sonatype

8th Annual

State of the Software Supply Chain

Sonatype's industry-defining research on the rapidly changing landscape of open source

Within this report, we reflect on the good practices that create ideal outcomes, and likewise, the poor practices that produce problems. As always, the goal of our reporting efforts is to provoke developer-level practices that improve software supply chain security and create fulfilling work experiences.

We draw from public and proprietary data sources to look at

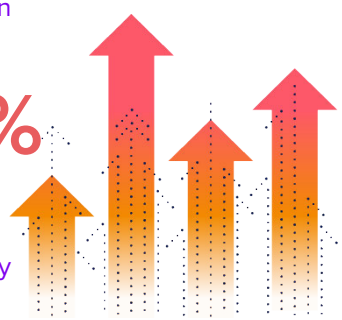
- Ongoing growth of the software supply chain, as well as persistent security concerns.
- Insights on choosing the best dependencies for your projects.
- Developer behavior and recommendations.
- A look at enlightened supply chain management and perception versus reality for maturity.
- Current and upcoming regulation status on an International level.

Key Report Findings

There has been an astonishing

742%

average annual increase in Software Supply Chain attacks.



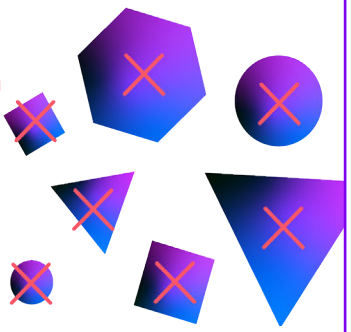
About

6 out of every **7**

project vulnerabilities come from transitive dependencies.

"More mature software supply chain managment equate to more job satisfaction."

1.2 billion vulnerable dependencies are downloaded each month.



96%

of known-vulnerable open source download are avoidable

For a deeper analysis of the state of the software supply chain:

Access the full interactive version of the report.

Download a PDF version of the full report.

Section 1: Open Source Supply, Demand, and Security

What's happened since Sonatype's last report on open source?

This section discusses

- Open source supply and demand.
- The increasing number of open source projects.
- The download statistics and growth rate of each ecosystem.
- What we've learned from the Log4j vulnerability.
- The growth of software supply chain attacks.
- Dependency confusion, malicious code injections, and the emergence of protestware.

FIGURE 1.1 SOFTWARE SUPPLY CHAIN STATISTICS, 2022

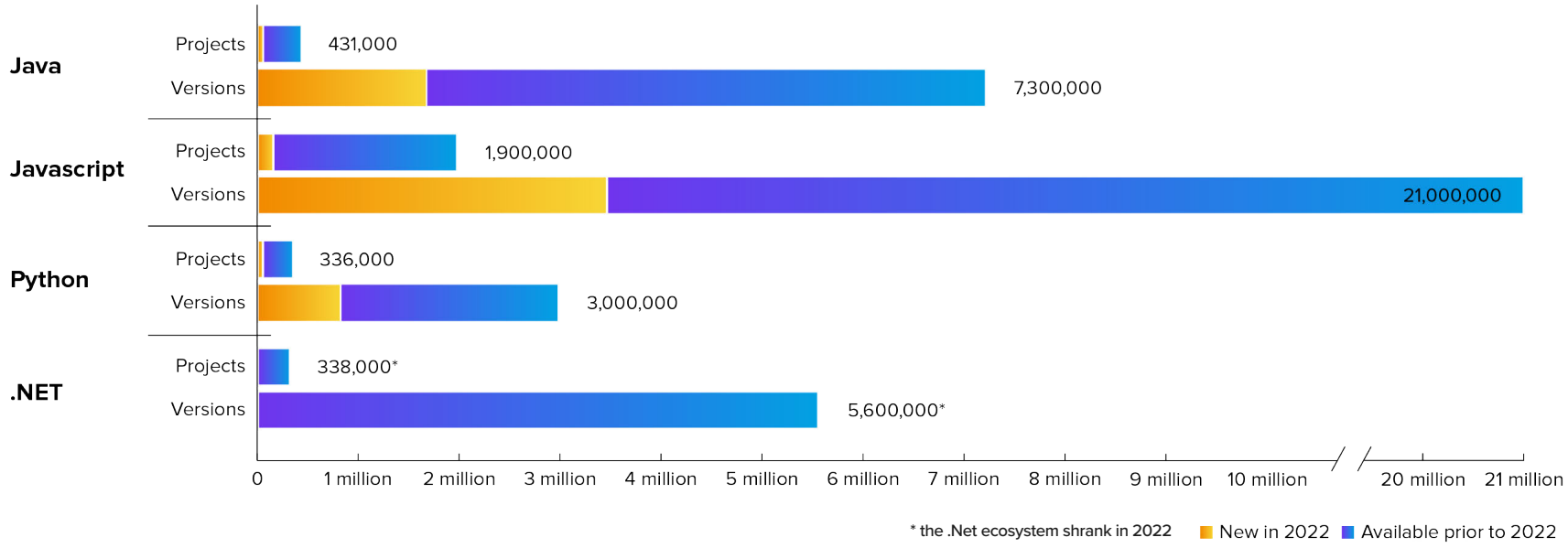
Ecosystem	Total Projects	Total Project Visions	2022 Annual Request Volume Estimate	YoY Project Growth	YoY Download Growth	Average Versions Released per Project
Java (Maven)	492k	9.5M	675B	14%	36%	19
JavaScript (npm)	2.06M	29M	2.1 [1]	9%	32%	14
Python (PyPI)	396K	3.7M	179B[2]	18%	11%	9
.NET (NuGet)	321K	4.7M	96B [3]	-5%	23%	15
Total/ Avgs	**3.3M**	**47M**	**3.1T**	**9%**	**33%**	**14**

The supply of open source continues to grow at an impressive rate. The expansion of the overall volume available combined with the increase in consumption means threats also continue to expand in scope, impact, and volume.

Malicious software supply chain attacks increased another 633% YoY, averaging a 742% average annual increase in software supply chain attacks over the past three years. *(Fig. 1.1)*

At a macroscopic economic level, the overall growth rate of adoption seems to be stabilizing around 30-35% across all ecosystems, which is down from previous years. This convergence most likely signifies the evolution of the wider open source economy. *(Fig. 1.2)*

FIGURE 1.2. OPEN SOURCE PROJECTS AND VERSIONS GROWTH, 2022



1 Figure estimated using npm download counts to from January to August 2022
2 YoY growth estimated based on known PyPI downloads from January to August 2022 as queried from
3 YoY growth estimated based on known NuGet Gallery downloads from January to August 2022

FIGURE 1.3 ESTIMATED ANNUAL DOWNLOAD VOLUMES, 2018-2022

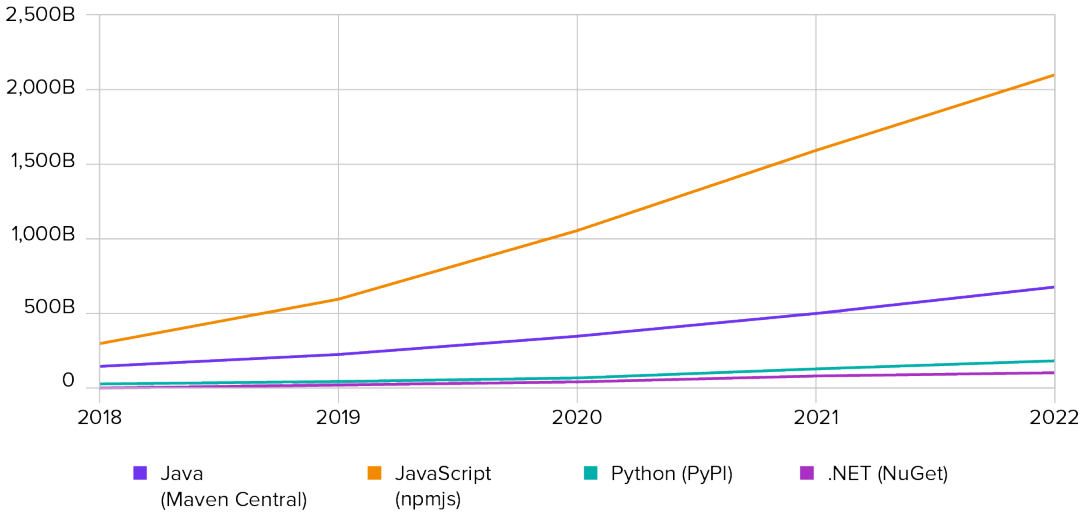
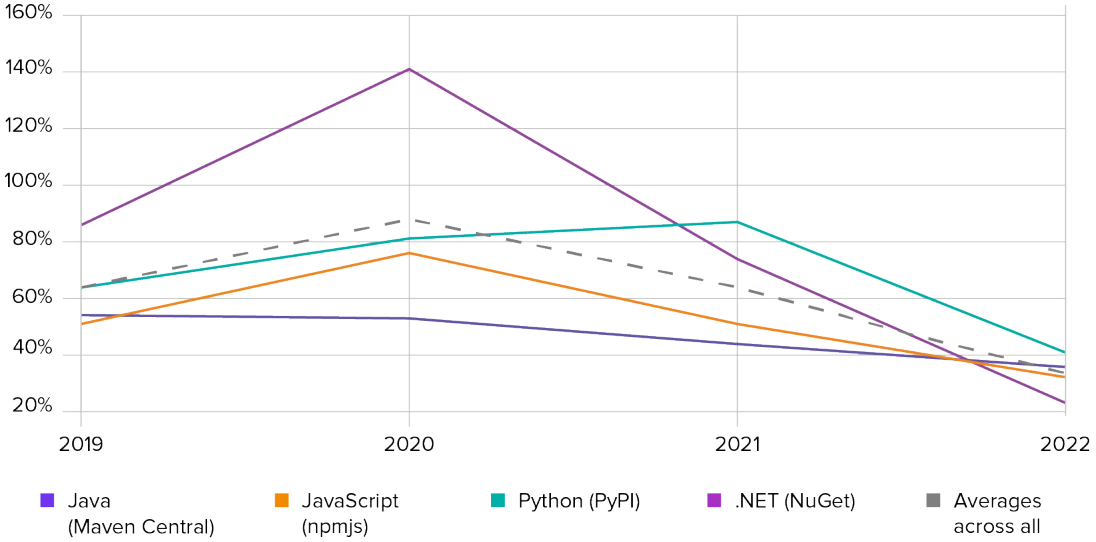


FIGURE 1.4 GROWTH RATE ACROSS ECOSYSTEMS, 2019-2022



The number of available open source projects grew an average of 9% across the monitored ecosystems to 3,274,208 unique projects. *(Fig. 1.3)*

Overall download volume across the four major ecosystems is now projected to top 3 trillion downloads overall, with npmjs poised to serve nearly as many downloads in 2022 as the four ecosystems combined in 2021. *(Fig. 1.4)*

Individual ecosystem analysis

Java (Maven)

▶ 675 billion packages projects requests volume.

