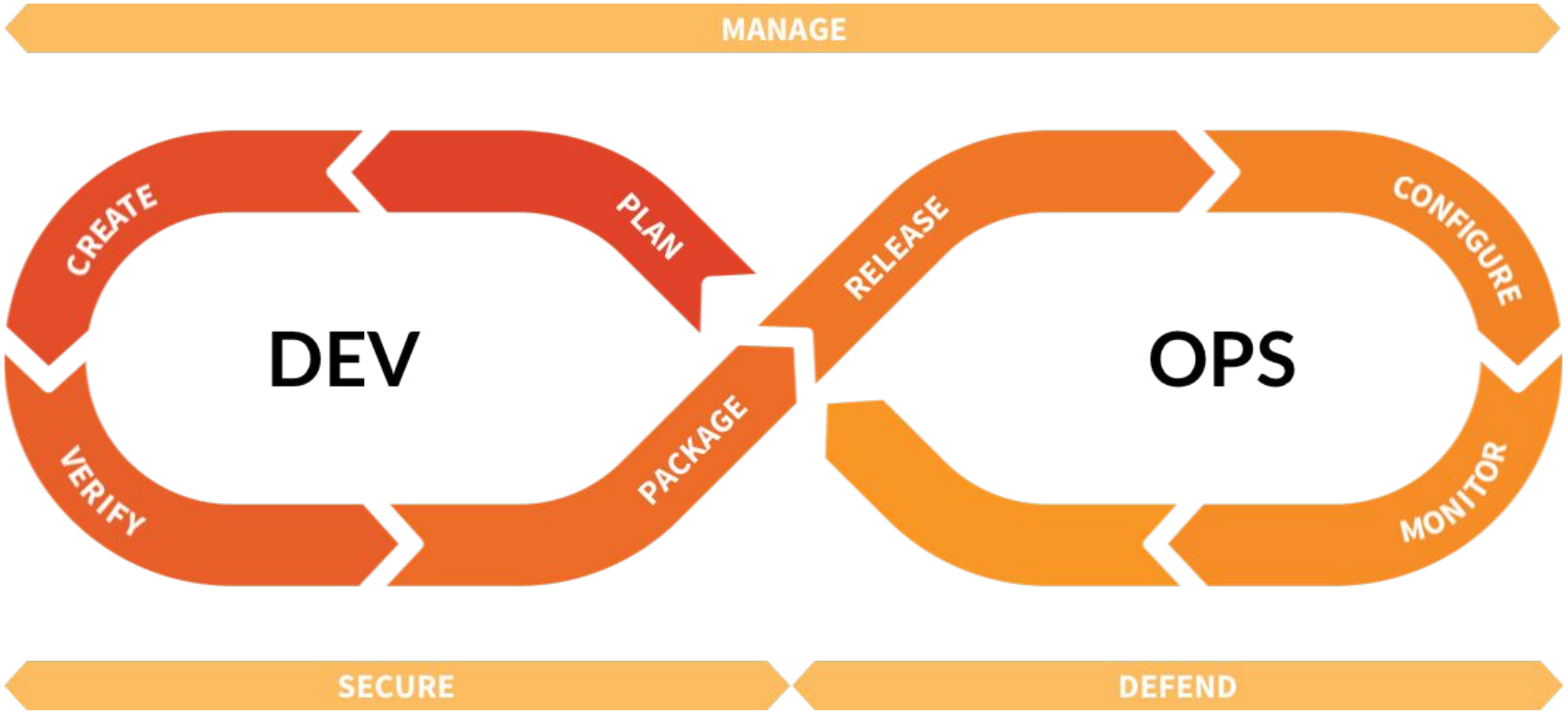
GitLab

**Francis Potter**
Solution Architect
fpotter@gitlab.com
https://about.gitlab.com

# Application Security at High Velocity

GOTO Conference
Apr 27-28, 2020

# DevOps


MANAGE
CREATE
PLAN
DEV
VERIFY
PACKAGE
RELEASE
CONFIGURE
OPS
MONITOR
SECURE
DEFEND

# It’s expensive

**“We estimate that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.”**

-- White House Council of Economic Advisors
Feb 2018

https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

# Vulnerabilities lead to Exploits

**Adobe**
153 mil user records
October 2013

**eBay**
145 mil users
May 2014

**Equifax**
148 mil consumers
July 2017

**Marriott**
500 mil customers
2014-2018

**LinkedIn**
165 mil user accounts
2012 and 2016

**Zynga**
218 mil user accounts
September 2019

*The 15 biggest data breaches of the 21st century* https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

