PUBLIC SECTOR

Continuous Software Supply Chain Security Management

‘Only Software That Is Built Secure Runs Secure’

WWW.LINEAJE.COM

This presentation contains information that shall not be duplicated, used, or disclosed in whole or in part for any purpose other than evaluation of this presentation.

TRUSTED AND RECOGNIZED
BY LEADING BRANDS

Technology Partners and Value-Added Resellers

Our government clients include leading edge organizations

Lineaje is a **trusted industry leader** in the Cybersecurity industry

Digital Innovator Award

2023 Application Security

Best Supply Chain Software

GSA MAS 8F
Contract #: 47QSWA18D008F
Contract Period: August 22, 2018 - August 21, 2028

NASA SEWP
Contract #: NNG15SC03B/NNG15SC27B
Contract Period: May 1, 2015 – April 30, 2025

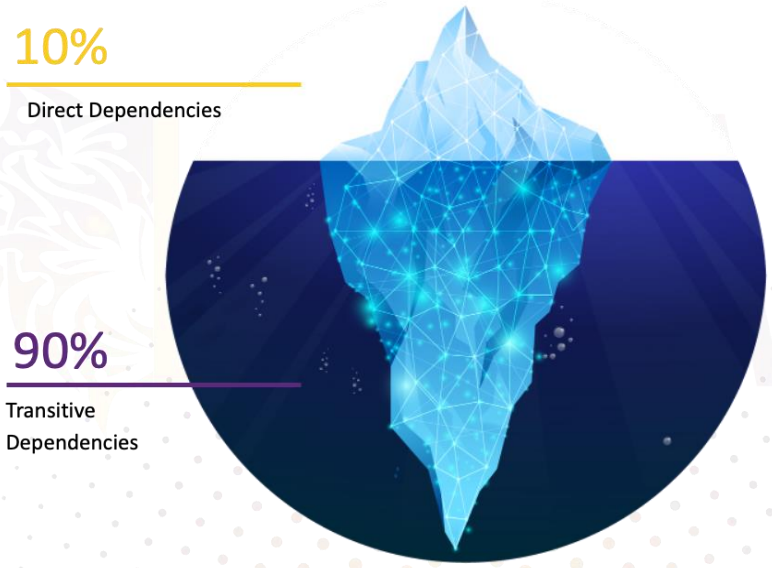
Army CHESS ITES-SW2
Contract #: W52P1J-20-D-0042
Contract Period: August 31, 2020 - August 30, 2025

Lineaje, Inc.
Founded: 2022
Headquarters: Santa Clara, CA
GAGE: 9LUG6
DUNS: 111562408
SAM (UEI): FZ82SG7VMEV6
NAICS: 541512, 513210, 541519, 541690, 541715

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

THE SOFTWARE SUPPLY CHAIN IS UNDER ATTACK

- **600% YoY increase** in software supply chain attacks.
- Cyber incidents, such as **SolarWinds, Log4j, and XZ** highlight significant vulnerabilities in the software supply chain.
- **Hidden vulnerabilities** are buried within millions of line of code, masquerading as authentic code, **making detection nearly impossible**.
- **State-sponsored actors exploit these vulnerabilities**, posing serious threats.



90% of software components in Open-Source are transitive, invisible dependencies

In response, the Federal government has issued regulatory requirements to address software supply chain threats

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

Key Federal Regulations Lineaje Addresses

- **Executive Order (EO) 14028, Section 4(e)**, is part of the "**Improving the Nation's Cybersecurity**" order issued on May 12, 2021, which aims to enhance cybersecurity and software supply chain integrity.
    - **OMB M-23-16/M-22-18**, **Enhancing the Security of the Software Supply Chain through Secure Software Development Practices**
    - **OMB M-21-30**, **Protecting Critical Software Through Enhanced Security Measures**
    - **NIST 800-218, Secure Software Development Framework (SSDF):** provides a core set of high-level secure software development practices that can be integrated into each SDLC implementation.
- **NIST 800-161, Cybersecurity Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations:** provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations.
- **FISMA (NIST 800-53r5) and FedRAMPr5**, **Supply Chain Risk Management (SR)** family of controls.
- **NIST 800-207, Zero Trust Architecture (ZTA),** Software Supply Chain Security ZTA Capabilities Activities 3.2, 3.3, 3.3.1.
- **DOD CMMC 2.0, Cybersecurity Maturity Model Certification (CMMC),** DIB cybersecurity for safeguarding the information that supports and enables our warfighters
- **US Army, Software Bill of Materials Policy**, requires submission of SBOMs for Commercial Off The Shelf (COTS) and Contractor Software starting Feb 2025.
- **US Dept of Commerce, Bureau of Industry and Security (BIS), Notice of Proposed Rulemaking (NPRM)** that would prohibit the sale or import of connected vehicles integrating specific pieces of hardware and software, or those components sold separately, with a sufficient nexus to the People's Republic of China (PRC) or Russia.
- **North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), Software Supply Chain Risk Management,** specifies requirements for securing the supply chain for internally developed and third-party software:
    - **CIP-013-2 R1 -** Verification of software integrity and authenticity of all software and patches provided by vendor
    - **CIP-007-6 R2** - Know, track, and mitigate known software vulnerabilities
    - **CIP-010-4 R1.6** – Verify integrity of software and identity of the software source

