SRC CYBER SOLUTIONS LLP

CMMC and Software Supply Chain Security - A Clear Case for Proactive Leadership

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

srccybrsolutions.com

Achieving mastery over an enterprise's digital supply chain is a critically important goal. Before jumping into a discussion on how such a journey is validated by current market sentiment, it is worth agreeing on some basic terminology and scope. The digital supply chain has its origins from around the 2000's, in the relatively modern sense. It's been over 20 years now since we as security professionals have been including SDKs in the software code that our development teams have been writing. In fact, looking at the ACM paper from the year 2000 [1] one can easily venture a guess that SDKs existed even pre the Dot Com Boom in 1999/2000.

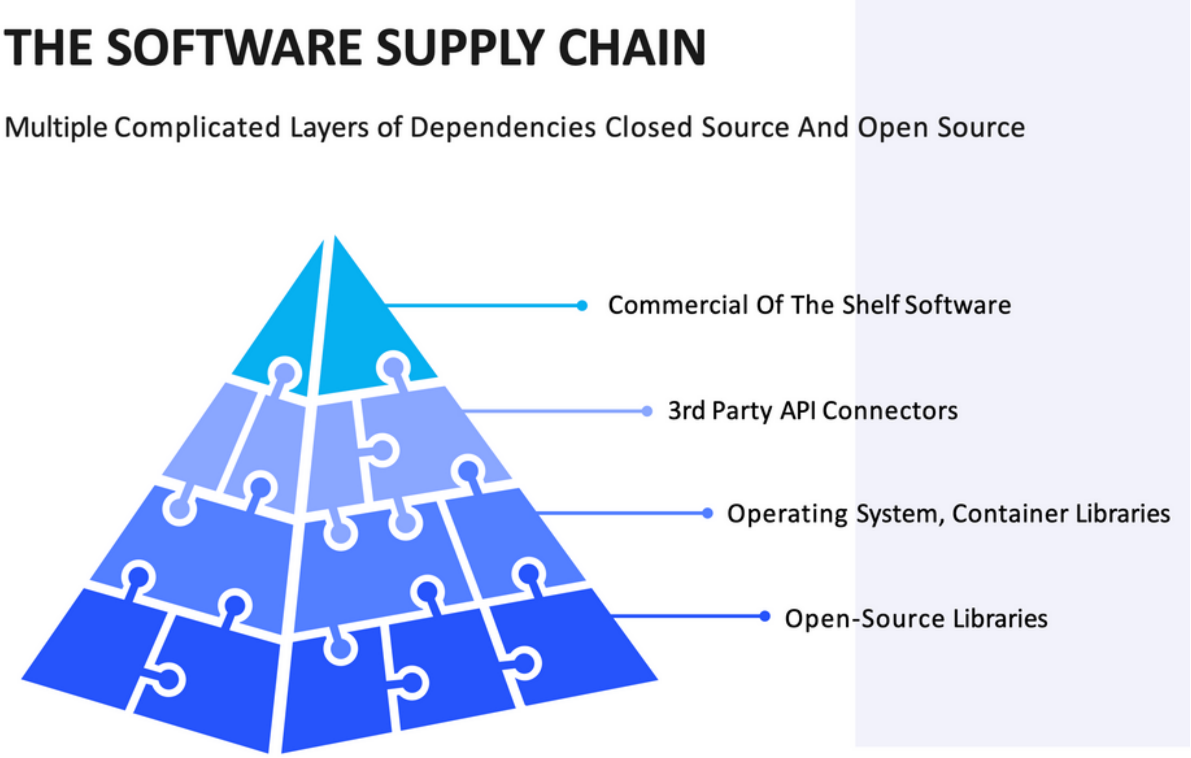
The digital supply chain consists of 4 pillars - APIs, Code Libraries, Operating System Libraries and Standalone software and services. We will discuss each one in detail and then link back to how one may go about building a successful program for achieving security for the digital supply chain.

APIs - APIs stand for Application Programmable Interfaces. APIs are used for connecting control and data transfer from one resource to another. APIs are now a primary source of data transfer between pieces of software. APIs are heavily used by enterprise organizations to transfer customer data to various third party services on order to build in user focused functionality as part of their services.

Code Libraries - Code libraries are pre-packaged pieces of code that expose certain easy to understand, and use, interfaces that developers can plug and ply to achieve functionality within a short period of time. Typical examples would be developers no longer have to write their own cryptographic algorithms, instead use code libraries that provide an easy way to achieve the functionality without writing code from scratch.

Operating System Libraries - Operating system libraries are functionality that is exposed by the operating system like Windows and Linux which allows the computer code crafted by developers to perform specific functions that are optimized for by the operating system. A typical example of an Operating System library would be a random number generator. Instead of the developer performing random number generation in code, they can tap into the operating system which would generate a random number with a combination of hardware and software, very efficiently.

Standalone Software and Services - The services typically fall in the bucket of kiosk based terminals which do not interact with product code. Another class of services that falls in this classification is SaaS services being employed directly through the browser of an employee, having no hooks whatsoever in the company's code base.


THE SOFTWARE SUPPLY CHAIN
Multiple Complicated Layers of Dependencies Closed Source And Open Source
Commercial Of The Shelf Software
3rd Party API Connectors
Operating System, Container Libraries
Open-Source Libraries

The path to success for a watertight digital supply chain security program is neither short, or easy. However, it is achievable and attainable with a reasonable level of effort. However, this requires focus and a minimum level of technical sophistication from an enterprise's security, ops teams as well as sufficient support from the C suite.

The risks of not doing anything, and giving in to inertia are significant. We have all seen breaches beginning with the Target breach to Solarwinds, Kaseya, Log4j and more over the years. Time and time again companies have paid the price for not having visibility, control and processes to manage their software supply chains. The revenue generating engines for each enterprise depend on competent software to keep powering the engine. Not understanding the inner workings, and simply buying cyber insurance is not a viable strategy.