▶ 36% YoY growth.

JavaScript (npmjs)

▶ 2.1 trillion packages projected download volume.

▶ 32% YoY growth.

Python (PyPI)

▶ 176 billion packages projected download volume.

▶ 41% YoY growth.

.NET (NuGet)

▶ 96 billion packages projected download volume.

▶ 23% YoY growth.

Dependency confusion, typosquatting, and malicious source code injections are still among the

key tactics used in software supply chain attacks, but the emergence of protestware is an important development. *(Fig. 1.6)*

Lessons learned from Log4Shell

- It's not only the direct inclusion of the code that matters. It's also the indirect inclusion of all kinds.
- Dependencies may be pulled in as part of a transitive dependency chain for a given program.
- Dependencies might also be embedded into other software in use.
- It's not enough to know where developers are using Log4j-core. Organizations need to know all software that uses the Log4j vulnerability. *(Fig. 1.5)*

Dependency confusion

A form of attack relying on spoofing internal package names and publishing them to an open source registry with an abnormally high version number.

Malicious code injections

A type of attack that leverages a popular component as a vector for the malicious payload.

It relies on an adversary gaining access to the source code of a library either through compromise or pretending to be a benevolent open source committer.

Typosquatting–and its cousin Brandjacking

An attack that relies on the simple technique of misspelling the name of a popular component and waiting for developers to download the wrong one mistakenly.

Protestware

An attack where a maintainer deliberately sabotages their own project to cause harm or malfunction in a way that disrupts its adopters' work.

FIGURE 1.5 ADOPTION OF LOG4SHELL RELEASES FROM AUGUST 2021–AUGUST 2022

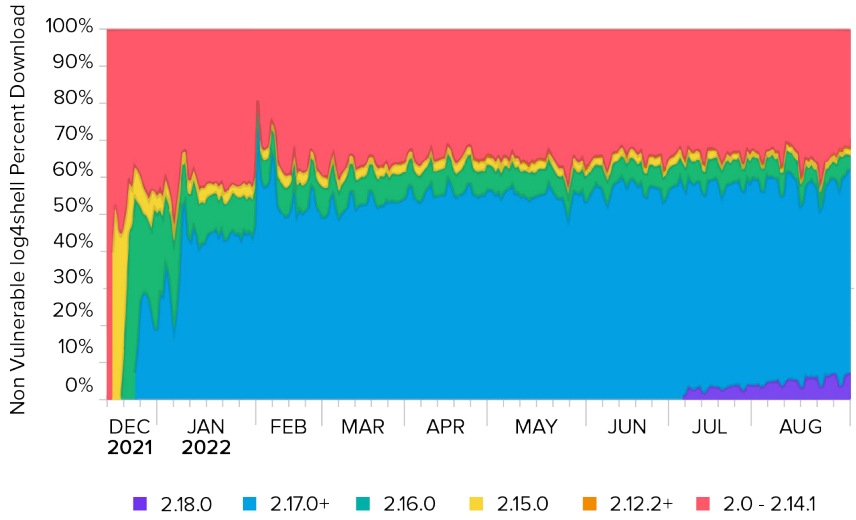


FIGURE 1.6 NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS, 2019-2022

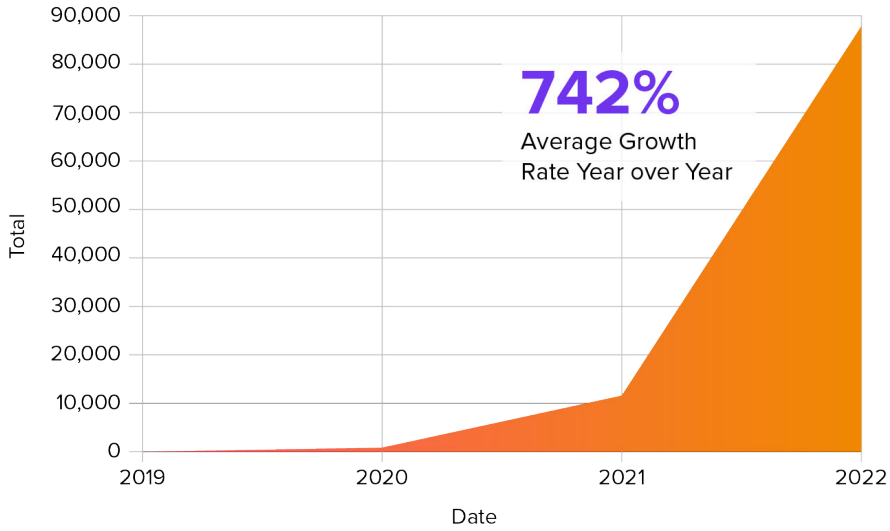
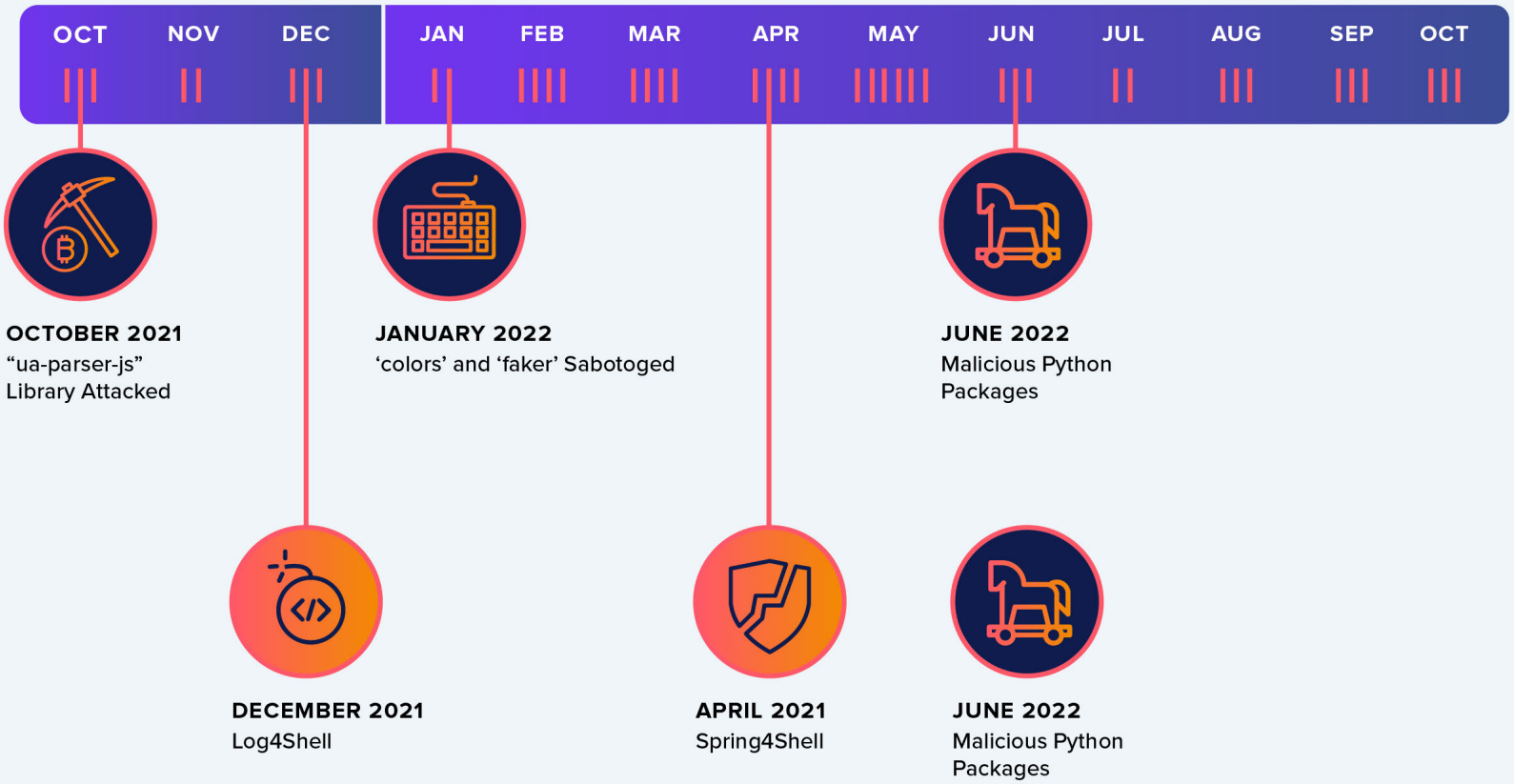


FIGURE 1.7 HIGHEST PROFILE VULNERABILITIES AND ATTACKS, 2021-22



View the full timeline to see how these attacks continue to evolve.

