Manage Open Source Threats. **Intelligently.**

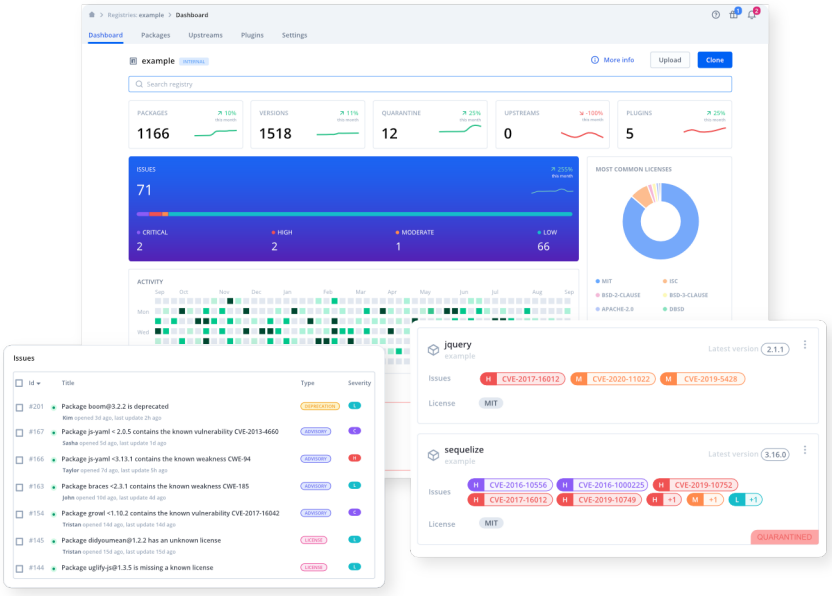
Open source components are essential in many applications and boost productivity. As reliance on external code grows, so do the potential security threats. Being unaware of the components used leave companies vulnerable to attacks.

Don’t wait - proactivity is key to avoiding these threats and the associated costs.

Bytesafe is a cloud-based security platform for enterprises that reduces risk and protects revenue - without slowing down developers.

The Open Source Challenges

- No way of blocking vulnerable dependencies
- Balancing security needs with productivity goals
- Constant inflow of new packages with insufficient control
- Keeping track of open source licenses
- Lack of a central source for dev teams and automated environments
- Detecting vulnerabilities and risks in the supply chain



Key Benefits of Bytesafe

- Brings visibility into open source usage
- Allows security teams to enforce open source usage policies
- Quarantines packages with critical vulnerabilities and non-compliant licenses
- Protects both developer and production environments
- Avoids 0-day attacks by filtering newly released packages
- Prevents Dependency Confusion attacks

INCREASE YOUR OPEN SOURCE SECURITY POSTURE WITH AUTOMATED BEST PRACTICES - WITH A UNIFIED WORKFLOW FOR SECURITY AND DEVELOPER TEAMS

BYTESAFE

https://bytesafe.dev
contact@bytesafe.dev

Intelligent Threat Management

100x
More malicious packages compared to 2020

$1.4 M
Average cost per cybersecurity incident

10 TB
Stolen data each month by ransomware

Vulnerabilities

Not knowing what open source code you depend on or including dependencies directly from public repositories exposes your organization to risks.

When a developer or CI/CD system installs a dependency it might already be too late.

Malware

Not applying centralized security policies can lead to unintentionally installing malware like crypto miners or password stealers.

Attackers are often targeting popular packages and therefore no external package should be trusted.

Compliance

When using open source in applications, ensuring compliance is an important task.

