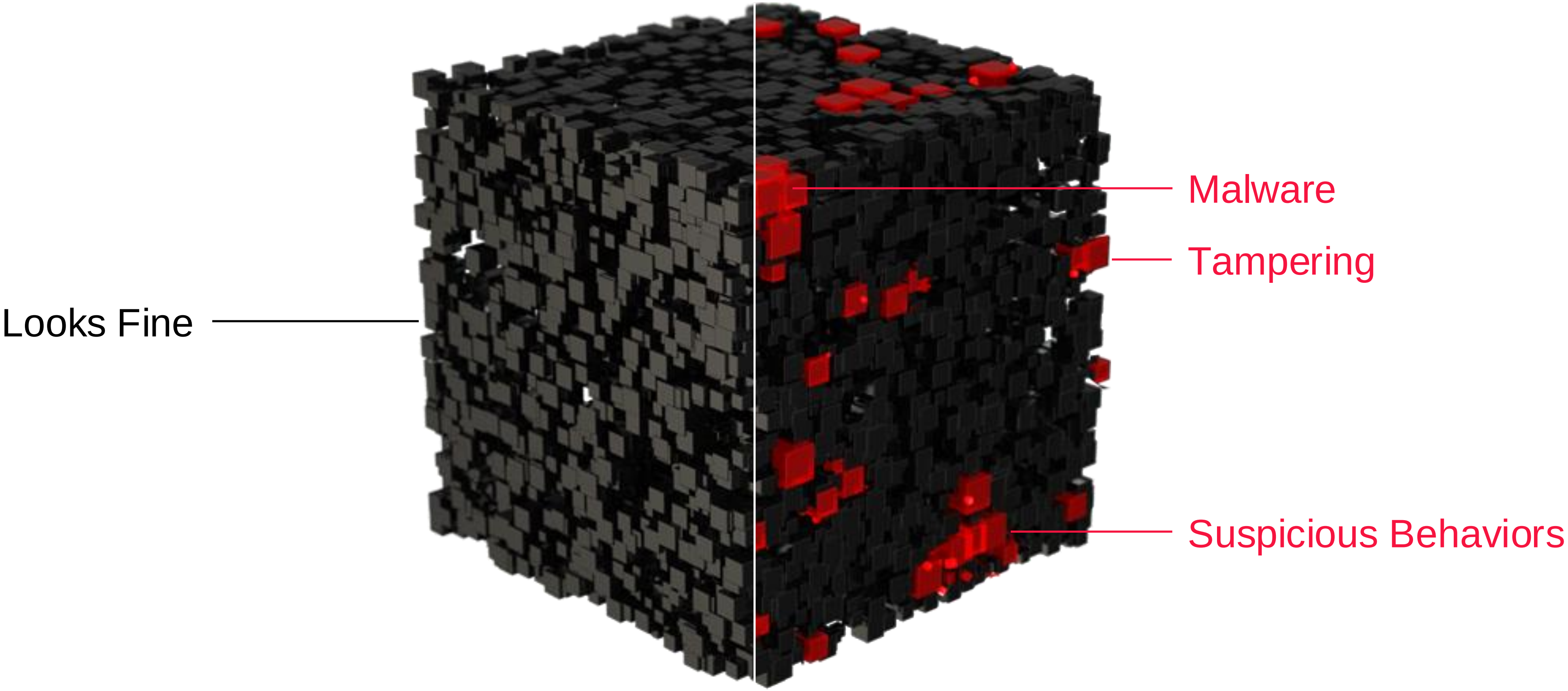
- Costly and requires execution or “detonation”
- Resource intensive, costly, and not scalable

> “SOC 2, ISOs, questionnaires, information in spreadsheets… that evaluation doesn't really give you enough to be able to truly assess the risk of the product that you're buying.”

