

 GitHub Enterprise

# Introduction to GitHub



April 2021

# Every company is becoming a software company

62% of CEOs have an initiative to make their businesses more digital



**DevOps alone is not enough...**

**Open source is  
changing how  
software is  
developed.**

Changing software development

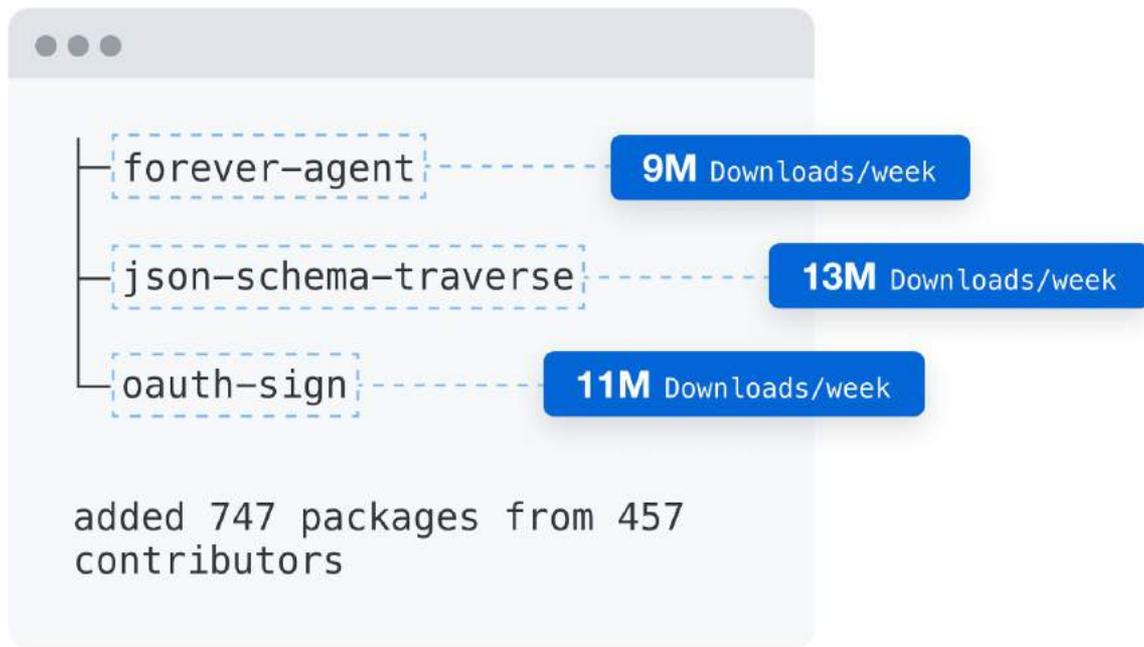
**96%**

Deployed applications  
using open source software

**50%**

Usage of open source  
software in codebases

# 80-90% of new applications are built on open source.



Security and compliance

# An existential challenge

Using open source introduces new challenges, including security and compliance risks.

**Check your repos... Crypto-coin-stealing code sneaks into fairly popular NPM lib (2m downloads per week)**

Node.js package tried to plunder Bitcoin wallets

By [Thomas Claburn](#) in [San Francisco](#) 26 Nov 2018 at 20:58 49  [SHARE](#) ▼

SECURITY UPDATE —

**Dear readers, please change your Ars account passwords ASAP**

Recovery from the critical Heartbleed crypto bug enters the password reset phase.

[DAN GOODIN](#) - 4/8/2014, 5:49 PM

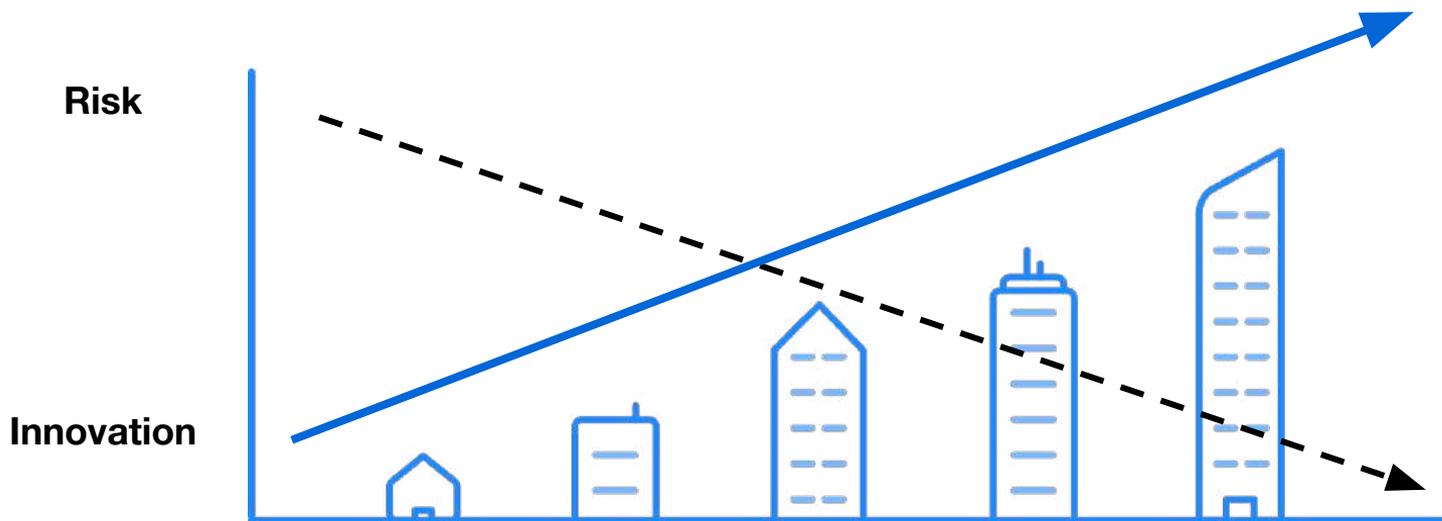
TECH • EQUIFAX

**Thousands of Companies Are Still Downloading the Vulnerability That Wrecked Equifax**

By [ROBERT HACKETT](#) May 7, 2018

# Maximize innovation while minimizing risk

As custodians of the world's largest software community, GitHub's solution allows you to maximize innovative potential and minimize associated risks.