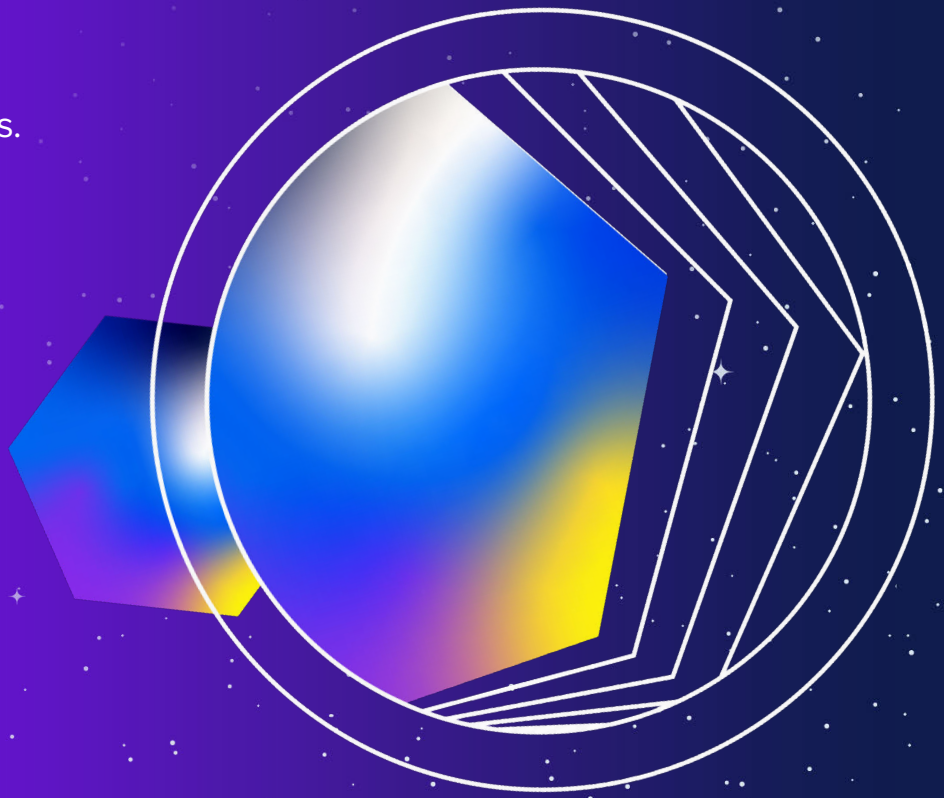
SEE THE FULL TIMELINE

Section 2: Project Quality Metrics

What metrics should be considered when choosing open source projects?

This section discusses

- Metrics to identify vulnerabilities.
- How popular projects equal more vulnerabilities.
- Characterizing vulnerable projects.
- Which quality metrics are most important.



Sonatype performed three levels of analysis:

- A series of statistical tests to determine whether any single metric can be used to identify whether a project is more likely to have a known vulnerability.
- A modeling exercise to determine if a combination of quality metrics can be used to identify non-vulnerable components.
- An analysis of transitive vulnerability risk and whether various quality metrics are associated with decreased risk of inheriting vulnerabilities from transitive dependencies.

About **6** out of every **7** vulnerabilities affecting projects come from transitive dependencies.

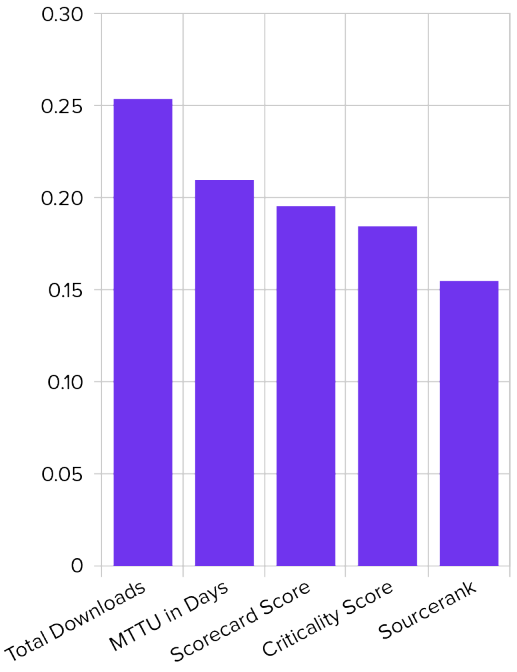
The analysis described in this section is a combination of the following sources:

- Project Data: 7.9 million releases of over 420 thousand Java projects hosted in Maven Central.
- Vulnerability Data: A set of over 14 million Common Vulnerabilities and Exposures (CVE) reports for these projects, drawn from the National Vulnerability Database, various public vulnerability feeds, and Sonatype's proprietary vulnerability analysis work.
- Commonly-used Projects List: A list of 60,648 open source projects frequently occurring in application security scans
- Project Versions List For Previous Year: A list of the project versions used in application builds since November 2020.
- Dependency Relationships: A list of all dependencies for each project release.
- Libraries.io Sourcerank Ratings: A list of ratings according to the Libraries.io SourceRank project rating provided by Tidelift.
- OpenSSF Security Scorecard: An aggregate measure of project security practices developed by the Open Source Security Foundation.
- Security Scorecard Metrics: The individual project quality measurements that feed into the Scorecard Score above.
- OpenSSF Criticality: This measures a project's influence and importance, i.e., how critical is this project to the open source ecosystem and how much it is relied upon.
- Mean Time To Update (MTTU) Metric: A measure of how quickly a project updates its dependencies when new versions are released. Measures the average number of days it takes a project to incorporate a newly-released version of a dependency.
- Popularity: Data on the number of Maven Central downloads for each project.

Because enterprise software teams commonly use these projects, this ensures our findings are applicable to open source management decisions commonly faced by these organizations.

The more users a project has, the more likely it is that developers will stumble across a security-relevant bug. As a result of these factors, more popular projects tend to have more known vulnerabilities–but that doesn't necessarily mean that they're safer. *(Fig. 2.1)*

FIGURE 2.1 RELATIVE IMPORTANCE OF QUALITY METRICS IN RESEARCH MODEL



Code review emerged as the most important factor for identifying vulnerable projects. The second most important factor was not having binaries checked into the repository. *(Fig. 2.2)*

A combination of machine learning and metrics can be used to accurately identify projects with known vulnerabilities – we've established this as the Sonatype Safety Rating, and are rolling it out as an experimental tool in both Central and OSS Index.

We will be monitoring the projects in our Sonatype Safety Rating dataset over the next year to see if high-scoring projects are associated with lower vulnerability rates over time–and will report those findings in next year's report.

The Sonatype Safety Rating corresponds closely to vulnerability: 88% of projects with a Sonatype Safety Rating less than 5 have a known vulnerability.

Of the data analyzed, on average a library contained 5.7 dependencies. *(Fig, 2.3)*

Including security issues in these dependencies significantly increases the number of vulnerable projects. While only 10% had a vulnerability directly affecting the code in that project, 62% of these projects had a direct or transitive vulnerability.

FIGURE 2.2 ELEMENTS MOST USEFUL FOR IDENTIFYING VULNERABLE PROJECTS

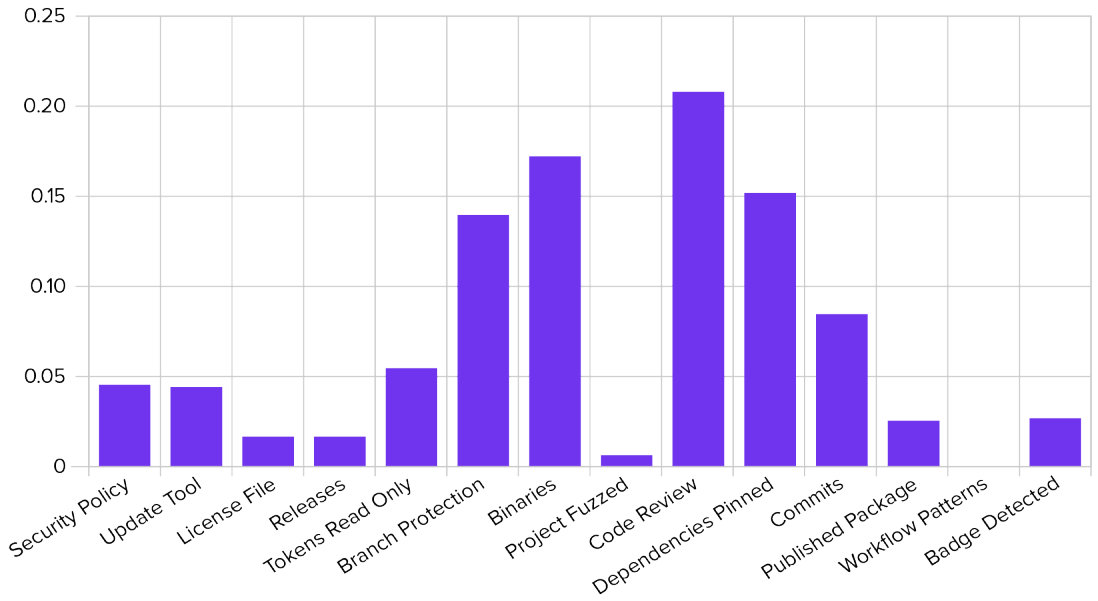
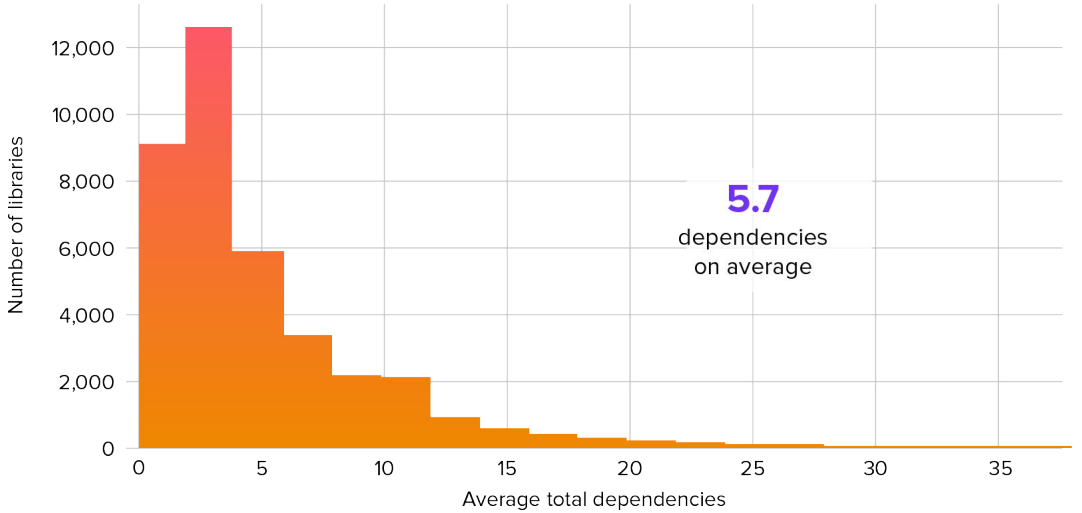


FIGURE 2.3 AVERAGE TOTAL DEPENDENCIES IN COMMONLY-USED LIBRARIES



Section 3: Open Source Dependency Management: Trends and Recommendations

An analysis of developer migration trends and best practices of dependency management

This section discusses

- Dependency management insights.
- Whether maintainers or consumer are proliferating OS risk.
- Sonatype's Log4j case study.