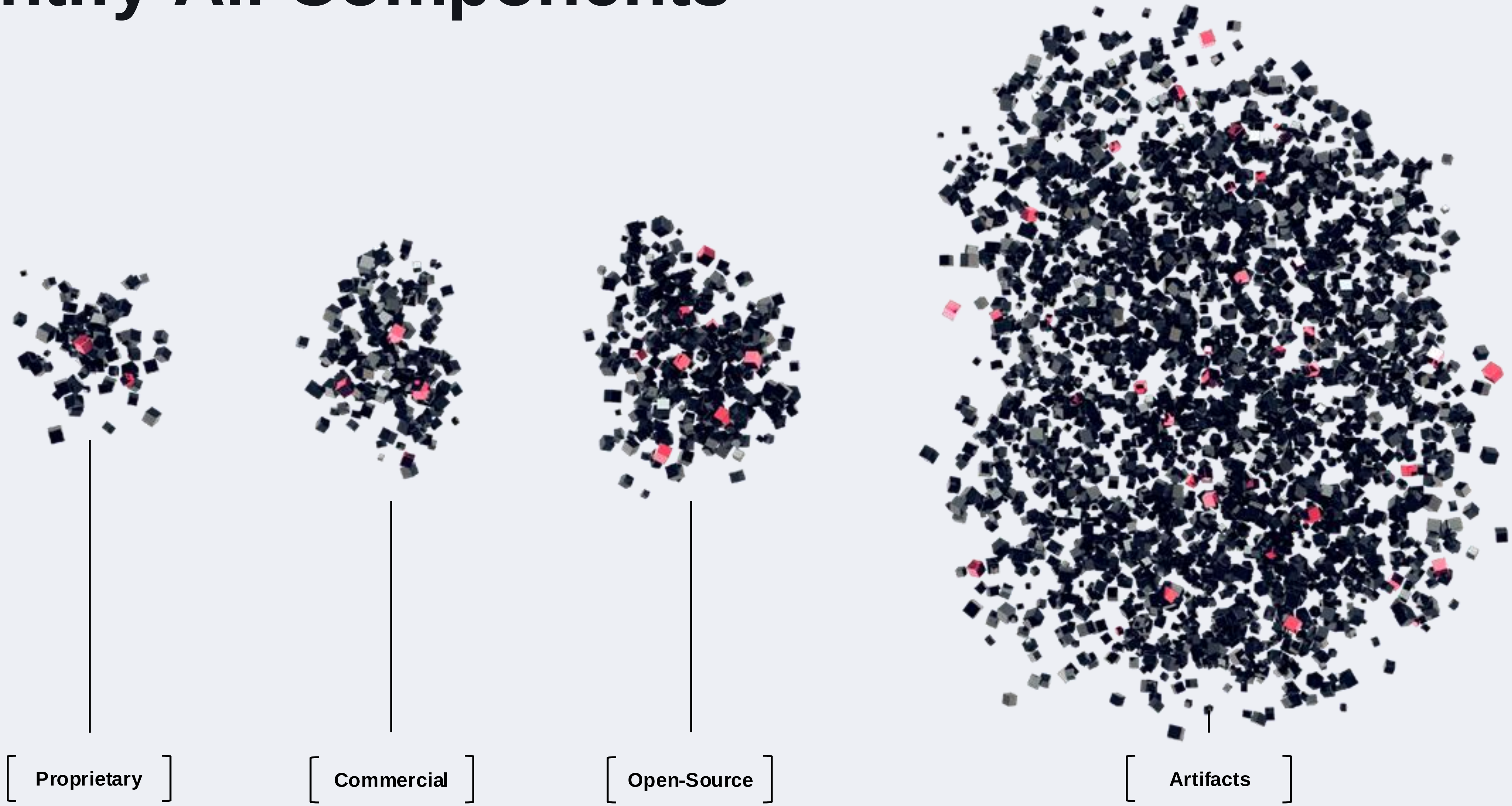
Tim Brown, CISO

SOLARWINDS

Software Buyer Challenge: **Lack of Visibility**



Identify All Components



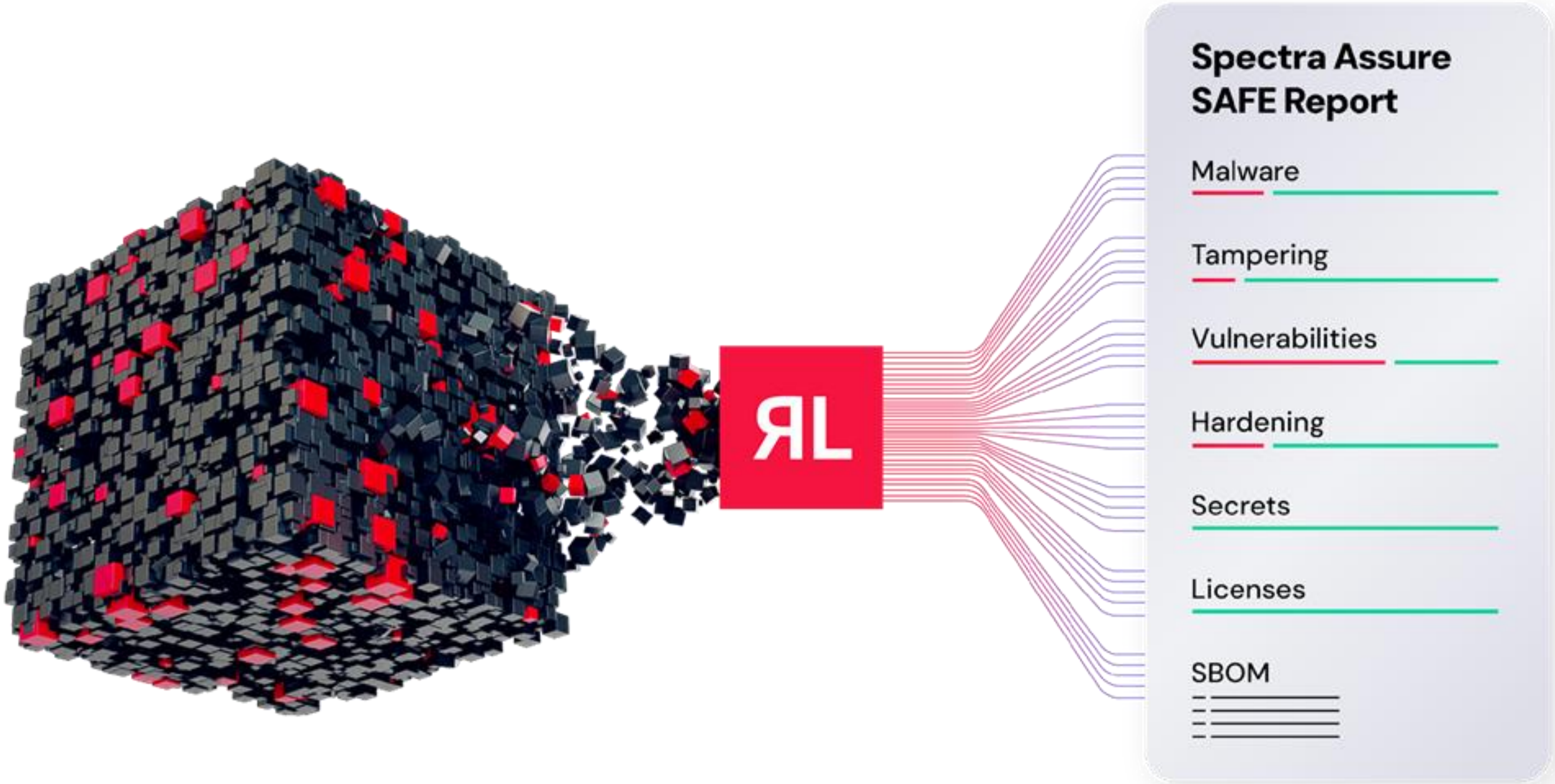
Proprietary

Commercial

Open-Source

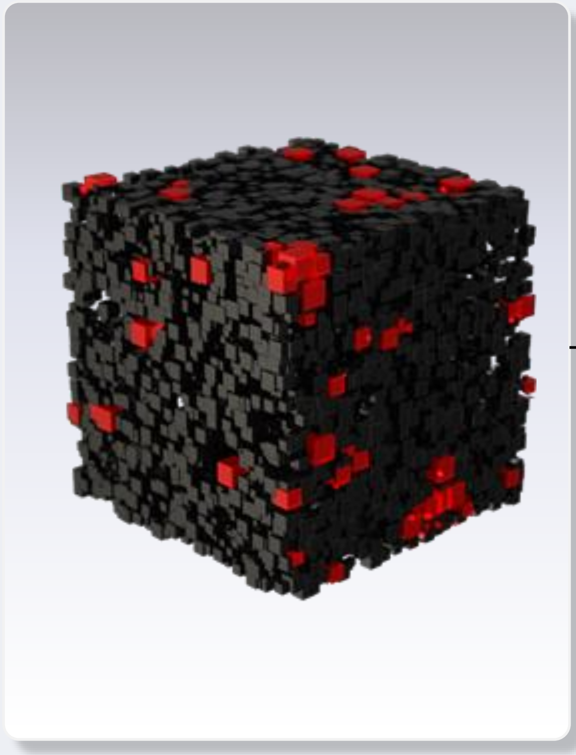
Artifacts

Identify Critical Risks and Threats



Software Buyers need a primary control to identify malware, tampering, and more - without source code.

Going Beyond the SBOM



Traditional SBOM

```
{
  author name
  supplier name
  component name
  component hash
  version string
  identifier
  Relationship
}
```

The Choice

A List?

or

The Risks?

Links in the Chain

3: Collaboration is Key

The Modern Approach: **Collaboration is Key**

Software Producers **IT Security** **Risk Management**

Application Security | Development | Engineering | Security Operations | Product Security Incident Response

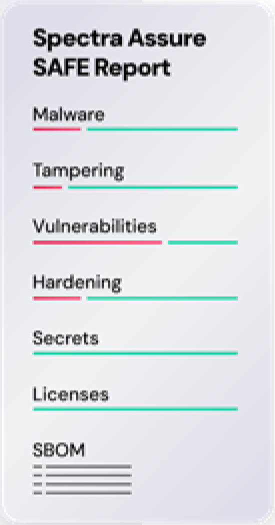
Identify Software Supply Chain Issues Before Release

Continuously Monitor For Supply Chain Attacks

Find Hidden Threats Before Deployment or Updates

A NEW ERA OF TRANSPARENCY

Software Providers



Spectra Assure SAFE Report

Malware

Tampering

Vulnerabilities

Hardening

Secrets

Licenses

SBOM

Software Buyers

We would love to hear from you.