# GitHub is the #1 platform for Digital Transformation

**56M+**

Developers

**100M+**

Private and public  
repositories

**1,000s**

Top open source  
communities

**1B+**

Contributions  
per year

**2M+**

Organizations

**50%**

Fortune 500  
companies



kubernetes



GraphQL



Apache



ANSIBLE



TensorFlow

The most innovative companies

The most innovative software

# GitHub is a critical partner for Digital Transformation



**DevOps**



**Security**



**Collaboration**

# GitHub enables a fully integrated code-to-cloud DevOps platform



# GitHub Packages

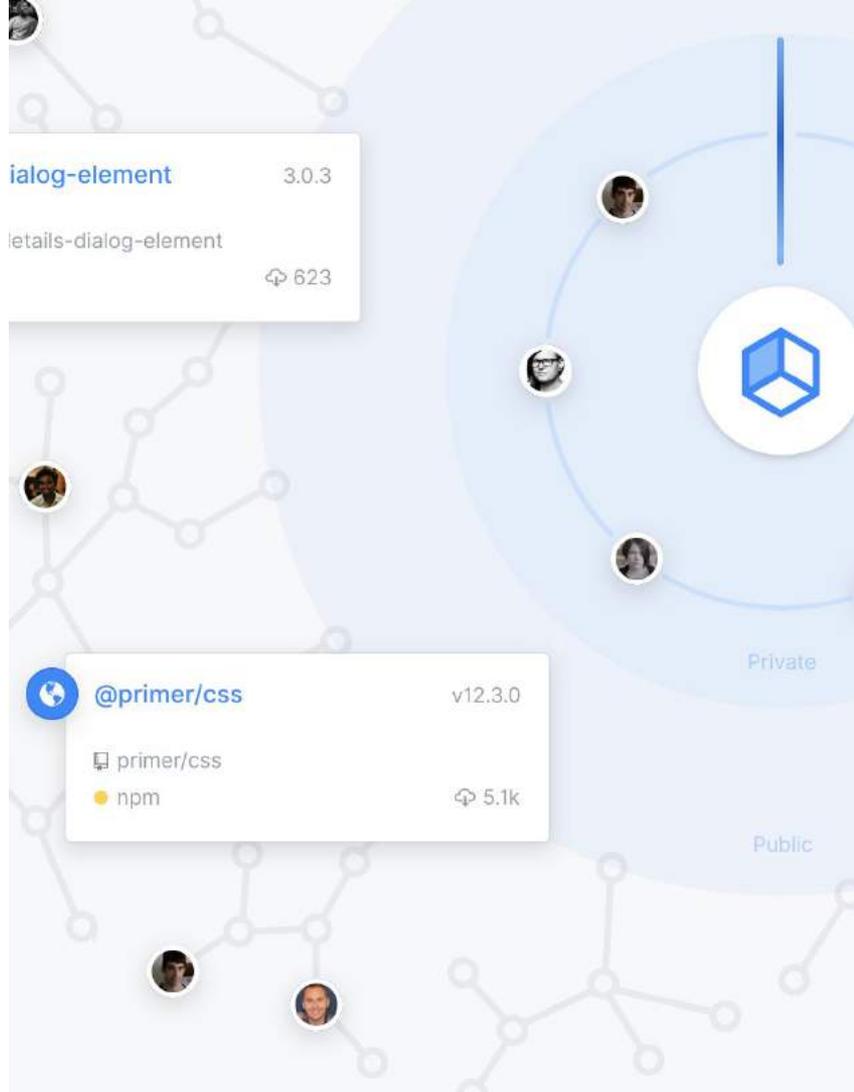
## Publish private and public packages, next to your code

Plan	Storage	Data Transfer out within Actions	Data transfer out outside Actions
Free	500MB	Unlimited	1GB / month
Pro	500MB	Unlimited	5GB / month
Team	2GB	Unlimited	10GB / month
Enterprise	50GB	Unlimited	100GB / month

Additional storage: \$0.25 / GB

Additional data transfer out (outside of Actions): \$0.50 / GB

**FREE** for public repositories



# GitHub Actions

## Community-led innovation for automated workflows

- 1150+ actions from the community
- Now with self-hosted runners and dependency caching

 <b>Assignee to reviewer</b> Automatically create review requests based on assignees 40 stars	 <b>Automatic Revert</b> Automatically revert a commit on '/revert' comment 15 stars
 <b>ClearlyNoticed Action</b> Maintain a NOTICE file based on your package-lock.json 6 stars	 <b>ESLint checks</b> Lint your code with eslint in parallel to your builds 93 stars
 <b>GraphQL query</b> An action that acts a client for GitHub's GraphQL API 18 stars	 <b>Hugo Actions</b> Commands to help with building Hugo based sites 15 stars
 <b>Jekyll Action</b> A GitHub Action to build and publish Jekyll sites to GitHub Pages 38 stars	 <b>Jest Snapshots</b> GitHub action that shows Jest Snapshots in the GitHub interface 18 stars
 <b>Node App Helper Actions</b> Provides some helper scripts to aid in basic Node.js app delivery 6 stars	 <b>Publish to Rubygems</b> Build and publish your gem to Rubygems 11 stars
 <b>Python Style Checker</b> Run PyCodeStyle on your Python 13 stars	 <b>Py Lambda Deploy</b> Deploy python code to AWS Lambda with dependencies in a separate layer 6 stars
 <b>Rubocop checks</b> Lint your Ruby code in parallel to your builds 28 stars	 <b>Release Notifier Action</b> Notifies developers on release with release notes via e-mail 48 stars
 <b>Run ESLint</b> Run ESLint on javascript files 22 stars	 <b>Run Jest</b> Use the Jest test runner CLI 37 stars
 <b>Snyk CLI Action</b> Run the Snyk CLI 14 stars	 <b>Actions for Discord</b> Outputs a message to Discord 26 stars