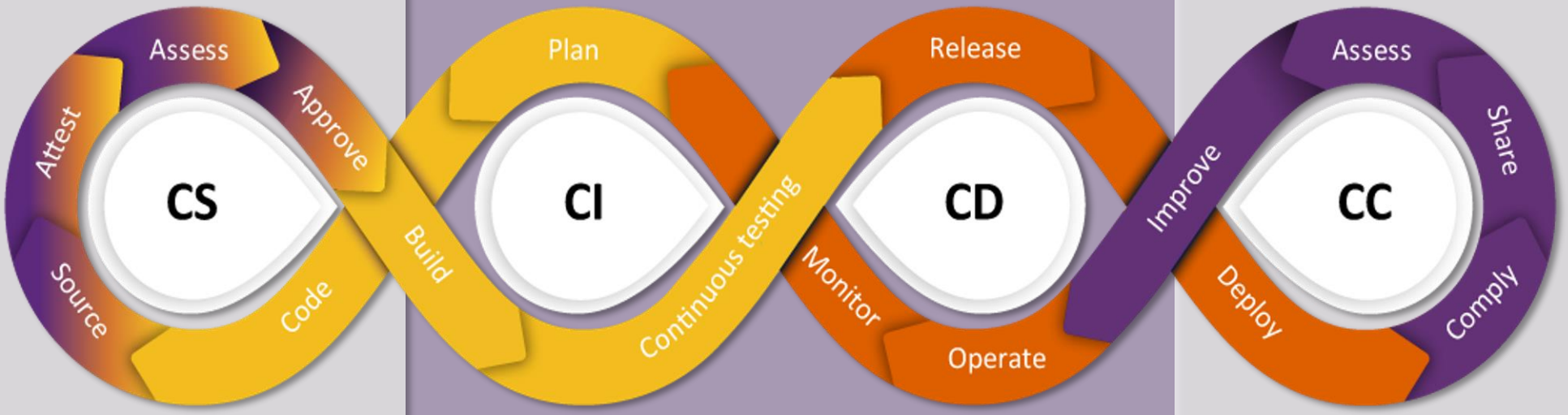
Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

CONCEPT AND SIGNIFICANCE OF PROBLEM/OPPORTUNITY:

To Address the Challenges of the Modern Vulnerability Management We Need to Shift Left of Shift Left and Automate Compliance Right

Shift Left of "Shift-Left"
proactively identify and mitigate supply chain risks

Automate Compliance
ensure security is integrated into every software release



Continuous Sourcing	Continuous Integration	Continuous Deployment	Continuous Compliance
70-90% of software is open-source which is opaque & tamperable	**95% of Vulnerabilities** are found **in open-source** **56% vulnerabilities have no fixes** in open-source	One third of **developers spend 50% of their time patching vulnerabilities** in open-source	In modern software development **a million releases a day is not uncommon**