CMMC Specific Discussion - Most organizations must focus on a couple of areas to understand their security posture and protect against software supply chain attacks - a) keep an inventory of the various libraries and the corresponding applications where they are used (clean and up to date CMDB for the codebase) b) include all 3rd party integrations in the overall enterprise’s continuous monitoring program.

We will now list one by one areas of CMMC that are applicable to this discussion and provide context for each topic. Publicly verifiable information which the following analysis is based upon is available here at this URL:
https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/

CMMC Level 1

(1) **CMMC Practice AC.L1-3.1.20** – External Connections: Verify and control/limit connections to and use of external information systems.

External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of FCI, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems.

Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

(2) **CMMC Practice AC.L1-3.1.2** – Transaction & Function Control: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of - origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

It is important to realize when account privileges and parameters are modified using automation software, workflow manager that there needs to be guardrails on what programmatic calls and API functionality can and cannot do without supervision and explicit authorization. Understanding what data can go through authentication and authorization API calls is critical as well as having control mechanisms to stop the above mentioned API calls in case inappropriate data passes through them.

(3) **CMMC Practice AC.L1-3.1.1** – Authorized Access Control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems.

Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications.

Automated processes, that manage access rights must be cataloged, introspected and managed appropriately to make sure no untoward incident is caused due to the wrong data being passed due to input validation errors and other errors in general. This means API calls to internal resources as well as to external resources must be analyzed and corrected as required.

(4) **CMMC Practice AC.L1-3.1.20** – Control Public Information: Control information posted or processed on publicly accessible information systems.

In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, FCI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post FCI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

Web based properties that display and provide access to information that is sensitive must be cataloged appropriately to understand what are the network calls via APIs to 3rd parties and other services. A review must be done to make sure no data is being passed to entities that should not have access to such data.

CMMC Level 2

(1) **CMMC Practice AC.L2-3.1.3** – Control CUI Flow: Control the flow of CUI in accordance with approved authorizations.

Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information.

Flow control restrictions include the following: keeping export-controlled information from being transmitted in the clear to the internet; blocking outside traffic that claims to be from within the organization; restricting requests to the internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.

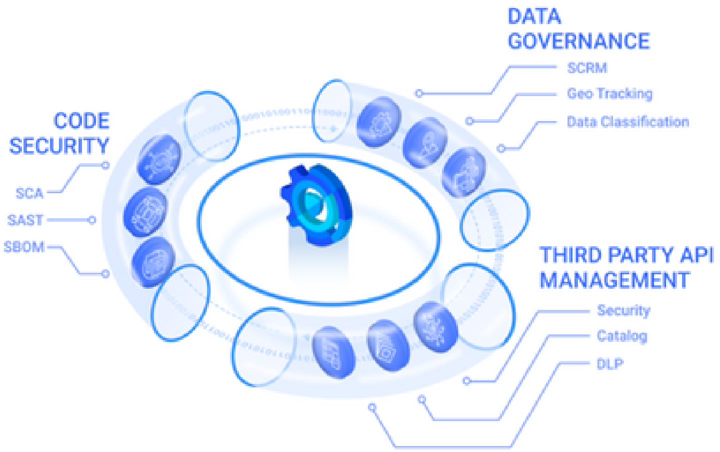
Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

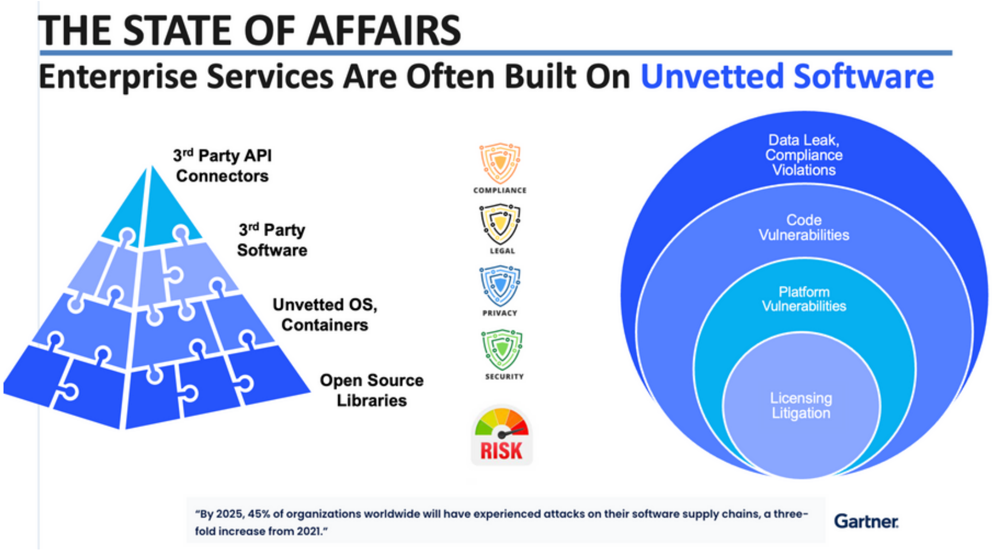
It is imperative to maintain a close watch on all transfer of data between systems especially using APIs to ascertain if compromised accounts and systems are passing information that should not traverse information boundaries or not. Furthermore keeping an accurate catalog of all physical locations, correlating to all end points of the data transfer must be maintained, as well as any drift from recorded locations must generate alerts.