# Collaborate with open source and innersource





**Interconnected community**

# Tap into the biggest open source community in the world and accelerate your innovation



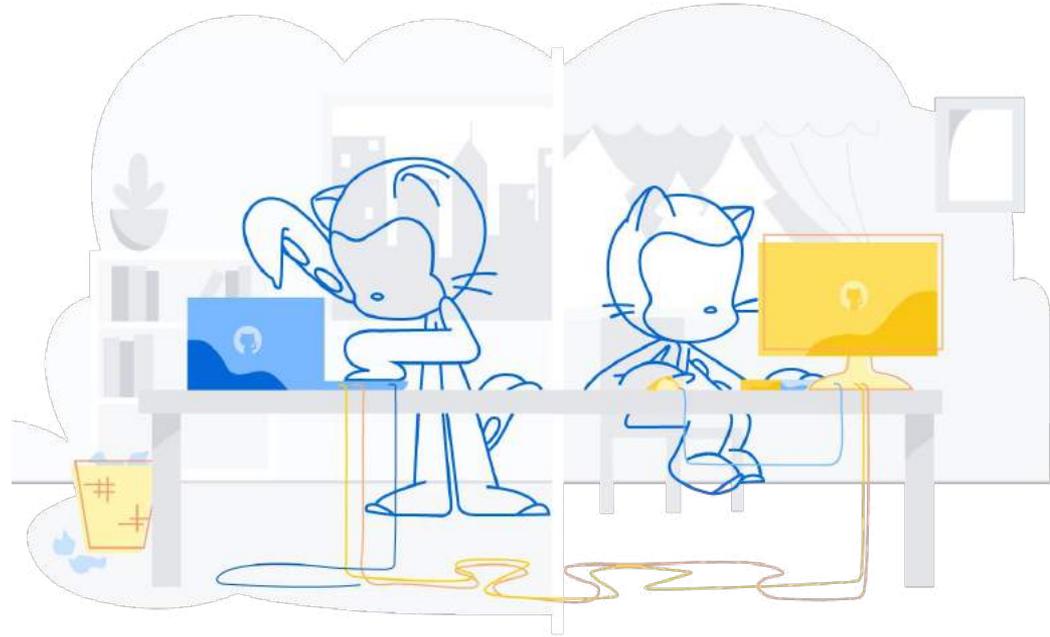
50+ million developers



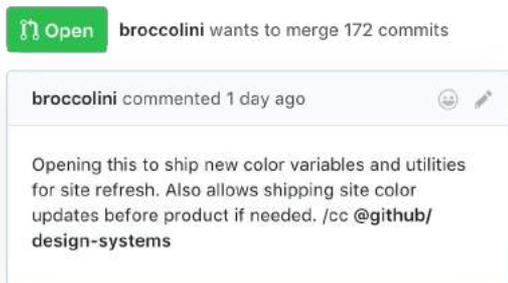
1000s of top OS communities



1+ billion contributors

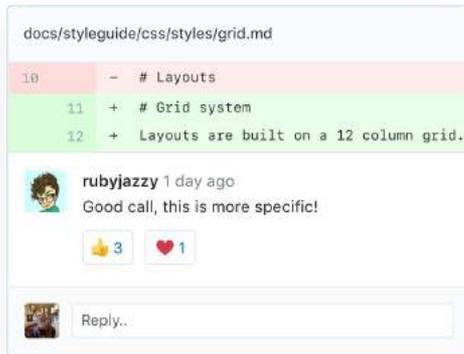


# Innersource



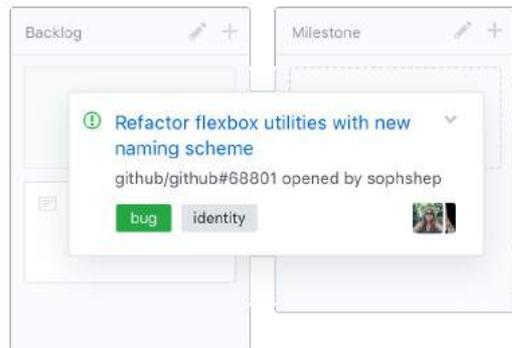
## Pull requests

Submit a change, invite collaborators, and start a conversation. Get more input from your team to expand ideas.



## Code reviews

Review line-by-line comments, suggest changes, and leverage integrations or robots to improve quality and speed.

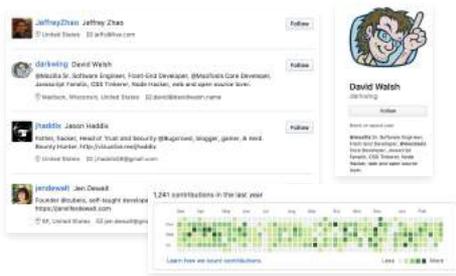


## Issues

Introduce discussion, create organizational knowledge, and a historical record and of ideas tried.



# Innersource



## Connect your Enterprise to GitHub with **Connect V2**

Connect your developers to GitHub's community with private forks of public projects, enterprise search, and hybrid build scenarios.



## Find experts to work with you with **Profiles and Experts**

Find the experts with the skills your team needs.



## Automate your SDLC with **Actions**

Customize your software development lifecycle (SDLC) with code hosted on GitHub's Cloud.

# Winning together



**90% reduction in merge times**  
Rewrote Nationwide Financial  
6-months ahead of schedule and  
40% below budget



**Faster, cheaper & better**  
We want you to consume OS  
because it's better, but we want you  
to contribute to the community



**Jet Propulsion Laboratory**  
California Institute of Technology

**Greater collaboration**  
Code reuse was greater than 90%.  
Collaboration increased 20-fold.



Deutsche Börse Group

**GitHub enabled transparency**



**4x increase in performance**

**SONY**

**30% increase in productivity**



## **Giving employees greater tools to affect positive culture change**

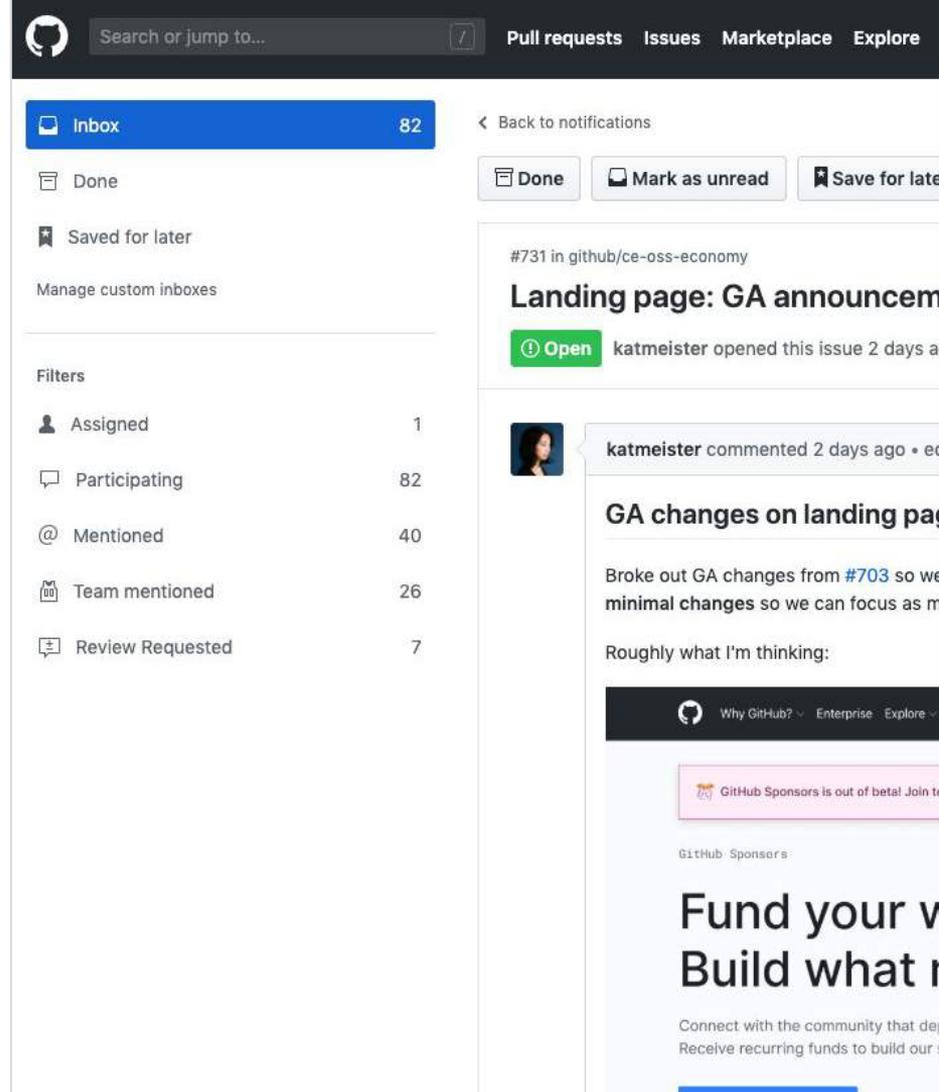
IBM teams using GitHub Enterprise to provide internal documentation - for engineering design, operations and support activities - have experienced 80% fewer escalation calls from first-line.