Developers are facing an overwhelming tide of decision-making when it comes to dependency management.

The average Java application contains 148 dependencies (20 more than 2021), and the average Java project updates 10 times a year–meaning developers are being asked to track nearly 1,500 dependency changes per year per project.

Along with choosing and managing 150 initial dependencies, developers are being asked to:

- **Track an average of 1,500 dependency changes per year per application.**
- **Possess significant security and legal expertise to choose the safest versions.**
- **Maintain a working knowledge of software quality at all times.**
- **Understand the nuances of ecosystems being used.**
- **Sift through thousands of projects to pick the best ones.**

FIGURE 3.1 FIVE GROUPS OF MIGRATION DECISIONS

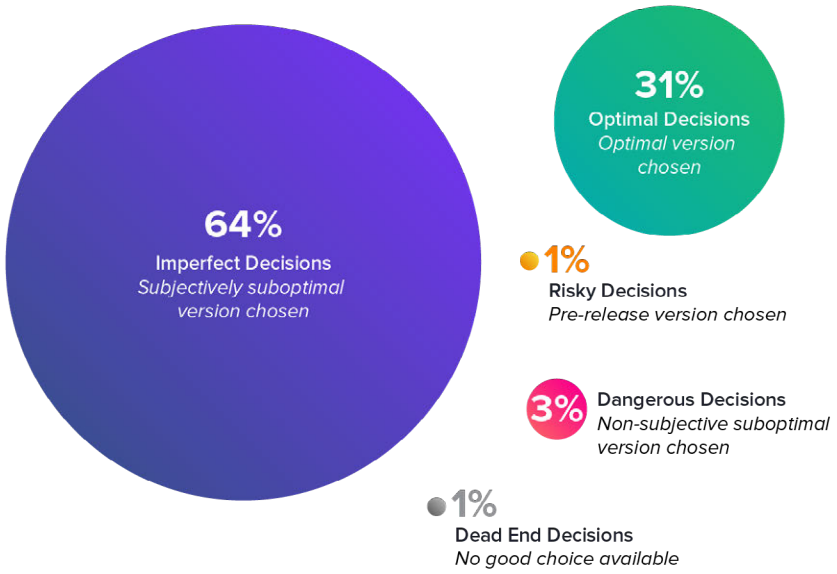
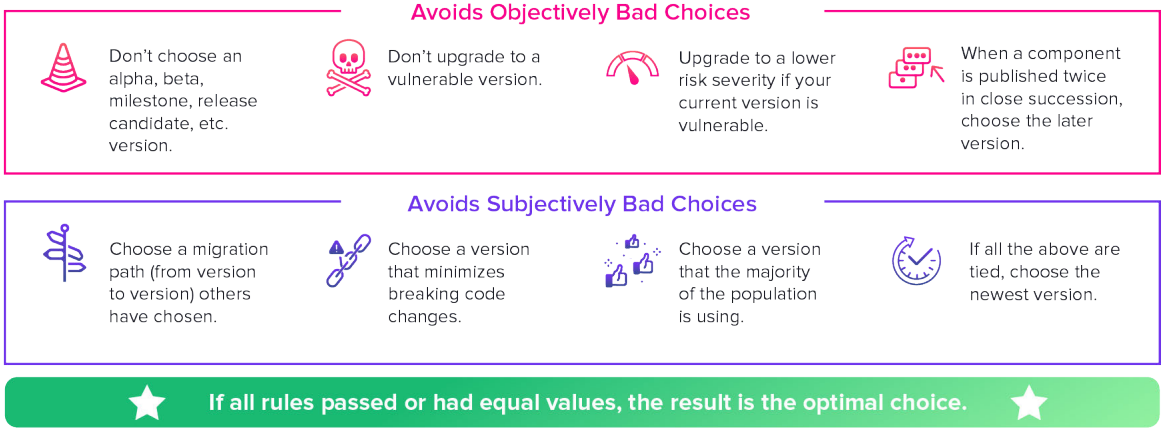


FIGURE 3.2 EIGHT RULES FOR UPGRADING TO THE OPTIMAL VERSION



In an analysis of vulnerable downloads, 96% of vulnerable downloaded releases had a fixed version available. *(Fig. 3.1)*

Sitting in the reactive zone is not only suboptimal, but it puts you at an immediate disadvantage and penalizes those development teams when an issue arises. *(Fig. 3.2)*

Open source consumers who are proliferating the majority of open source risk. We can't solve the issue of open source security without consumers changing their behaviors. *(Fig. 3.3)*

We have data showing that, given the right tools, consumers can change behaviors positively, which can help solve the problem. *(Fig. 3.4)*

Teams can reduce risk, save time, and save money by merely being close to the edge. *(Fig. 3.5)*

FIGURE 3.3. STRATEGIES FOR DEPENDENCY MANAGEMENT

FIGURE 3.4 UPDATE MANAGEMENT DECISIONS

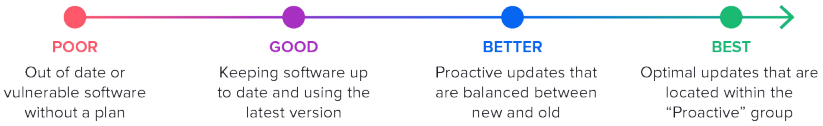
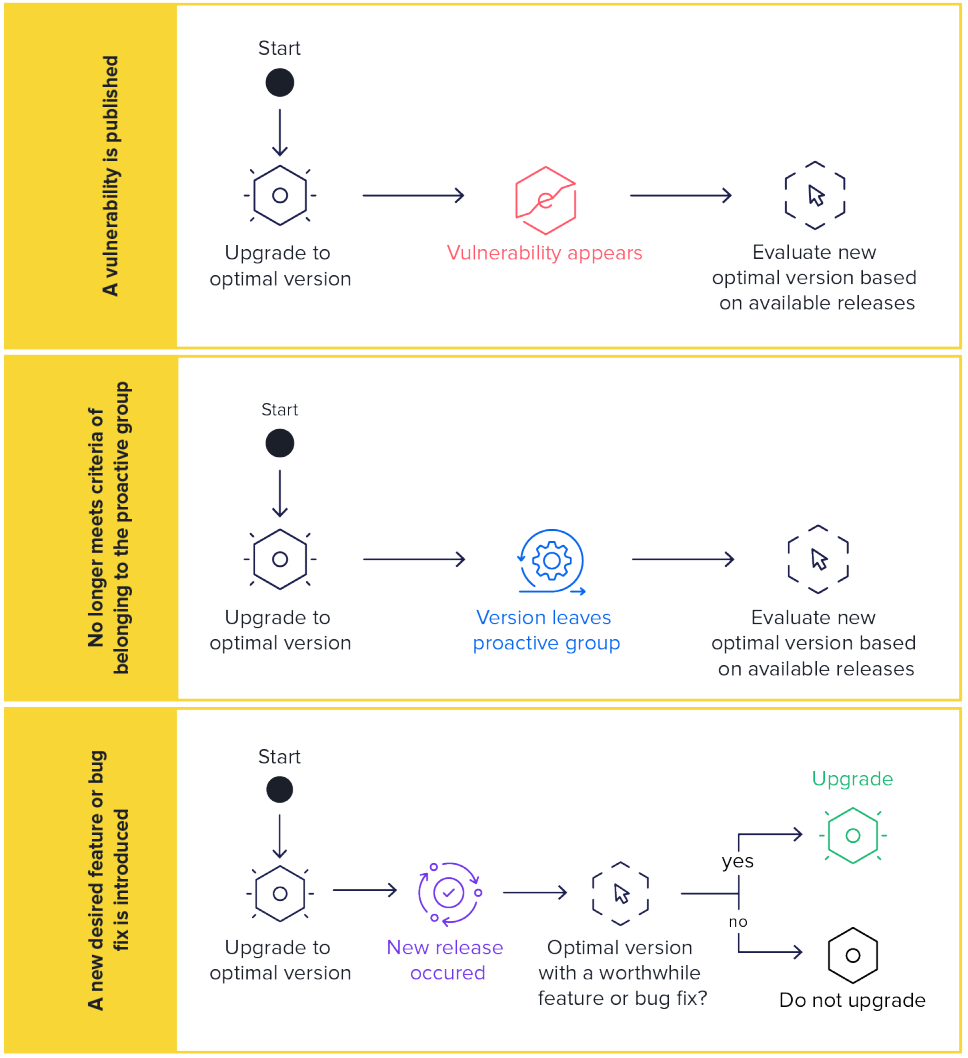


FIGURE 3.5 DEPENDENCY MANAGEMENT TRIGGERS

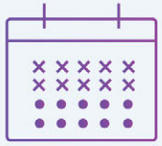


For individual teams, choosing the optimal version means you select the best balance of safety and efficiency. *(Fig. 3.6)*

Consumption behavior is at the root of this – if we change behavior, enormous risk is immediately eliminated. *(Fig. 3.7)*

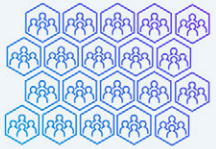
FIGURE 3.6 TIME SAVED WITH OPTIMAL UPGRADE DECISIONS

By making optimal upgrade decisions, organizations could save



two weeks

per development team per year.