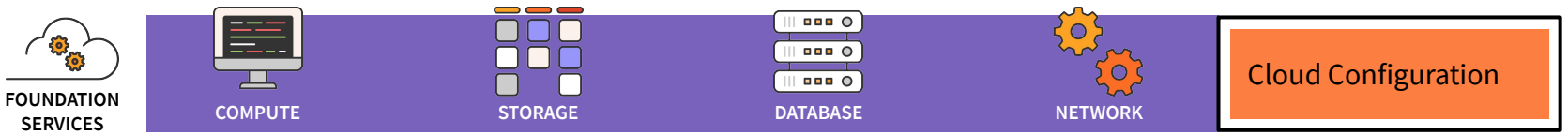
# It’s expensive

**More than half of all small businesses suffer a breach yearly but only 14% are prepared to defend themselves**

-- CNBC
Oct 2019

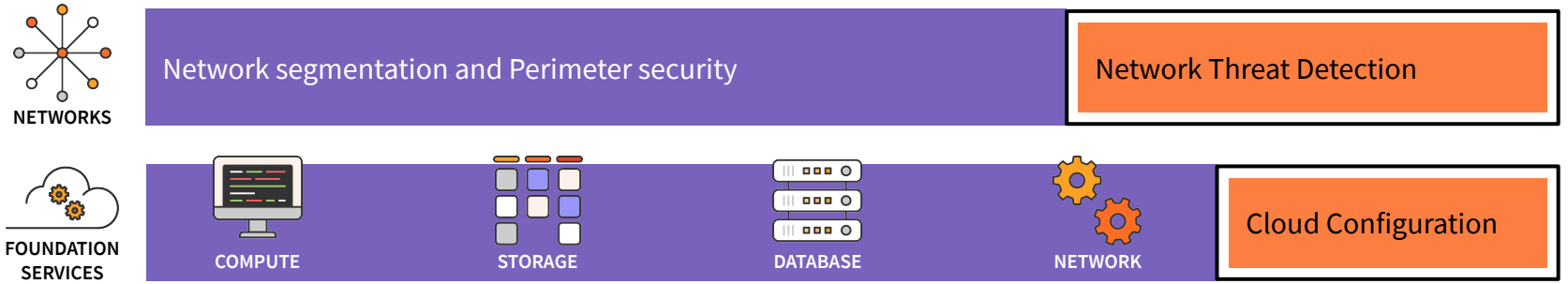
https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