# Notifications

## Easier filtering, triaging, and response

- Email inbox-like interface
- Filter by team mentions, direct mentions and code reviews
- Sort and separate with custom categories

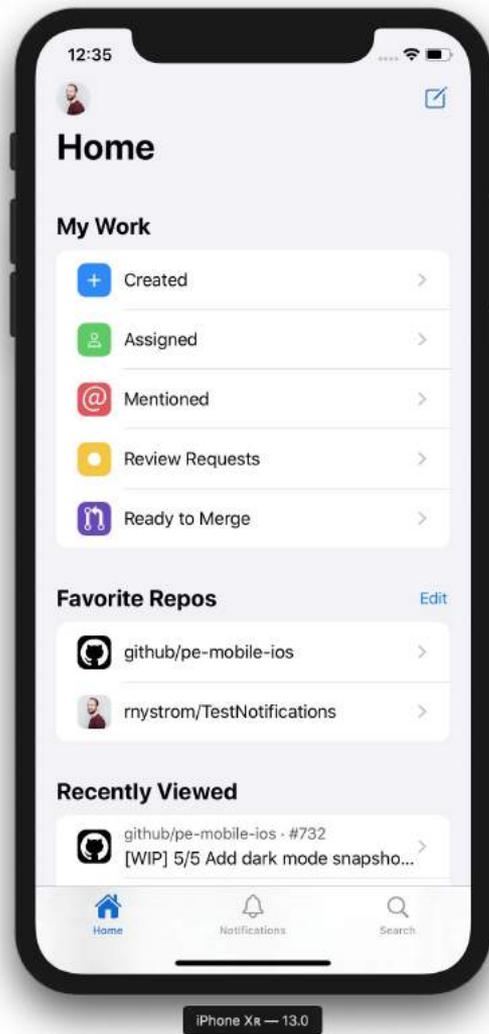
\*Must be in GitHub for mobile beta for access



# GitHub for mobile

## Collaboration anywhere

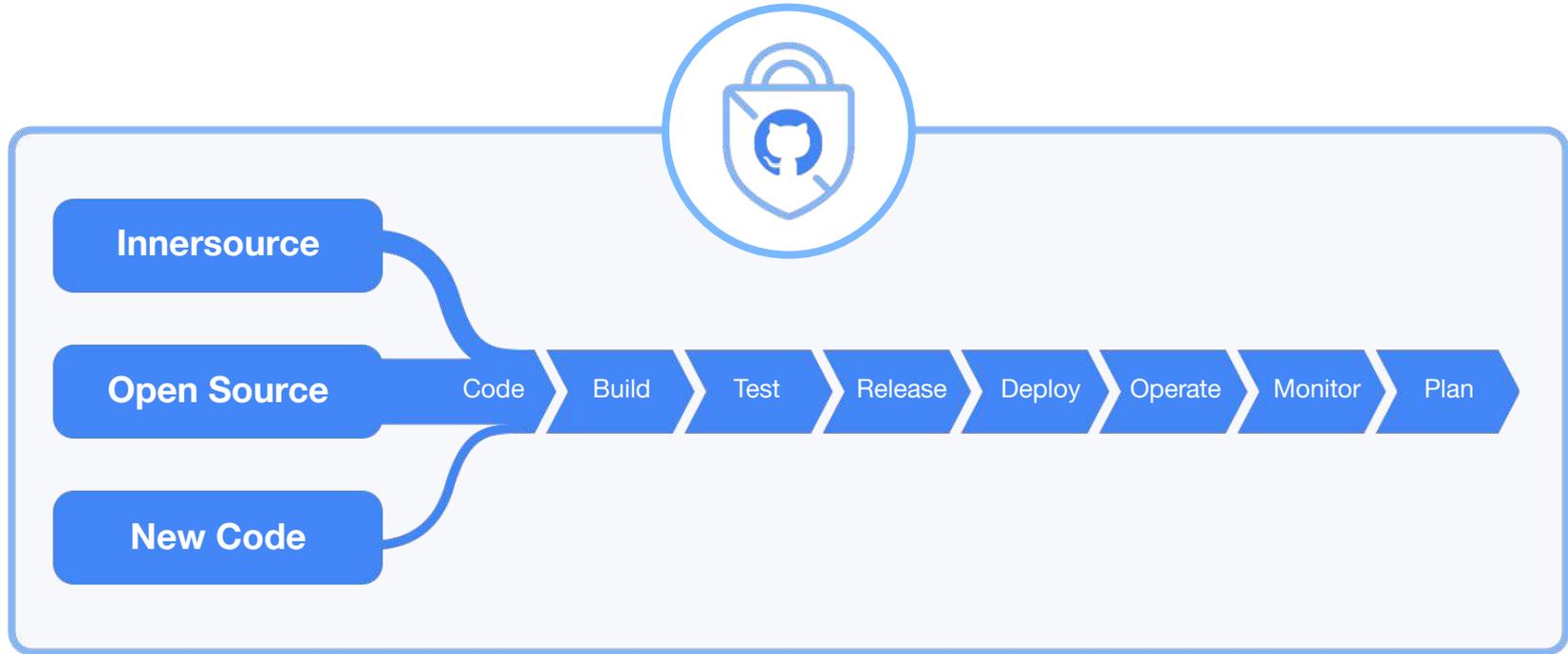
- Beautifully native: works on every phone size or iPad, with dark mode, and more
- Manage, triage, and clear incoming notifications
- Collaborate on issues and pull requests
- Available on iOS
  - Android coming soon