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

LINEAGE

LINEAJE PLATFORM

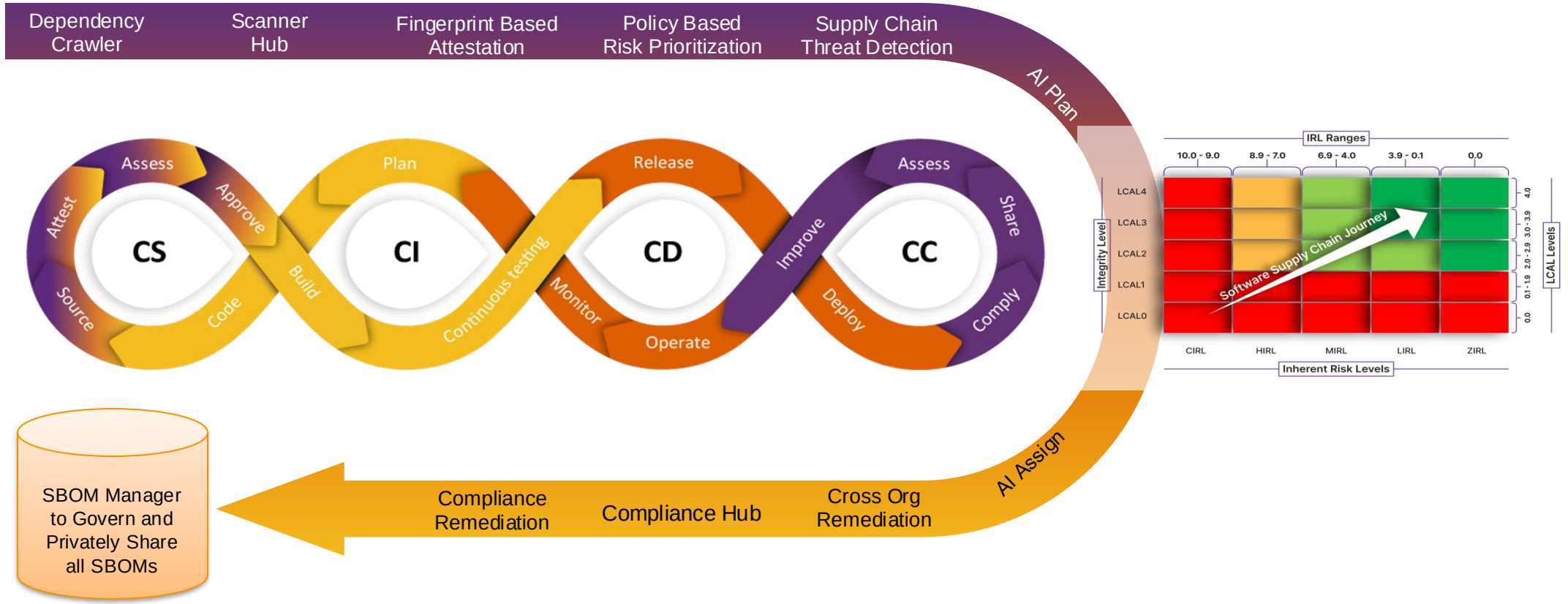
PURPOSE BUILT TO ADDRESS SUPPLY CHAIN CHALLENGES

At Lineaje, we designed unique solutions and capabilities purpose-built to address these challenges head-on.

CHALLENGE	BUSINESS IMPLICATIONS	LINEAJE SOLUTION CAPABILITY
The Software Supply Chain is Opaque	Invisible components in software you source, build, deploy or buy (e.g., log4j)	**100% Supply Chain Illumination**: ***Crawlers*** automate discovery of 100% of the components in your software, including all dependencies and transitive dependencies.
Unknown Risks Inherent in the Software Supply Chain	Dev teams introduce risky components because they lack visibility into the unknown risks in open-source	**Open-Source Risk Reputations**: Automated assessment including code quality, security posture, provenance, and vulnerabilities for inherent risks.
600% Increase in Supply Chain Attacks	Supply chain attacks such as SolarWinds and 3CX have resulted in millions of dollars in losses for affected businesses	**Supply Chain Threat Detection**: Attest the integrity of the supply chain including open-source, build, third-party COTS, and deployed software.
95% Of Vulnerabilities Are in Open Source	Over $13B annually spent on vulnerability management in the US	**Smart Patching:** Automate compatibility analysis and patch without breaking your software.
56% Of Vulnerabilities Lack Viable Solutions	Extensive resources expended to address vulnerabilities through increased monitoring, manual interventions, and work-arounds	**AI-Enabled OSS Remediation:** Automate fixing “unfixed” open-source code and contribute back to the ecosystem for components used in your software.