In addition to the above, the following requirements can be successfully handled with a data supply chain solution to different degrees:
CMMC Practice AC.L2-3.1.13 – Remote Access Confidentiality: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
CMMC Practice AU.L2-3.3.1 – System Auditing: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
CMMC Practice AU.L2-3.3.3 – Event Review: Review and update logged events.
CMMC Practice CM.L2-3.4.2 – Security Configuration Enforcement: Establish and enforce security configuration settings for information technology products employed in organizational systems.
CMMC Practice IR.L2-3.6.2 – Incident Reporting: Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

CMMC Practice RA.L2-3.11.2 – Vulnerability Scan: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
CMMC Practice RA.L2-3.11.3 – Vulnerability Remediation: Remediate vulnerabilities in accordance with risk assessments.
CMMC Practice SC.L2-3.13.2 – Security Engineering: Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
CMMC Practice SC.L2-3.13.8 – Data in Transit: Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

More detailed information can be found on each at this link:
https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/





THE STATE OF AFFAIRS

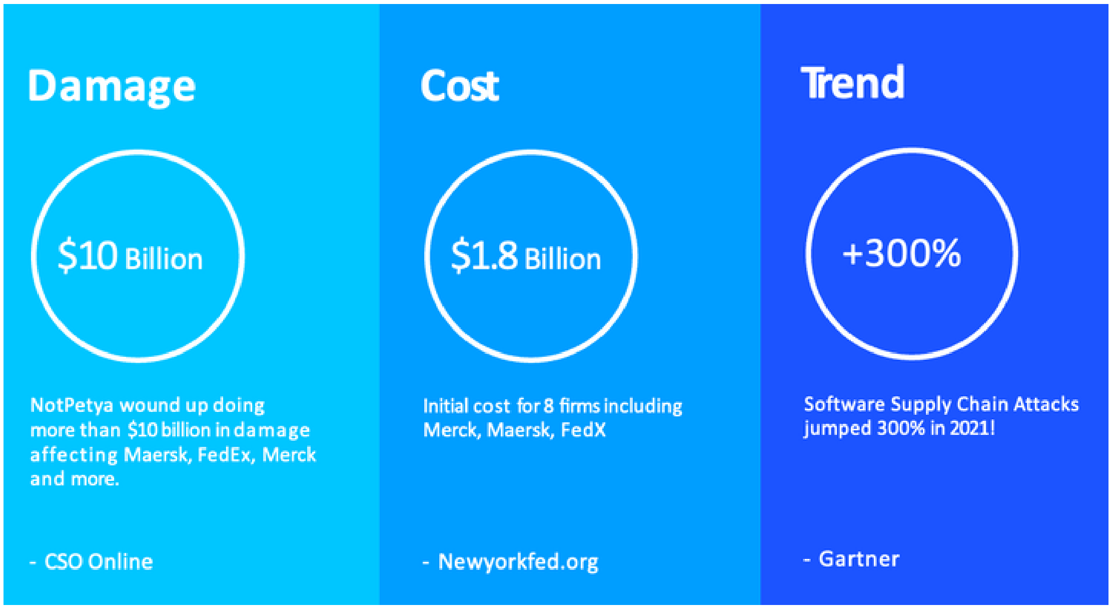
Enterprise Services Are Often Built On Unvetted Software

"By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021." Gartner

The benefits for any enterprise that takes a second look at making sure they have everything buttoned down is tremendous - the ability to have your cake and eat it too. It makes perfect sense to let development teams maintain their level of freedom yet at the same time provide the security and compliance teams. The risk reduction and peace of mind for security, compliance, and legal teams is massive. To be able to understand whether the building blocks on which your revenue generation engine is based off, is a potential liability or an asset, is critical to the long-term success of the company.

Compliance teams can respond faster to customer inquiries for security posture. The security team can have a tighter handle and make sure the attack surface is kept under tight check while the legal team can lower the liability from a data leak perspective and manage the process better by having vendors map to the various minimum criteria required for safely conducting business.

The threat is real, as we present below the risks of not having a robust software supply chain security program in place are quite real. Market leaders in the enterprise and mid market sectors in various verticals like technology, healthcare, financials and manufacturing are waking up rapidly to the fast paced threat environment.



Damage

$10 Billion

NotPetya wound up doing more than $10 billion in damage affecting Maersk, FedEx, Merck and more.

- CSO Online

Cost

$1.8 Billion

Initial cost for 8 firms including Merck, Maersk, FedX

- Newyorkfed.org

Trend

+300%

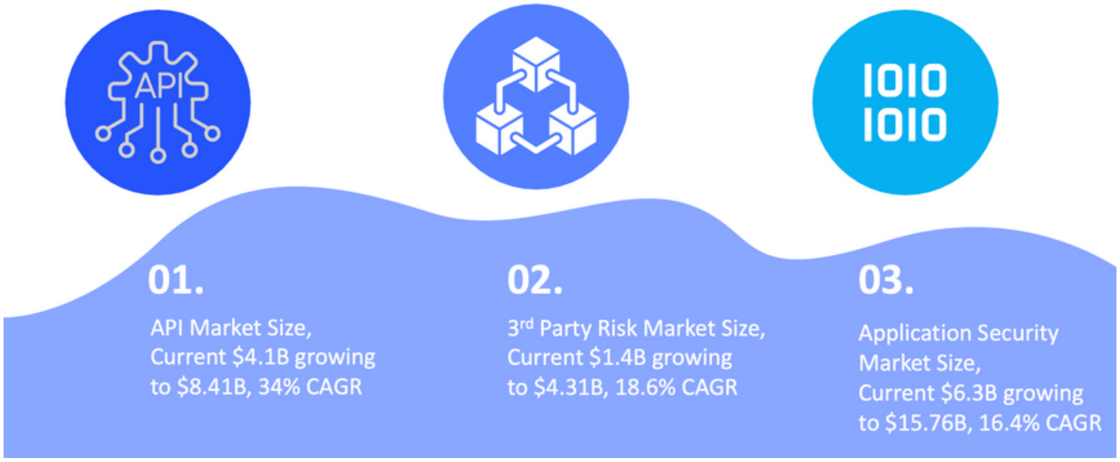
Software Supply Chain Attacks jumped 300% in 2021!