# Securing the Software Supply Chain



# GitHub secures the SDLC from open source maintainer to enterprise developer



Security

# GitHub secures the SDLC from open source maintainer to enterprise developer



Automated security fixes



Dependency graph analysis



Maintainer security advisories



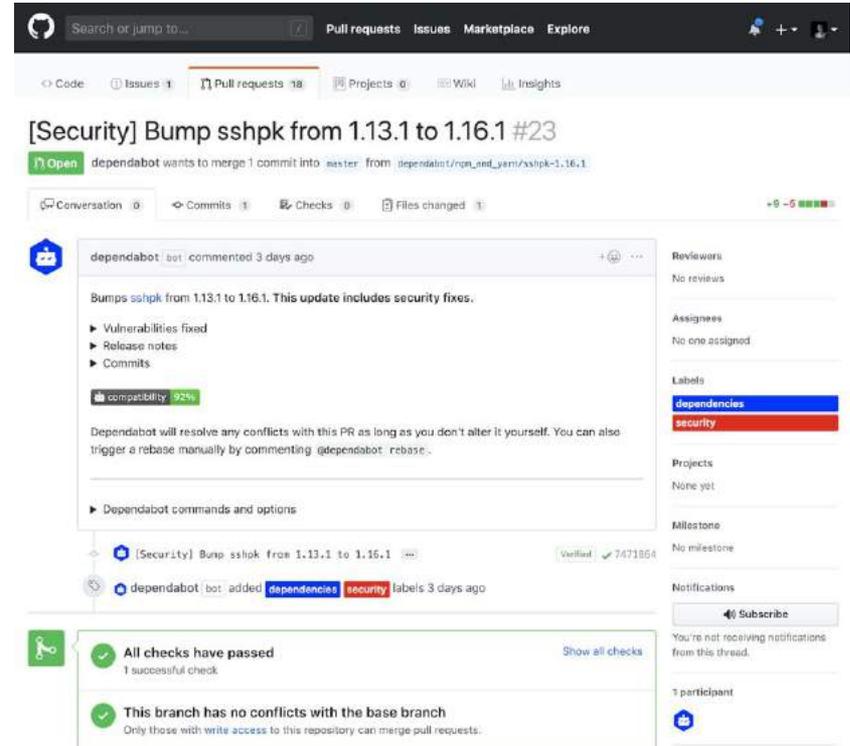
Code & Token scanning



# Automated Security Fixes

## Keep your code secure and up-to-date

- Remediation patches -> pull-requests
- Confidence Score on merge
- Planet scale “update” workflows



The screenshot shows a GitHub pull request interface. At the top, the title is "[Security] Bump sshpk from 1.13.1 to 1.16.1 #23". Below the title, it says "dependabot wants to merge 1 commit into master from dependabot/ron\_and\_jam/sshpk-1.16.1". The pull request is open, and the status bar shows "9 -5" with a green progress indicator. The main content area shows a comment from dependabot bot, dated 3 days ago, which reads: "Bumps sshpk from 1.13.1 to 1.16.1. This update includes security fixes." Below this, there are expandable sections for "Vulnerabilities fixed", "Release notes", and "Commits". A "compatibility" badge shows "92%". Below the comment, there is a "Verified" badge and a checkmark with the number "7471854". The pull request is labeled with "dependencies" and "security". The right sidebar shows "Reviews" (No reviews), "Assignees" (No one assigned), "Labels" (dependencies, security), "Projects" (None yet), "Milestone" (No milestone), and "Notifications" (Subscribe). At the bottom, there are two green checkmarks: "All checks have passed" (1 successful check) and "This branch has no conflicts with the base branch" (Only those with write access to this repository can merge pull requests).

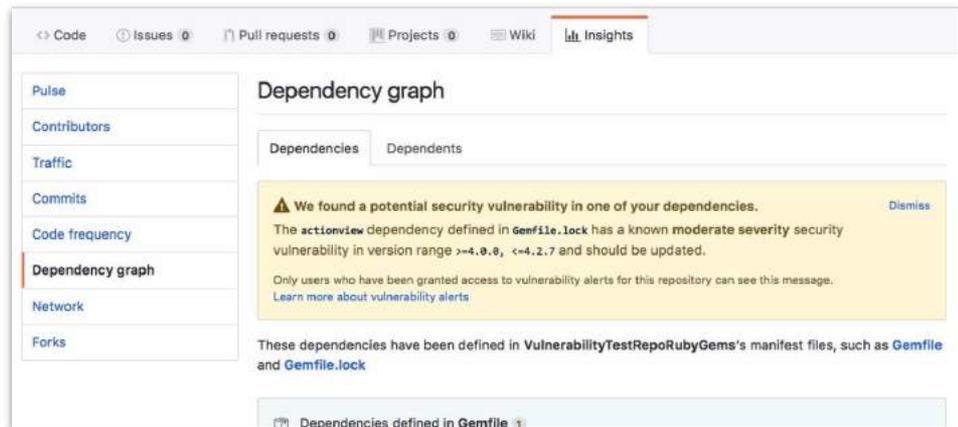
# Security vulnerability alerts + WhiteSource

Track your dependencies on open source components

Notifications of vulnerabilities in dependencies—fix before you ship

WhiteSource data - partnership broadens coverage and provides additional remediation recommendations