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

Lineaje Platform enables Find-to-Fix Capabilities

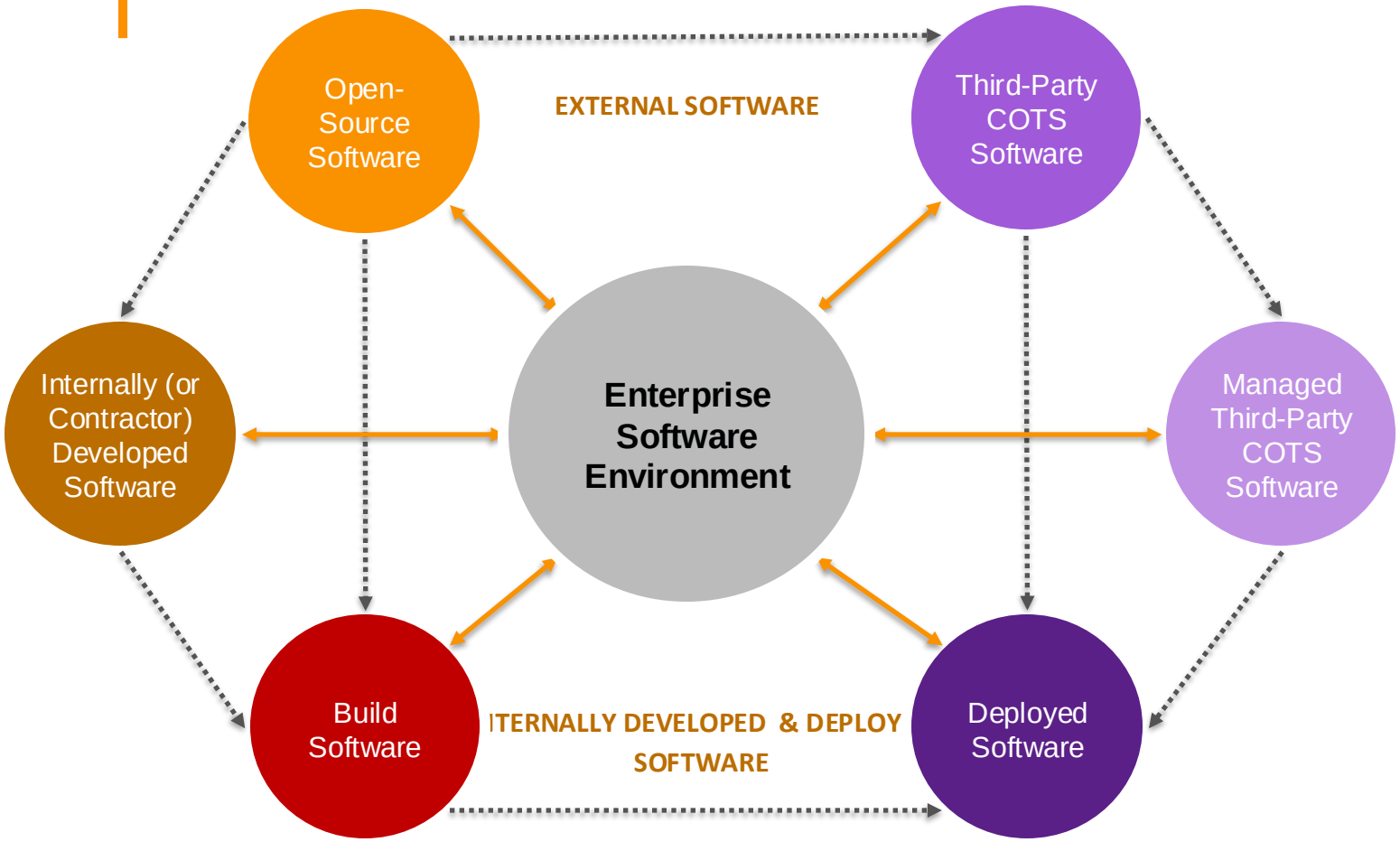


Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

THE SOFTWARE SUPPLY CHAIN ECOSYSTEM

THE ECOSYSTEM IS ONLY AS SECURE AS THE "WEAKEST LINK".

Agencies are required to **track and manage thousands of software for security and compliance** including third-party, open-source and internally (including contractor) developed and managed applications at time of acquisition and continuously for deployed software.



Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

Lineaje Portfolio of Products - Securing The Ecosystem

OSM (open-source manager)

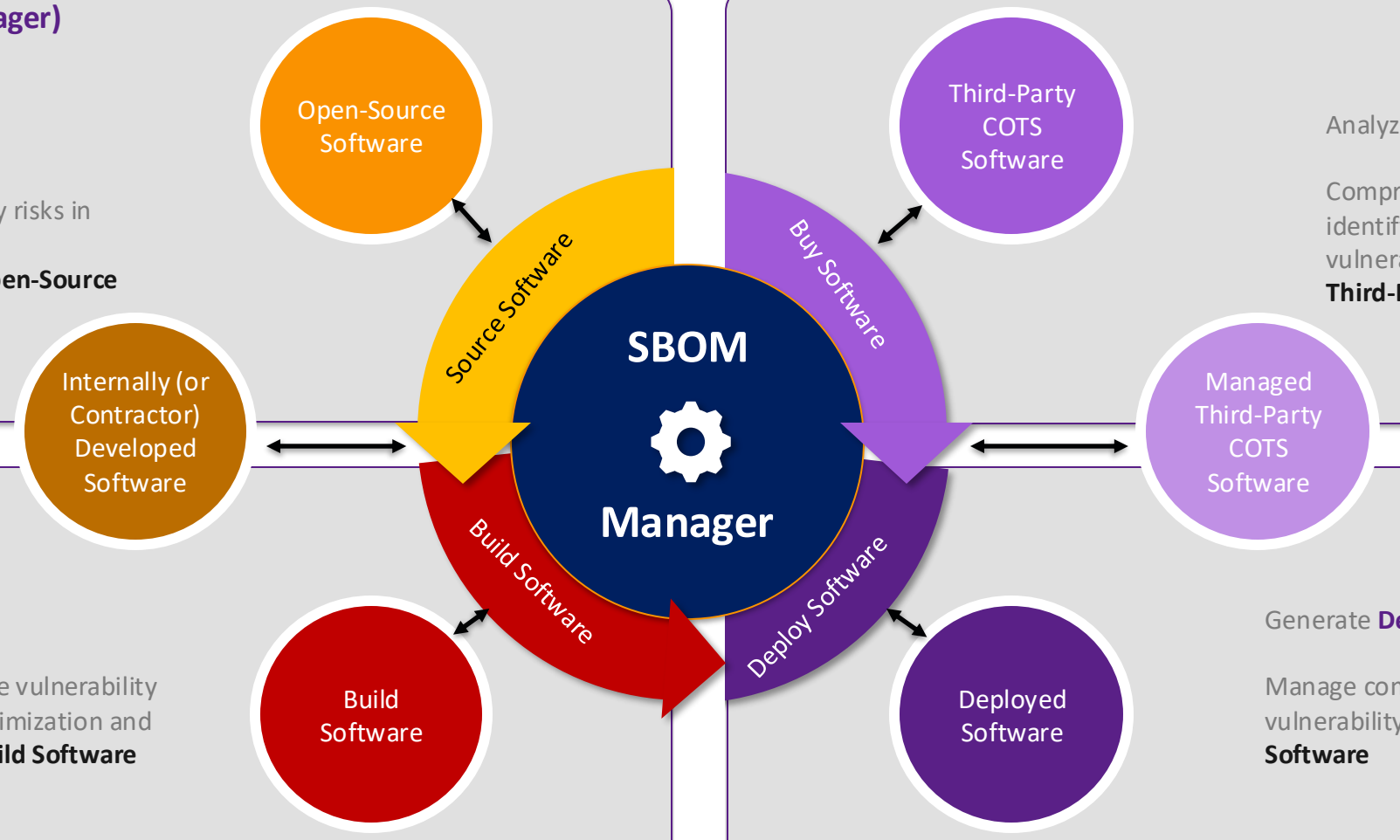
Generate **Source SBOMs**

Identify, and mitigate security risks in components, adhering to organizational policies for **Open-Source Software**

