TRUST DELIVERED

Get to “Yes” faster:

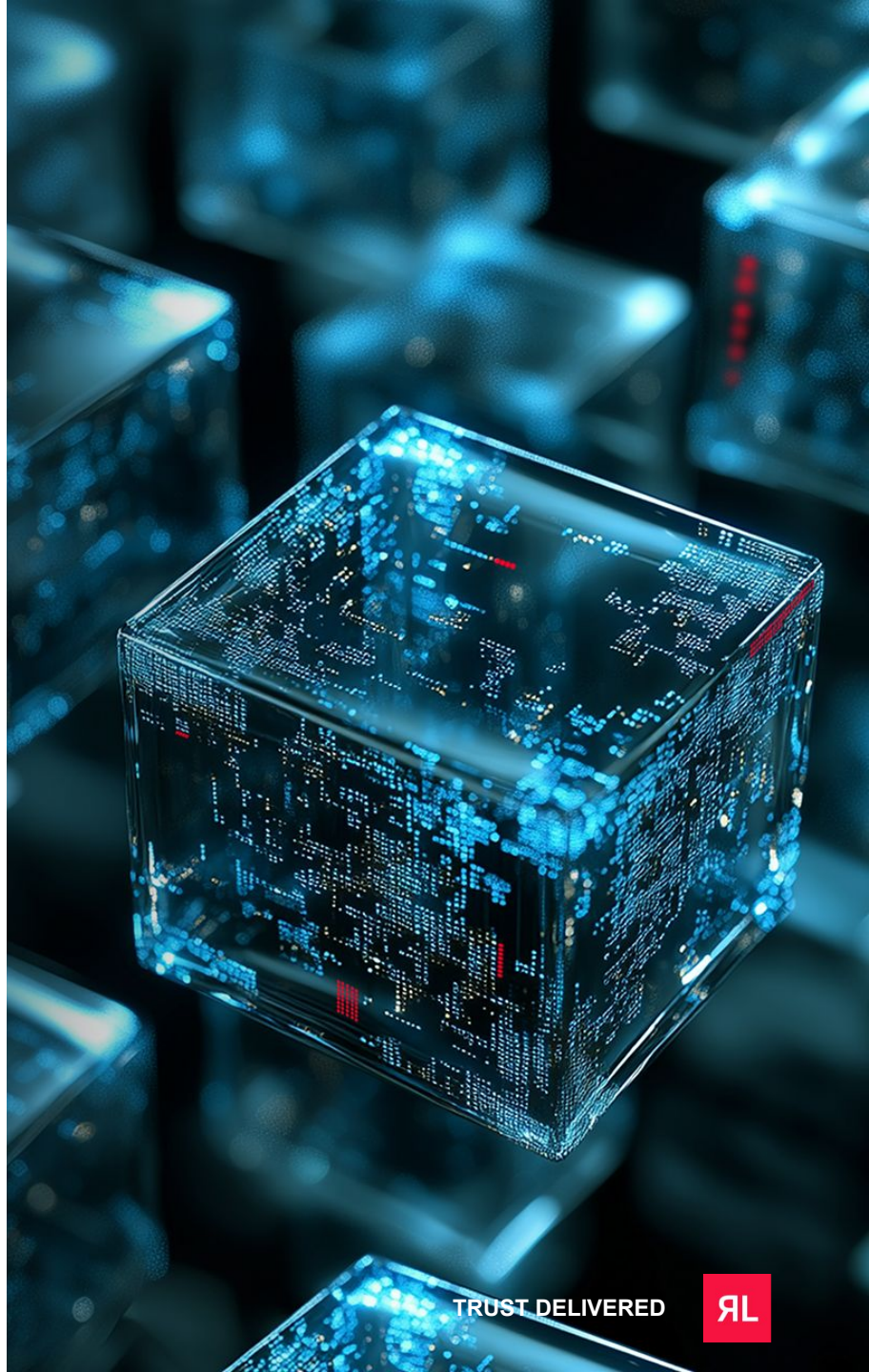
Simple, Scalable, and Secure Software Onboarding

Brought to you by ReversingLabs

Meet Today's Speakers:

AGENDA

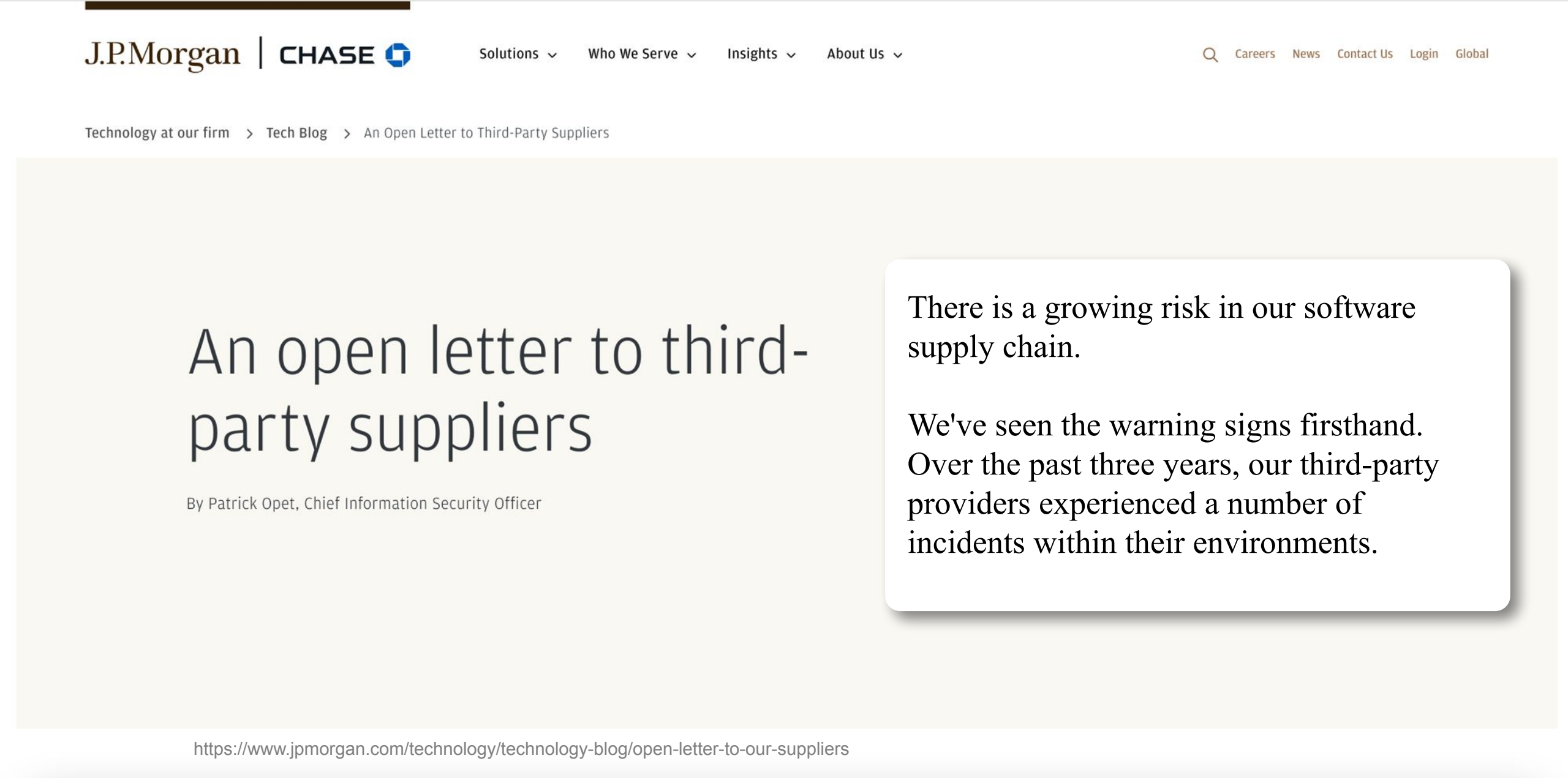
- The State of the Software Supply Chain
- Federal Call to Action
- SalesLoft/Drift Breach
- Growing Complexity of Software Supply Chain
- Software Risk Takes Many Forms
- Binary Analysis: A New Control for Onboarding
- Automating Within ITSM Workflows
- Key Takeaways