# Four tiers of threats



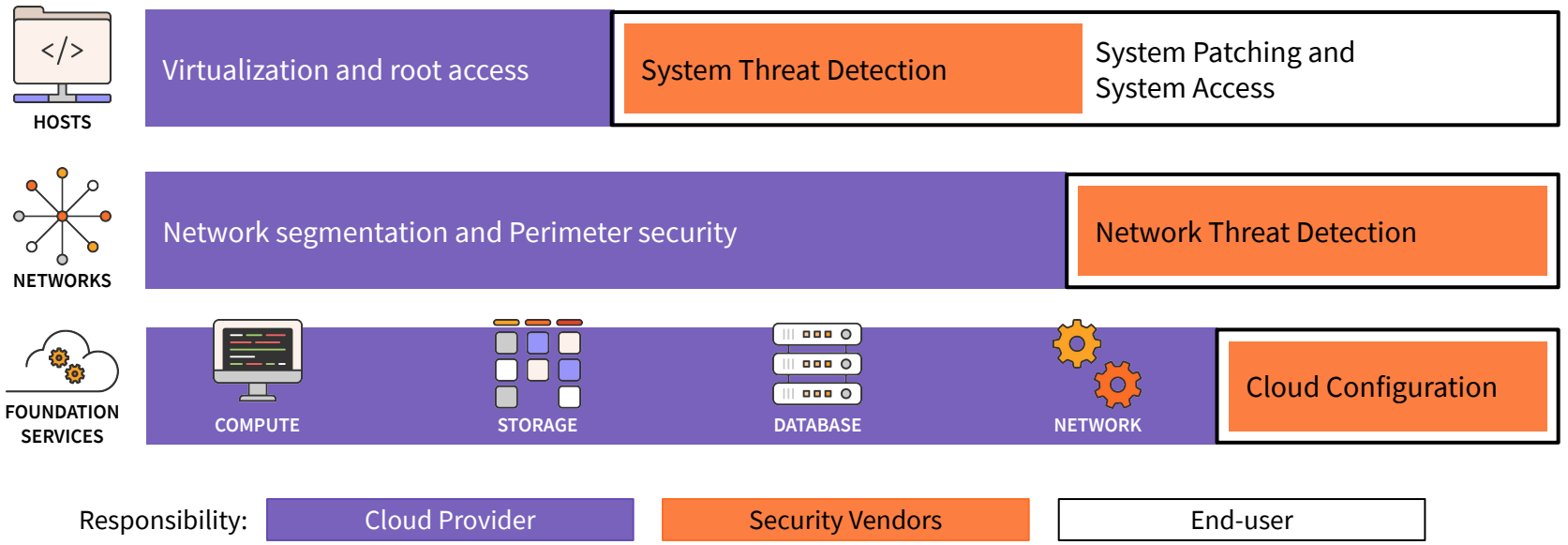

Responsibility: Cloud Provider | Security Vendors | End-user

# Four tiers of threats




Responsibility: Cloud Provider | Security Vendors | End-user

# Four tiers of threats



# Four tiers of threats

APPS

Application Threat Detection

Application Access

App Configuration and
App Patching


HOSTS

Virtualization and root access

System Threat Detection

System Patching and
System Access

NETWORKS

Network segmentation and Perimeter security

Network Threat Detection

FOUNDATION
SERVICES

COMPUTE

STORAGE

DATABASE

NETWORK

Cloud Configuration

Responsibility: Cloud Provider | Security Vendors | End-user

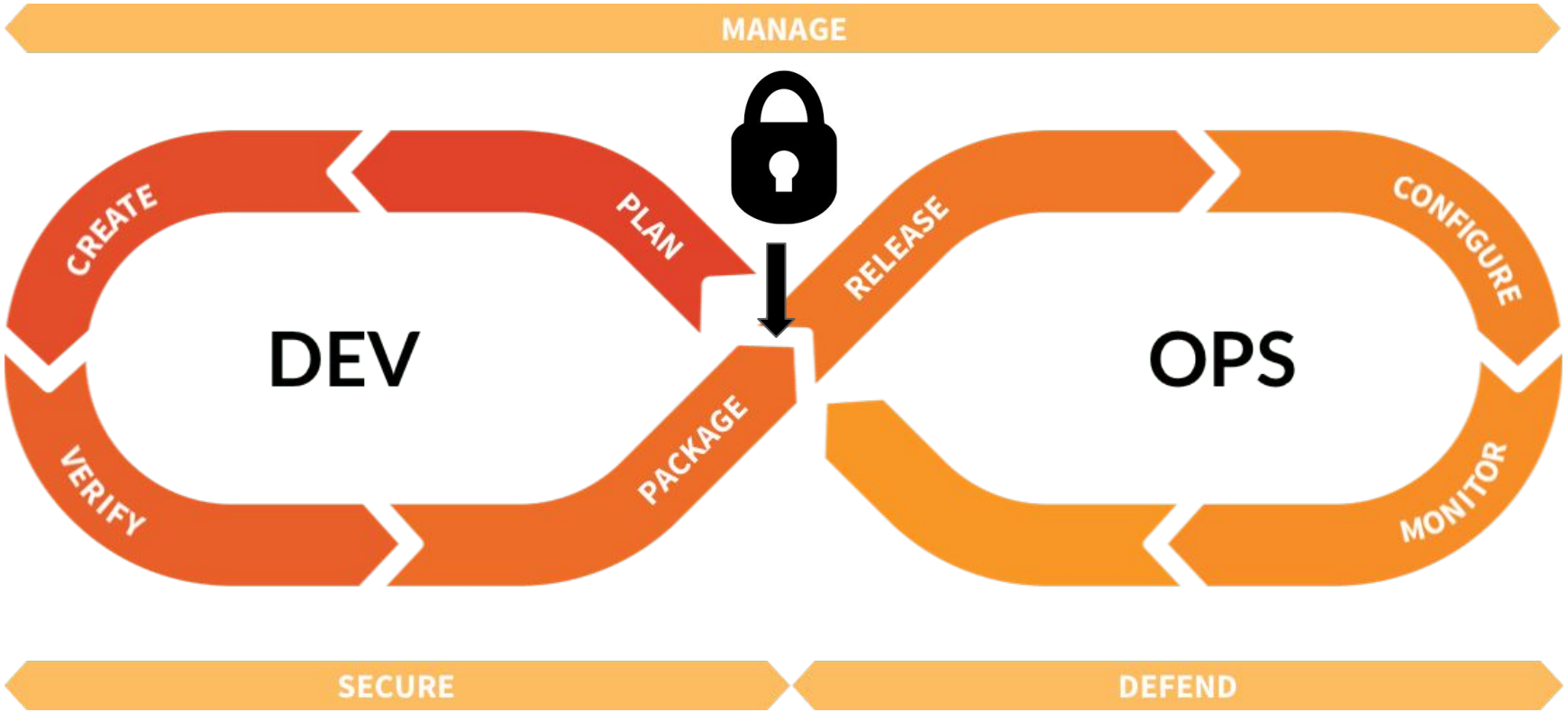
# Application Security vendors

# Is Security a Square Peg in a Round Hole of DevOps?

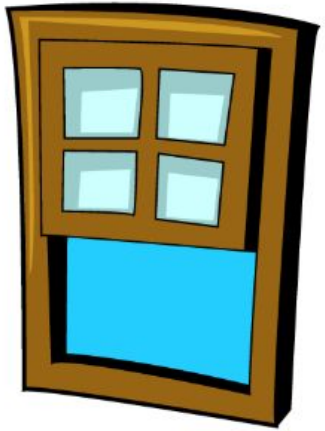
Established security tools were intended for a waterfall process at the end of SDLC and are incongruent with DevOps's

