



# Solving Application Security with Artificial Intelligence

Stefan Streichsbier - CTO  
[stefan@guardrails.io](mailto:stefan@guardrails.io)



# What we'll cover today



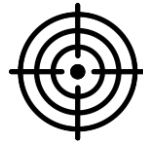
**Why this is an important problem**



**Challenges with current state of AppSec**



**How AI is Revolutionizing AppSec**

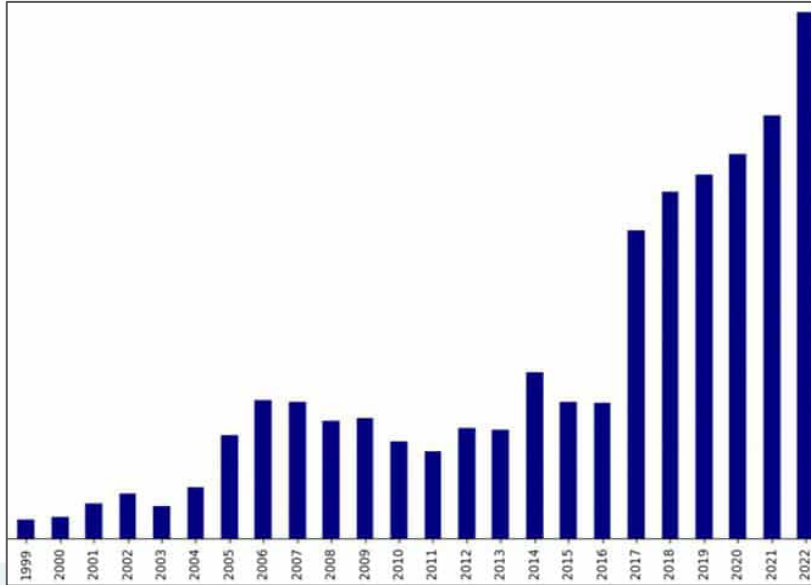


**GuardRails.ai: Timeline and Expectations**

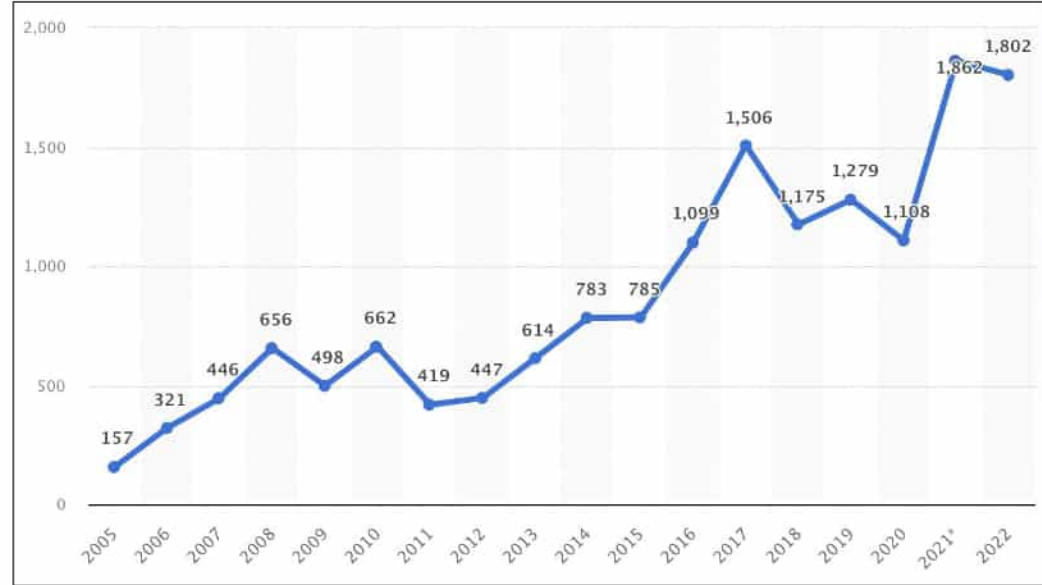
Why this is important



# The problem is getting worse ...



Percentage of CVEs Published



Annual number of data breaches (US)

# ... despite an unlimited supply of solutions

**CYBER SCOPE**
**2022**

**Network & Infrastructure Security**

Advanced Threat Protection  
AhnLab, Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Endpoint Protection  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

VPN  
Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

DDoS Protection  
Cloudflare, Akamai, Imperva, Fortinet, Cisco, SonicWall, Palo Alto Networks, Palo Alto Networks, Palo Alto Networks