TPRM/C-SCRM

Analyze **Third-Party SBOMs**

Comprehensive supply chain visibility, identifying risks and critical vulnerabilities of **Third-Party COTS Software**



SBOM360

Generate **Build SBOMs**

Utilize Lineaje AI to automate vulnerability remediation, continuous optimization and strategic management of **Build Software**

SBOM360 Hub

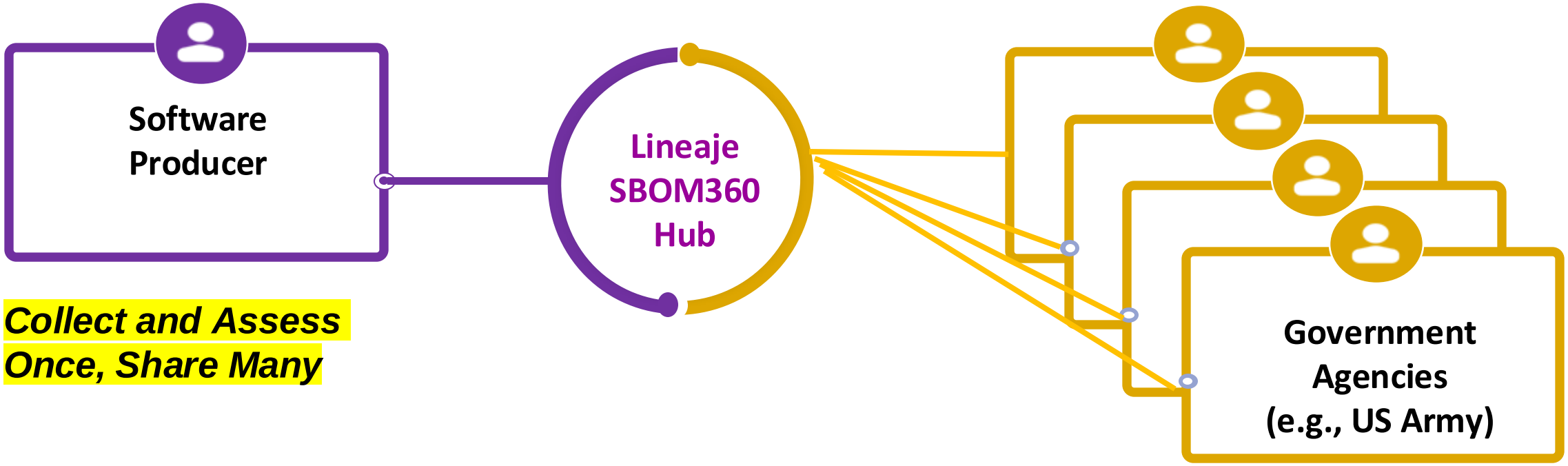
Generate **Deployed SBOMs**

Manage compliance artifacts and vulnerability information for **Deployed Software**

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

LINEAJE SBOM360 Hub: Secure SBOM Exchange

Simplify acquisition and procurement processes – with secure, private sharing SBOMs Software Producers and Government Agencies

