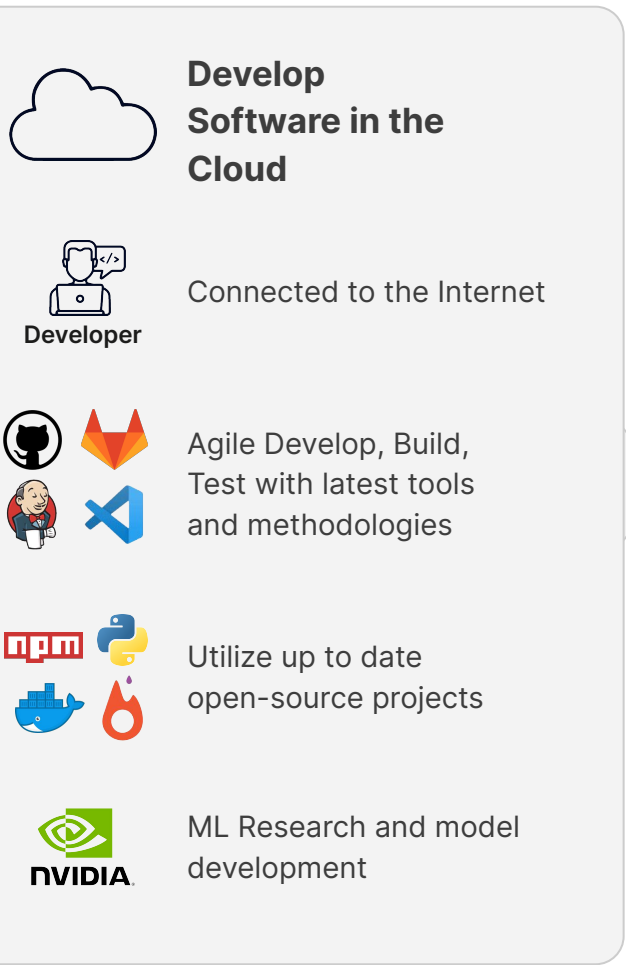
How highly secured organizations can utilize the public cloud for the safe development of software

A USE CASE OF USING SCRIBE TRUST HUB

ABSTRACT

Highly secured organizations use air-gapped networks to protect their sensitive data and systems from cyberattacks. While developing software in air-gapped networks can be inefficient and expensive, it is necessary for organizations that require the highest levels of security. Cloud-based development environments offer a more efficient and cost-effective option for less secure environments. Developing software in the cloud offers benefits for developers, such as access to cutting-edge tools and technologies, developer tools as a service, and machine learning resources.

Scribe's solution helps organizations develop in the public cloud by preventing tampering with digital assets, authenticating and authorizing developers, and filtering out dependencies for reputable open-source components. It also collects, manages, and signs evidence from the development lifecycle in the cloud environment, which is verified in the air-gapped network by a Scribe gateway to ensure the integrity of the code and adherence to secure software development policies. With Scribe, organizations can efficiently develop and deploy software while adhering to strict security policies in air-gapped environments.



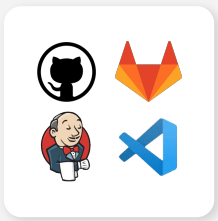
DEVELOP SOFTWARE IN THE CLOUD

Developing software in an air-gapped network is challenging and time-consuming due to limited access to external resources, external tools, and limiting developers' work to specific physical sites. The lack of access to open-source code libraries, online forums like Stack Overflow, and tools such as GitHub's Copilot hinders the development process. Additionally, transferring code and updates to the isolated network from external open-source code repos is difficult, expensive, and results in the usage of out-of-date dependencies. Limited computing power and storage, further hamper the development process. Furthermore, setting up and maintaining on-prem development environments in air-gapped networks costs more than using SaaS. Finally, developers have fewer options to collaborate and share code with team members.

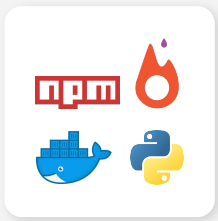
Organizations that can operate in less secure cloud-based development environments benefit from a more efficient and cost-effective way to develop software. Developers benefit from the latest advances in open-source projects and online development tools and take advantage of cutting-edge technologies. Tools as a service mean developers can focus on writing code instead of managing infrastructure. In some cases, developers can also work remotely. Finally, cloud providers offer machine learning resources that developers can leverage to build and train models. These resources can be expensive to run on-premise, making the cloud a cost-effective option.

Develop Software in the Cloud

Connected to the Internet



Agile Develop, Build, Test with latest tools and methodologies



Utilize up to date open-source projects

ML Research and model development

To adopt the development of software in the public cloud, highly secured organizations address the following risks with adequate security controls.