- **People**
- **Process**
- **Technology**

# “Traditional” Application Security

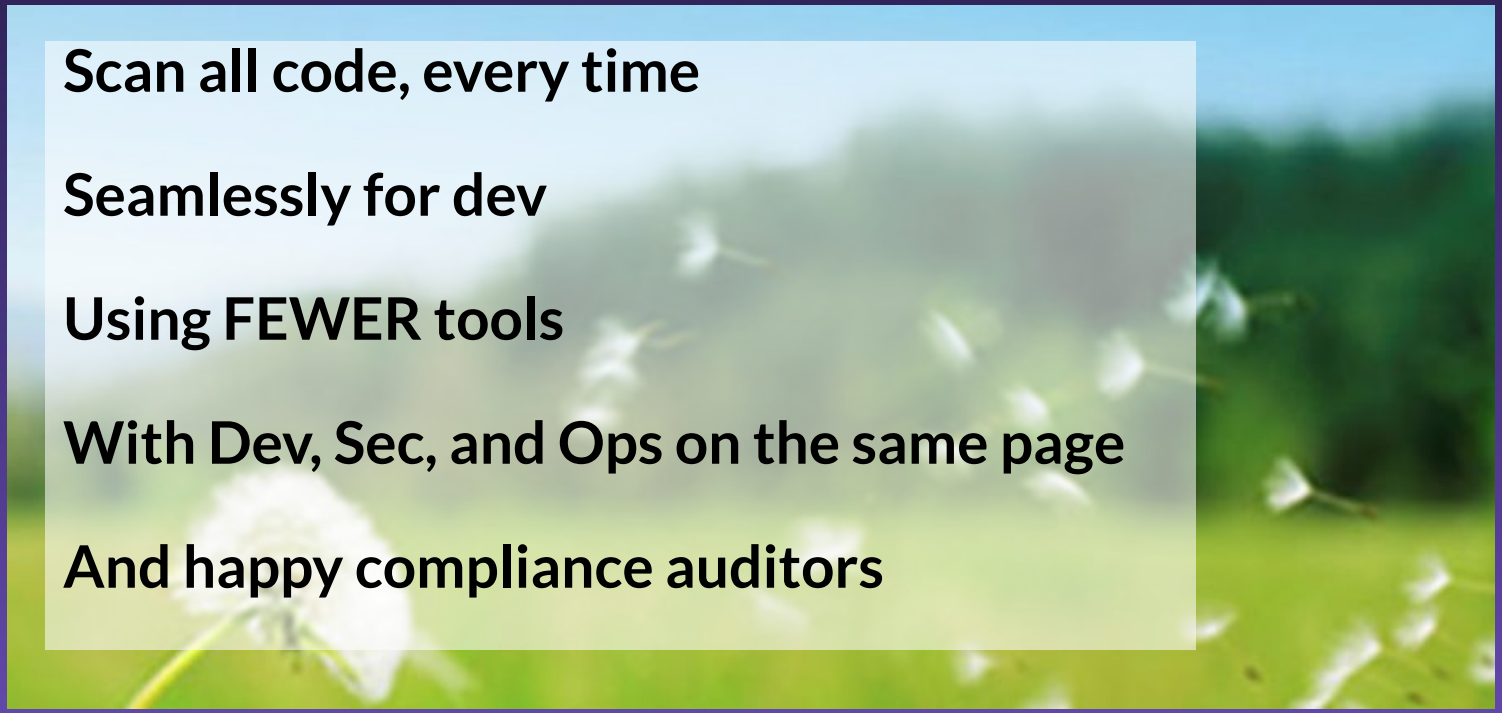


# Have to cover all your