- Gartner

In the very first day of the well publicized "NotPetya" Ransomware attack, which was essentially a version of a Software Supply Chain compromise - Merck lost about $280 Million USD due tot he shutdown of a critical drug manufacturing plant. Revenue loss at this scale is not sustainable for public and for profit enterprises.

The enterprise market segment for Software Supply Chain security straddles a few overlapping areas. This is because to answer the question in a complete and effective manner it is not recommended to pigeon hole the security prioram to just traditional vendor risk management principles. In fact, forward looking programs in the market are often consuming complementary ideas from areas like API security, Vulnerability management and incidence response all within the umbrella of Software Supply Chain security.

MARKET SIZE



01.
API Market Size,
Current $4.1B growing
to $8.41B, 34% CAGR

02.
3rd Party Risk Market Size,
Current $1.4B growing
to $4.31B, 18.6% CAGR

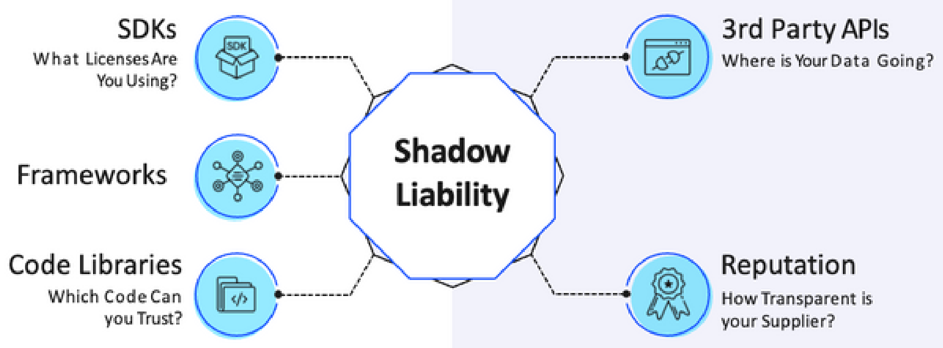
03.
Application Security
Market Size,
Current $6.3B growing
to $15.76B, 16.4% CAGR

The market opportunity for the Software Supply Chain space is tremendous to say the least. Sitting at the intersection of API security, Third Party Risk Management and Application security, Software Supply Chain security is poised to be the next significant change in the world of enterprise security programs. CAGR based growth number just in the North America segment is estimated to be more grater than 30% in 2022 alone. It is estimated that by 2025 the market for Software Supply Chain security will be north of 40 Billion USD.

There are some significant changes though that are predicted to take place in the next few years. We predict that the understanding, remediation and auditing of "Shadow Liability" is going to. emerge in the market as a staple for many a security, GRC and risk management programs.

Shadow liability as understood today, in the market between the various segments and verticals is defined below.

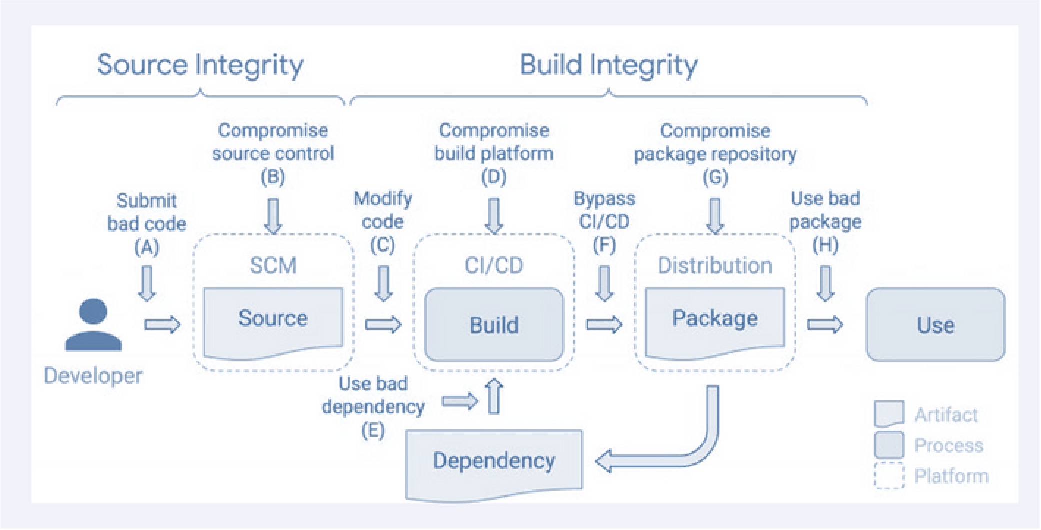
INVISIBLE RISK


SDKs
What Licenses Are You Using?
Frameworks
Code Libraries
Which Code Can you Trust?
Shadow Liability
3rd Party APIs
Where is Your Data Going?
Reputation
How Transparent is your Supplier?

Shadow Liability is the business risk that your organization absorbs as a result of using 3rd party software, services and code from commercial IT/software vendors, open-source projects and Consulting Organizations.