SSCS Attacks On The Rise

"By 2028, 80% of organizations worldwide will have experienced attacks on their software supply chains, a 48% increase from 2024"

Gartner®, The Software Supply Chain Security Playbook, Aaron Lord, Manjunath Bhat, et al., 23 October 2025



Software Fast Track (SWFT)

What is SWFT
DoW initiative to modernize how the Fed ***acquires, tests, and authorizes 3rd party software****.*

Drivers for Change

- Software procurement processes have historically been slow and outdated
- SWFT aims to ***expedite software delivery to the Warfighter*** without compromising security

- **April 2025:** Memo issued w/ 90-day sprint to establish SWFT Framework & Implementation Plan
- **May 2025:** 3 RFIs issued to gather capabilities for secure software delivery to Federal Government
  - SSCS Tooling
  - External Assessments
  - Automation and AI
- **September 2025:** DoW releases Cybersecurity Risk Management Construct (CSRMC)
  - Addresses gaps in RMF by shifting from "snapshot in time" to automated/continuous assessments

Onboarding decisions increasingly need to be supported by technical evidence that can be reused, automated, and monitored over time, not just documented once.

NDAA: AI Governance

What is the NDAA

Annual bill to set defense policy, authorize funding levels, and provide necessary resources for the Department of War (DoW)

Drivers for Change

- Recognition of new risks/threats presented by AI:
  - Model serialization attacks
  - Model tampering
  - Data Leakage
  - Adversarial Prompt Injection
  - Model Provenance
- Traditional SBOMs don’t provide visibility into AI/ML components

Significant Changes in 2026

- Section 1512 of NDAA Text introduces the need for policy and action to better manage cybersecurity and governance risk of AI and machine learning systems
- NDAA Joint Explanatory Statement provides explicit linkage between software bills of materials (SBOMs) and AI systems.

What’s coming

- SBOMs + AI/ML-BOMs for transparency and traceability
- Evidence-based assurance before deployment, not attestations
- Continuous & automated assurance, not manual one-time assessments

Salesloft Drift Breach: Covering the Basics

What is Salesloft Drift?

AI Chatbot platform enabling allows sales teams to engage with website visitors, commonly integrated with enterprise CRM & Sales productivity systems (Salesforce, Slack, Google Workspace, etc)

Attack period: August 8–18 2025.

Scope: **Over 700 organizations impacted**, including high-profile vendors such as Google, Cloudflare, Zscaler and Palo Alto Networks.

Attack Path:

1. Salesloft's GitHub account compromised
2. Lateral movement to Salesloft's AWS environment hosting Drift application
3. OAuth tokens linked to the Drift integrations (e.g. Salesforce) stolen
4. Large volumes of data (CRM + other credentials) exfiltrated

Salesloft Breach: Key Takeaways

Vendor to vendor connectivity remains an enticing target for malicious actors

Salesloft Breach: Key Takeaways

Vendor to vendor connectivity remains an enticing target for malicious actors

3rd/4th party relationships must be considered as a part of inherent risk

Salesloft Breach: Key Takeaways

Vendor to vendor connectivity remains an enticing target for malicious actors

3rd/4th party relationships must be considered as a part of inherent risk

A rising need for 3rd party software onboarding controls & audit traceability

Software Risk Takes Many Forms

In their recent publication of CISO's Playbook for Commercial Software Supply Chain Security, Gartner® recognizes two kinds of supply chain risks typically associated with third-party software:

"Back doors/malware implanted in **externally procured** software"

"Known vulnerabilities in **third-party or open-source** dependencies"

How can companies address these risks?

"Gartner recommends collaborating with security and compliance stakeholders to review third-party software prior to its implementation."

Gartner, The Software Supply Chain Security Playbook, Aaron Lord, Manjunath Bhat, et al., 23 October 2025

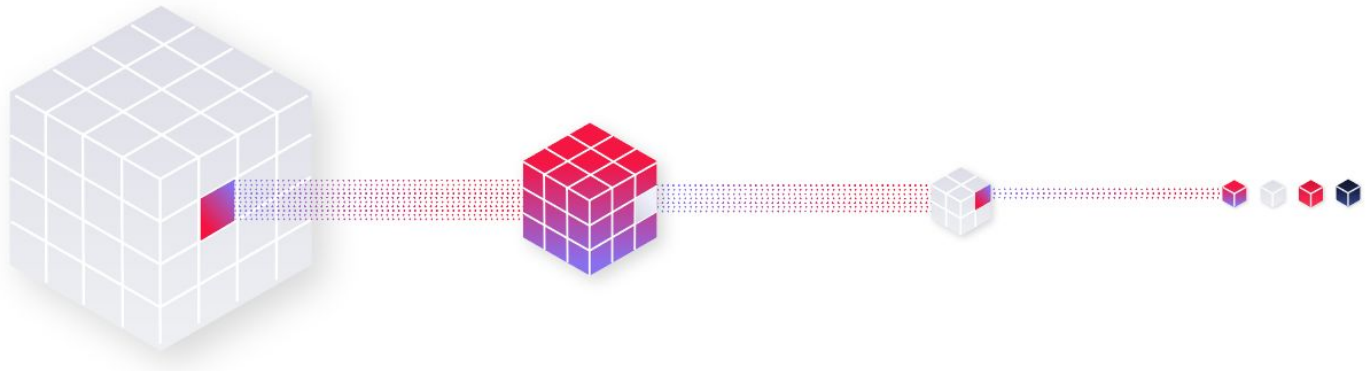
Addressing The 3rd Party Software Visibility Gap