JavaScript, Ruby, Python, Java, .NET



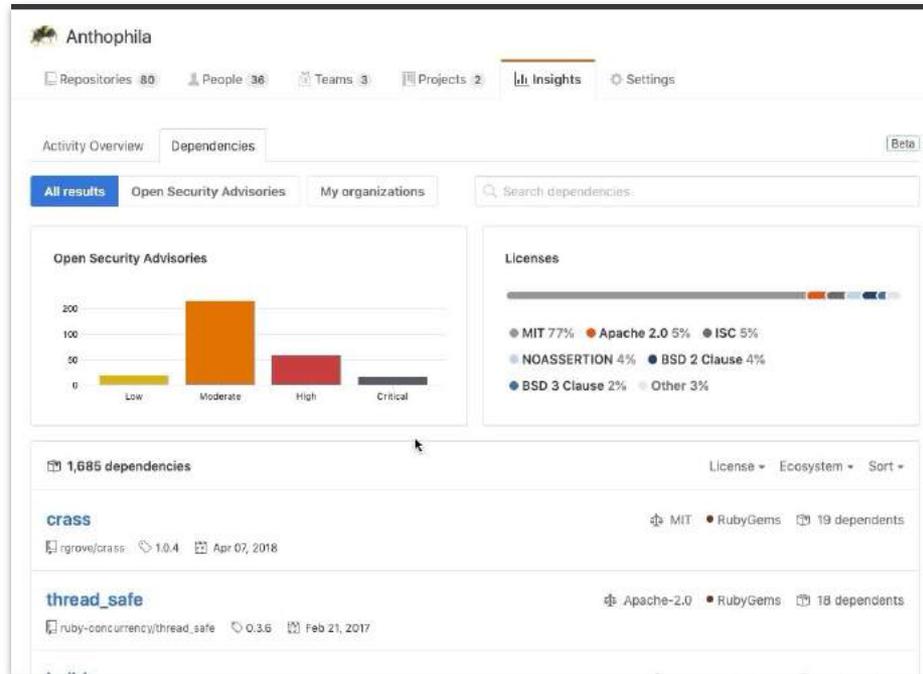
The screenshot shows the 'Insights' tab of a GitHub repository. The 'Dependency graph' section is active, displaying a warning for a security vulnerability in the 'actonview' dependency. The alert text reads: 'We found a potential security vulnerability in one of your dependencies. The actonview dependency defined in Gemfile.lock has a known moderate severity security vulnerability in version range >=4.0.0, <=4.2.7 and should be updated.' Below the alert, it notes that the dependencies are defined in 'VulnerabilityTestRepoRubyGems's manifest files, such as Gemfile and Gemfile.lock'. A 'Dismiss' link is visible in the top right of the alert box.

# Dependency insights

Understand open source dependencies and how they impact your business.

Drill-down to discover which dependencies have **security advisories** or risky **licenses** (e.g. GPLv3)

- Identify the repositories
- Take corrective actions



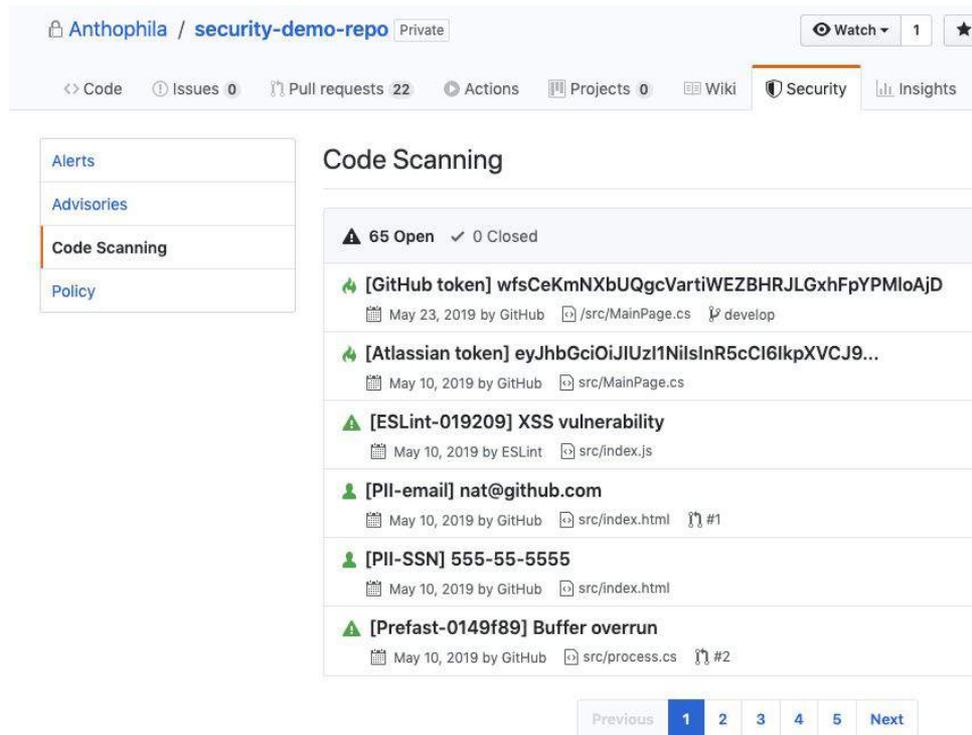
# Code Scanning Platform

## Platform and best-in-class tools for

- Scanning and analyzing code
- Searching for vulnerabilities
- Finding and remediating credentials and secrets

## Actionable, integrated into developer workflows

## Ecosystem and community-powered

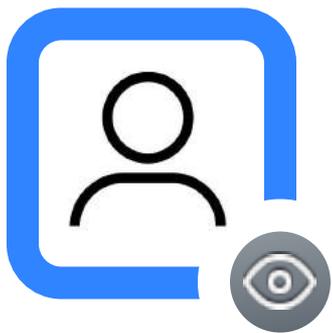


The screenshot shows the GitHub interface for a repository named 'Anthophila / security-demo-repo'. The 'Code Scanning' tab is active, displaying a list of detected vulnerabilities. The page header includes navigation links for Code, Issues (0), Pull requests (22), Actions, Projects (0), Wiki, Security, and Insights. A sidebar on the left contains links for Alerts, Advisories, Code Scanning (highlighted), and Policy. The main content area shows a summary of 65 Open and 0 Closed vulnerabilities. The list includes:

- [GitHub token] wfsCeKmNXbUQgcVartiWEZBHRJLGxhFpYPMloAjD (May 23, 2019 by GitHub, src/MainPage.cs, develop)
- [Atlassian token] eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9... (May 10, 2019 by GitHub, src/MainPage.cs)
- [ESLint-019209] XSS vulnerability (May 10, 2019 by ESLint, src/index.js)
- [PII-email] nat@github.com (May 10, 2019 by GitHub, src/index.html, #1)
- [PII-SSN] 555-55-5555 (May 10, 2019 by GitHub, src/index.html)
- [Prefast-0149f89] Buffer overrun (May 10, 2019 by GitHub, src/process.cs, #2)

At the bottom, there is a pagination control with 'Previous', '1' (selected), '2', '3', '4', '5', and 'Next' buttons.