bases

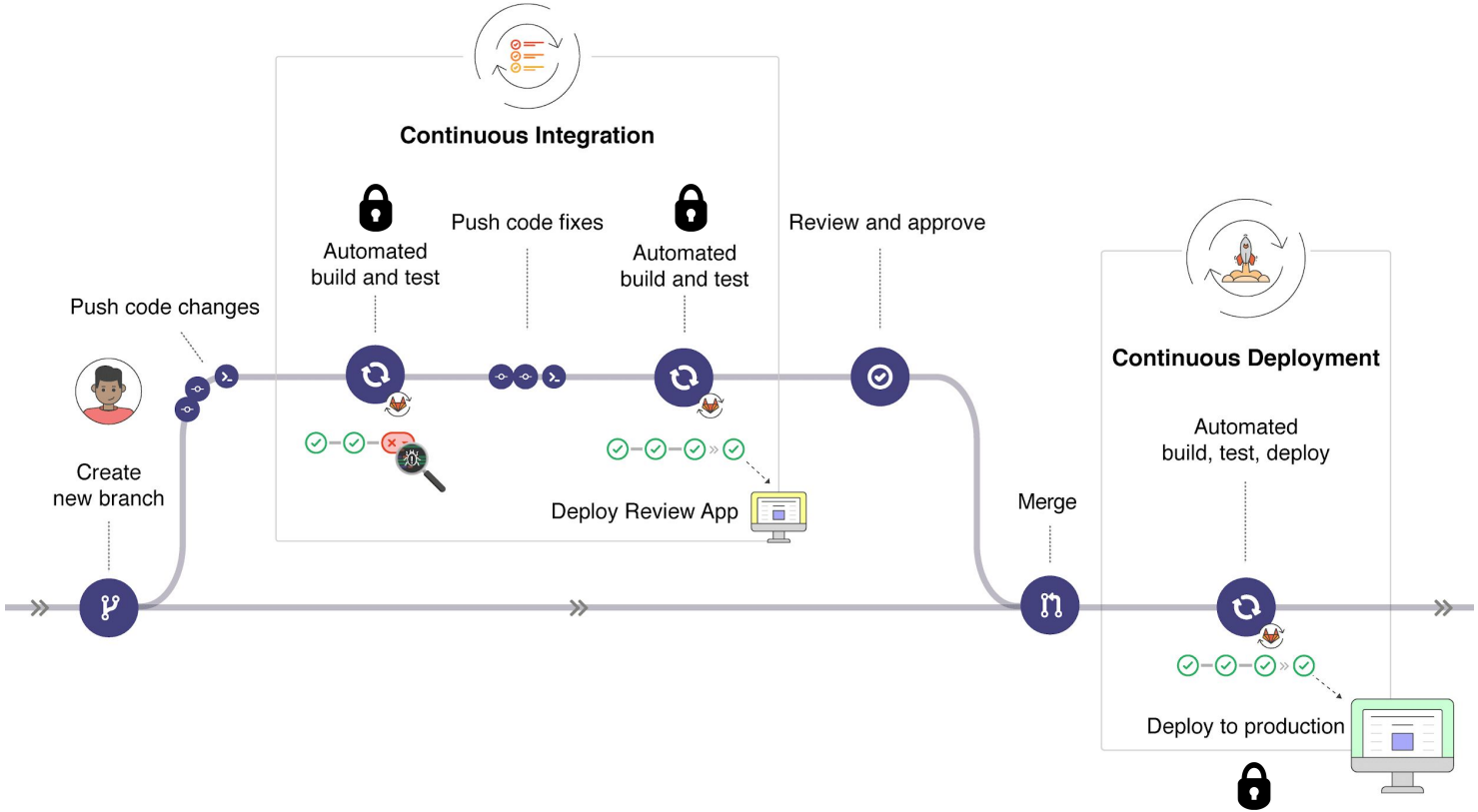


Images from http://clipart-library.com

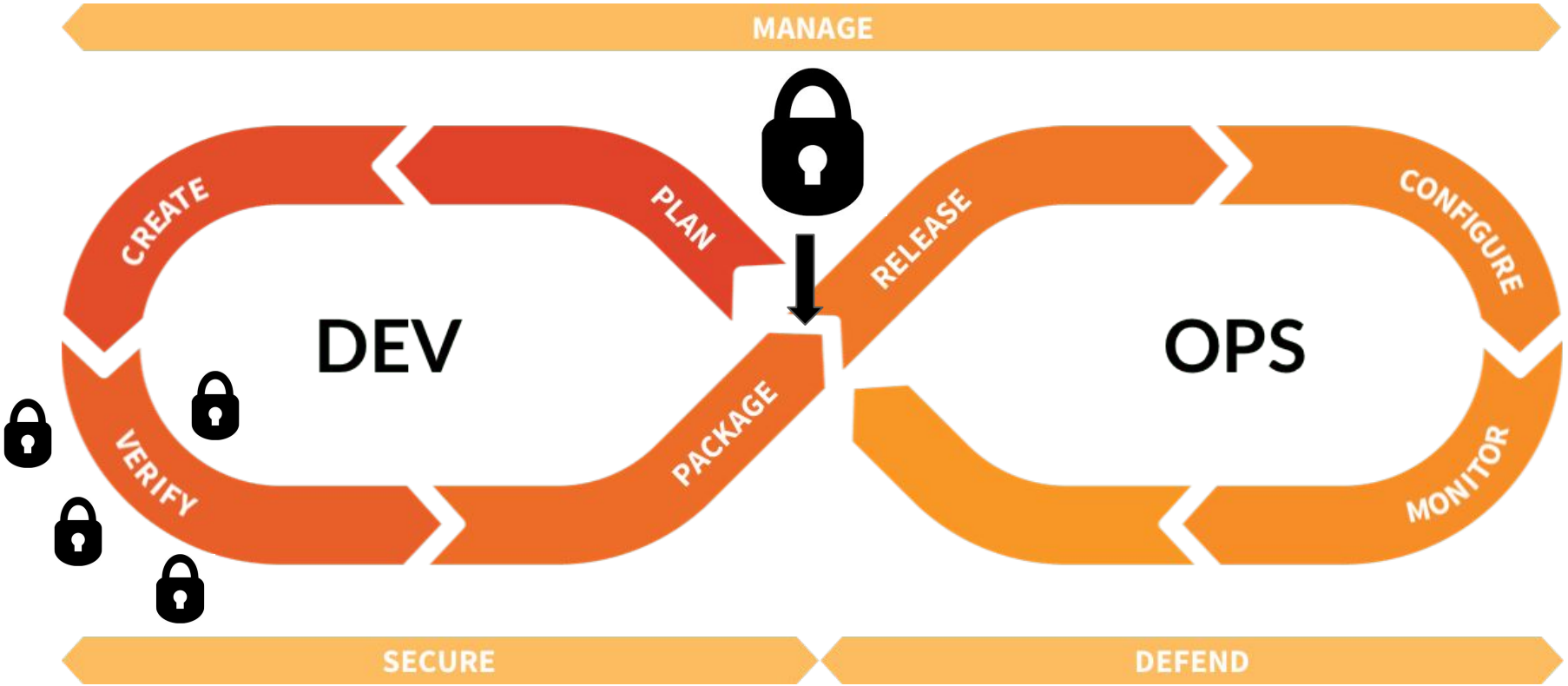
# What if you could...