Common Barriers

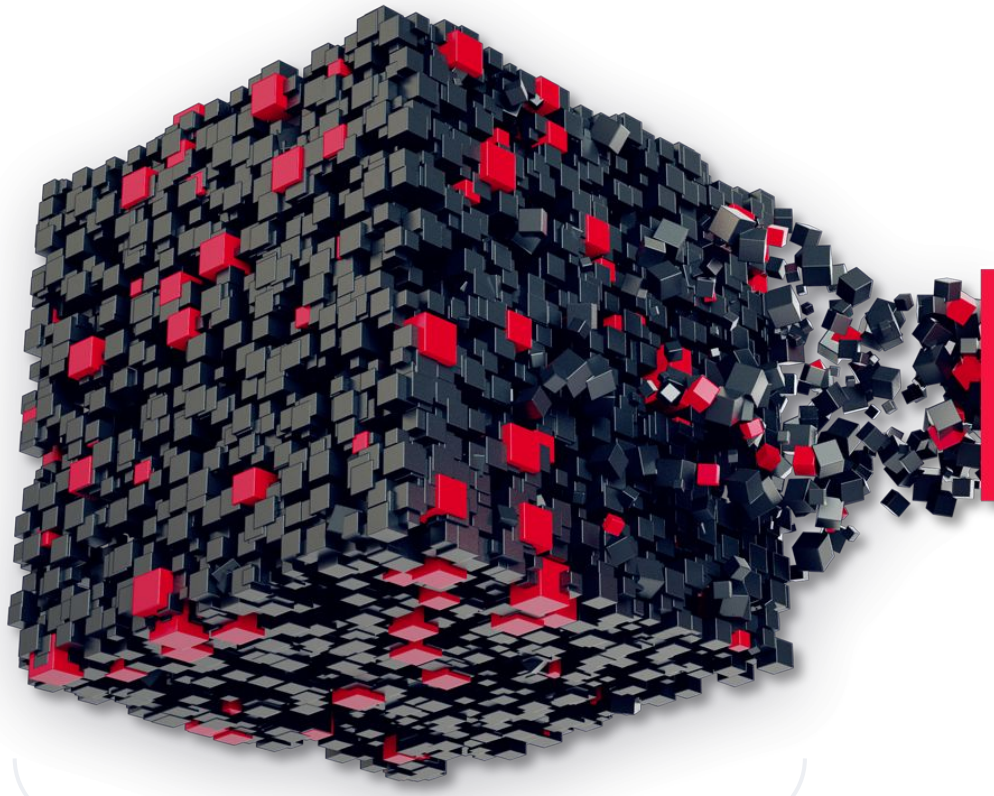
- Right to audit not present in software vendor contract?
- Limited time and skilled resources to perform the assessment?
- Supplier unwilling to provide evidence of control effectiveness?
- Security testing (e.g. pen testing or source code analysis) too invasive/expensive?
- Assessment scalability issues due to manual nature of testing?

Binary Analysis - A New Control

Did you know that binary analysis can provide visibility into software risks and threats without the need to engage a vendor or gain access to source code?



Layering Threat Intelligence with Binary Analysis



- Proprietary
- Open Source
- Commercial
- Other Artifacts

COMPLEX BINARY ANALYSIS

- Malware
- Tampering
- Vulnerabilities
- Hardening
- Secrets
- Licenses
- XBOM
  - *SBOM*
  - *SaaSBOM*
  - *CBOM*
  - *ML-BOM*

3rd Party Software Scanning

Four Main Use Cases Considered

New Software

Scan newly acquired software for risks & threats present in the package prior to onboarding

Maturity Path

3rd Party Software Scanning

Four Main Use Cases Considered

New Software

Scan newly acquired software for risks & threats present in the package prior to onboarding

Existing Software

Retroactively test critical software already deployed in production to identify active exposures and establish a security baseline.

Maturity Path

3rd Party Software Scanning

Four Main Use Cases Considered

New Software

Scan newly acquired software for risks & threats present in the package prior to onboarding

Existing Software

Retroactively test critical software already deployed in production to identify active exposures and establish a security baseline.

Software Changes

Scan updates to software (patches, hotfixes, feature releases) for risks & threats introduced by version changes

Maturity Path

3rd Party Software Scanning

Four Main Use Cases Considered

New Software

Scan newly acquired software for risks & threats present in the package prior to onboarding

Existing Software

Retroactively test critical software already deployed in production to identify active exposures and establish a security baseline.

Software Changes

Scan updates to software (patches, hotfixes, feature releases) for risks & threats introduced by version changes

Emerging Threats

Continuously re-scan and/or retroactively hunt for emerging risks & threats in software for not known during initial deployment

Maturity Path

New Software Onboarding

Most Commonly Operationalized Use Case

New Software

Scan newly acquired software for risks & threats present in the package prior to onboarding

Today's Focus

Existing Software

Retroactively test critical software already deployed in production to identify active exposures and establish a security baseline.

Software Changes

Scan updates to software (patches, hotfixes, feature releases) for risks & threats introduced by version changes

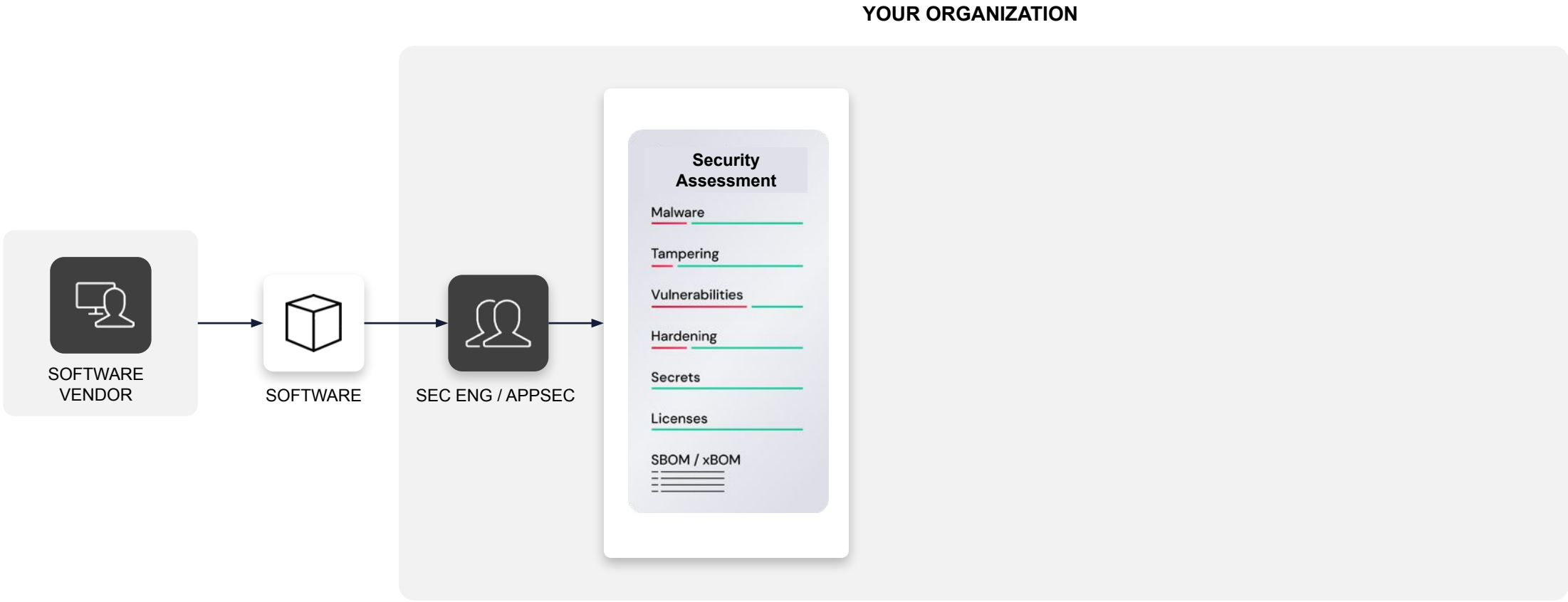
Emerging Threats

Continuously re-scan and/or retroactively hunt for emerging risks & threats in software for not known during initial deployment