Network Firewall  
Palo Alto Networks, Palo Alto Networks, Palo Alto Networks, Palo Alto Networks, Palo Alto Networks, Palo Alto Networks

**Web Security**

Web Proxy  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Web Gateway  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Web Filtering  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Network Analysis & Forensics  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Endpoint Security**

Endpoint Prevention  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Endpoint Detection & Response  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Endpoint Protection  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Application Security**

Web & Application Security  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Application Security Testing  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Application Security Testing  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**MSSP**

Traditional MSSP  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Advanced MSS & MDR  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Data Security**

Encryption  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

DLP  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Data Privacy  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Data Centric Security  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Mobile Security**

Mobile Device Management  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Mobile Device Security  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Risk & Compliance**

Risk Assessment & Visibility  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Risk Quantification  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Pen Testing & Breach Simulation  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Security Awareness & Training  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Security Ops & Incident Response**

SIEM  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Incident Response  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Threat Intelligence**

Threat Intelligence  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**IoT**

IoT Devices  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Automotive  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Connected Home  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Messaging Security**

Messaging Security  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Identity & Access Management**

Authentication  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Privileged Access Management  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Identity Governance  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Consumer Identity  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Digital Risk Management**

Digital Risk Management  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Security Consulting & Services**

Security Consulting & Services  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Blockchain**

Blockchain  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Fraud & Transaction Security**

Fraud & Transaction Security  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Cloud Security**

Cloud Security  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Container  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

Infrastructure  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

CASB  
Avast, Avira, Avast SecureLine, Avast SecureLine Business, Avast SecureLine Home, Avast SecureLine Mobile, Avast SecureLine Server, Avast SecureLine IoT

**Momentum**

# Challenges with current state of AppSec



# Challenges with the current State of AppSec



## 1. Diverse Vulnerability Types

- Affecting every part of the stack code, dependencies, secrets, cloud, etc
- Each type requires specialized attention and different mitigation strategies
- Rapid tech evolution means the emergence of more complex risk

## 1. Fragmented Tools

- No single tool excels in detecting all vulnerability types
- Companies resort to using multiple tools, straining budgets
- Integrating and managing these tools becomes complex

## 1. Alert Fatigue

- Tools often generate an overwhelming number of alerts.
- Sifting through these to identify genuine threats is time-consuming.
- Constant alerts cause fatigue, leading to potential oversight of critical vulnerabilities.

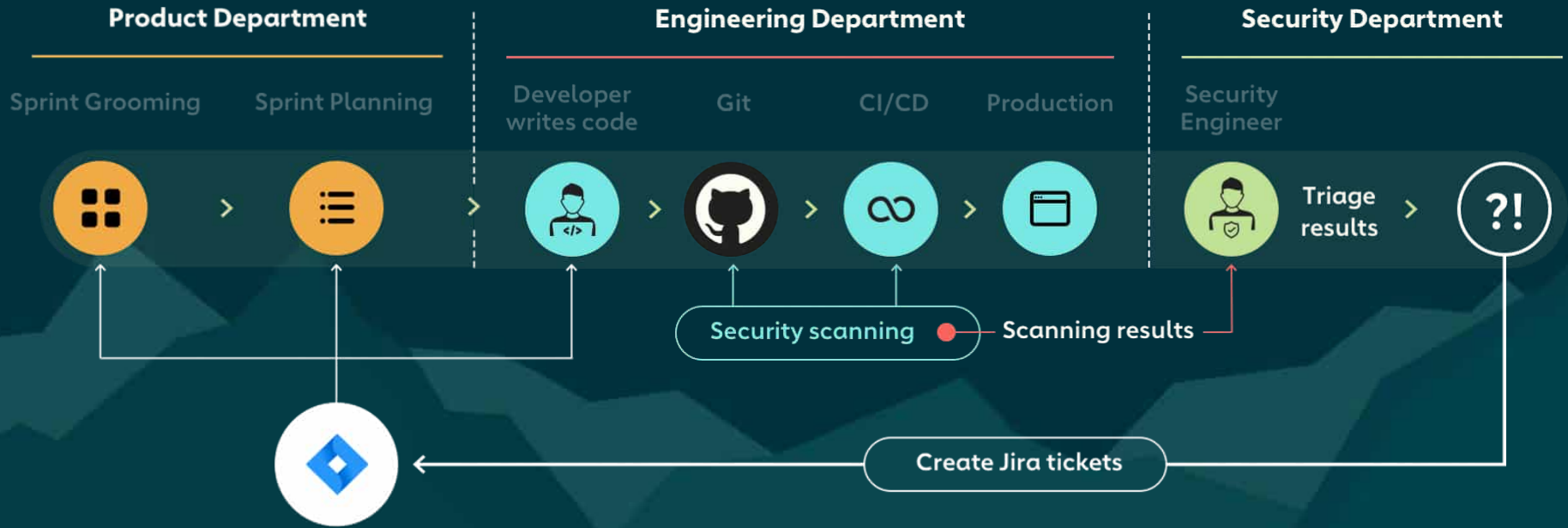
## 1. False Positives

- Many flagged vulnerabilities might be false positives.
- Discerning real threats from noise is a daunting task.
- The effort to validate issues takes away from actually addressing genuine threats.