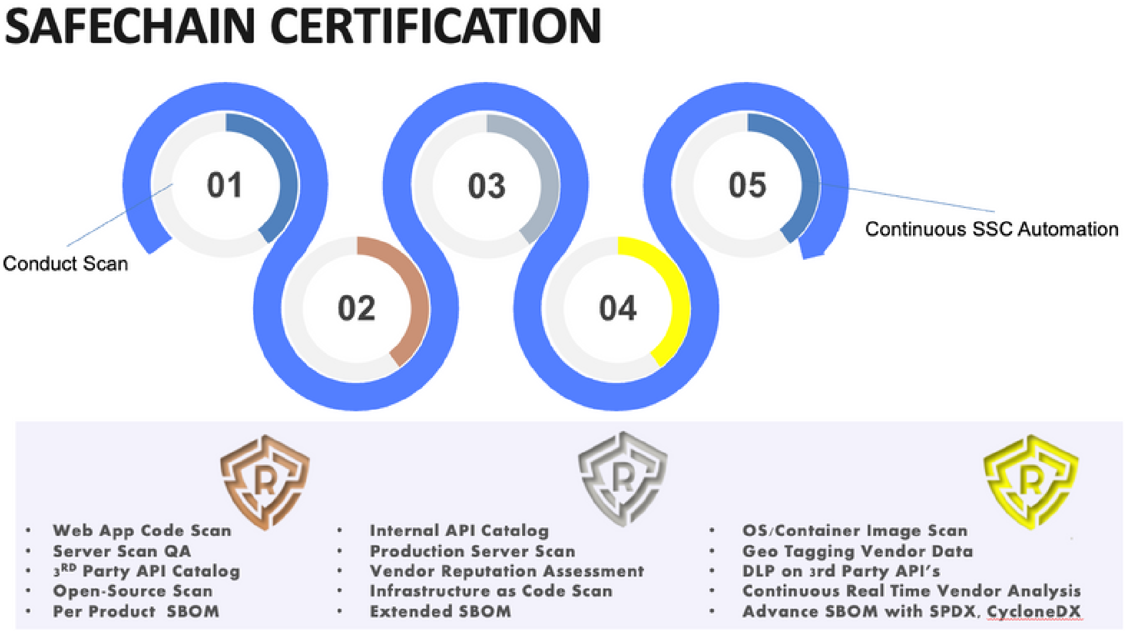
A practical depiction of a CI/CD pipeline where companies often find that shadow liability infests is also provided here.

SOFTWARE SUPPLY KILL CHAIN



In order to effectively tackle these challenges enterprise markets have started to adopt full fledged maturity model based programs. Akin to CMM models Software Supply Chain program models are also based n=on levels of sophistication that helps the organization in many ways.

We present below an example of a certification maturity model used by our customers to continuously improve their posture and highlight improvements and value for investment to company boards and auditors.



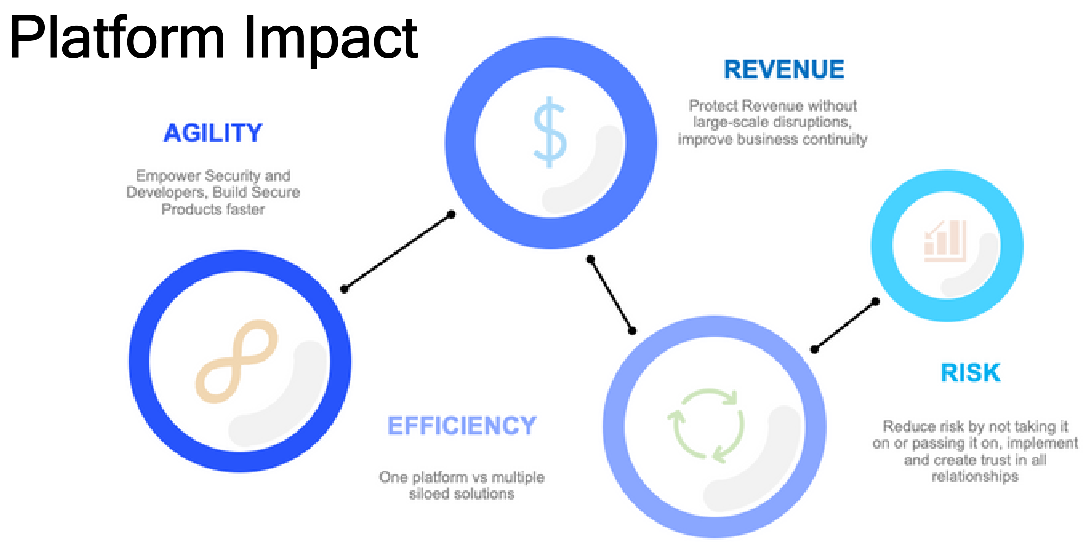
SAFECHAIN CERTIFICATION

- Web App Code Scan
- Server Scan QA
- 3^{RD} Party API Catalog
- Open-Source Scan
- Per Product SBOM

- Internal API Catalog
- Production Server Scan
- Vendor Reputation Assessment
- Infrastructure as Code Scan
- Extended SBOM

- OS/Container Image Scan
- Geo Tagging Vendor Data
- DLP on 3rd Party API's
- Continuous Real Time Vendor Analysis
- Advance SBOM with SPDX, CycloneDX

The business impact of a Software Supply Chain security program is immediate, measurable and quite meaningful. We present below how an organization can benefit from such a program in 4 easy to verbalize steps.



Platform Impact

AGILITY

Empower Security and Developers, Build Secure Products faster

REVENUE

Protect Revenue without large-scale disruptions, improve business continuity

EFFICIENCY

One platform vs multiple siloed solutions

RISK

Reduce risk by not taking it on or passing it on, implement and create trust in all relationships

We present below a more tangible representation of how companies in various sectors can benefit from these types of programs reduce their "Shadow Liability".

SHADOW LIABILITY

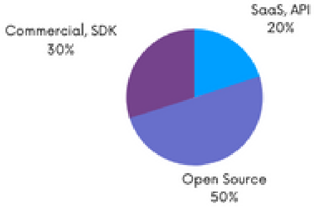
SHADOW LIABILITY IS THE BUSINESS RISK THAT YOU ABSORB AS A RESULT OF USING 3RD PARTY SOFTWARE AND SERVICES

THE PROBLEM

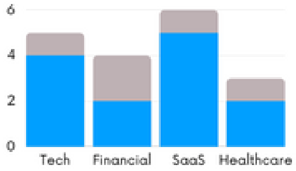
98% of all Businesses have no easy way to quantify **Shadow Liability.**
Contributing Factors - Commercial, Open Source Software, SaaS & APIs

BREAKDOWN

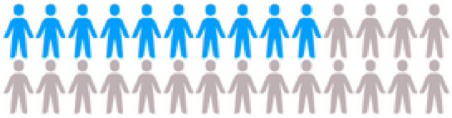
What Is Used To Build A Revenue Generating Service?