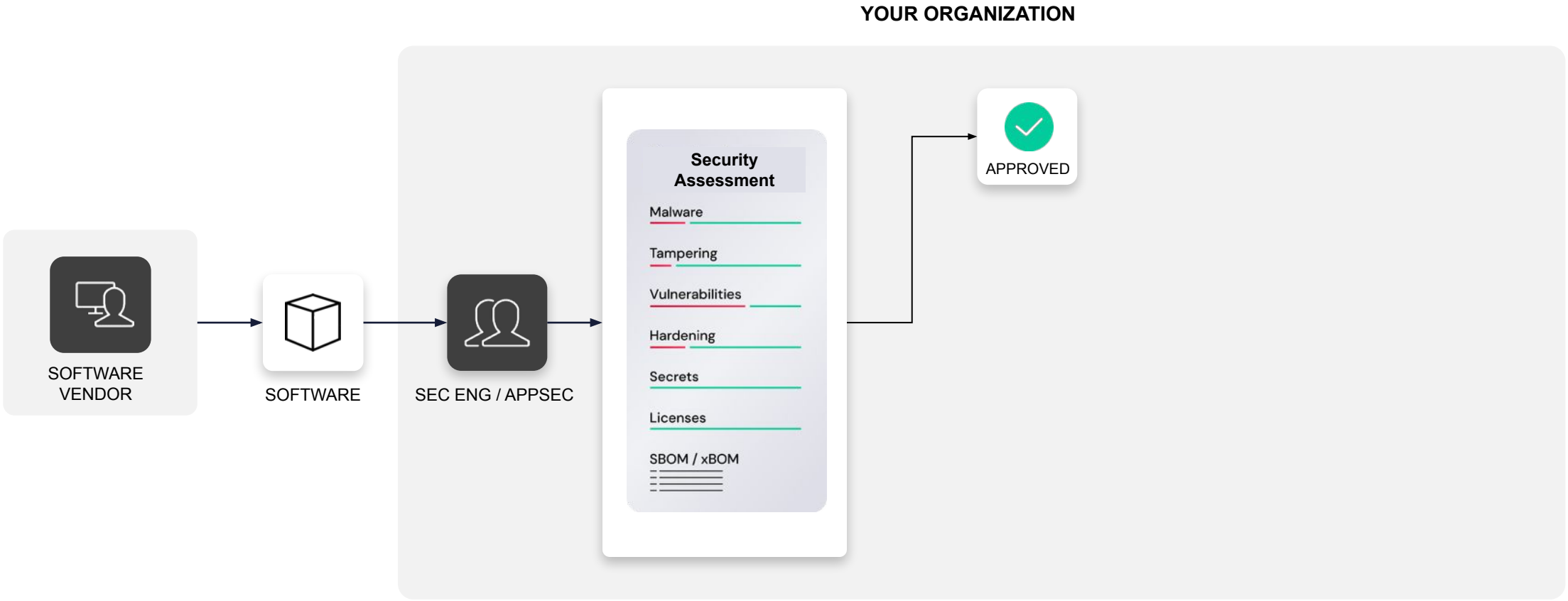
Why New Software Onboarding?

1. Natural point of control enforcement with existing process (quickest route to value)
2. Opportunity for organizations to mitigate risks before deployment
3. Non-invasive to business relying on software active in production

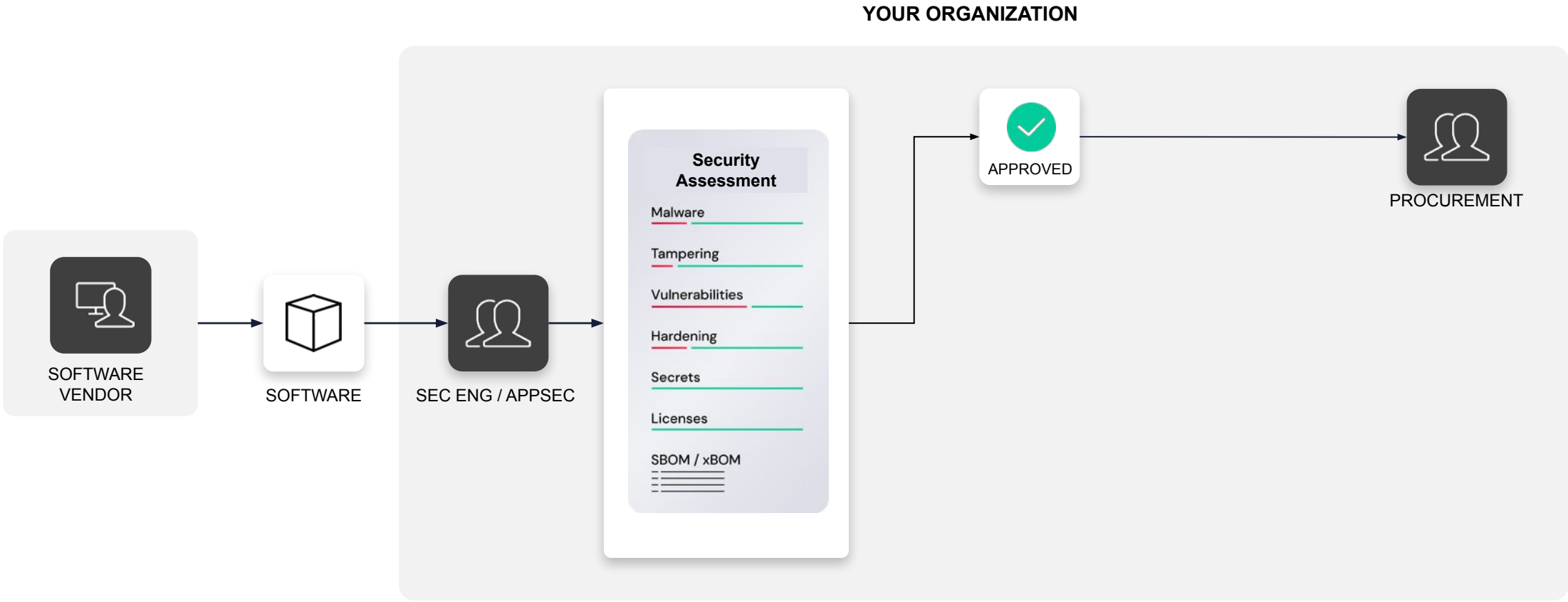
1 How to Leverage Binary Analysis in Software Onboarding