# “Shifting Left” is Key



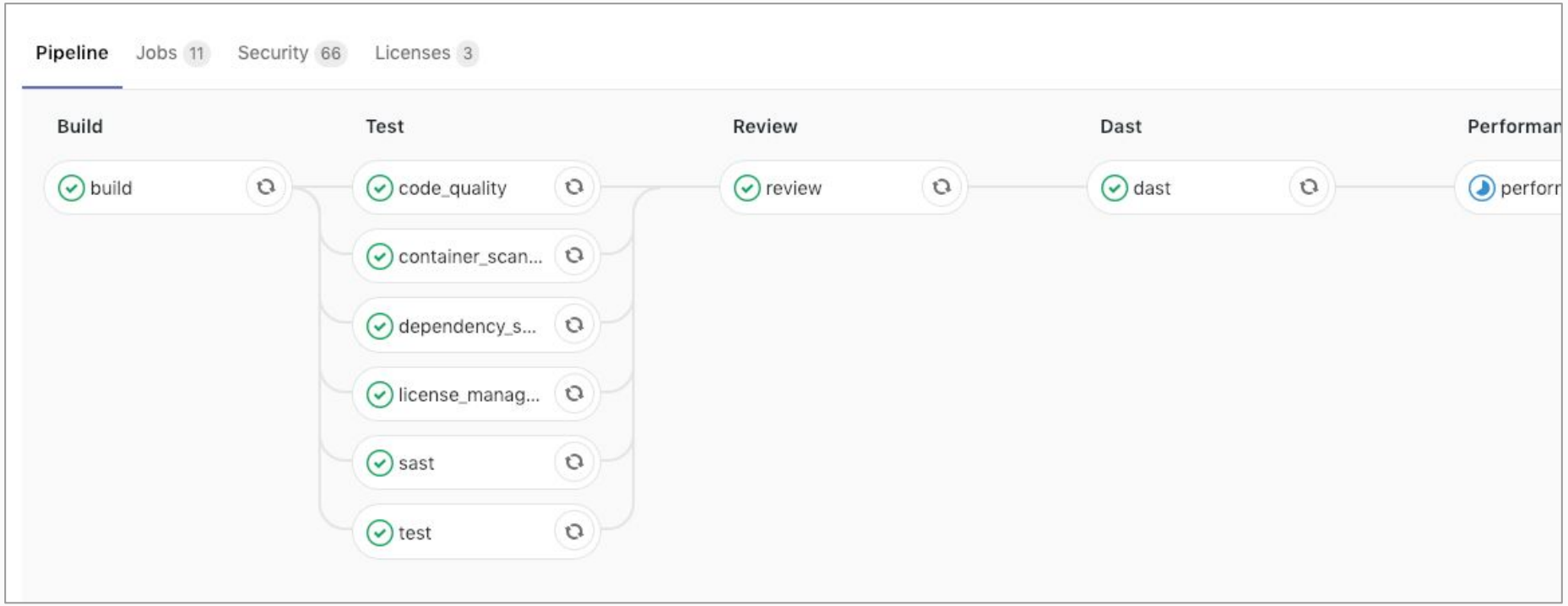
# “Traditional” Application Security



# Types of Application Security

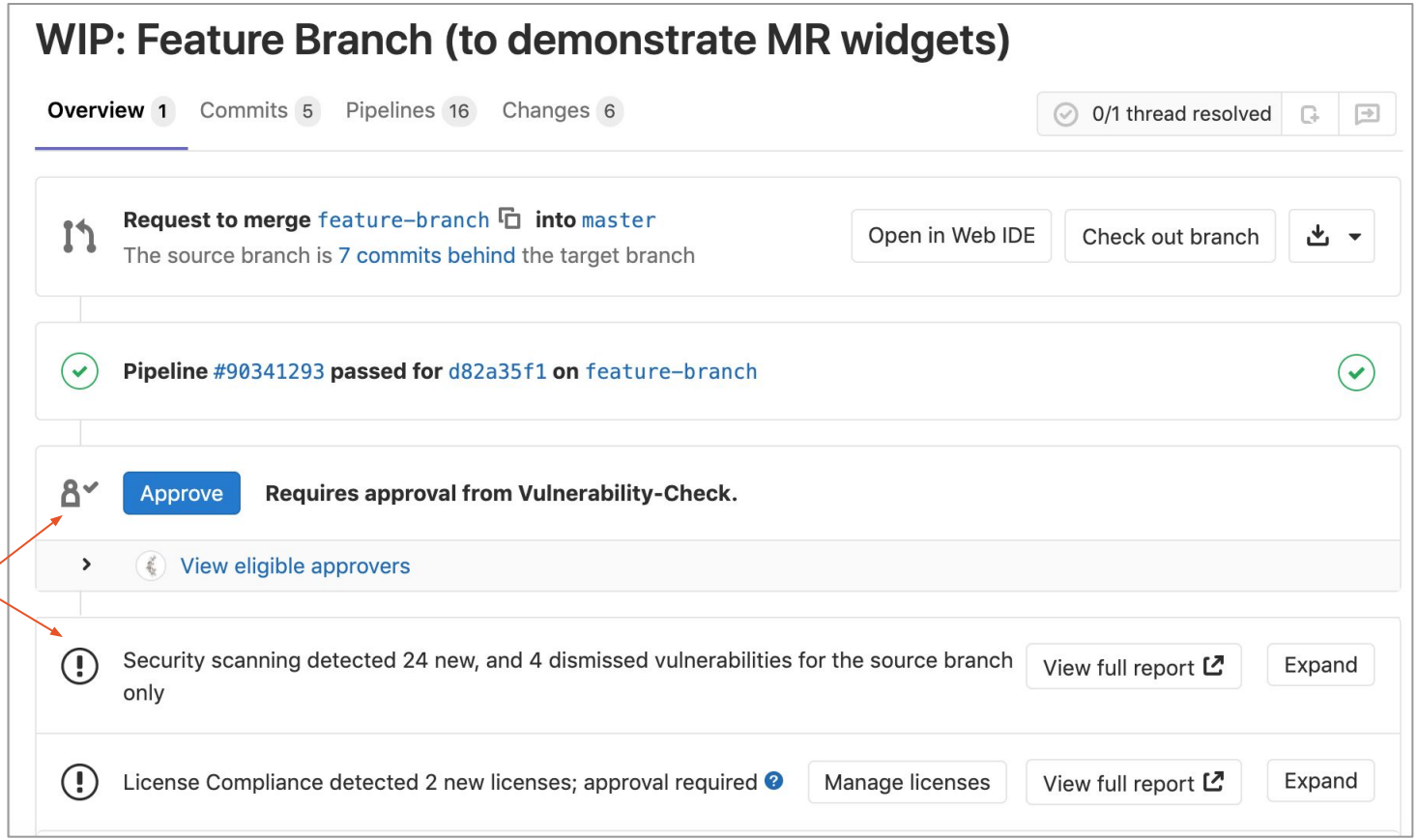
| Type | Description |
| --- | --- |
| **Static Application Security Testing (SAST)** | Reads your code and finds vulnerabilities based on patterns |
| **Dependency Scanning** | Looks through your dependencies for those with known vulnerabilities |
| **Container Scanning** | Looks through your Docker (and other) containers for those with known vulnerabilities |
| **Secret Detection** | Finds passwords, API keys, and the like in your code |
| **License Compliance** | Assures that all dependency licenses comply with policy |
| **Dynamic Application Security Testing** | Scans a running application for potential attacks |
| **Interactive Application Security Testing (IAST)** | Sort of a combination of SAST and DAST |
| **Fuzz Testing** | Provides invalid, unexpected, or random data as inputs |