Software Types in an Enterprise



Sector-wise 3rd Party API Usage
x100 API calls per 10K Lines of Code



85% Of 3rd Party Software Suppliers Cannot Provide Satisfactory Software Quality and Data Privacy Assurance Reports

DISCOVER

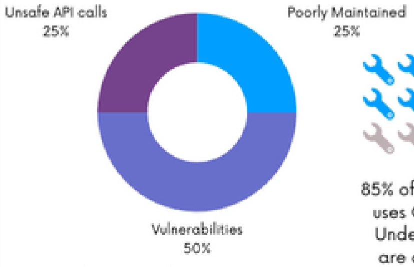
Get a complete SBOM with Software Component Analysis, API catalog, supplier reputation analysis

QUANTIFY

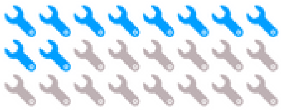
Correlate with Revenue per Product, network posture of product and type of data being handled (PII, PHI)

REMEDIATE

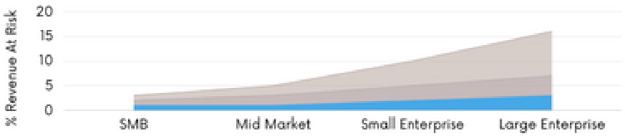
Use Your Software Bill Of Materials to reduce your business risk



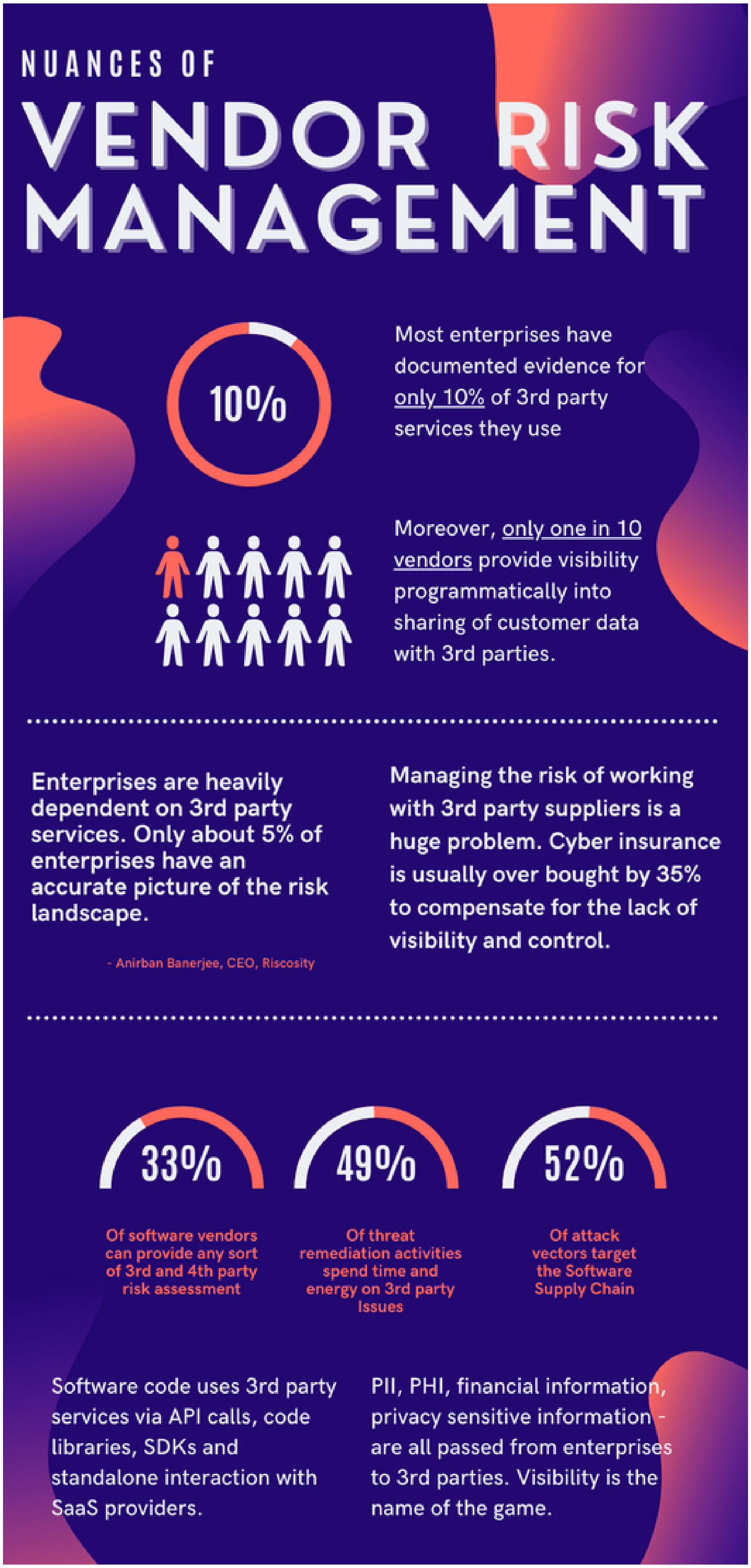
Typical Issues With Using Open Source Code In your Product



85% of Commercial Software (COTS) uses Open Source under the hood. Understand which COTS products are dumping Shadow Liability on your shoulders. Get Real Time visibility.