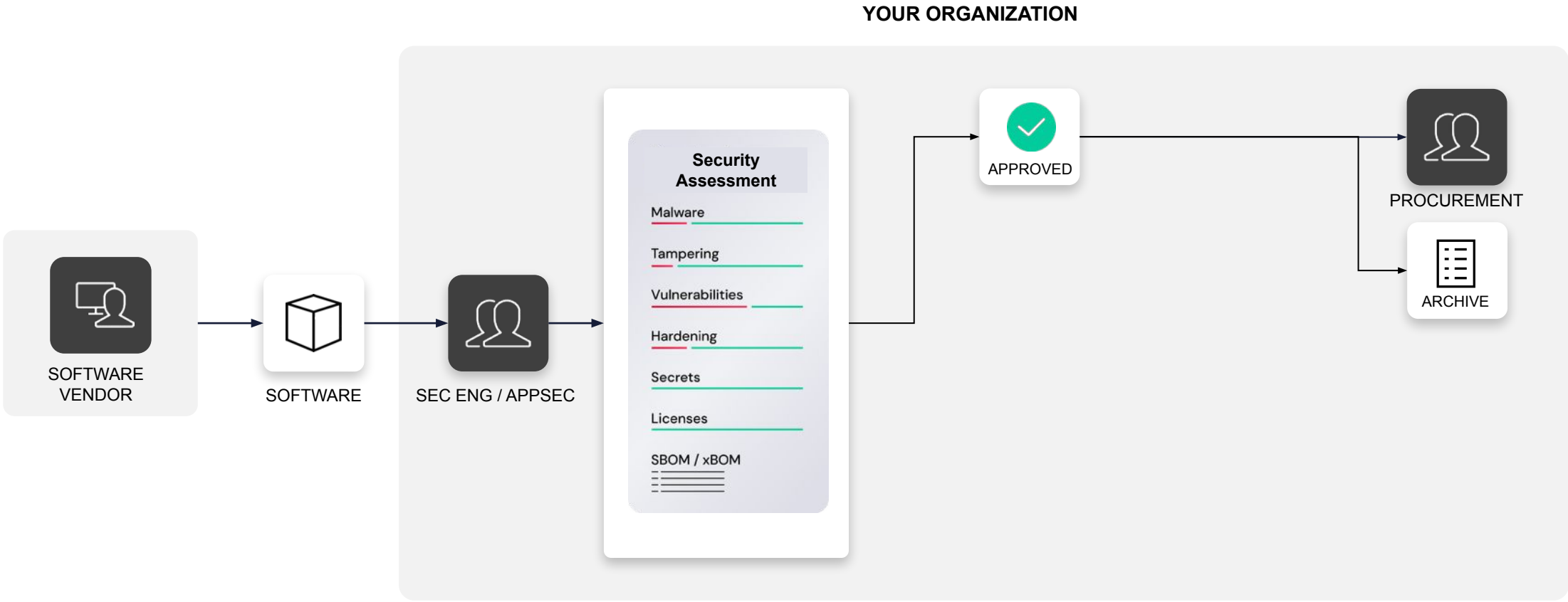
2 Approve Software Free of Critical Issues



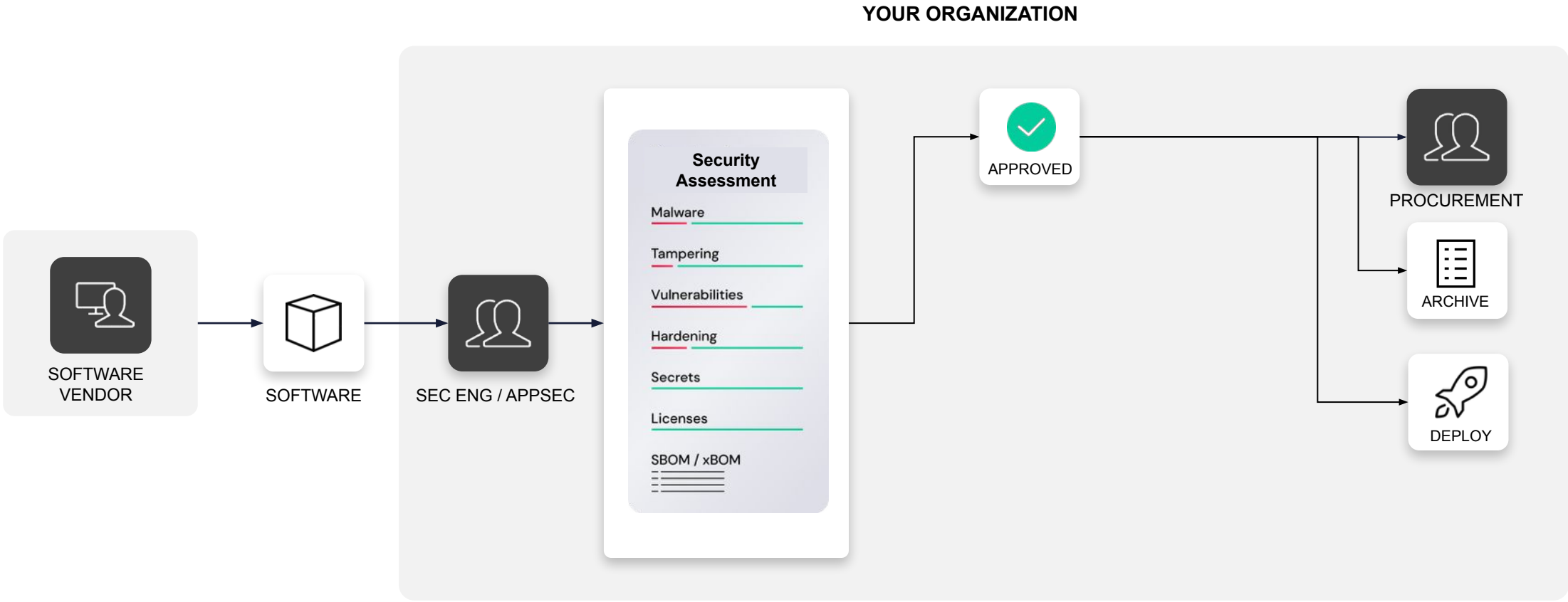
3 Notify Procurement of Assessment Outcome



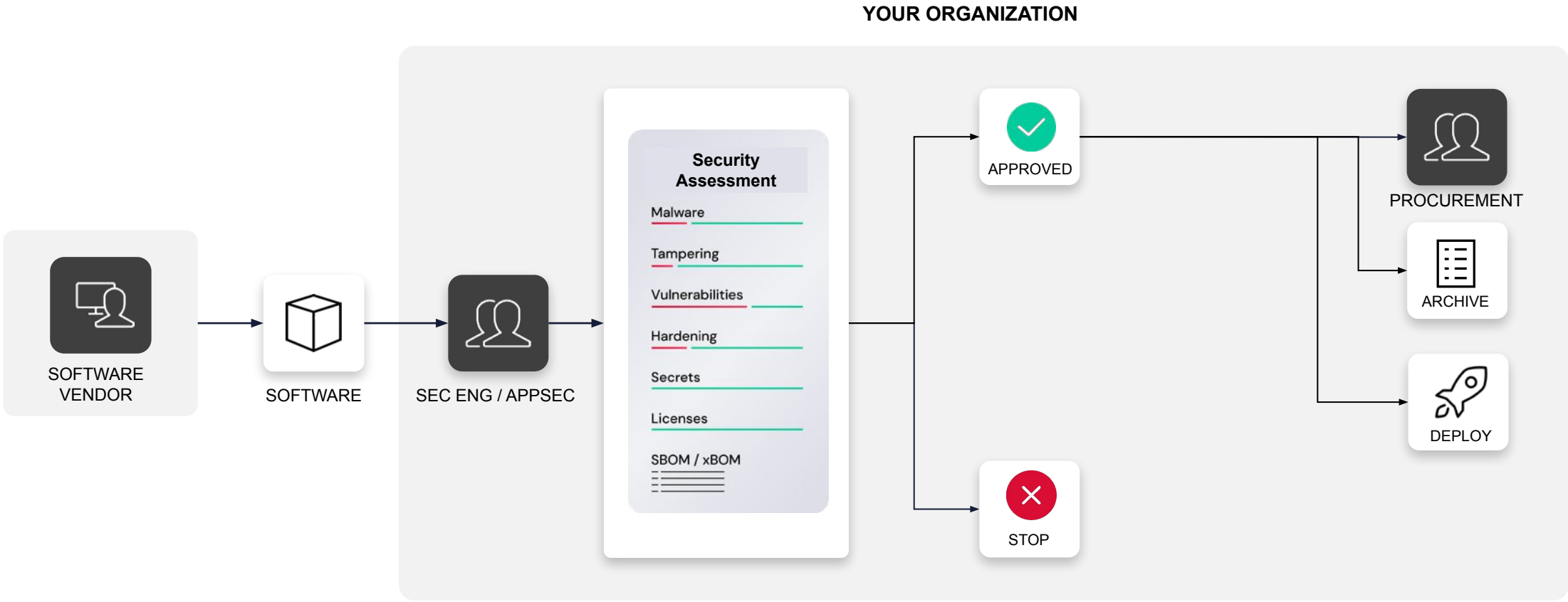
4 Archive Assessment Artifacts For Audits