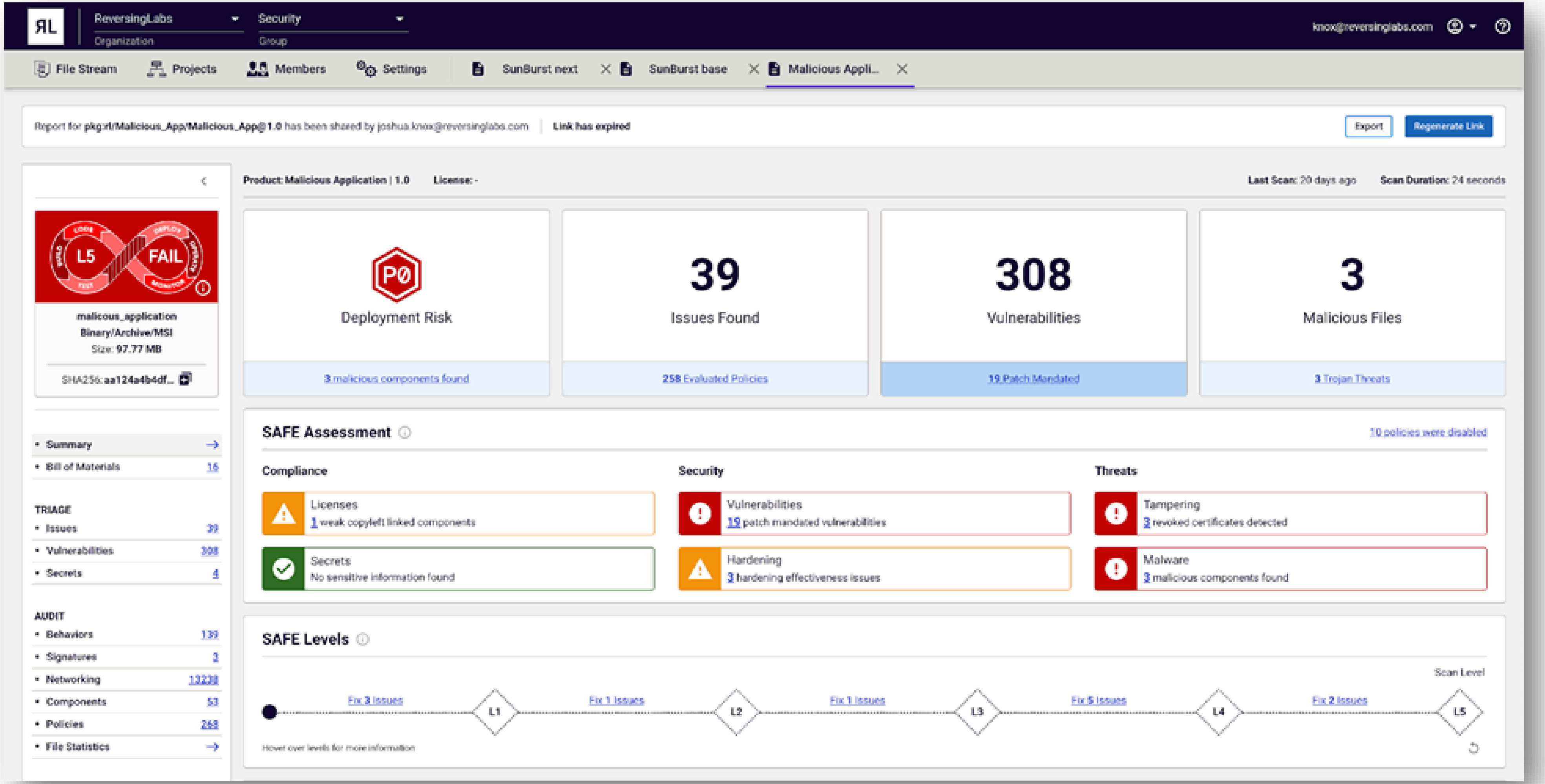
How would you rate the level of transparency between you and your vendors?

ЯL Spectra Assure™

Addressing ALL Links in the Chain

4: End to End SSCS

Spectra Assure SAFE Report



Report for **pkg:rl/Malicious_App/Malicious_App@1.0** has been shared by joshua.knox@reversinglabs.com | **Link has expired**

Product: **Malicious Application | 1.0** **License:** -

Last Scan: 20 days ago **Scan Duration:** 24 seconds

malicous_application
Binary/Archive/MSI
Size: **97.77 MB**
SHA256: **aa124a4b4df...**

Summary	→
Bill of Materials	16

TRIAGE

Issues	39
Vulnerabilities	308
Secrets	4

AUDIT

Behaviors	139
Signatures	3
Networking	13238
Components	53
Policies	268
File Statistics	→

P0	39	308	3
Deployment Risk	Issues Found	Vulnerabilities	Malicious Files
3 malicious components found	258 Evaluated Policies	19 Patch Mandated	3 Trojan Threats

SAFE Assessment

10 policies were disabled

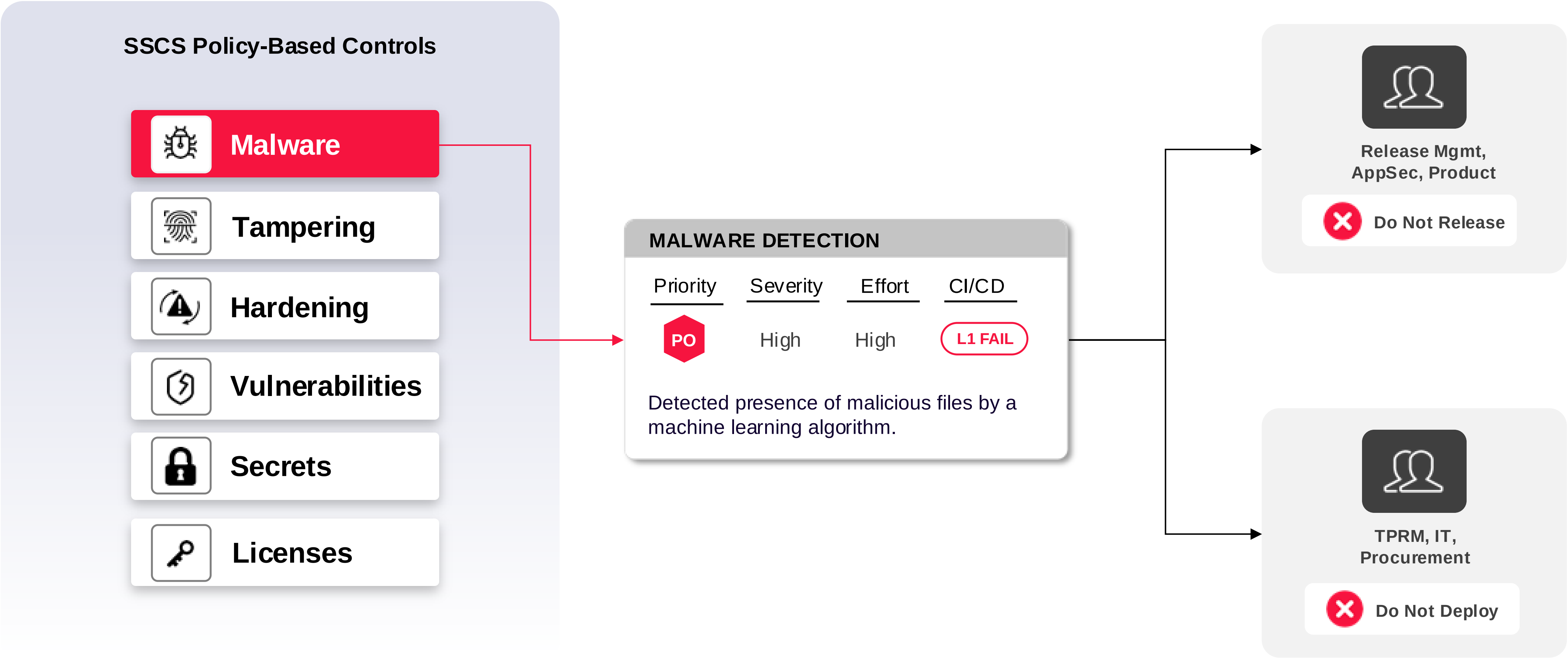
Compliance	Security	Threats
Licenses 1 weak copyleft linked components	Vulnerabilities 19 patch mandated vulnerabilities	Tampering 3 revoked certificates detected
Secrets No sensitive information found	Hardening 3 hardening effectiveness issues	Malware 3 malicious components found