Revenue Risk Grows With Company Size and Dependence on Products and Services



NUANCES OF

VENDOR RISK MANAGEMENT

10%

Most enterprises have documented evidence for only 10% of 3rd party services they use

Moreover, only one in 10 vendors provide visibility programmatically into sharing of customer data with 3rd parties.

Enterprises are heavily dependent on 3rd party services. Only about 5% of enterprises have an accurate picture of the risk landscape.

- Anirban Banerjee, CEO, Riscosity

Managing the risk of working with 3rd party suppliers is a huge problem. Cyber insurance is usually over bought by 35% to compensate for the lack of visibility and control.

33%

Of software vendors can provide any sort of 3rd and 4th party risk assessment

49%

Of threat remediation activities spend time and energy on 3rd party Issues

52%

Of attack vectors target the Software Supply Chain

Software code uses 3rd party services via API calls, code libraries, SDKs and standalone interaction with SaaS providers.

PII, PHI, financial information, privacy sensitive information - are all passed from enterprises to 3rd parties. Visibility is the name of the game.

For More Information On How Software Supply Chain Security Programs can benefit your organization please feel free to get in touch with our team .

Who Will Benefit

01

Sales and Revenue Generation Teams

Riscosity helps increase the bottom-line for companies. Lowering deal close times as well as allowing customers to do more with less – maintaining small governance, risk and compliance teams yet being able to respond faster and more completely to potential due diligence questions from buyers propels sales momentum.

02

C Level Execs and Company Boards

Riscosity provides effective and clear reporting that enables executives to understand the risk posture for the company and take appropriate recommended actions in line with fiduciary responsibilities.

03

CIO's Organization, Governance, Legal and Compliance Teams

Riscosity correlates the vendors and data being exchanged with various compliance standards. This helps CIOs present an accurate picture of the organization to the board. GRC teams can cut down compliance effort by 40% using auto cataloging of vendors and compliance mapping. General Counsels can get much more accurate information in real time, and hence can evaluate liability to the company appropriately.

Value for Multiple Groups

04

CISO and Security Teams

Riscosity accelerates security reviews and helps maintain control over the security posture of the organization. Gain total, and reliable (with low false positives) coverage when analyzing and cataloging all 3rd party interactions. Automated services, with intelligent policies cut down effort needed for security teams to act quickly and generate, audit reports .

05

Development and Ops Teams

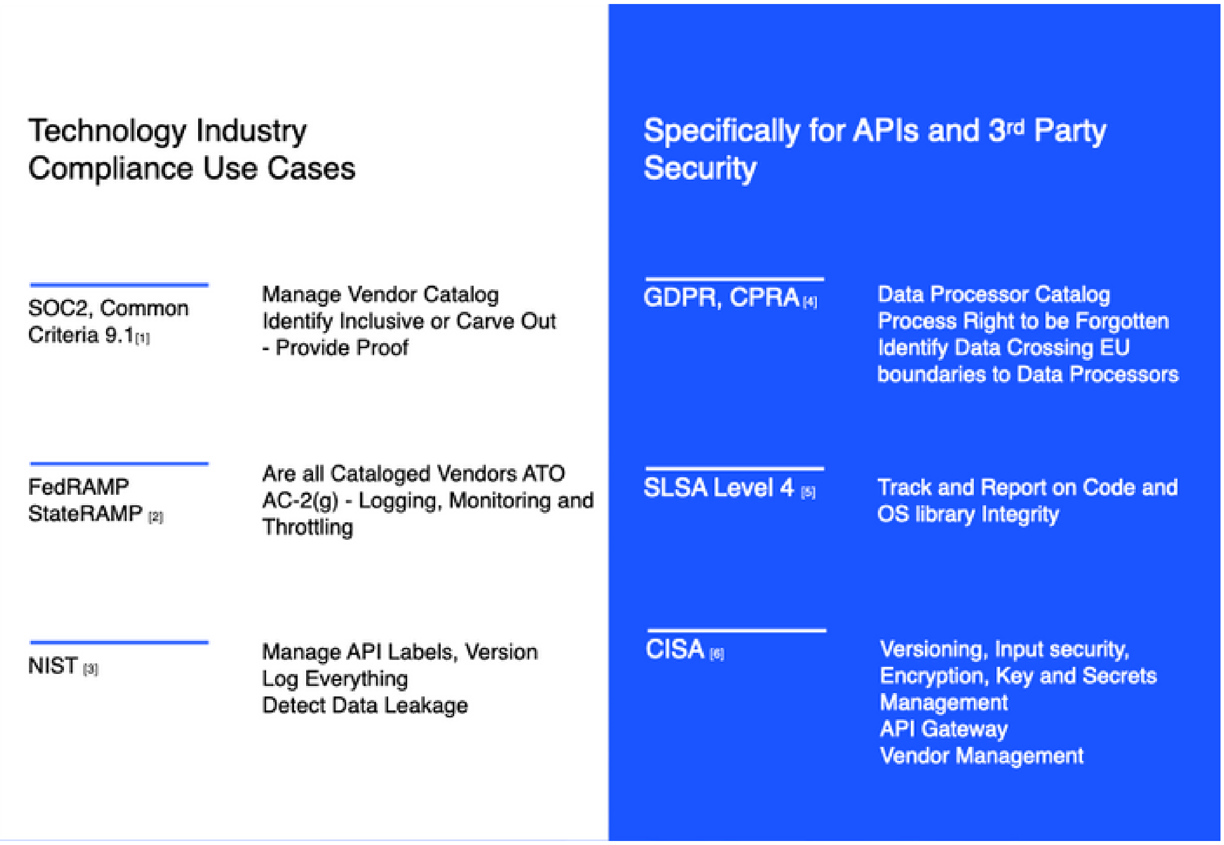
Riscosity helps Development teams identify opportunities to improve 3rd party integration points in the native codebase. With automated failover switching (to secondary services) if the primary 3rd party service provider fails, ops teams can rest easy knowing that they will not have to perform middle of the night, manual configuration changes in production environments.