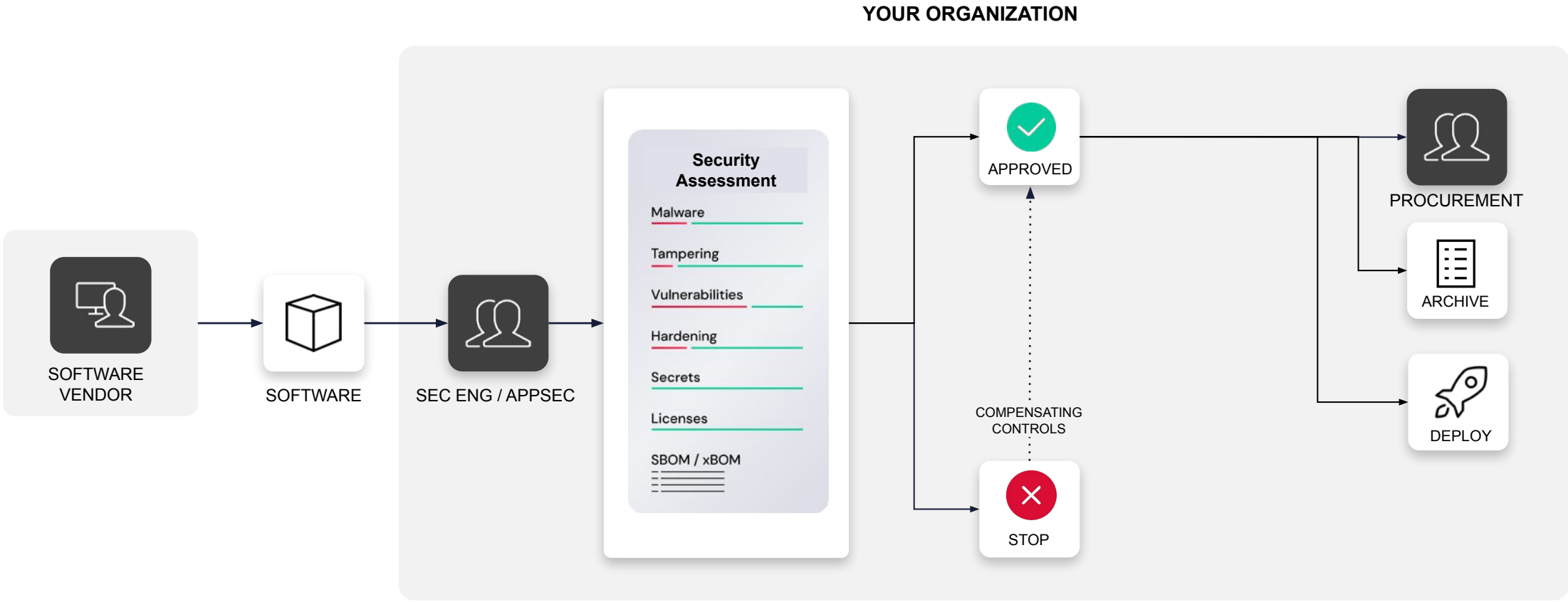
5 Deploy Only Safe Software



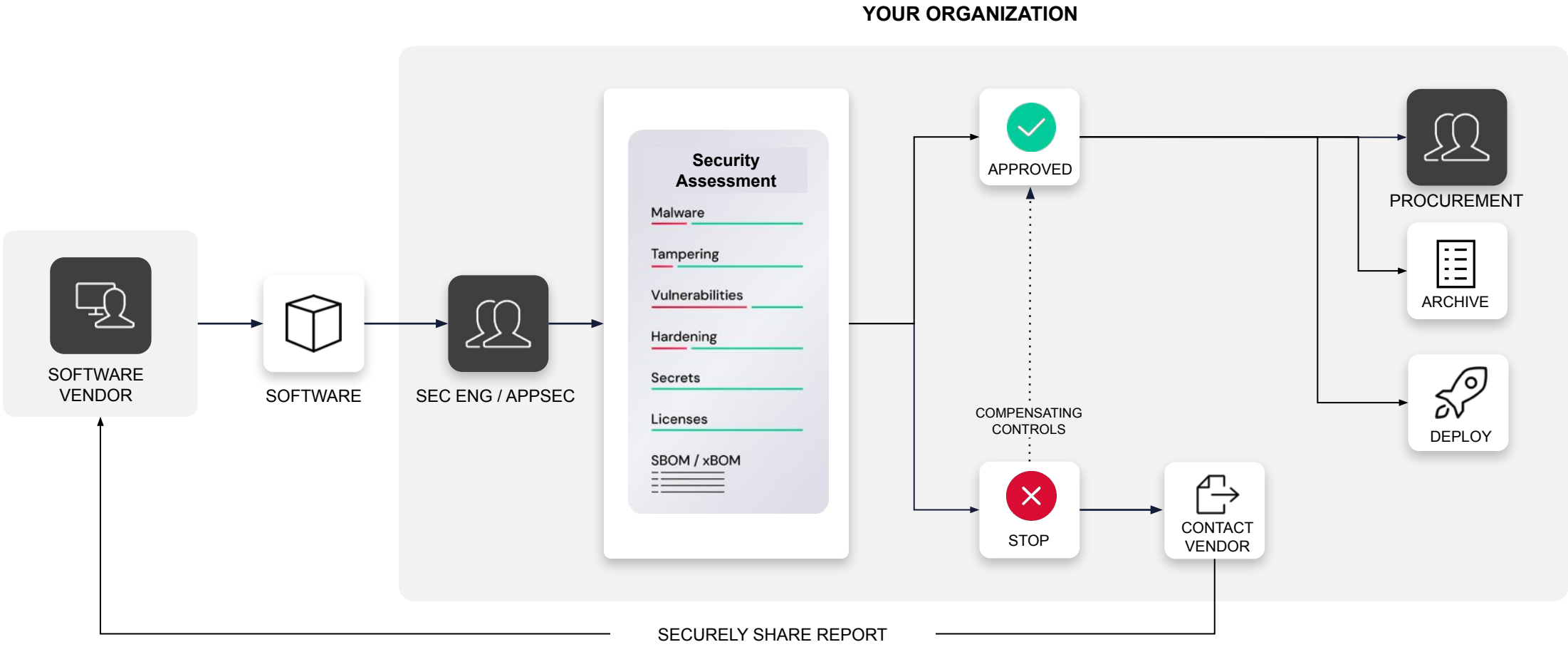
6 Halt Software Deployment When Critical Issues Arise



