# Your Source for Software Supply Chain Security

Software supply chains are a blind spot for many organizations: weaknesses can come from any component in your software supply chain, and threat actors know this.

Scanning for known vulnerabilities is not enough to identify the hidden risks that lurk when you inherit, purchase or outsource software capabilities. Vendor risk is your risk, and suppliers' under-investment in software maintenance and security exposes you as a customer when it takes them months to remediate critical vulnerabilities. Exiger has acquired a unique capability with a massive and detailed data set to assess software risk, including the pedigree and provenance of open source components, including adversarial contribution and control, and chronic under-maintenance that makes software products brittle. This capability allows customers to build resilience in their software supply chain, select higher-quality products and suppliers, and to enforce terms and conditions for security response with continuous automated software audit. These advanced capabilities simplify compliance with U.S. government regulations like Executive Order 14028 and CISA's Software Bill of Material (SBOM) guidance.

The combination of Exiger and Ion Channel brings you unprecedented depth of analysis in vendor and open-source software risk. Leverage real-time exploration tools for pro-active risk management, software supply chain assurance, and SBOM management throughout your supplier ecosystem.

## Software Risk  Is Product Risk

Software risk is the missing piece for unified visibility of vendor and product risk in a supply chain, especially one reliant on technology. Exiger has a robust SCRM framework for understanding software risk —even if you're not a software developer and don't have technical knowledge about how software is made. Exiger measures risk in software by measuring quality in different dimensions, because risk is primarily a quality problem.

Because software is a perishable good—new exploits emerge against outdated components every week—the risk-management of software products requires the same time sensitivity as food safety. If an SBOM is the ingredients label, Exiger's cyber SCRM provides insight on what went into those ingredients, whether they were safely handled and when the product is no longer safe to consume.

SCAN TO LEARN
MORE ABOUT
EXIGER'S
ACQUISITION OF
ION CHANNEL

EXIGER

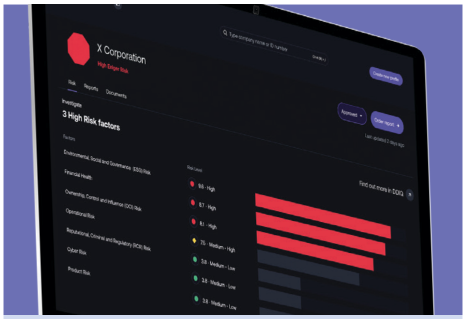
# Exiger and Ion Channel bring you a holistic view of software risk to:

- Uncover Minimize surprise from open source software components and reject fragile code with dubious pedigree and provenance.
- Illuminate unacceptable supply chain attack surface and concentration risk.
- Analyze and prioritize leading risk indicators in a Software Bill of Materials (SBOMs)
- Generate, analyze and monitor SBOMs if all you have is legacy FLOSS lists or spreadsheets from assurance packages.
- Get authoritative software names and identities from inventories with incorrect or incomplete data, or low quality SBOMs with minimal (or sub-minimal) data.
- Understand when vulnerability remediation would require overwhelming resource commitment.
- Understand which vendors are likely unable to remediate known vulnerabilities in their product, and which vendors are well-positioned to update and secure their products in a timely fashion.

## How It Works

The 1Exiger platform continuously ingests software supply chain data to identify where software dependencies show:

- Changes to open source components, maintenance and compliance history
- Leading indicators of risk in the absence of known vulnerabilities
- Supplier risks that software scanners don't detect, like change-of-control



Investigate

3 High Risk factors

| Factors | Risk Level |
|---|---|
| Environmental, Social and Governance (ESG) Risk | 9.6 - High |
| Financial Health | 8.7 - High |
| Ownership, Control and Influence (OCI) Risk | 8.1 - High |
| Operational Risk | 7.5 - Medium - High |
| Reputational, Criminal and Regulatory (RCR) Risk | 3.8 - Medium - Low |
| Cyber Risk | 3.8 - Medium - Low |
| Product Risk | 3.8 - Medium - Low |

## The Exiger FedRAMP SaaS Platform

16.8M

Unique Supply Chains

600M

Legal Entities

7B

Source Records of Supply Chain Installations

1.5T

Open-source and Proprietary Software Component Events Daily

100,000+

Software Products and Projects Analyzed Daily

As software is delivered by vendors, contractors or in-house developers, our secure platform:

- Ingests Ingests or builds a SBOM
- Analyzes all transitive dependencies, maps supplier risk metrics, automates pass/fail security rules
- Maintains continuous monitoring on all components and SBOMs.
- Provides scheduled and event-driven updates in assurance data to trigger contractual and security workflows
- Differentiates security-aware and security-responsive suppliers based on vulnerabilities, cyber hygiene, technical debt, supply chain fragility and mean-time-to-remediation
- Automates gating functions based on risk criteria to verify and enforce customer terms and conditions and safeguard software