## 1. Shortage of Expertise

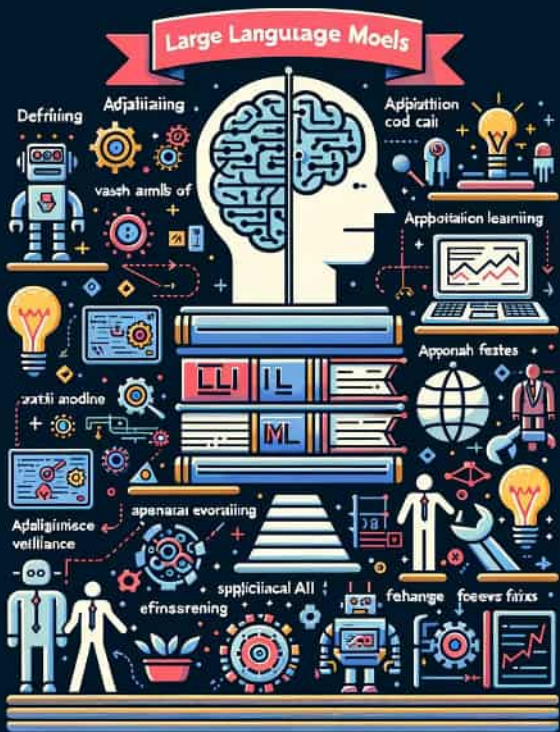
- Limited availability of skilled security experts and trained developers
- Current team members face a steep learning curve in application security
- Time is spent on analyzing, prioritizing, and fixing vulnerabilities rather than on core development tasks, which is prohibitive

# Security workflows are broken





# Brief Overview of Large Language Models



## 1. Defining Large Language Models (LLMs)

- LLMs are state-of-the-art AI models trained on vast amounts of text data
- Capable of understanding, generating, and interpreting human language
- Evolved from simple keyword recognition to deep semantic understanding

## 1. LLMs vs Traditional AI (ML)

- Traditional ML models often rely on specific use-cases
- LLMs autonomously identify patterns and relationships in data
- LLMs can perform tasks they weren't explicitly trained for

## 1. LLMs in Application Security

- Contextual Analysis: Primed with context about the code and business risk
- Reasoning Capabilities: Going beyond simple pattern/logic
- Generating Fixes: Provide code fixes for vulnerabilities

## 1. Adaptability of LLMs

- Tool use allows LLMs to achieve complex tasks requiring real time knowledge
- Few shot prompting can fine-tune LLMs for specific use-cases
- With feedback loops, LLMs get better over time, adapting to specific company codebases and workflows.

## 1. Synergy with Human Expertise (Co-pilot paradigm)

- LLMs amplifying human expertise rather than replacing it
- Automating repetitive free up security experts for higher-level strategic work
- Collaboration bridges the skill gap in security and development teams

# How AI is Revolutionizing AppSec



# Revolutionizing AppSec with AI



## 1. Understanding Code and Business Context

- Business context and risk about an application are key inputs to the analysis
- LLMs can understand code, dependencies, and purpose of an application
- Allows people to interact with applications in entirely new ways

## 1. Accurate Vulnerability Detection

- Hybrid approach can leverage traditional detection and super charge it with AI
- LLMs are primed with specific code, business and vulnerability context
- Detection can be improved through human feedback loops

## 1. Reduction in False Positives

- Interpret the broader context of the code to ensure precise alerts
- Context-awareness ensures only relevant vulnerabilities are flagged
- Reduced noise allows focus on genuine threats.

