npm, Inc.

1999 Harrison Street
Suite 1150
Oakland, CA 94612

1 510 907-3049
npmjs.com

npm Enterprise security features

npm, Inc. is the world's expert at shipping JavaScript quickly and safely. Everything from our security practices and encryption to the architecture of the Registry itself comes from years of experience securing the workflows of the world's largest JavaScript community. Our unique insights into the practices and preferences of over ten million JavaScript developers allowed us to design an Enterprise product that serves their security needs and those of the companies they work for.

Built on a solid foundation

Operated by the same team that runs the world's largest package registry

npm is the world's supplier of JavaScript. Serving over 1.1 billion downloads a day to over 10 million JavaScript developers, the npm team knows how to scale and operate the Registry while keeping millions of users secure.

Secured by the npm Security team

In 2018, npm acquired **^Lift Security**, founders of the Node Security Project—the world's largest database of known JavaScript vulnerabilities. npm has used this core expertise to establish npm Security, a dedicated team that looks out for the safety of npm users, products, and services.

Physical security

npm's infrastructure runs inside data centers designed and operated by Amazon Web Services and Google Cloud, offering state-of-the-art controls against fire, power loss, and unauthorized access.

npm's offices in Oakland, CA, are protected with physical access controls, video surveillance, and 24×7 security guards.

Security is built into everything we do

Architecture

To isolate customers' installations, npm Enterprise is built using modern containerization and orchestrated using Kubernetes. Each npm Enterprise instance is a single-tenant cluster that runs within its own project, to provide isolated access controls and dedicated storage.

Data security

Encryption

npm ensures that customer's data remains their data by encrypting it in transit and at rest. Data in transit is protected using HTTPS, while private package data is stored in Google Cloud Storage. Other private data is stored on disk on Google Kubernetes Engine. Both provide industry best practices for encryption of data at rest.

Integrity

npm ensures that data requested from and sent to npm Enterprise arrives at its destination unaltered. Packages are verified using the SHA-512 secure hash algorithm.

DDoS mitigation

npm services are protected by CloudFlare to mitigate DDoS attacks, including those that target UDP and ICMP protocols, SYN/ACK, DNS and NTP amplification, and Layer 7 attacks.

Employee access

npm's policy is that employees are given access to only the resources needed to do their job. New employees are introduced to security policies during the onboarding process and as policies are updated.

npm policies are reviewed periodically as part of standard operating practices to ensure they are continually up to industry standards.

Verified security practices

npm conducts internal code reviews, design reviews, threat modeling, and internal assessments of security controls and practices on an as-needed basis. If a vulnerability is discovered during an assessment, a documented response process ensures rapid mitigation.

npm works with external security vendors for external validation of security practices using penetration testing.

Coordinated disclosure

npm works closely with the JavaScript development community and security researchers to improve the security of the npm Registry and the 825,000 packages it contains. Each package page has a *report a vulnerability* button to make reporting security flaws in packages easy.

For other issues, npm has a dedicated security point of contact, security@npmjs.com, that can be used to communicate with the npm security team if a vulnerability is discovered.