ADDING SECURITY TO PRODUCTS AND PROCESSES

BYTESAFE

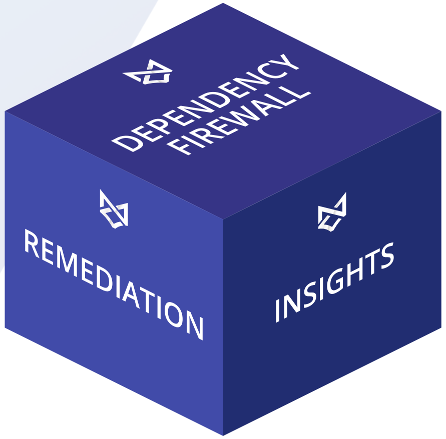
Prevent unwanted dependencies from getting in to your organization

Just like your company is using a firewall to control incoming and outgoing traffic from your business, you should invest in a dependency firewall that controls the 3rd party dependencies that your organization is using.

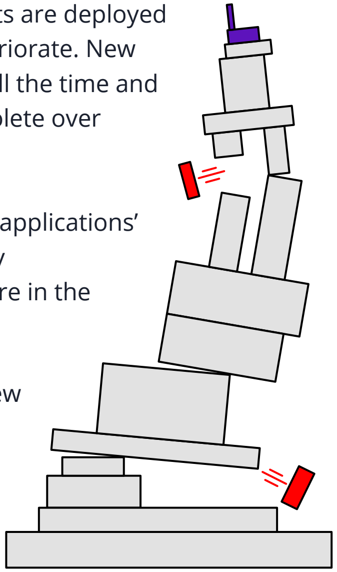
Without protection on a corporate level - individual developers and build systems are likely to install packages that have not been properly checked - including malicious ones.

By using a dependency firewall you will be able to:

- ☑ **Block unwanted packages** from entering your software supply chain. Shifting security from individual-level to a corporate-level.
- ☑ **Automatically enforce business rules.** Remove the dependency on individuals to uphold proper security.
- ☑ **Secure your workflows** to your current processes. Make sure that all developers and environments use the exact same versions as you intend.



Automate monitoring for vulnerable & malicious components



Once development projects are deployed - they slowly begin to deteriorate. New vulnerabilities are found all the time and components become obsolete over time.

Manually keeping track of applications' dependencies is practically impossible as they often are in the range "hundreds".

Automatically detecting new vulnerabilities in components is crucial and the only way to avoid harm to your business.

By automatically monitoring components to find problematic components you will be able to:

- ☑ **Be informed immediately** by getting notifications with remediation recommendations
- ☑ **Remediate issues early** to avoid unnecessary cost
- ☑ **Automatically quarantine components** that surpass security threshold levels

Keep components up to date - across all applications

Outdated and vulnerable components are listed in the top 10 risks according to the non-profit security organization OWASP.

Not knowing what components you're using or lack of an existing patch management process where you keep 3rd party dependencies up to date, you're likely to expose your organization to the risk of being attacked.

By keeping your components up to date you will be able to:

- ☑ **Avoid attackers from exploiting your systems** using existing vulnerabilities
- ☑ **Reduce dependency on external developers** by removing unused components

BYTESAFE

We are here to help!

Bytesafe is a dependency firewall that secures companies' software supply chains. The service prevents unwanted components from getting into the organization and automatically finds problematic components for you.

If you need any guidance or consultation you can email me at daniel@bytesafe.dev. We are here to help you.