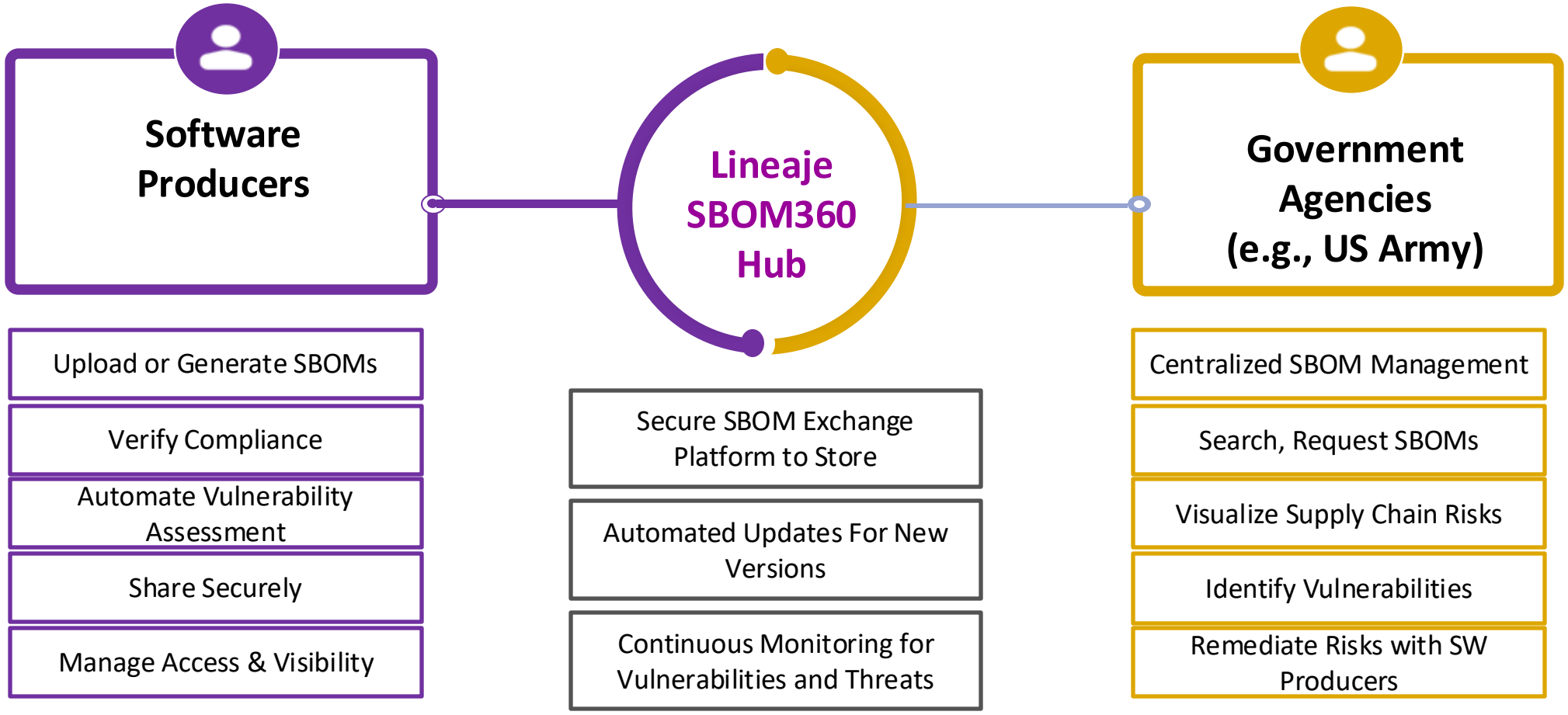


Collect and Assess Once, Share Many

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

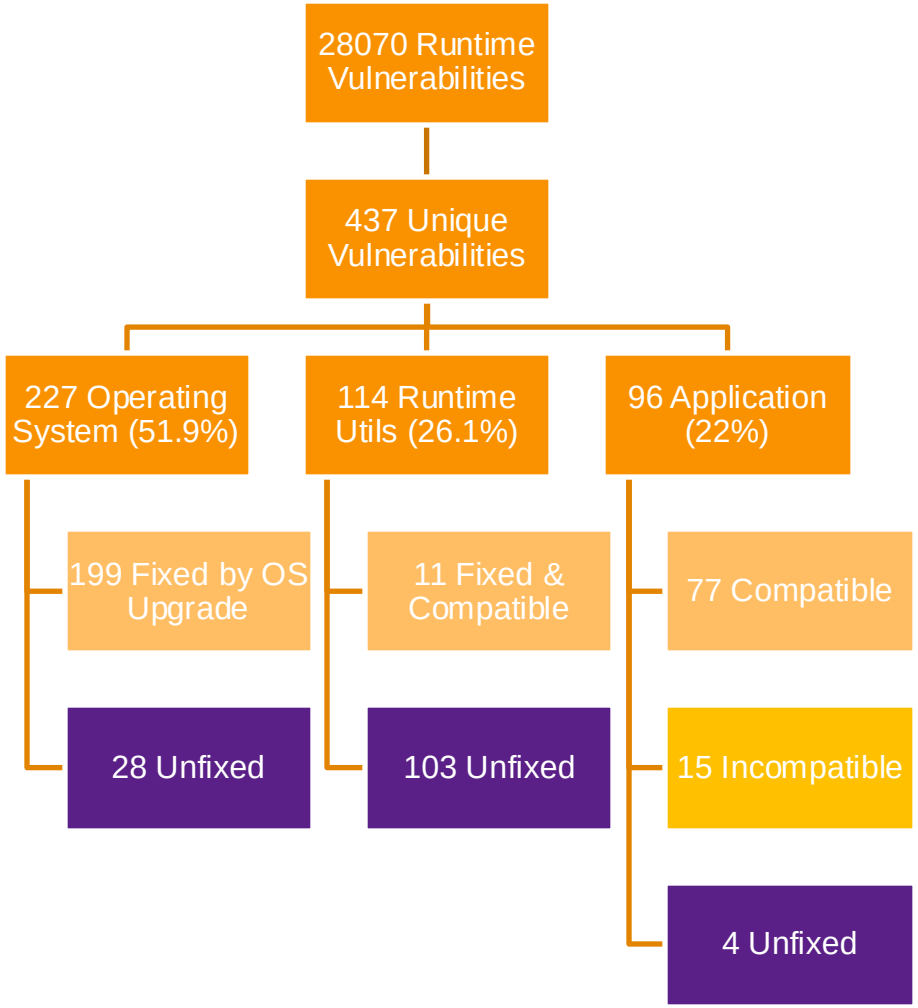
LINEAJE SBOM360 Hub: Secure SBOM Exchange

SBOM360 Hub provides **security controls** for software producers to manage permissions, access controls, document versioning, and **secure and private sharing** of SBOMs and other information.



Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

EXAMPLE: LINEAJE VULNERABILITY MANAGEMENT PATH TO ZERO



Lineaje AI Driven Remediation Planning & Remediation

- **Fix Right: DevOps upgrades the container with compatible* updates (65.67%) across OS, Runtime Utils and application**
- **Fix Left: Developers must deal with only 15 (4%) vulnerabilities dramatically reducing developer overhead (-95% load). Alternatively, backported by Lineaje if compatibility is desired.**
- **Fix Source: Managed Open-Source Crew fixes 135 (30.9%) unfixed vulnerabilities and publishes secure packages**

Ship with **Zero** Vulnerabilities

Reduce Tech Debt to **Zero**

Source OSS with **Zero** policy violations

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

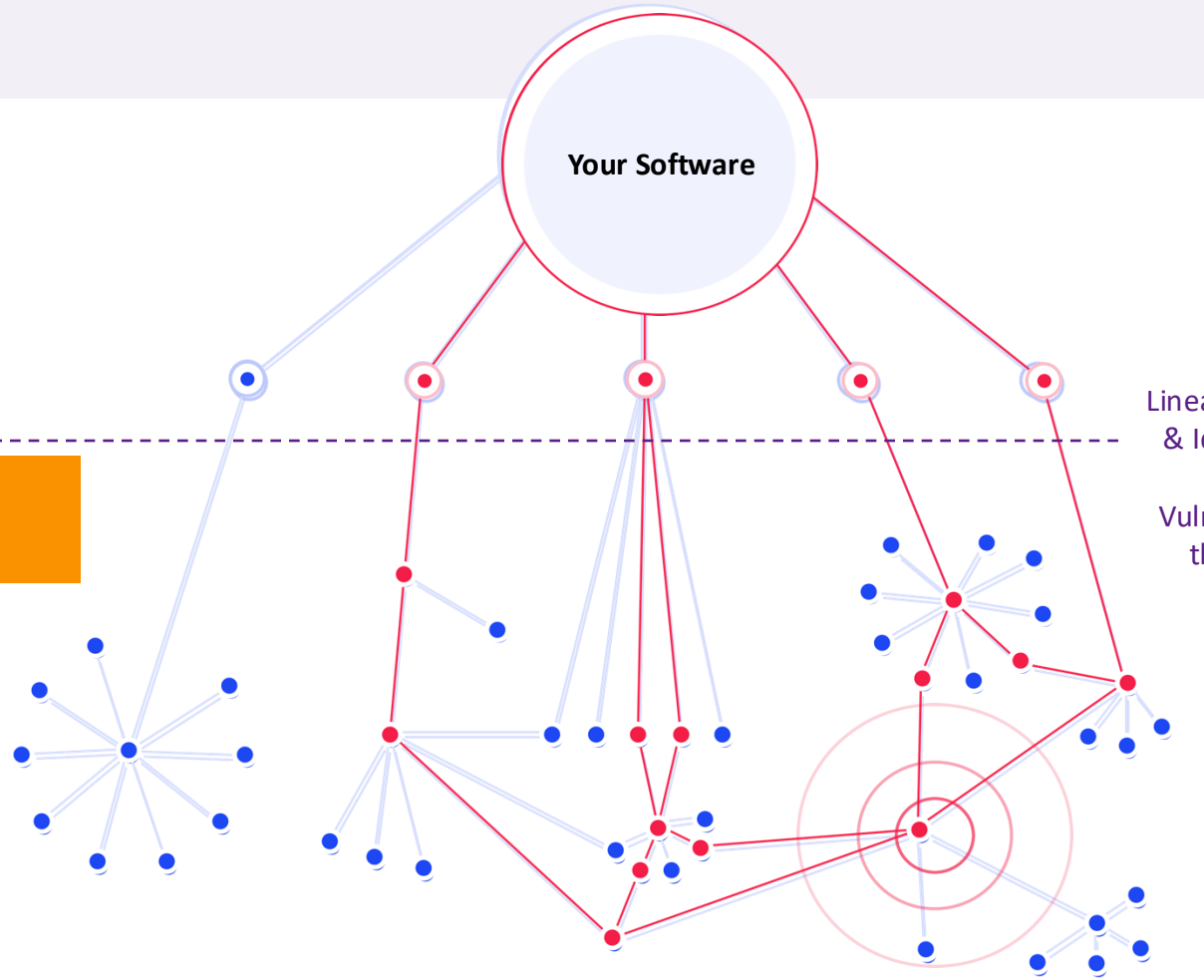
LINEAJE

RELATED WORK

CLIENT	OUTCOMES
U.S. Air Force Business Enterprise Systems (BES)	• **Efficient SW Dev Management:** Successfully oversee 100+ dev teams utilizing our software supply chain security solutions. • **Streamlined SW Development**: Integrated development management dashboards for seamless and optimized software development across Business Enterprise Systems (BES). • **Enhanced Collaboration**: Facilitated collaboration and actionable insights, connecting 56 organizations, 100 + dev teams, and 20 executives through intuitive dashboards.
VERITAS	• **Regulatory Compliance**: Streamlined EO14028 compliance by automating SBOMs compliance across six business lines and over 50 products. • **Secure, Private SBOM Sharing**: Ensured secure and private exchange of product SBOMs with customers, fostering trust and transparency. • **Proactive Risk Analysis**: Implemented continuous software supply chain risk assessment, empowering product security teams with ongoing insights and risk mitigation strategies.
PURESTORAGE	• **Automated Regulatory Compliance:** Streamlined processes by integrating with artifact repositories for automated compliant SBOM generation across xx product lines. • **Secure, Private SBOM Sharing:** Ensured secure and private exchange of product SBOMs and vulnerability information with customers, fostering trust and transparency. • **Proactive Risk Analysis**: Implemented continuous software supply chain risk assessment, empowering product security teams with ongoing insights and risk mitigation strategies.