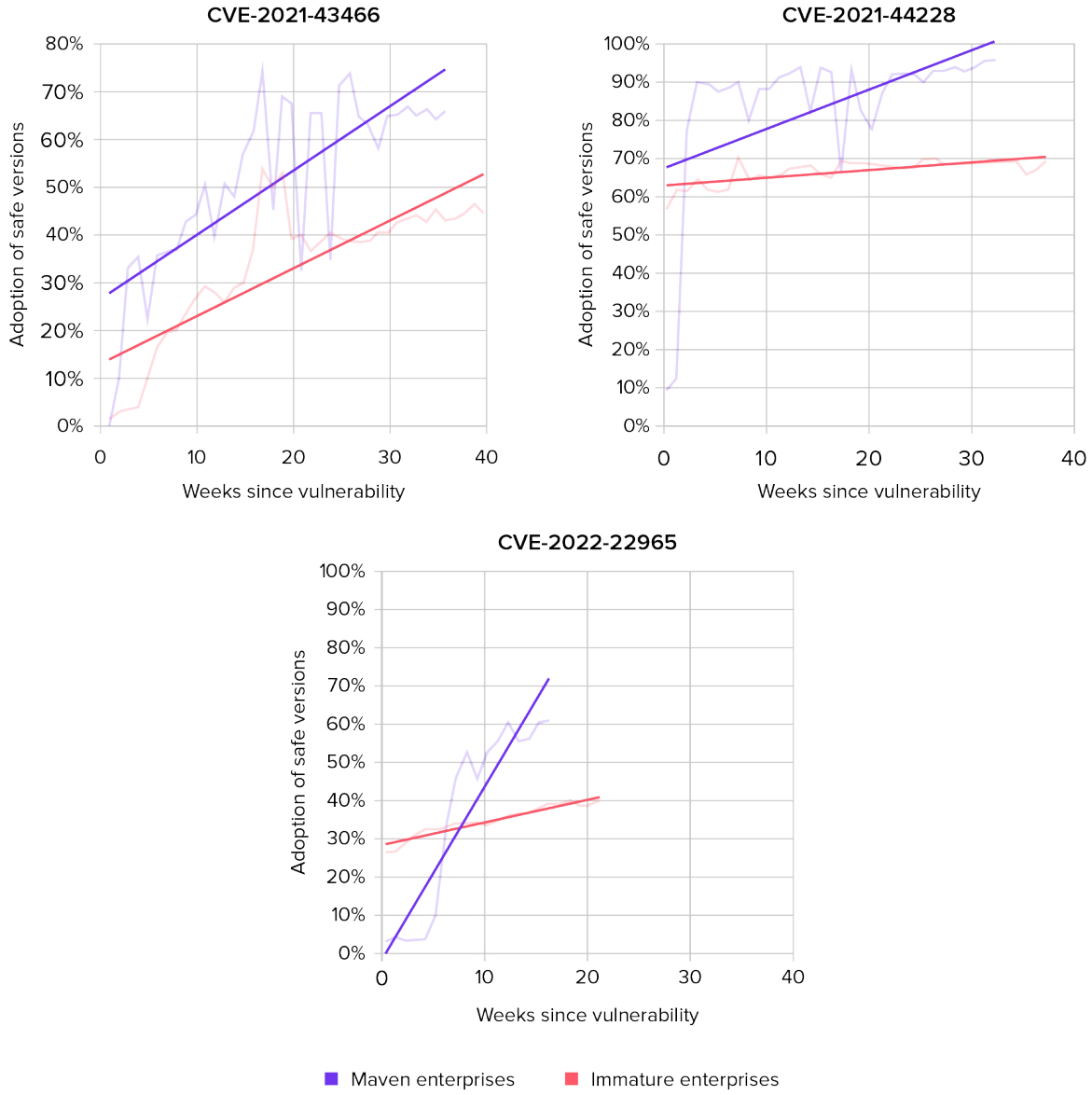
A medium-sized enterprise with 20 application development teams

would save 1,600 hours

and $240,000 per year

at a fully loaded cost of $150 per hour.

FIGURE 3.7 COMPARISION OF MATURE VS. IMMATURE CONSUMPTION BEHAVIOR OVER TIME



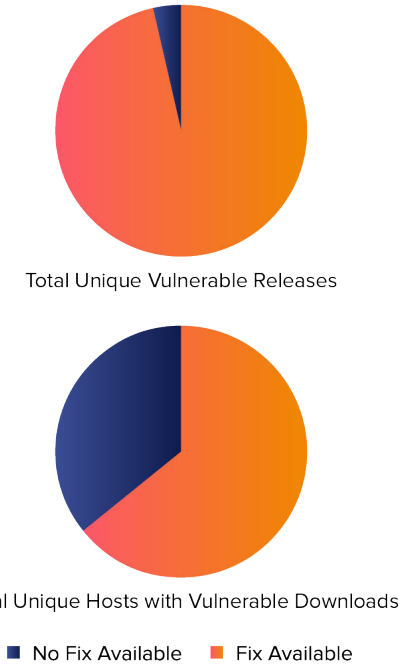
Source: Maven Central download statistics and a sampling of enterprise customers (Sonatype Nexus Lifecycle)

From the OpenSSF's Open Source Software Security Mobilization Plan to the establishment of community funds for maintainers, we continue to see most open source risk solutions focus heavily on maintainers. However, this one-pronged approach will only help solve part of the problem. *(Fig. 3.8)*

1.2 billion avoidable vulnerable components are being consumed each month.

In an analysis of vulnerable downloads, 96% of vulnerable downloaded releases had a fixed version available.

FIGURE 3.8. CONSUMER VS MAINTAINER OF VULNERABLE DOWNLOADS



Possible Explanations for Poor Component Choice

Popularity- When deciding which dependencies to use in a development project, popularity is often used as a proxy for quality (i.e., "everyone else is using it, so it must be safe, secure, and reliable"). Theoretically, this makes sense as, more popular projects should be getting fixed faster. But they aren't. As revealed in our 2019 State of the Software Supply Chain Report, the popularity of a dependency does not correlate with a faster median update time. Developers may feel safe in selecting more popular projects, but just because a dependency is popular, doesn't necessarily mean it's "better."

Automation- Though there are plenty of open source automation tools, very few have security capabilities built in. Similar to the Clarity issue above, this automation may mask potential vulnerable dependencies, enabling developers to unknowingly build upon projects with unknown vulnerabities.

Clarity- Oftentimes, developers aren't manually selecting individual versions when building software supply chaings & dash those dependencies are already part of a projects that's being used or built upon. As cited in the 2020 State of the Software Supply Chain Report, 80-90% of modern applications consist of open source software. If an SBOM and proper DevSecOps practices are not implemented, developers and software engineering teams may have no way of knowing that those vulnerable component are being used, pulled, or built upon.

Inactive Releases- There are almost 500,000 projects within Maven Central, but only ~74,000 projects are actively used. That means 85% of projects are sitting in this repository and taking up space, potentially overwhelming developers with available options.

In late 2021, a serious vulnerability surfaced in a widely-used open source logging framework–Log4j. The flaw impacted almost every Java-based software application from Minecraft to Tomcat.

The Log4j vulnerability is a strong example of rapid, effective response by project maintainers. *(Fig. 3.9)*

It was clear from the publicity surrounding the Log4j vulnerability that organizations can and will prioritize critical vulnerabilities. *(Fig. 3.10)*

Dependency Update Issues Arising During Log4j

Maintainer vs consumer

Although the maintainer quickly released an update, consumers were slow to react.

Sluggish updates

Despite the update process requiring little effort (the changes were non-breaking), shifting to the safe versions has not been universal, with successful Log4j attacks still happening.

Organizations can proiritize critical issues

How did the industry react to the high profile Log4j critical notice versus other, less publicized vulnerabilities

FIGURE 3.9 MAVEN CENTRAL DOWNLOADS OF VULNERABLE VS. SAFE VERSIONS OF LOG4J

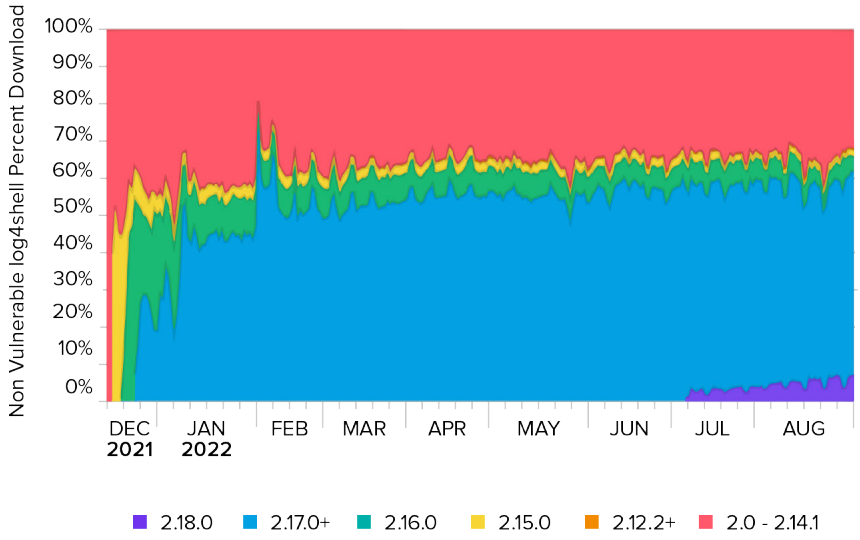
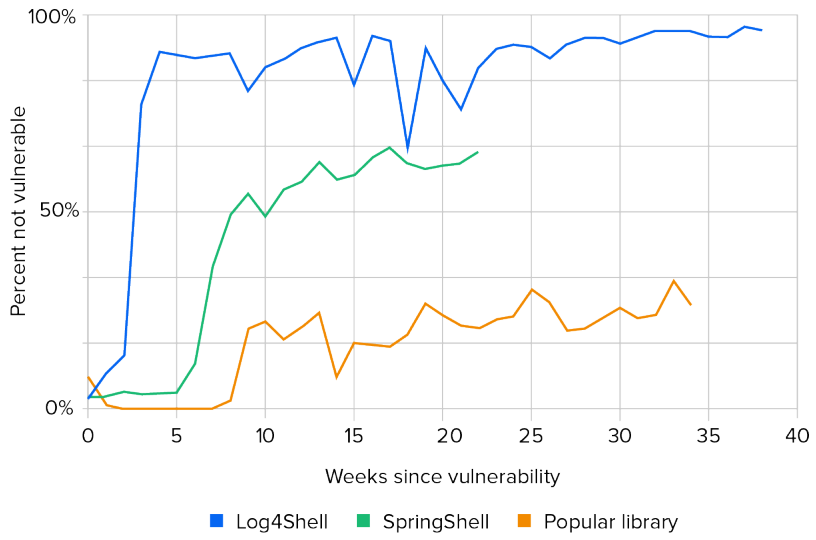


FIGURE 3.10 ENTERPRISE RESPONSE OVER TIME OF CRITICAL VULNERABILITIES BASED ON MEDIA COVERAGE



Section 4: Software Supply Chain Maturity

Survey results and peer insights from engineering professionals or software supply chain management.

This section discusses

- Sonatype's methadologies and objectives.
- The eight themes of SSCM practices.
- The five stages of SSCM maturity.
- How mature today's software supply chains are.