# Continuous Application Security = a United Workflow

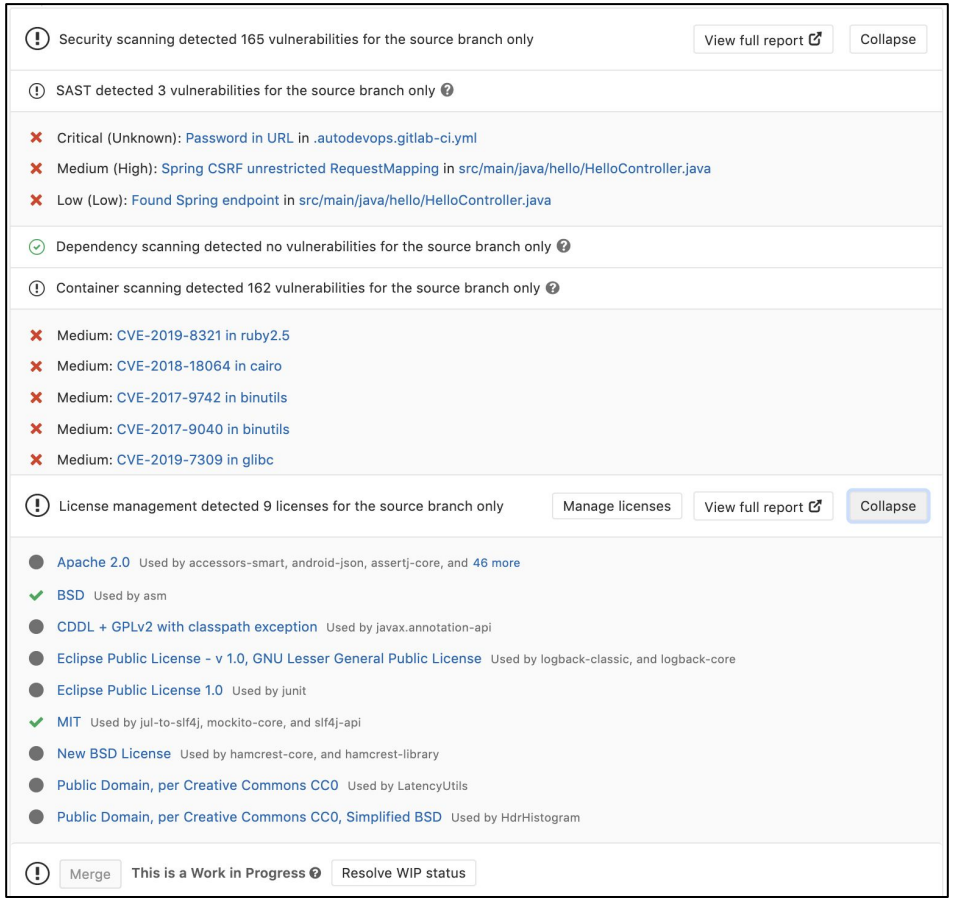


# Enabling Developer To Address Security Findings *Quickly*

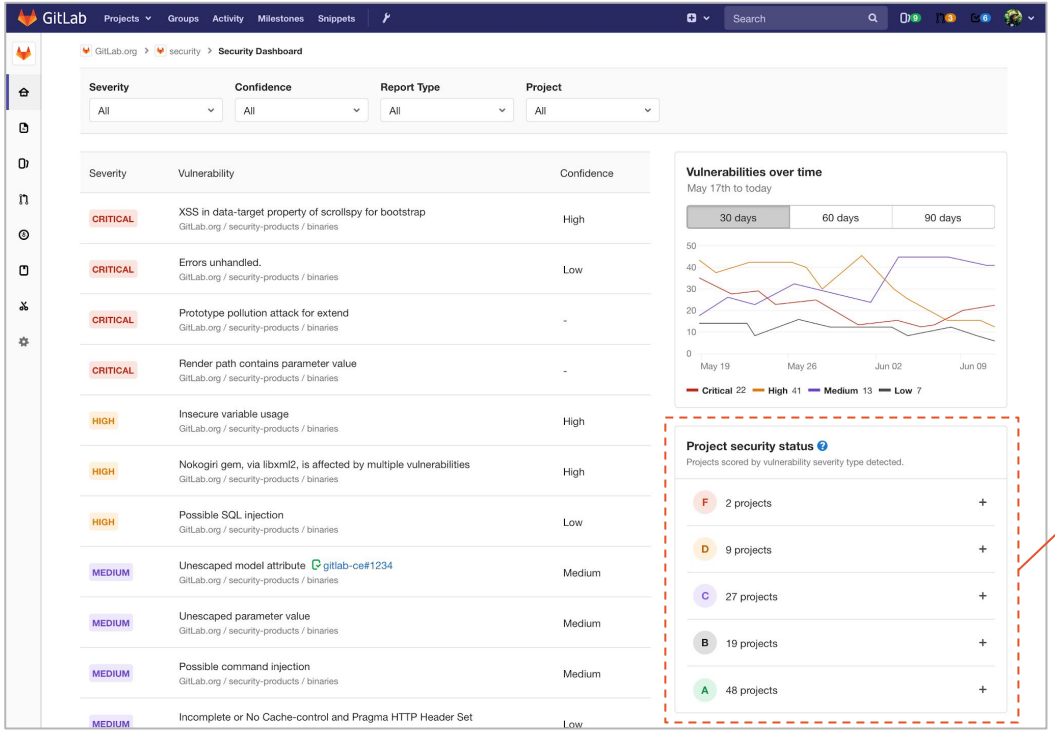
When vulnerabilities are present in an MR, you can easily **see** and **triage** them before the MR moves forward.

