



# Security By Design

- *JPMorgan*
- *Security By design*
- *Supply Chain Vendor & Cyber Security*
- *Secure Software Development Life Cycle*

Aprile 2025

Il colosso bancario [#JPMorgan](#) Chase ha invitato i fornitori di software come servizio a migliorare le pratiche di sicurezza informatica in una lettera aperta, accusandoli di "favorire silenziosamente i cybercriminali«.

Le aziende non hanno altra scelta che affidarsi al [#SaaS](#), "spesso l'unico formato in cui oggi viene distribuito il software", ha scritto [Pat Opet](#) , Chief Information Security Officer [#CISO](#) di JP Morgan.

"Ci troviamo in un momento critico. I fornitori devono urgentemente ridefinire le priorità della sicurezza, ponendola al pari o addirittura al di sopra del lancio di nuovi prodotti"

è un approccio che considera la sicurezza un elemento fondamentale e integrato nell'architettura di un sistema informatico fin dalle prime fasi di sviluppo, invece di considerarla come un'aggiunta o una correzione successiva.

Questo significa che la sicurezza non è solo un'opzione, ma un requisito cruciale che deve essere preso in considerazione durante la progettazione, lo sviluppo e l'implementazione di software e hardware

Le certificazioni possono essere:

- vendor-specific, ovvero focalizzate su prodotti di un determinato fornitore (vendor)
- altre, invece, sono vendor-neutral e coprono principi generali della sicurezza informatica

Il Secure Software Development Life Cycle (Secure SDLC) è un approccio che integra la sicurezza in ogni fase del ciclo di vita di sviluppo del software, invece di trattarla come un'aggiunta postuma.

Ciò significa che i requisiti di sicurezza vengono raccolti insieme ai requisiti funzionali, la progettazione tiene conto dei rischi di sicurezza, e i test di sicurezza vengono eseguiti parallelamente allo sviluppo.