Securely use in classified networks/OT

Prevent tampering with digital assets (sign, review code)

Authenticate & Authorize developers

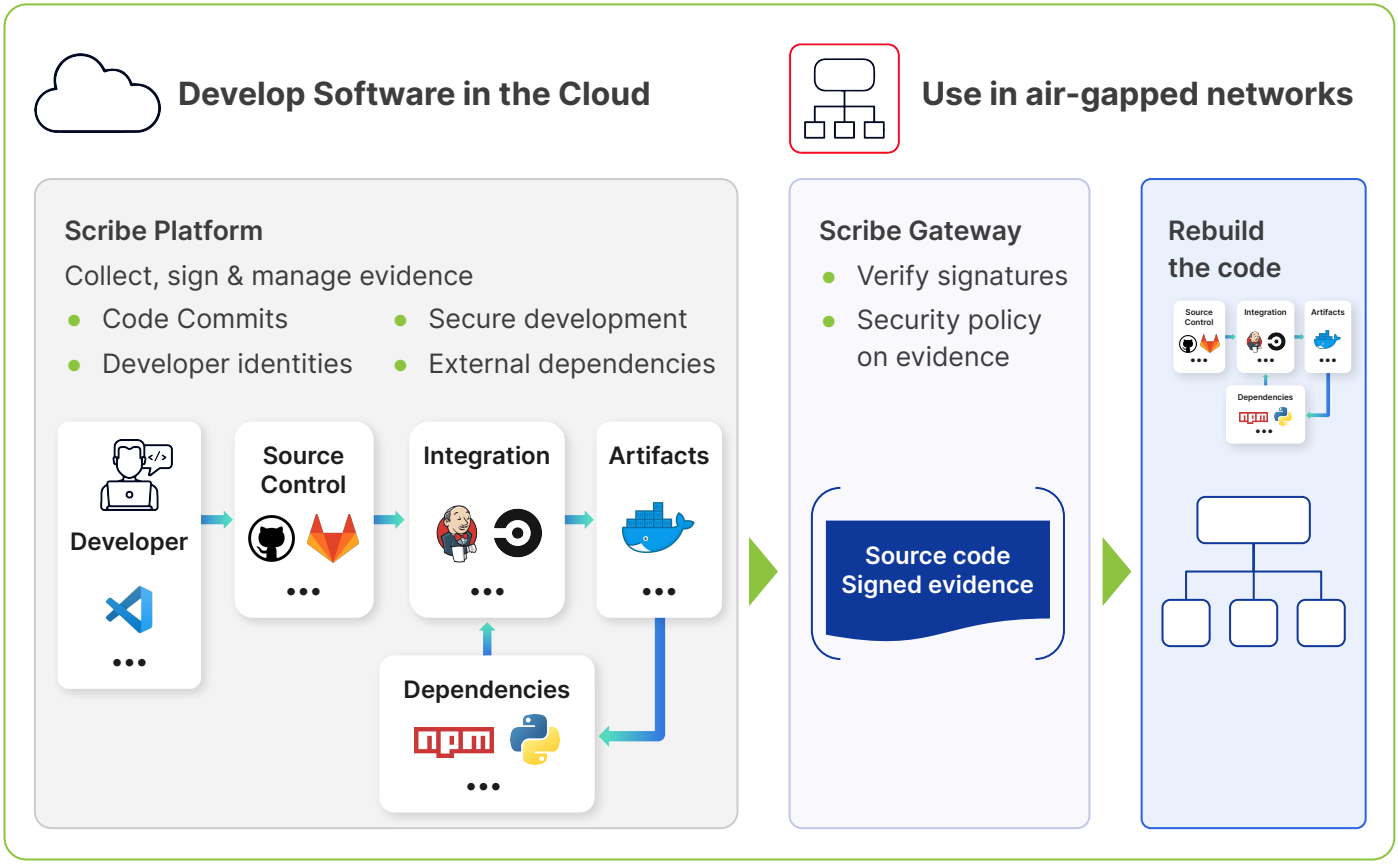
Filter reputable open-source

Risk Scenario	Mitigating Controls
External attacker Tamper with code and data	• Validate a strong environment security posture (esp. 2FA) • Code signing • Authenticate and authorize developers • Enforce code reviews by trusted peers
Internal attacker Tamper with code and data	• Authenticate and authorize developers • Code signing • Enforce code reviews by additional pairs of eyes
Dependencies Insecure open-source components	• Filter for reputable resources • Verify provenance of components • Enforce automated security testing

Scribe is a cloud-based platform that offers to bridge this gap by enabling organizations in developing in the cloud and incorporating the necessary measures to safeguard digital assets, validate and authorize developers, and filter credible open-source components.

The concept is that organizations can perform complete coding, building, and testing cycles within the cloud environment. After a cycle is completed, the source code and attestations about its trustworthiness are transferred to the air-gapped network. A Scribe gateway then examines the code's integrity and applies a security policy to the attestation's secure development process evidence collected as part of the attestation.

Finally, The organization rebuilds the software from the trusted code in the air-gapped network and deploys it. While this approach is only suitable for sensitive, but not classified code, it is applicable to many software projects.



Scribe provides continuous attestation of the code development process's security and reliability by gathering, managing, and signing with PKI or GPG proof for each code version.

The evidence includes

- Code Commits including file listings and hash values
- Code reviews performed
- Developer identities involved
- Open-source dependencies
- Source Control Manager (such as GitHub) security configuration
- Automated security scans

On the air-gapped side, a Scribe gateway verifies the integrity of the code by verifying the signatures and applies a security policy to the attestation of the development process. This is parallel to a bleaching or CDR function commonly used for entering data into such networks. Example verifications include:

- Allow only signed code and signed artifacts
- Allow specific roles to sign specific artifacts
- Deny unsafe dependencies
- Mandate 2FA & branch protection
- Deny commits by unauthorized users

Overall, Scribe's approach provides a secure and efficient way for organizations to develop and deploy software while adhering to strict security policies in air-gapped environments.