## 1. Automated Code Fixes

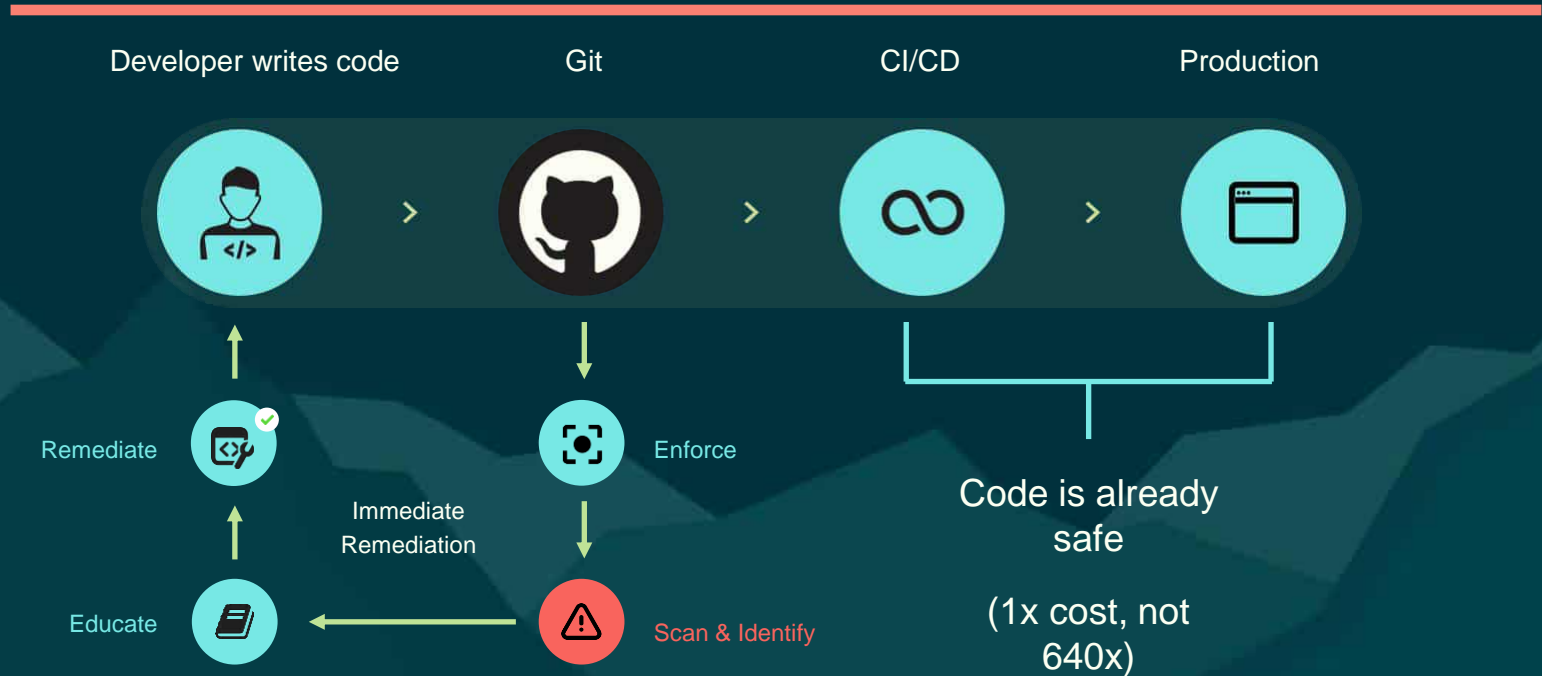
- Developers iterate on solutions to create optimal code fixes
- Streamline the mitigation process, reducing time from detection to resolution
- Preferred fixes can be added to company-wide skill arsenal

## 1. 100x your existing teams

- Faster time to triage and fix a vulnerability
- Security and Software engineers are skilled up through the interaction
- Higher engagement and satisfaction with “boring” tasks

# GuardRails.ai boosts developer security & productivity

Engineering Department



# GuardRails.ai

## Timeline and Expectations





# GuardRails.ai - The Future of AppSec

## 1. Get Started with GuardRails.io

- a. GuardRails.io already covers SAST, SCA, IaC, and Secrets for 22+ languages
- b. An easy upgrade path to GuardRails.ai will be provided
- c. Reach out to our team to learn more and get early access to GuardRails.ai

## 1. Launch Timeline

- a. Anticipated launch by the end of Q4 or early Q1
- b. Early users will be able to shape the direction and order of the roadmap
- c. Continual development ensures consistent advancements post-launch

## 1. First Version Highlights

- a. Reimagined UI/UX including "perfect workflow"
- b. Initial support for GitHub, both cloud and on-premise
- c. Precise static analysis and secret scanning with unparalleled accuracy

## 1. Upcoming Features

- a. Dependencies and additional scanning methods to be integrated soon
- b. Integrations with GitLab, BitBucket and Azure DevOps
- c. Deep workflow integrations with chat tools, issue trackers, and IDEs

# Q & A