Sonatype had two objectives with this year's survey:

- Provide a benchmark and maturity model that facilitates how organizations can evaluate themselves in comparison to their peers.
- Examine whether certain reported software supply chain practices correlate with desirable results.

Eight Themes of Software Supply Chain Management Practices

Remediation
How do you implement fixes to address indentified OSS component risk?

Application inventory
Do you know all the applications your organization has in development/production, and who the stakeholders/owners are? Do you know the detial about them, including how they are build, and the Software Bill of Materials (SBOM) for the OSS components they include?

Build & release
Do you understand how your software "parts" and processes come together to build and release applications into production?

Policy control
What is your tolerance for risk? Do you have automated policy enforcement?

Project consumption
Do you govern OSS component selection?

Giving back
Do you contribute to the OSS community?

Supplier hygiene
Do you know if your OSS component comes from a trusted, quality supplier?

Digital transformation
What plans, resources, and trainig do you have to help institutionalized new processes and tools?

FIGURE 4.1 FIVE STAGES OF SOFTWARE SUPPLY CHAIN MANAGEMENT MATURITY

Less Mature

UNMANAGED

This first stage is referred to as the Unmanaged stage because organizations are often operating with an "anything goes" mindset, are often reactive, and have minimal process/oversight related to the themes.

EXPLORATION

A realization of some sort is usually the impetus for thrusting an organization into the Exploration stage. This is often triggered by an "event" that causes an "all hands on deck" reaction to uncover necessary information/solutions, or a champion of some sort leading an improvement effort. This stage is often focused on identifying the perceived problem/inefficiency, learning about current implementations, and starting to explore potential solutions.

AD HOC

In the midst of starting to define processes and implement tooling to improve the identified problem, Ad Hoc solutions reign as the teams work toward institutionalization and socialization of new tooling and processes.

CONTROL

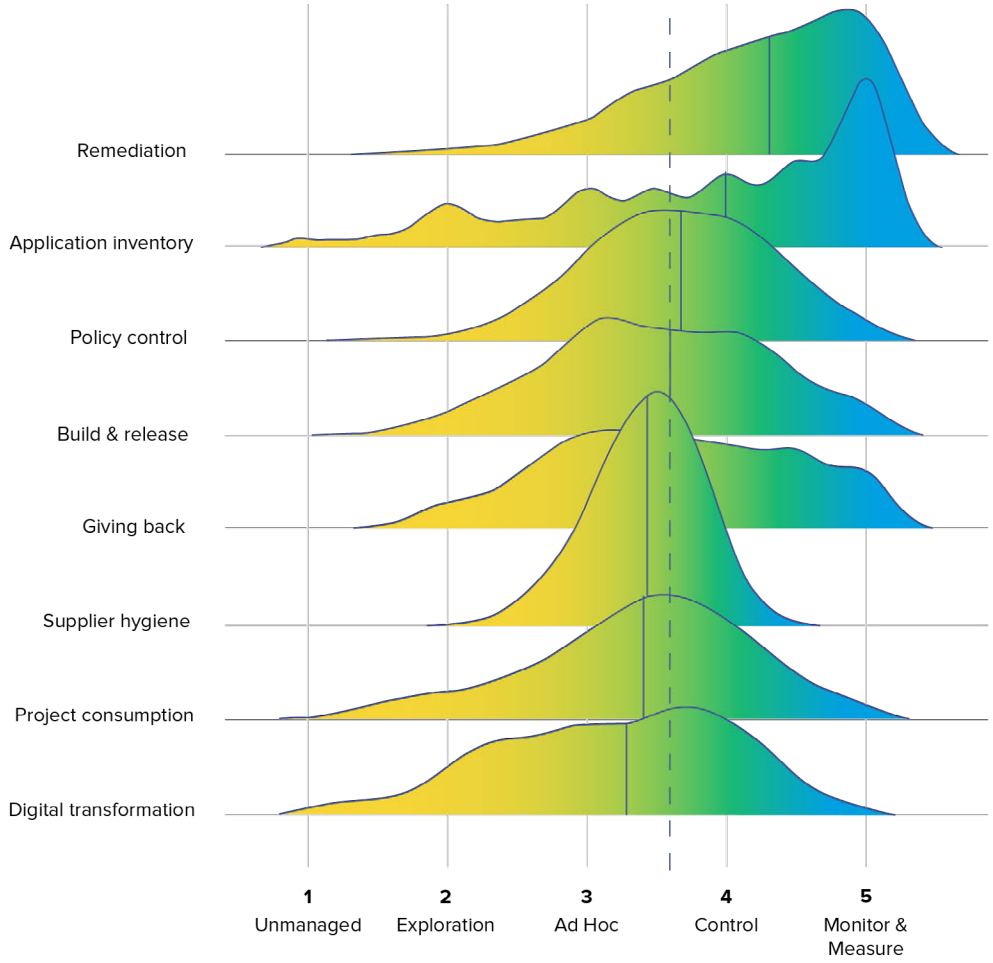
In the Control stage, ad hoc solutions give way to more formalized governance processes across the enterprise. Socialization and institutionalization of these processes and tools is ongoing, but for the most part, stakeholders are bought in to the need for improvement measures and are working towards compliance.

MONITOR MEASURE

The Monitor and Measure stage occurs once new processes and tools have been institutionalized, and organizations have reached a phase of being able to proactively address OSS component risk. In addition, a healthy amount of ROI is realized, and measurements to demonstrate success are available.

More Mature

FIGURE 4.2 SOFTWARE SUPPLY CHAIN MATURITY SCORE BY THEME



There is still room for improvement in terms of software supply chain maturity. *(Fig. 4.1)*

Across the various themes, we see that the majority of respondents were graded less than the "4 - Control" level of maturity. The "Control" level of maturity is when an organization transitions from "figuring it out" to a minimal level of maturity that will enable high-quality outcomes. *(Fig. 4.2)*

The data shows a clear disconnect between what security is actually happening and what people think is happening. This is especially prevalent among IT managers.

Compared to respondents working in information security, the IT managers are:

1.8 times more likely to strongly agree to

"We know the Software Bill of Materials (SBOM) for every application."

2.4 times more likely to strongly agree to

"We address to remediation of security issues as a regular part of development work (i.e., security issues treasted as normal defects)."

3.5 times more likely to respond with "Less than 1 day" to

"When our team becomes aware of a vulnerability in an open source software component that we use, how long does it take (estimated) to mitigate this vulnerability across our application(s)?"

In an ideal world, management's perception should align with information security's experiences.

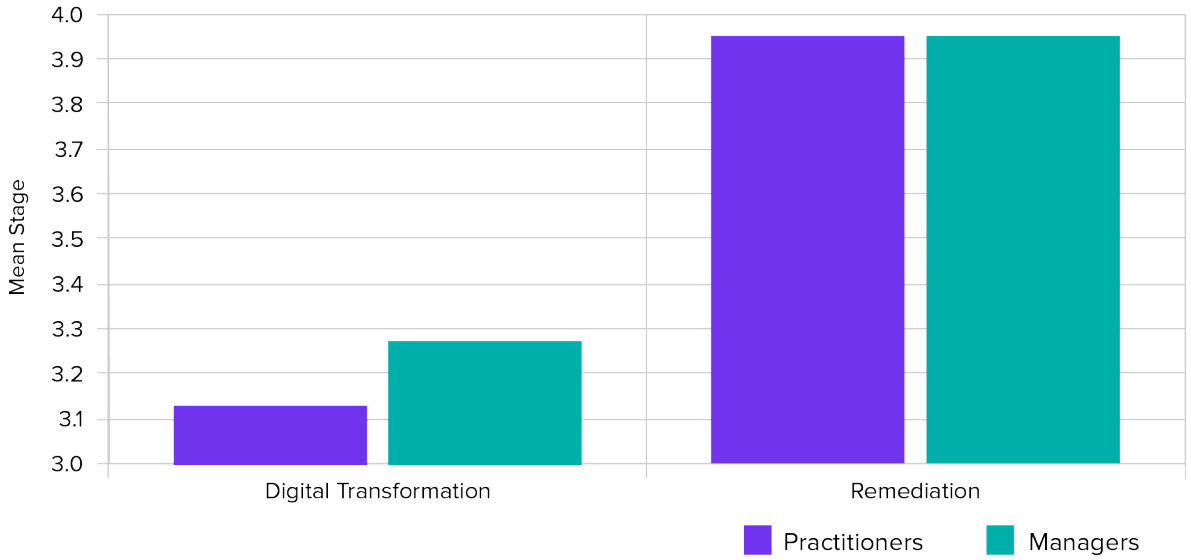
68% of respondents are confident that their applications are not using vulnerable libraries.

84% of respondents reported using security history as criteria in deciding to use an open source component. However, in a random scan of 55,000 enterprise applications from security-conscious organizations, 68% had known vulnerabilities in their OSS components.

Another interesting finding was the observed gap between Digital Transformation, the lowest self-scored maturity theme, and Remediation, the highest-scored maturity theme. *(Fig. 4.3)*

The higher the level of SSC maturity, the higher the reported employee satisfaction, and vice versa. *(Fig. 4.4)*

FIGURE 4.3 MEAN STAGE OF MATURY OF PRACTITIONERS VS MANAGERS



Individuals from organizations with higher level (control and above) were:

2.7 times more likely to
strongly agree to “I am satisfied with my job.”