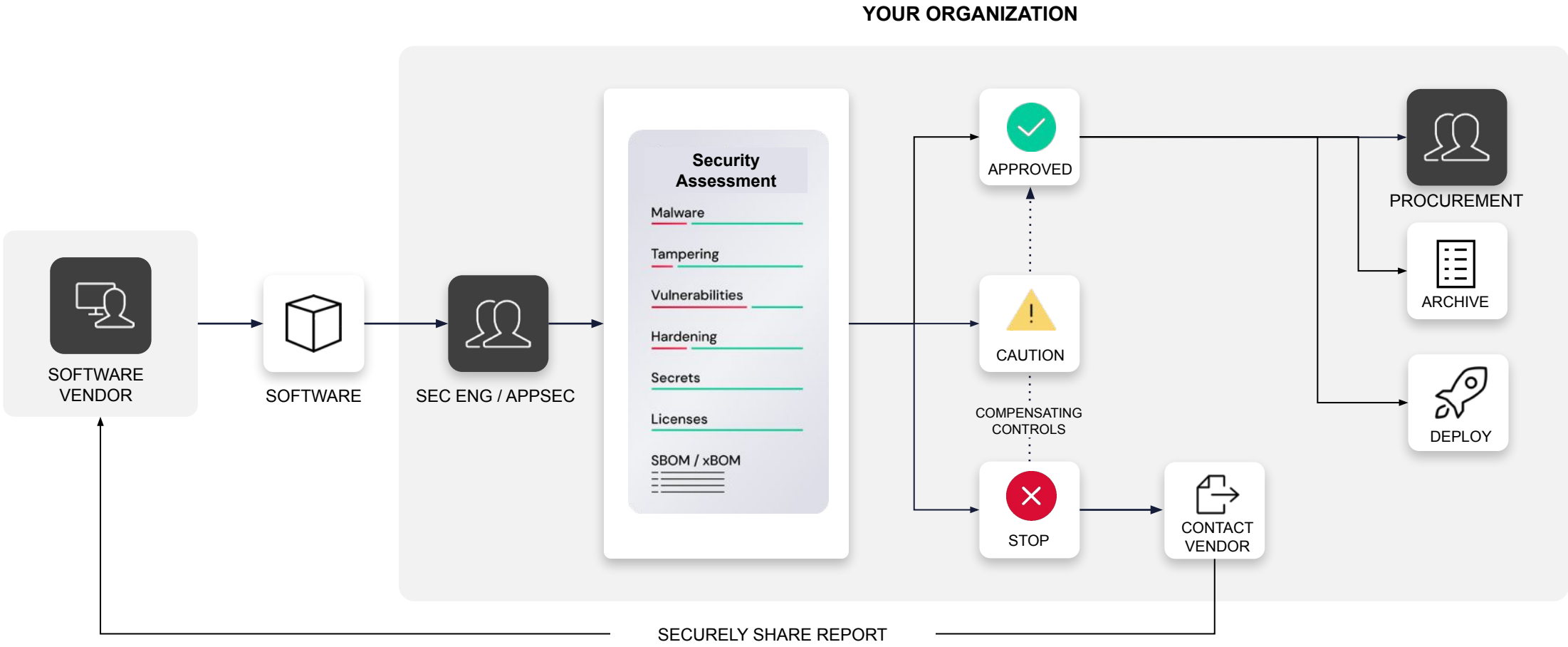
7 Consider Compensating Controls to Reduce Risk



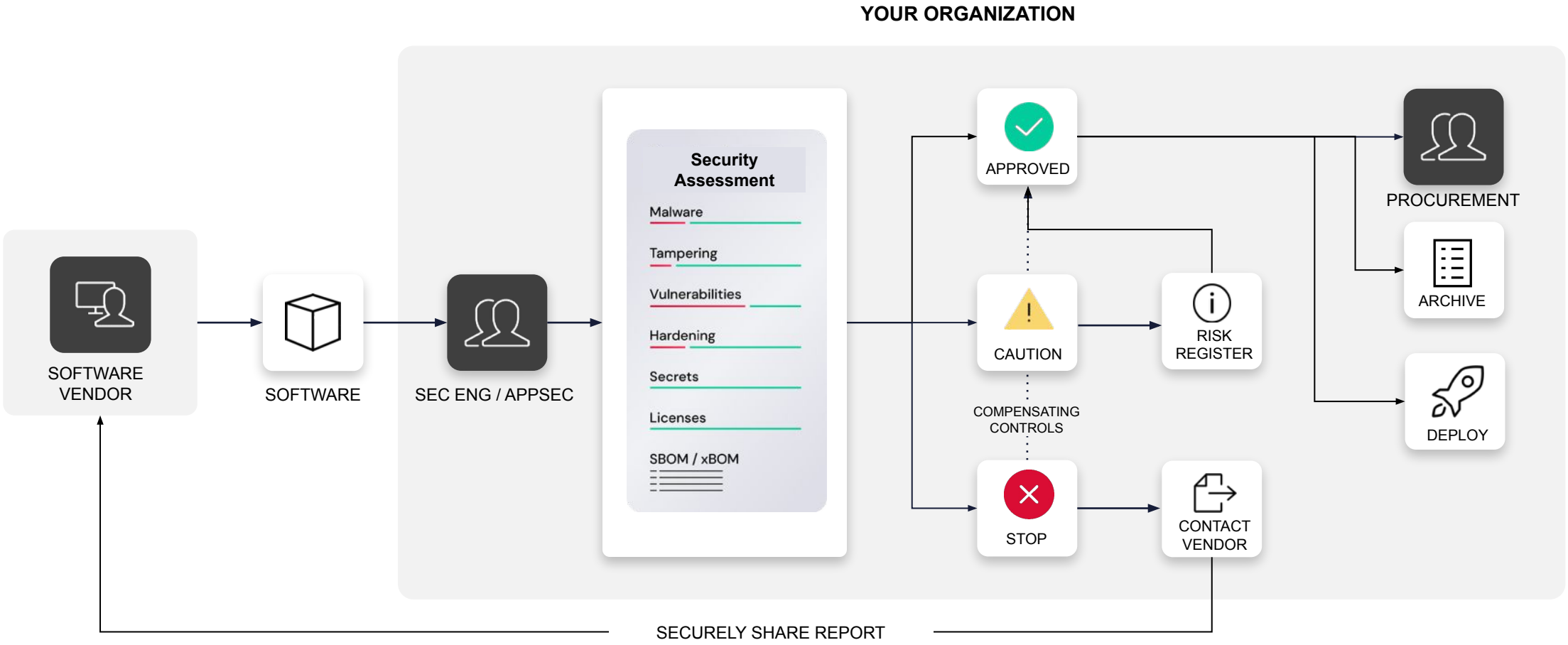
8 Collaborate with Vendor to Address Issues