SAFE Levels

Hover over levels for more information

Spectra Assure report delivers the most comprehensive SBOM and risk assessment for an application.

How Spectra Assure Stops The Next Attack



SSCS Policy-Based Controls

- Malware
- Tampering
- Hardening
- Vulnerabilities
- Secrets
- Licenses

MALWARE DETECTION

Priority	Severity	Effort	CI/CD
PO	High	High	L1 FAIL

Detected presence of malicious files by a machine learning algorithm.

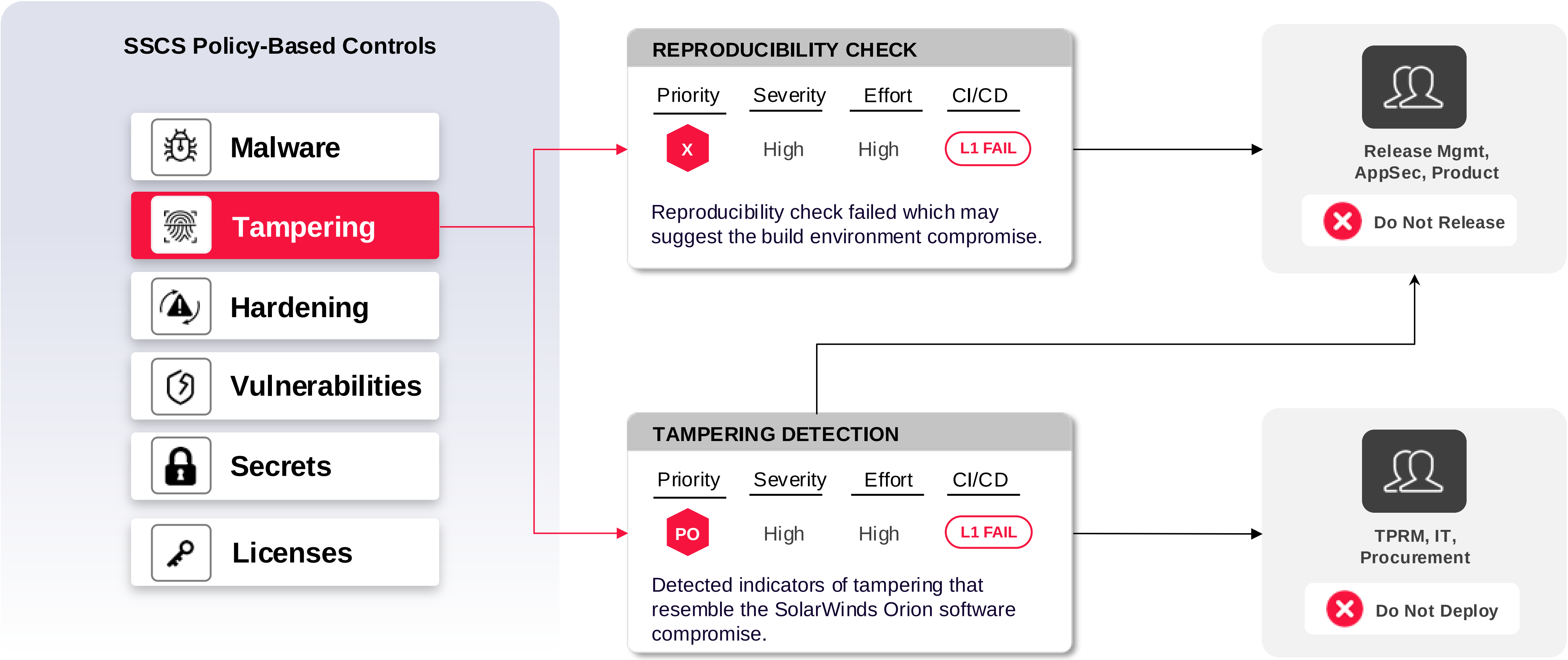
Release Mgmt, AppSec, Product

☒ Do Not Release

TPRM, IT, Procurement

☒ Do Not Deploy

How Spectra Assure Stops The Next Attack



SSCS Policy-Based Controls

- Malware
- Tampering
- Hardening
- Vulnerabilities
- Secrets
- Licenses

REPRODUCIBILITY CHECK

Priority	Severity	Effort	CI/CD
X	High	High	L1 FAIL

Reproducibility check failed which may suggest the build environment compromise.