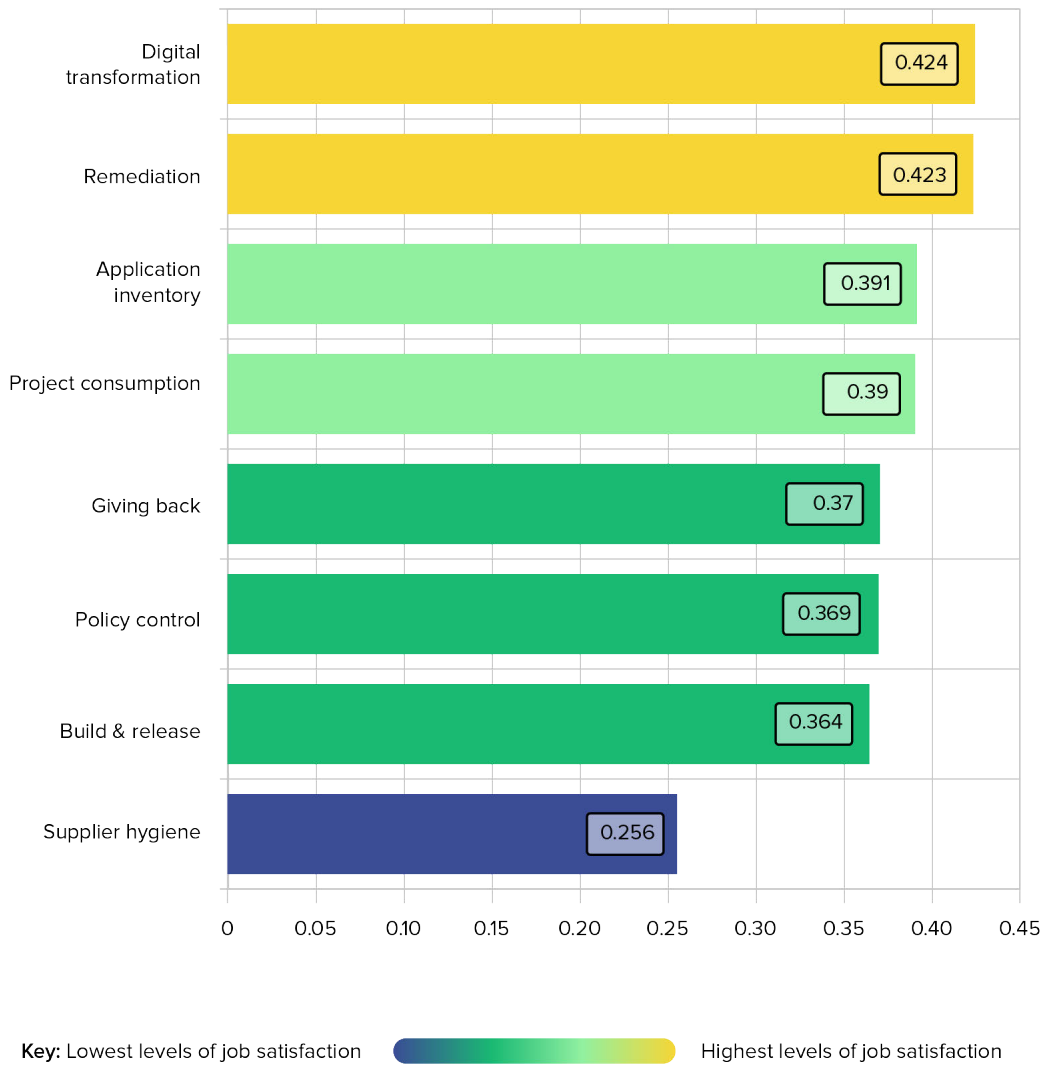
2.8 times more likely to
strongly agree to “My job makes good use of my skills and abilities.”

2 times more likely to
strongly agree to “I would recommend this organization as a good place to work.”

3.6 times more likely to
strongly agree to “I have the tools and resources to do my job well.”

Compared to individuals working at organizations with software supply chain practives at the Ad Hoc level and below.

FIGURE 4.4 JOB SATISFACTION CORRELATIONS WITH SOFTWARE SUPPLY CHAIN MATURITY



Section 5: Establishment and Expansion of Software Supply Chain Regulation and Standards

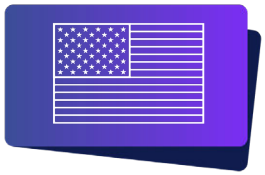
A global update on what's happened around software supply chain regulation and standards since the last report.

This section discusses

- What's happening in the United States, Canada, the UK, Germany and the EU.

The United States Presidential Executive Orders of February 2021 and May 2021 highlighted the growing sophistication and intensity of cyber threats and the necessity for supply chain integrity.

What's Happening in the United States?



January 2022

The Office of Management and Budget (OMB) issued the Memorandum: "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles."

- This set an end-of-2024 fiscal year deadline for agencies to meet specific cybersecurity standards and objectives in accordance with the Presidential Executive Orders of 2021.

Agencies already complete a Security Assessment Report (SAR) as part of the authorization process for information systems. The OMB wants to lean further into this application security testing. To help accomplish this, OMB advised agencies to follow the NIST July 2021 "Guidelines on Minimum Standards for Developer Verification of Software."

February 2022

As a follow up to the July minimum standards publication, the National Institute of Standards and Technology (NIST) released: "Software Supply Chain Security Guidance Under Executive Order 14028."

This document introduced the concepts of

- Attestation: a statement that requirements have been met.
- Artifact: a piece of evidence.

March 2022

The Securities and Exchange Commission (SEC) issued a proposed rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

> *"When a federal agency (purchaser) acquires software or a product containing software,* ***the agency should receive attestation from the software producer that the software's development complies with government-specified secure software development practices.*** *The federal agency might also request artifacts from the software producer that support its attestation of conformity with the secure software development practices."*
>
> *Software Supply Chain Security Guidance Under Executive Order (EO) 14028, NIST.*

- This could require public companies to make public disclosures to investors about cybersecurity incidents within days of the discovery.

April 2022

The Food and Drug Administration (FDA) sought comment on medical device cybersecurity in "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions."

- It recommended that "Cybersecurity Bill of Materials" be replaced with "Software Bill of Materials" on pre-market submissions.

Idaho National Laboratory, associated with the U.S. Department of Energy, continues the work it initiated in 2021 on an Energy sector SBOM Proof of Concept.

May 2022

NIST provided additional, comprehensive guidance in "Software Security in Supply Chains" related to the "acquisition, use, and maintenance of third-party software."

The guidance also offered recommended concepts and capabilities spanning

- Software Bill of Materials (SBOM)
- Vendor risk assessments
- Open source software controls
- Practices for vulnerability management

September 2022

The OMB issued another memorandum: "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices."

- This memo provides further direction on how to comply with the Order's demand that federal

systems and vendors utilize software that meets common cybersecurity standards.

Software vendors now need to vouch for the security of their product, and self-certify that their software has been developed in accordance with best security practices outlined in two documents published by the NIST:

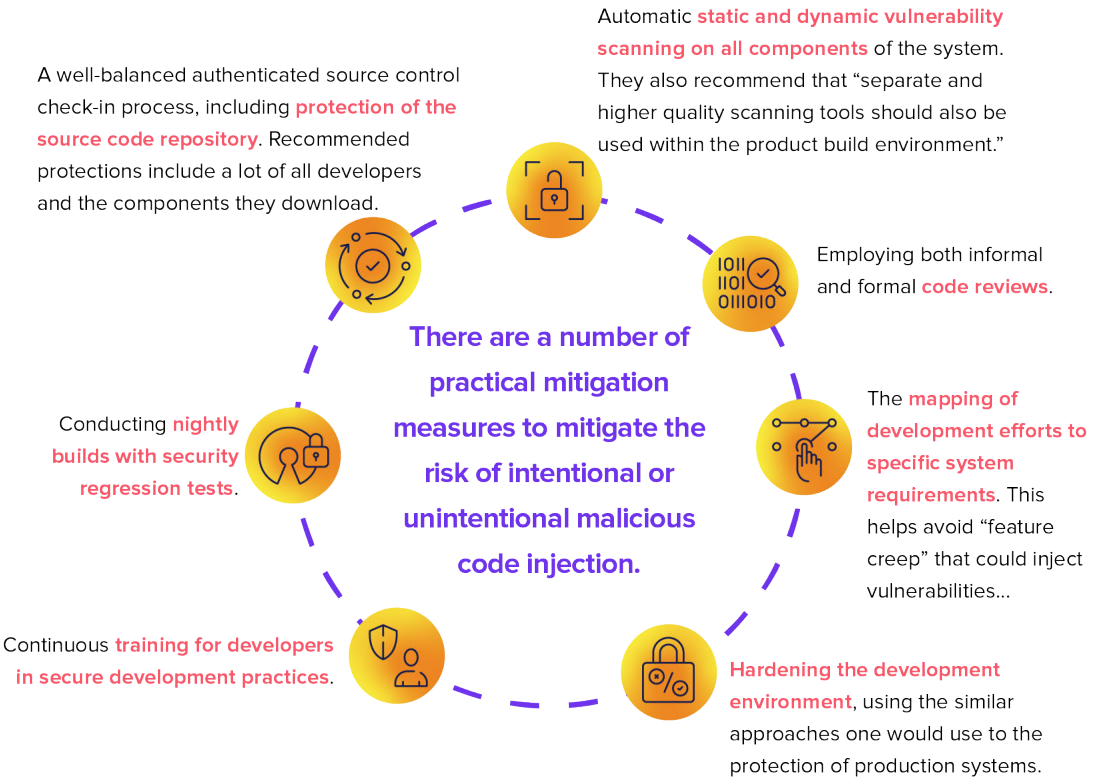
- "Secure Software Development Framework" (SSDF), published in February 2021
- "Software Supply Chain Security Guidance"

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI) released "Securing the Software Supply Chain: Recommended Practices Guide for Developers."

- It specifically highlighted the changing nature of threats and the outsized and pervasive impact of malicious code.

In 2018, the National Telecommunication and Information Administration (NTIA) began collaborating with other groups to promote software component transparency. This later became 2021's Elements for a Software Bill of Materials, as well as an online resource center for all things SBOM.

SBOMs are evolving. The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has continued to evolve and refine the concept of an SBOM.



June 2022

The Supply Chain Security Training Act of 2021 became law.

- This directs the Federal Acquisition Institute to develop a training program that "mitigate[s] supply chain security risks that arise throughout the acquisition lifecycle, including for the acquisition of information and communications technology.

August 2022

The Supreme Court Security Funding Act of 2022 passed.

- This specifically calls out software supply chain security practices.

Other bills that continue to move through the legislative process and focus on the supply chain as the key element in strengthening cybersecurity:

- DHS Software Supply Chain Risk
- Management Act of 2021

September 2022

The Securing Open Source Act of 2022 was introduced in the Senate, underscoring the

strategic importance of open source to the federal community.

- Indicated that CIOs "should enable, rather than inhibit, the secure usage of open source software at each covered agency."
- Imposed deadlines related to publishing a framework for assessing risk for software components and performing an assessment of open source software components "used directly or indirectly by Federal agencies."
- Directed engagement with private companies, nonprofit organizations, and individuals within the open source software community.