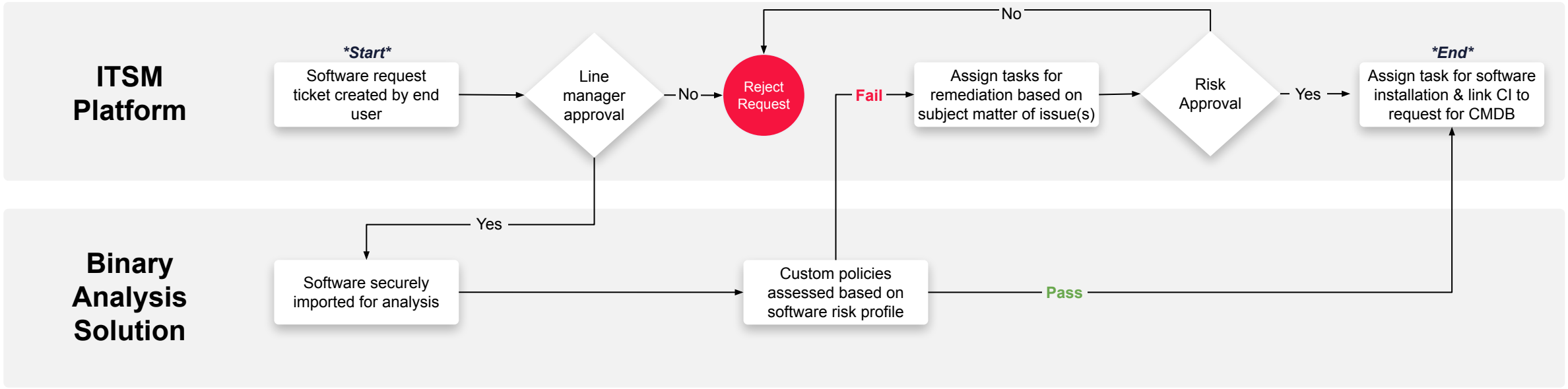
9 Document Non-Critical Issues



10 Centrally Track Issues & Compensating Controls



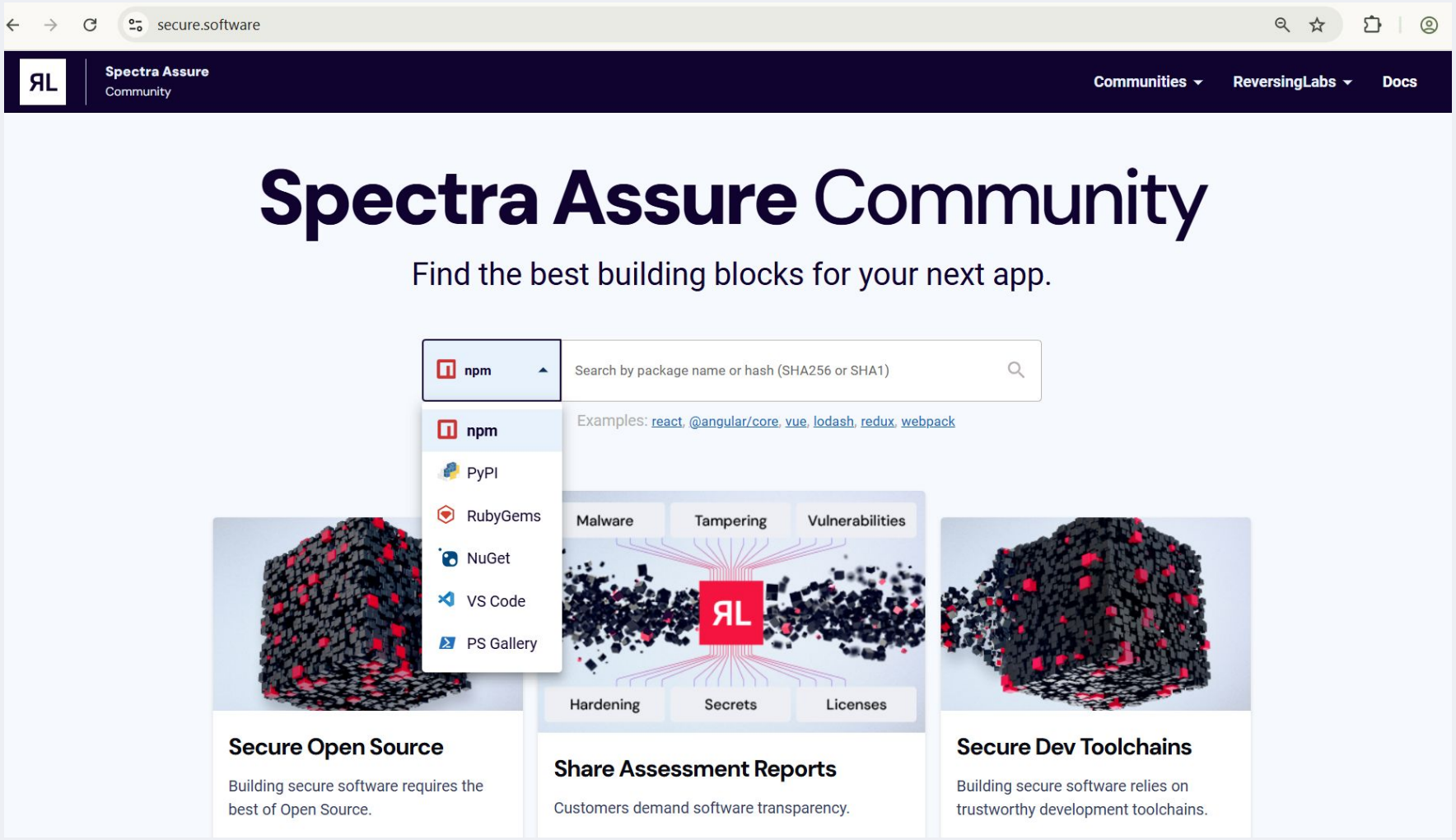
Integrating Binary Analysis with ITSM Workflows



Summary and Next Steps

- Third-party breaches through commercial software are on the rise
- Traditional, inherent trust-based models are no longer sufficient
- Binary analysis introduces a critical new control for software onboarding
- Integrate with ITSM workflows to accelerate safe software onboarding
- Extend software assurance to AI/ML systems

Secure.Software



Relevant Resources

White Paper

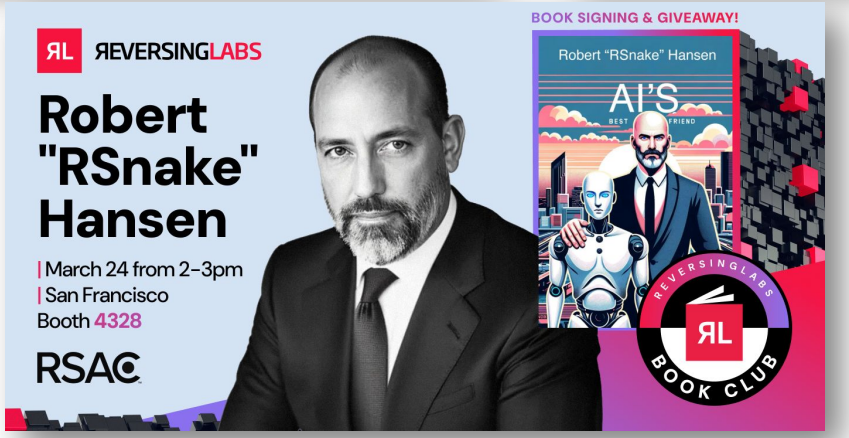
Solution Brief

Annual Report

Gartner® Playbook

Questions

Upcoming Events



https://www.reversinglabs.com/webinar/webinar-line-up
https://www.reversinglabs.com/rl-rsac-2026


Thank You