U.S. Dept of Education Office of the CIO	• **Centralized SBOM Collection**: Successfully gathered SBOMs from third-party software vendors through a secure online exchange, ensuring a centralized and efficient process. • **Risk and EO14028 Compliance Verification**: Verification and validations of risks, ensuring compliance with EO14028 for IT software vendors, and managing associated risks. • **Proactive Risk Analysis**: Implemented proactive risk analysis strategies, enabling our client to stay ahead of potential threats and ensure a resilient software supply chain

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

Traditional Security Measures Fail To Detect Or Prevent Increasingly Sophisticated Software Supply Chain Attacks

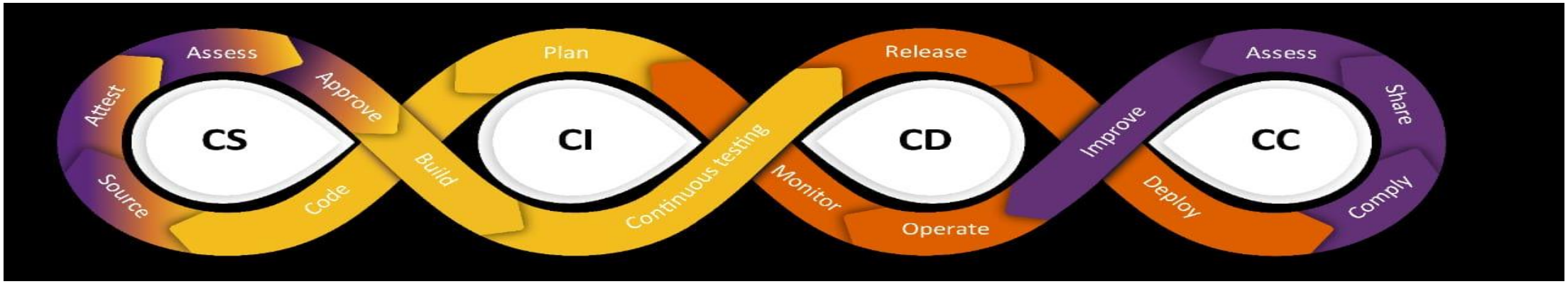


Lineaje Discovers 100% of the Software Supply Chain Down to n-th Level Dependencies

- **Crawlers discover the entire** "**lineage**" of your software supply chain**.**
- Automate **proactive risk assessments across 170 different dimensions**, including author contributors, age, code quality, vulnerabilities, and security posture.
- Lineaje Component Attestation Levels (LCAL) **detect tampers within the supply chain**.

Use or disclosure of data contained on this page is subject to the restriction on the first page of this volume.

Shifting Left of "Shift-Left" for Proactive Risk Mitigation and Right for Continuous Compliance



Software Supply Chain Challenges

Hidden Risks in Open Source

600% YoY increase in Software Supply Chain Attacks.

70-90% of Software is composed of Open Source.

Significant Costs of Vulnerability Management

Over **95% of vulnerabilities are open-source.**

One-third of developers spend over half their time patching open-source vulnerabilities.

Vast Majority of Vulnerabilities Have No Fix

Over **56% of open-source vulnerabilities have no fixes**.

Increased Regulatory and Compliance Mandates

Regulatory response is growing with EO14028, NIST SSDF, C-SCRM, ZTA, FDA, NIST CSF, EU CRA, EU DORA, CMMC, and FedRAMP require Software Supply Chain security controls.

LINEAJE PLATFORM

Lineaje "crawls" open-source to discover 100% of the supply chain and identifies inherent and integrity risks.

Lineaje continuously monitors software supply chain threats.

Lineaje AI identifies vulnerabilities and provides automated remediation recommendations.

Proactively recommends more secure open-source compatible with your application tech stack.

Lineaje AI, Bombots identify vulnerabilities and automates tasks of vulnerability remediations, without breaking your application.

Fix vulnerabilities with no fixes with the Lineaje CREW.

Lineaje automates SBOM generation and compliance verification for EO14028 and NIST SSDF requirements for every software release.

Centrally collects and manages SBOMs and evidentiary artifacts for compliance with each SBOM.