What's Happening in Canada?

June 2022

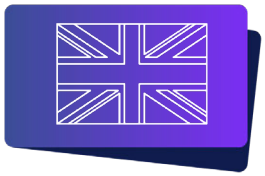
The Canadian government completed the first reading of Bill C-26, titled "An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts."

- The bill specifically pertains to telecommunication service providers. Still, it would require them to "manage any organizational cyber security risks, including risks associated with the designated operator's supply chain and its use of third-party products and services."

Data shows that software supply chain integrity is a concern across the broader Canadian business community.

In its "2022 Canadian Digital Trust Insights" survey, PwC reported that 54% of Canadian respondents expect a reportable increase in 2022 from attacks on the software supply chain. But only 44% say they thoroughly understand their third-party cyber and privacy risks.

What's Happening in the United Kingdom?



February 2022

The UK government unveiled its National Cyber Security Strategy 2022, specifically citing supply chain vulnerabilities as an area of concern.

- The strategy specifically tasks the Department for Digital, Culture, Media, and Sport (DCMS) with the implementation of Network and Information Systems (NIS) regulations in coordination with the National Cyber Security Centre (NCSC).

July 2022

The UK government issued a Proposal for Legislation to "Improve the UK's Cyber Resilience."

- The proposal specifically highlighted the outsized impact even small security risks in the supply chain can have on the wider economy.

In parallel, the DCMS issued its "Cyber Security Breaches 2022" survey.

- This asked UK businesses about cyber attack impact, response, and readiness for future challenges.

In This Survey:

31% of businesses

estimate a cyber attack happens **at least once a week.**

1 in 5 businesses

say they have experienced **a negative income** as a direct response to a cyber attack.

49% of businesses

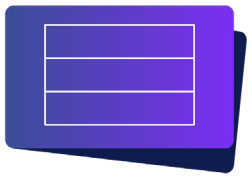
have action on at five of the National Cyber Security Cetner's 10 Steps to Cyber Security.

Only 7% of businesses have looked at their wider supply chain.

This is not specific to businesses in specific verticals. According to this survey, fewer than one in two firms in any sector are reviewing the potential security risks in their wider supply chain.

What these survey results suggest is that, while the risks are pressing and clearly identified, businesses are not yet taking action to remediate them.

What's Happening in Germany?



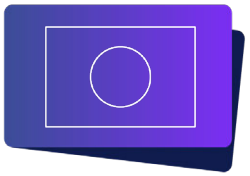
January 2022

In 2021, Germany issued the Information Security Act 2.0 (IT-SiG) and the Second Ordinance Amending the BSI Criticality Ordinance (BSI KritisV), the latter of which went into effect in January 2022.

- IT-SiG specifically states that manufacturers of critical components will be subject to certain obligations to safeguard the entire supply chain. This includes a requirement to proactively report vulnerabilities to customers and to eliminate said vulnerabilities.

Organizations identified to be of critical importance to the government and community are subject to these regulations. Penalties can go as high as several million Euros. These critical groups include a broad cross-section of government services and industries.

What's Happening in Japan?



May 2022

Japan passed "Act on Promotion of Economic Security by Integrated Implementation of Economic Measures," landmark national security legislation.

- The act has four main pillars. The first two focused on supply chain stability and security for critical infrastructure, and the latter was said to be modeled on the U.S. and German approaches. The law is expected to take effect on or before February 2023.

August 2022

The Open Source Security Summit came to Japan.

- The event served as a follow-up to May 2022's Open Source Software Security Summit II.

Following the Executive Orders of 2021, these industry groups, in association with the White House's National Security Council and prominent technology companies, have collaborated on a 10-Point Open Source and Software Supply Chain Security Mobilization Plan.

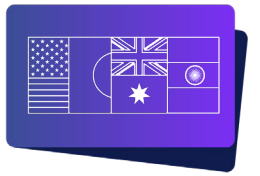
What's Happening in the European Union?

May 2022

The European Union joined with the United States government to launch the U.S.-European Union Trade and Technology Council.

European Parliament and European Union Member States reached an agreement on New Rules on Cybersecurity of Network and Information Systems, which advocates for a high common level of cybersecurity across the European Union. This is known as the NIS 2 Directive.

What's Happening in the Indo-Pacific Region?



May 2022

The Prime Ministers of Australia, India, Japan, and the President of the United States announced a collective approach to addressing cybersecurity issues.

The Quad's activities are coordinated under the banner of the Quad Cybersecurity Partnership. They have also collaborated on a "Common Statement of Principles on Critical Technology Supply Chains," which aligns around four key principles:

- Security
- Transparency
- Autonomy
- Integrity

What's Happening Globally?

January 2022

The NATO Cooperative Cyber Defence Centre of Excellence released a report titled: "Recent Cyber Events: Considerations for Military and National Security Decision Makers."

The report highlighted various types of supply chain compromises, including

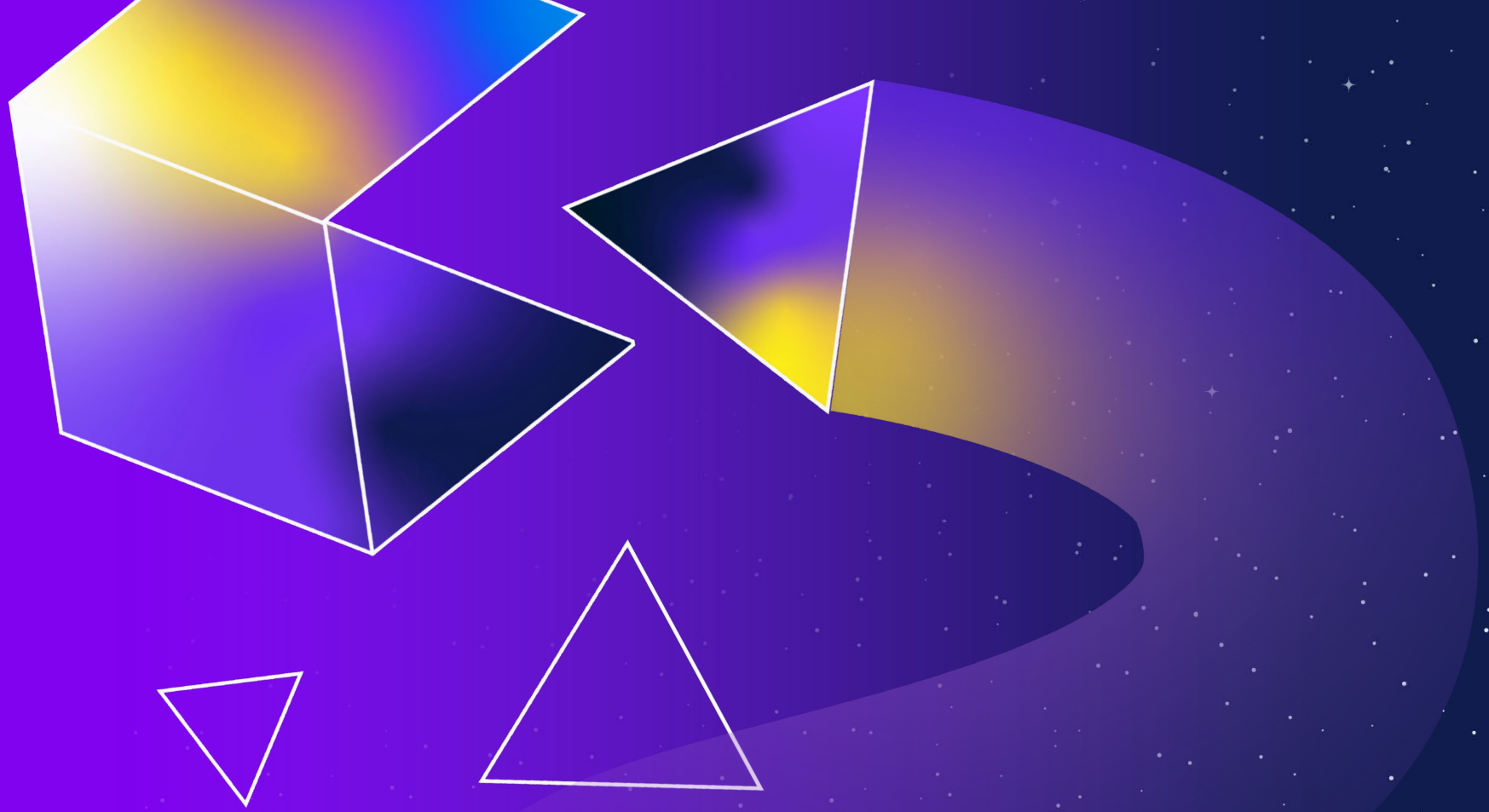
- The exploitation of software development tools.
- The role businesses and their developers play in protecting the supply chain.

Looking Ahead

The early 2020s demonstrated just how interdependent we are on one another and how supply chains are a byproduct of that. A bad actor and a bit of malicious code can cause a cascade of wreckage across the digital ecosystem, impacting governments, businesses, and consumers. We should expect compliance requirements, and timelines to become increasingly more prescriptive and concrete both within and beyond the government sector.

About the Analysis

The authors have taken great care to present statistically significant sample sizes with regard to component versions, downloads, vulnerability counts, and other data surfaced in this year's report. While Sonatype has direct access to primary data for Java, JavaScript, Python, .NET, and other component formats, we also reference third-party data sources as documented. Further, Sonatype's research analyzed scan data from 185,000 anonymized, validated applications.



sonatype

Sonatype is the software supply chain management company. We empower developers and security professionals with intelligent tools to innovate more securely at scale. Our platform addresses every element of an organization's entire software development life cycle, including third-party open source code, first-party source code, infrastructure as code, and containerized code. Sonatype identifies critical security vulnerabilities and code quality issues and reports results directly to developers when they can most effectively fix them. This helps organizations develop consistently high-quality, secure software which fully meets their business needs and those of their end-customers and partners. More than 2,000 organizations, including 70% of the Fortune 100, and 15 million software developers already rely on our tools and guidance to help them deliver and maintain exceptional and secure software. For more information, please visit **Sonatype.com**, or connect with us on **Facebook**, **Twitter**, or **LinkedIn**.

Headquarters
8161 Maple Lawn Blvd, Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place, Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com