Financial Industry Risk Management Use Cases

FFIEC - FIL Aug 11 2021 [1]	Understand Risks Inventory of Systems MFA, Rate Limiting
23 NYCRR 500 [2,3]	Manage Risk MFA, Rate Limiting
PCI DSS 2016v1.1 3rd Party Security Assurance[4]	Risk Assessment for 3rd Party, Nested providers - sec 3.3, 3.4 Monitor 3rd Party - sec 6.1 Network Diagrams

Specifically for APIs and 3rd Party Security

Quick Impact	Comply with Best Practices for Banking and Card Processing Industry
Free Up Cycles	Save significant manual effort on cataloging, tracking sensitive data flows
Real Time Reports	Get real time alerts if any changes occur in posture, one click report download

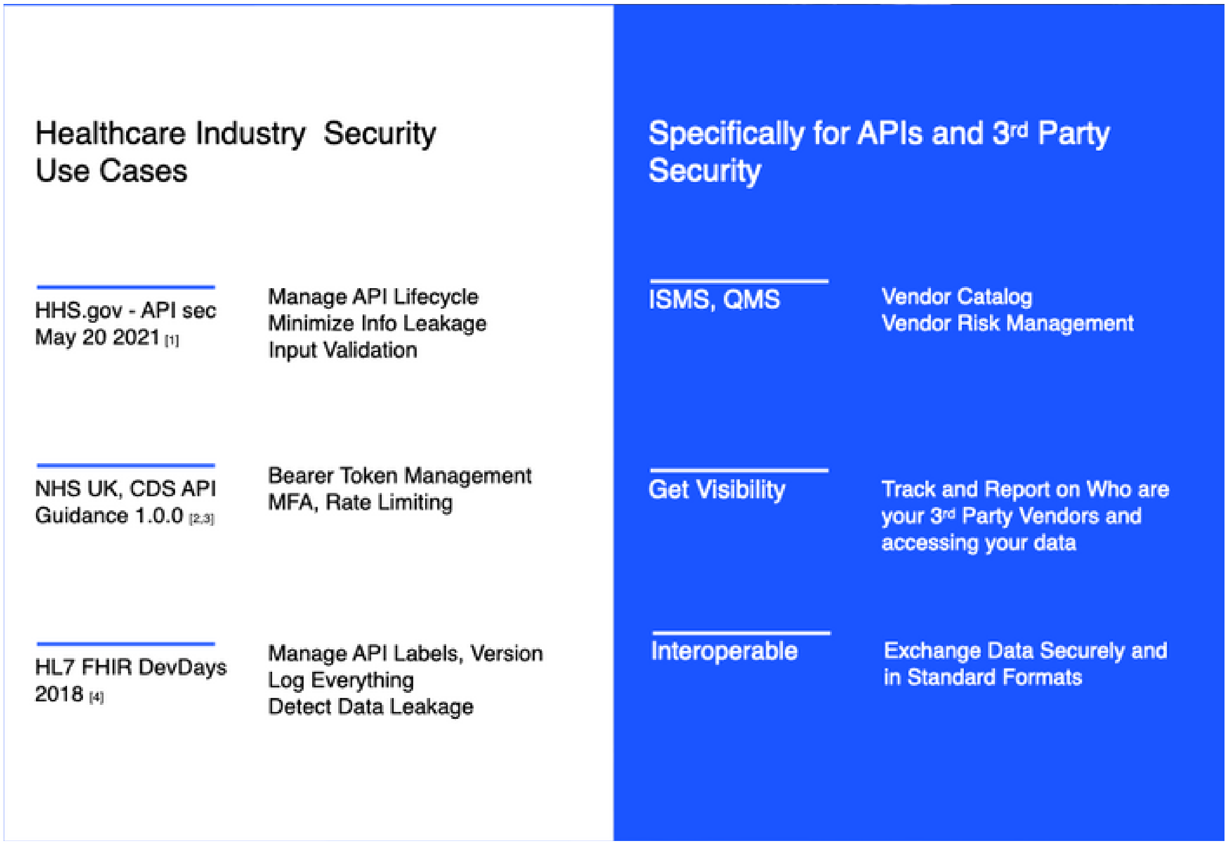


Technology Industry Compliance Use Cases

SOC2, Common Criteria 9.1[1]	Manage Vendor Catalog Identify Inclusive or Carve Out - Provide Proof
FedRAMP StateRAMP [2]	Are all Cataloged Vendors ATO AC-2(g) - Logging, Monitoring and Throttling
NIST [3]	Manage API Labels, Version Log Everything Detect Data Leakage

Specifically for APIs and 3rd Party Security

GDPR, CPRA [4]	Data Processor Catalog Process Right to be Forgotten Identify Data Crossing EU boundaries to Data Processors
SLSA Level 4 [5]	Track and Report on Code and OS library Integrity
CISA [6]	Versioning, Input security, Encryption, Key and Secrets Management API Gateway Vendor Management



Healthcare Industry Security Use Cases

HHS.gov - API sec May 20 2021 [1]	Manage API Lifecycle Minimize Info Leakage Input Validation
NHS UK, CDS API Guidance 1.0.0 [2,3]	Bearer Token Management MFA, Rate Limiting
HL7 FHIR DevDays 2018 [4]	Manage API Labels, Version Log Everything Detect Data Leakage

Specifically for APIs and 3rd Party Security

ISMS, QMS	Vendor Catalog Vendor Risk Management
Get Visibility	Track and Report on Who are your 3rd Party Vendors and accessing your data
Interoperable	Exchange Data Securely and in Standard Formats