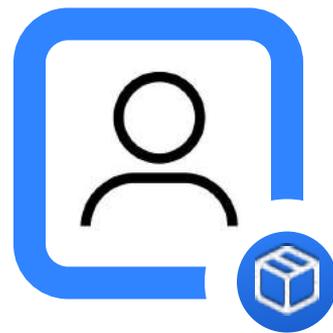
# Securing software, together



Researchers



Maintainers



Developers



Security  
teams

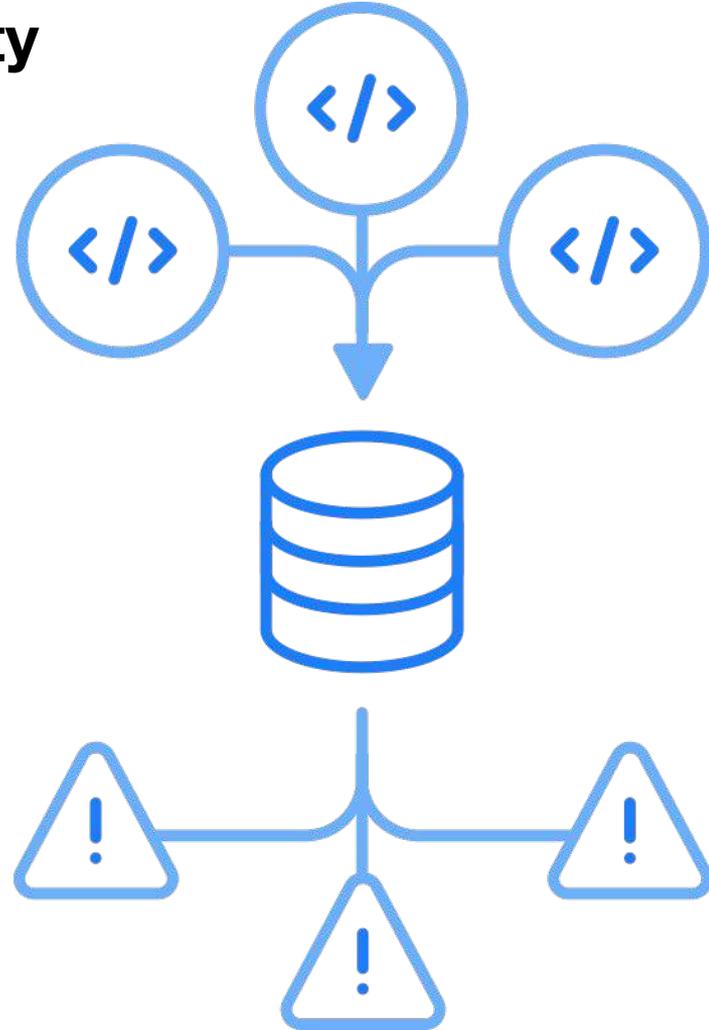
# GitHub Advanced Security

## Analyze code as data with CodeQL

Queries identify vulnerabilities and their variants

Prevents known variants as part of your CI

Community-led model continuously improves, 2000+ queries today

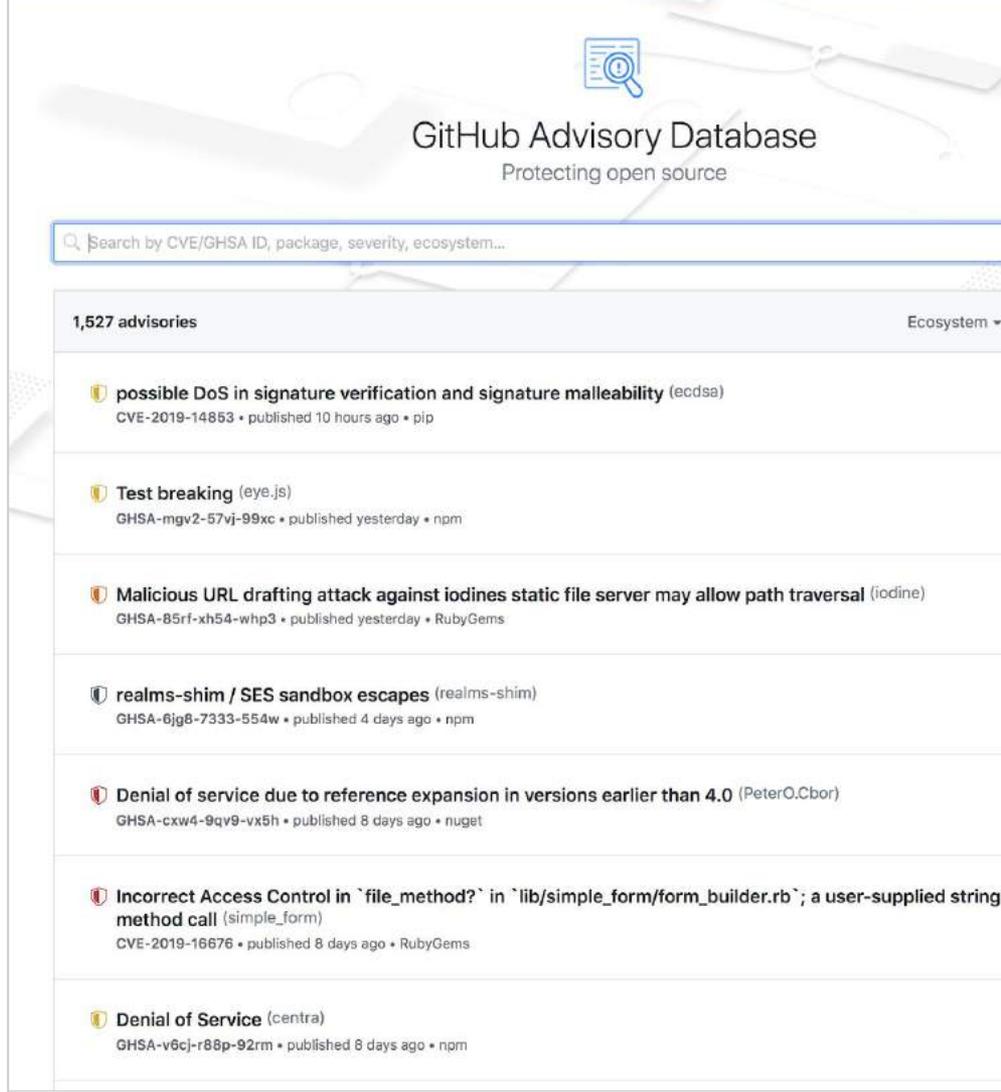


# GitHub Advisory Database

Our vulnerability database is free and publicly available

Basis of GitHub security alerts, includes:

- Curated alerts from national databases
- Advisories reported directly to GitHub



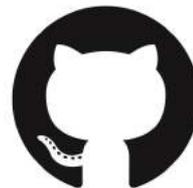
The screenshot displays the GitHub Advisory Database interface. At the top right, there is a search icon and the text "GitHub Advisory Database" and "Protecting open source". Below this is a search bar with the placeholder text "Search by CVE/GHSA ID, package, severity, ecosystem...". The main content area shows a list of 1,527 advisories, with a dropdown menu for "Ecosystem". The list includes several entries, each with a severity icon, a title, a package name, and a publication date.