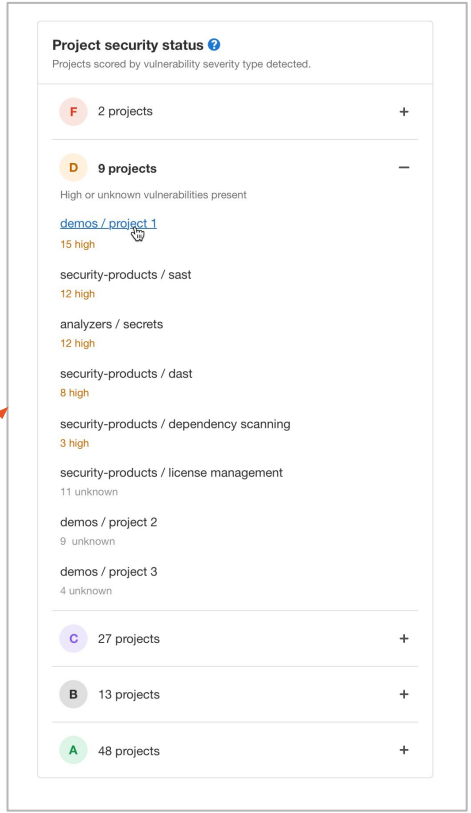


# Vulnerability information at Developer's fingertips



# Portfolio-level Executive Dashboards



# And now we have...

# Dev**Sec**Ops

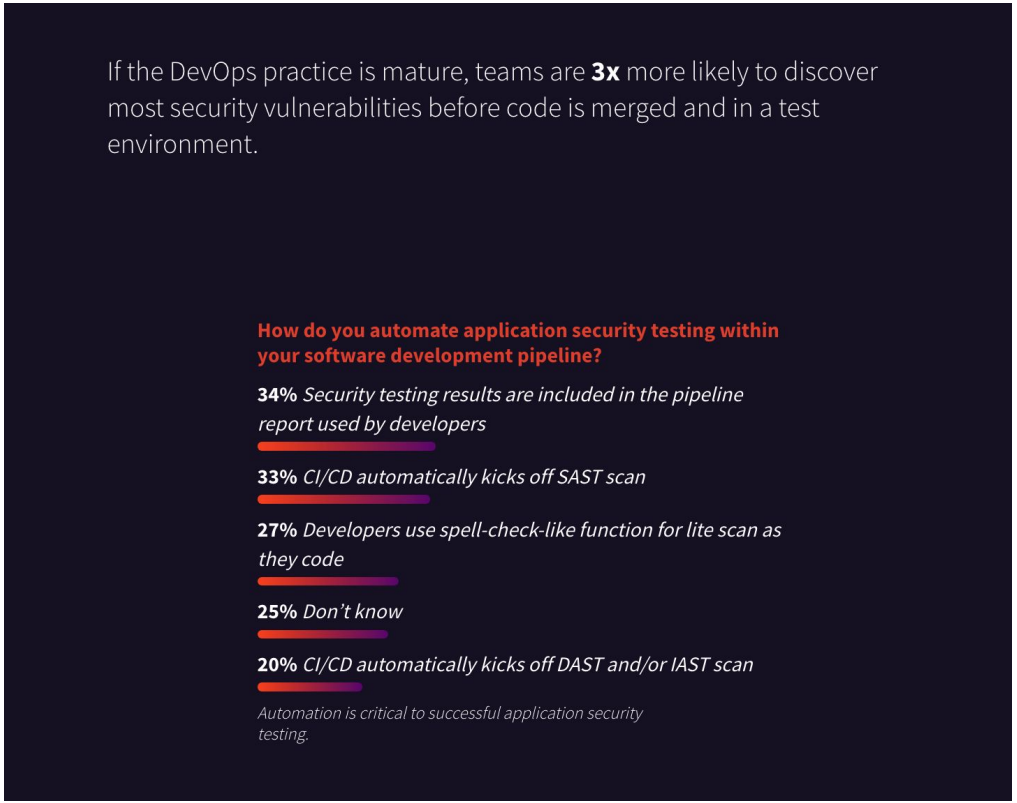
**Contextual**
Within existing developer workflows

**Congruent**
Supports rapid iteration and innovation

**Integrated**
File issues, auto remediate, track vulnerabilities

**Efficient**
Less tools and context switching

# It Works!




*2019 Global Developer Report: DevSecOps* https://about.gitlab.com/developer-survey/

# Examples

As part of their ramp up in GitLab, the dog-walking service recently furled automated security scanning and license management into their workflow, with Director of Engineering Dave Bullock noting how "great" it is to have those features baked into the pipeline so that immediate action can be taken when needed ... What previously took 40 minutes to an hour to accomplish, now takes just six minutes.


The security jobs in place are catching vulnerabilities from migrating to production through the product" explained Zaq Wiedmann, lead software engineer ... Wiedmann said the auditor also mentioned that Glympse had remediated security issues faster than any other company that he had worked with before in his 20-year career.

https://about.gitlab.com/blog/2019/01/16/wag-labs-blog-post/ https://about.gitlab.com/customers/glympse/

GitLab

**Francis Potter**
Solution Architect
fpotter@gitlab.com
https://about.gitlab.com

# Application Security at High Velocity

GOTO Conference
Apr 27-28, 2020