Securing your end-to-end supply chain

In this article

Introducing best practice guides on complete end-to-end supply chain security including personal accounts, code, and build processes.

What is the end-to-end supply chain?

At its core, end-to-end software supply chain security is about making sure the code you distribute hasn't been tampered with. Previously, attackers focused on targeting dependencies you use, for example libraries and frameworks. Attackers have now expanded their focus to include targeting user accounts and build processes, and so those systems must be defended as well.

For information about features in GitHub that can help you secure dependencies, see "About supply chain security."

About these guides

This series of guides explains how to think about securing your end-to-end supply chain: personal account, code, and build processes. Each guide explains the risk to that area, and introduces the GitHub features that can help you address that risk.

Everyone's needs are different, so each guide starts with the highest impact change, and continues from there with additional improvements you should consider. You should feel free to skip around and focus on improvements you think will have the biggest benefit. The goal isn't to do everything at once but to continuously improve security in your systems over time.

- "Best practices for securing accounts"
- "Best practices for securing code in your supply chain"
- "Best practices for securing your build system"

Further reading

- Safeguarding artifact integrity across any software supply chain
- Microsoft Supply Chain Integrity Model
- Software Supply Chain Security Paper - CNCF Security Technical Advisory Group