Severity	Title	Package	Published
High	possible DoS in signature verification and signature malleability (ecdsa)	ecdsa	published 10 hours ago
High	Test breaking (eye.js)	eye.js	published yesterday
High	Malicious URL drafting attack against iodines static file server may allow path traversal (iodine)	iodine	published yesterday
High	realms-shim / SES sandbox escapes (realms-shim)	realms-shim	published 4 days ago
High	Denial of service due to reference expansion in versions earlier than 4.0 (PeterO.Cbor)	PeterO.Cbor	published 8 days ago
High	Incorrect Access Control in `file_method?` in `lib/simple_form/form_builder.rb`; a user-supplied string method call (simple_form)	simple_form	published 8 days ago
High	Denial of Service (centra)	centra	published 8 days ago

# GitHub Security Lab

## Community coalition to advance software security for everyone

- Consists of industry leading organizations
- Leading tools, freely available to any affiliated or individual security researcher
- Bug bounties, research, and knowledge sharing

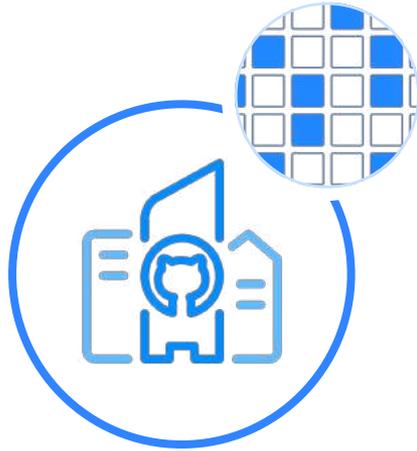


GitHub Enterprise

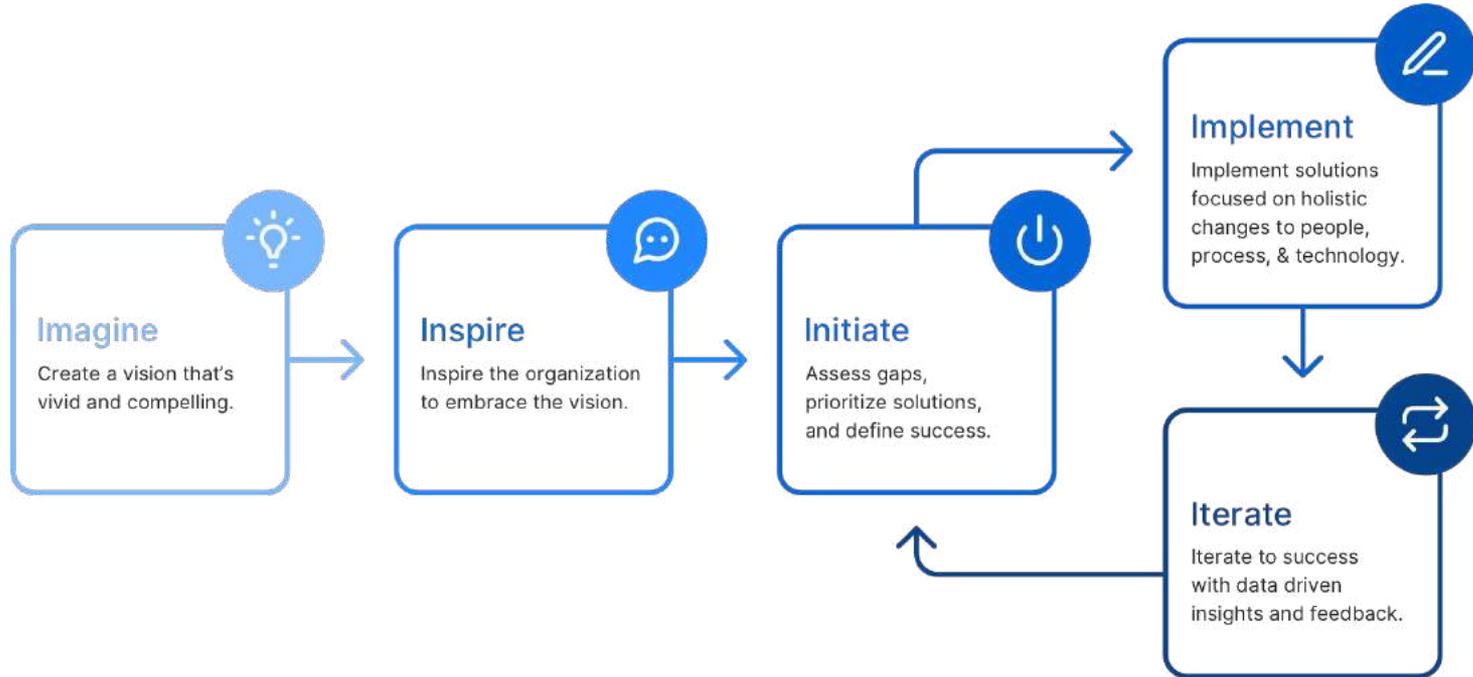
# Next steps, together



# No two journeys are identical

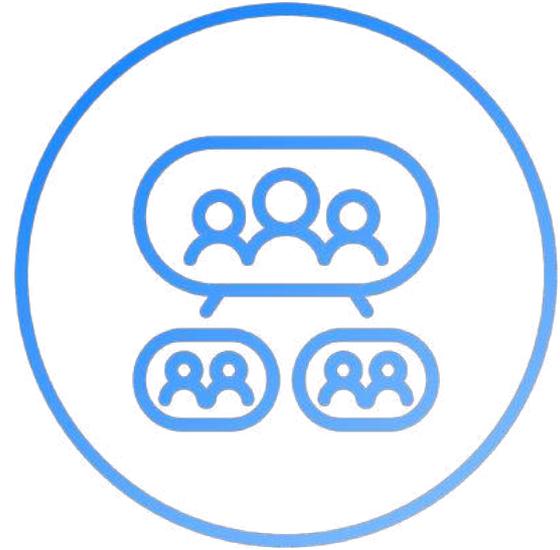


# Five I's Services Framework



**A team with over 200 years of collective experience building tailored solutions for customers.**

- Solutions architects
- DevOps engineers
- Implementation engineers



**Whatever your challenge, we are here to help**