Release Mgmt, AppSec, Product

☒ Do Not Release

TAMPERING DETECTION

Priority	Severity	Effort	CI/CD
PO	High	High	L1 FAIL

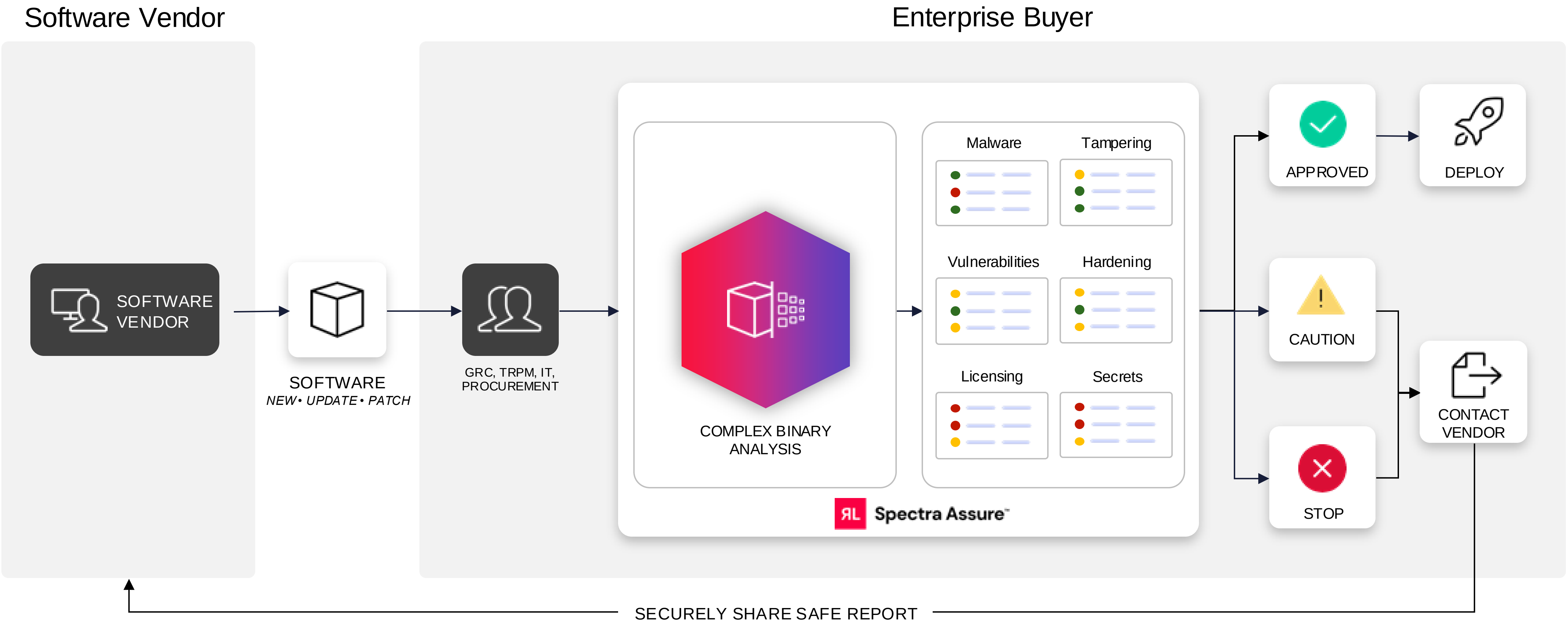
Detected indicators of tampering that resemble the SolarWinds Orion software compromise.