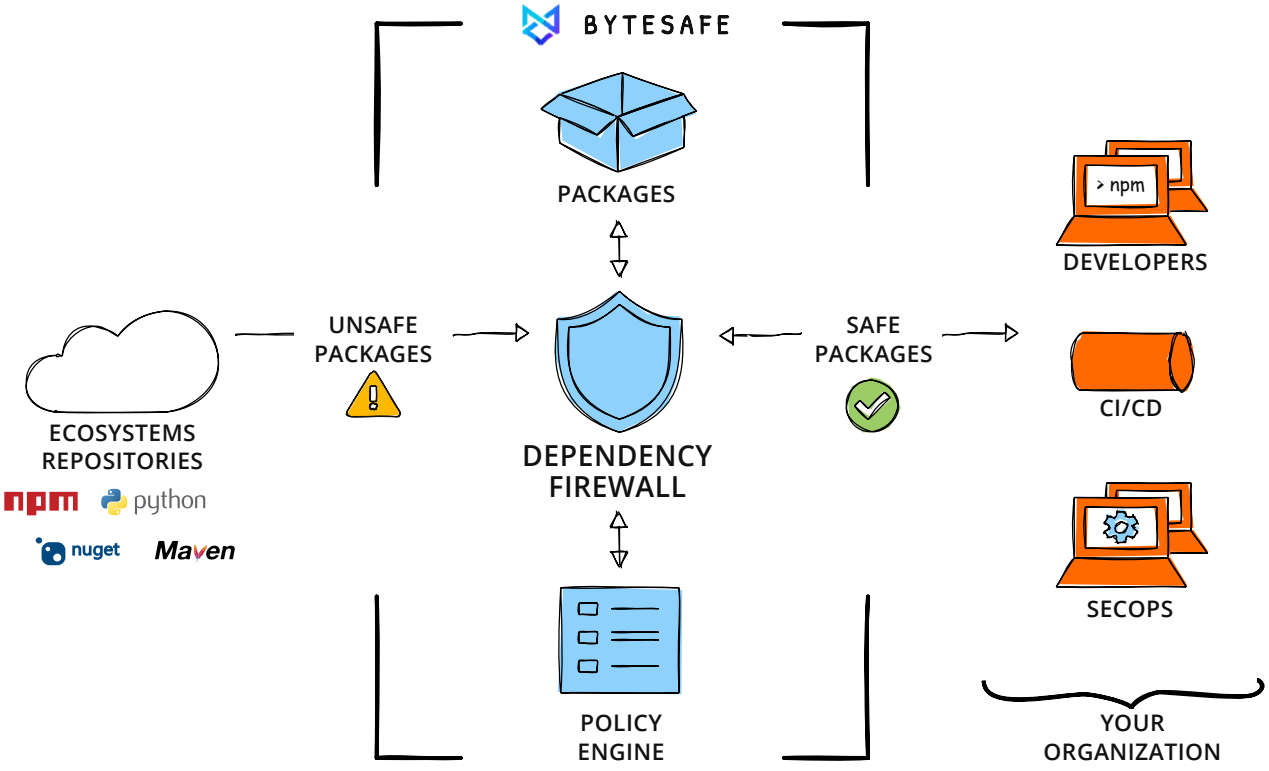
This includes avoiding breaching open source licenses, while keeping track of updates and changes in the external components used in your applications.

Dependency Confusion

Including dependencies directly from public repositories exposes your organization to risks.

When a developer or CI/CD system installs a dependency it might already be too late.

A Security Platform That Protects You From Open Source Software Supply Chain Attacks



Available in aws marketplace

BYTESAFE
https://bytesafe.dev
contact@bytesafe.dev

Intelligent Threat Management

Dependency Firewall

Block open source dependency threats

The Dependency Firewall quarantines malicious open source before reaching developers and infrastructure - protecting data, assets and company reputation.

Our policy engine evaluates threat signals such as known vulnerabilities, license information and customer defined rules.

Package Management

Secure source for your organization's packages

Control the dependencies used across your organization. Add both private and public packages to fully managed registries and gain a secure single source for your teams.

Analyze your dependencies and get insight into what packages are used where. Explore detailed information about your packages in an intuitive user interface.

Software Composition Analysis

Identify risk in your applications

Having insight into what Open Source components are used in applications is crucial to avoid exploitable vulnerabilities.

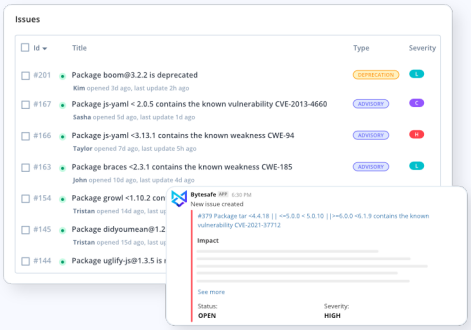
Software Composition Analysis (SCA) and Dashboard reporting give stakeholders a holistic overview with immediate insights into the current situation.

License Compliance

Continuous compliance and license inventory

Discover when new open source licenses are introduced in the codebase.

Automatically track license compliance issues and restrict problematic or unlicensed packages.



Maven npm GO Gradle python nuget yarn

Bytesafe integrates with your current tools

"EASY TO GET A GOOD OVERVIEW OF VULNERABILITIES IN PROJECTS! GREAT AND VERY FAST SUPPORT!"

- MARIA K, TECH LEAD

Swegon

4.5 / 5

Capterra
4.8 / 5

alternativeTo
5 / 5

Anton Aderum, CTO

bokadirekt.se

"We use Bytesafe in our CI/CD pipeline to keep our Javascript packages secure.

Setting up Bytesafe to use in combination with the regular public registries was super easy.

It helps us share our internal private packages securely and efficiently across all our development teams"

BYTESAFE

https://bytesafe.dev
contact@bytesafe.dev

Next steps

Learn more

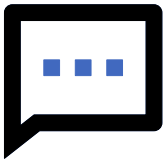
Learn more about software supply chain security and how to avoid being the weakest link by downloading our free e-book “Don’t be the weakest link”.

Download Ebook

Watch Webinar Now

Learn how Bytesafe helps allows you to increase your open source security posture with automated best practices - with a unified workflow for security and developer teams.

View on-demand



Talk to an Expert

Discuss your use needs or challenges with one of our solution experts to improve security in your software supply chain.

Let’s talk

Give it a try

Bytesafe your cloud-based security platform for enterprises that reduces risk and protects revenue - without slowing down developers.

Start your trial now.

Free trial

BYTESAFE
https://bytesafe.dev
contact@bytesafe.dev