TPRM, IT, Procurement

☒ Do Not Deploy

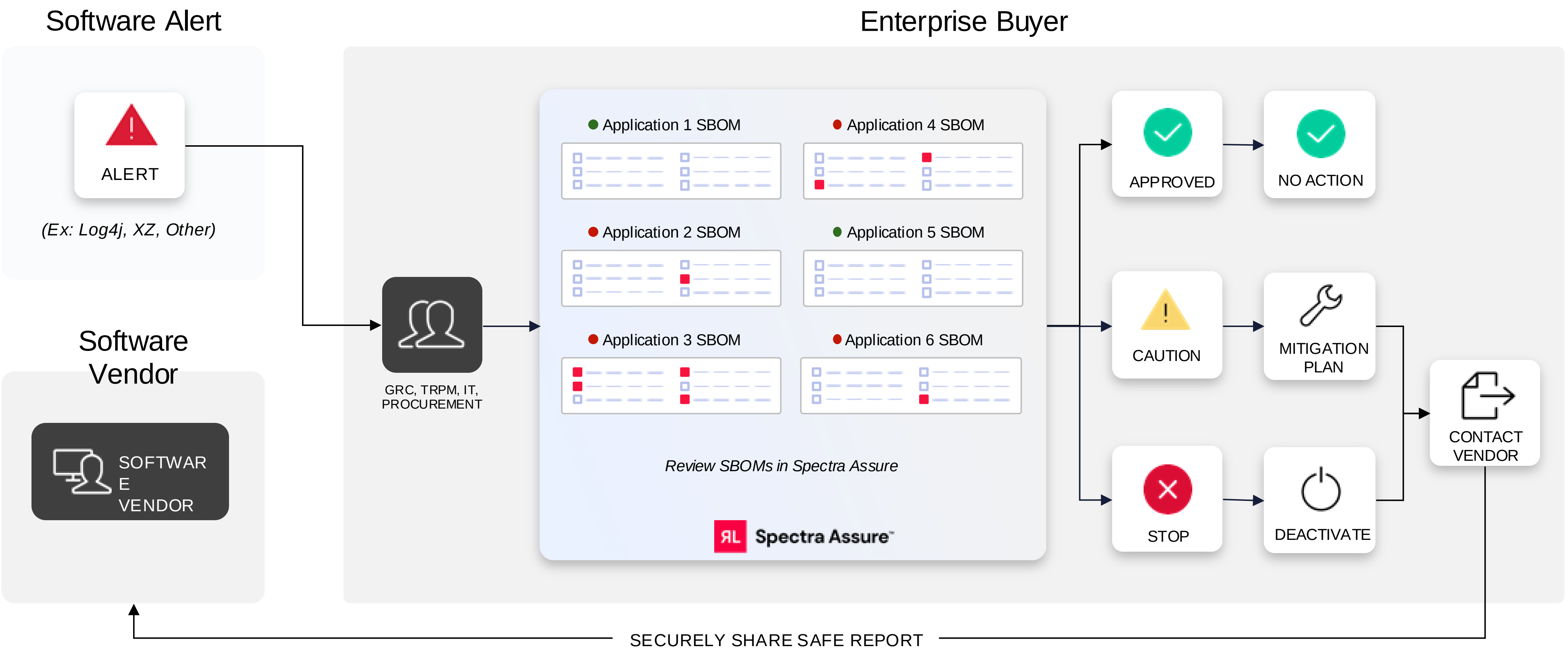
Mitigate Third-Party Software Risk

Control & Collaboration in Purchase & Deployment

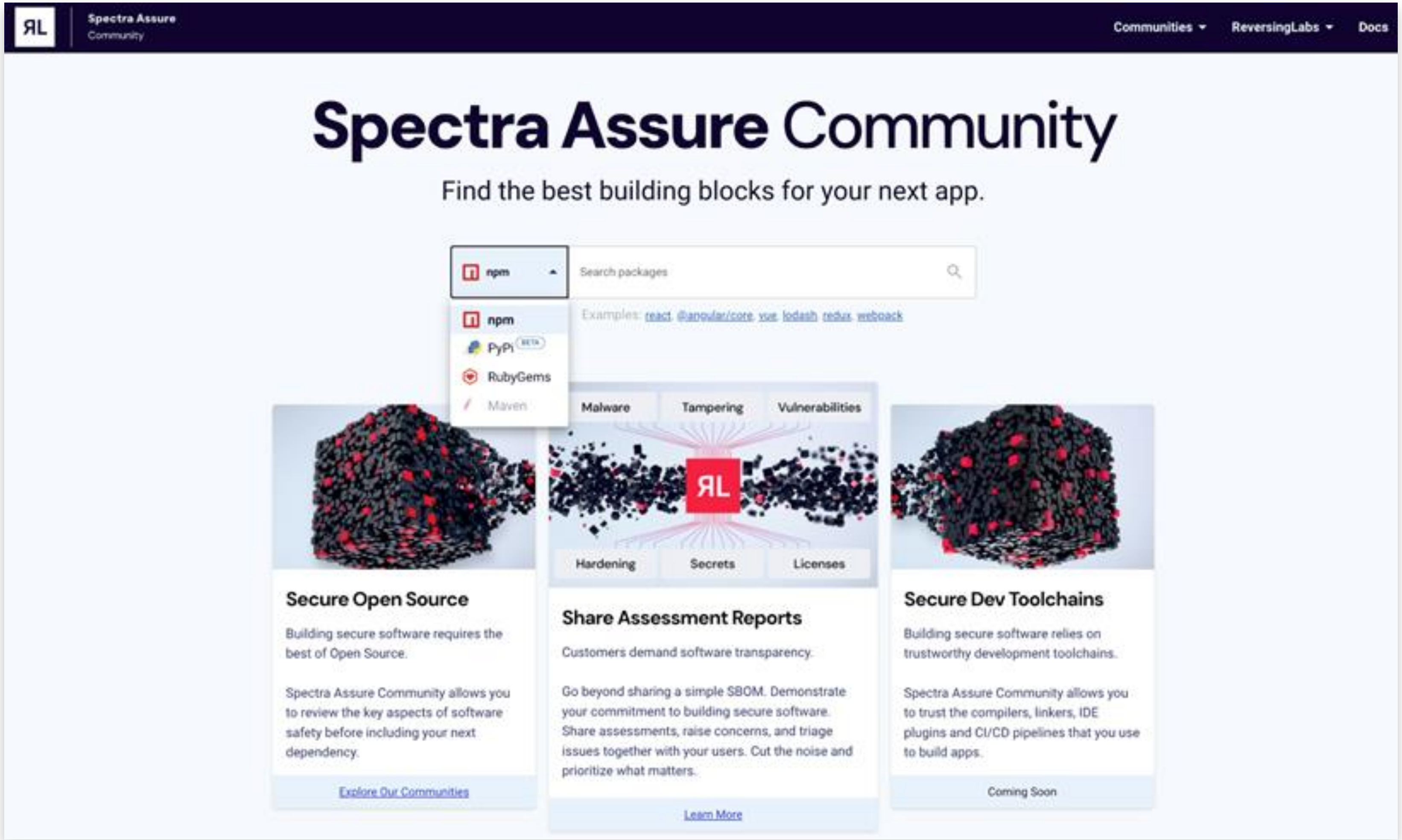


Mitigate Third-Party Software Risk

Monitoring Software



Free Resource…no strings attached, really.



Spectra Assure Community

Find the best building blocks for your next app.

Secure Open Source

Building secure software requires the best of Open Source.

Spectra Assure Community allows you to review the key aspects of software safety before including your next dependency.

Explore Our Communities

Share Assessment Reports

Customers demand software transparency.

Go beyond sharing a simple SBOM. Demonstrate your commitment to building secure software. Share assessments, raise concerns, and triage issues together with your users. Cut the noise and prioritize what matters.

Learn More

Secure Dev Toolchains

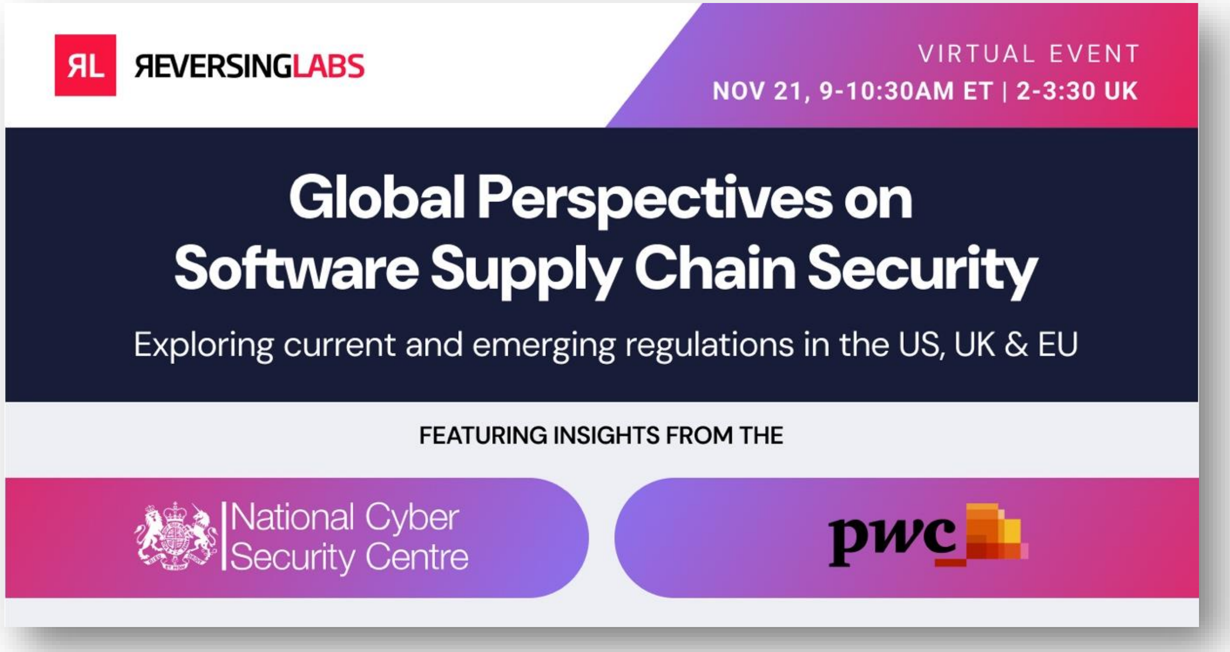
Building secure software relies on trustworthy development toolchains.

Spectra Assure Community allows you to trust the compilers, linkers, IDE plugins and CI/CD pipelines that you use to build apps.

Coming Soon

RL provides the largest, free resource of comprehensive risk assessments on open source software at https://secure.software

Upcoming RL Virtual Events



ЯL ЯEVERSINGLABS

VIRTUAL EVENT

NOV 21, 9-10:30AM ET | 2-3:30 UK

Global Perspectives on Software Supply Chain Security

Exploring current and emerging regulations in the US, UK & EU

FEATURING INSIGHTS FROM THE

National Cyber Security Centre

pwc

ЯL ЯEVERSINGLABS

WEBINAR

AI in the Software Supply Chain

Balancing Innovation and Security in the AI Age

Joe Coletta
SR. PRODUCT MARKETING MANAGER AT REVERSINGLABS

Viswanath Chirravuri
SOFTWARE SECURITY DIRECTOR, THALES

LIVE: DEC 5, 1-2 PM ET

https://www.reversinglabs.com/webinar/webinar-line-up

Thank you.

Follow RL on Social

twitter.com/ReversingLabs

linkedin.com/company/reversinglabs

youtube.com/reversinglabs