About me

With close to two decades of experience in the technology sector, Yashaswi is a cybersecurity leader and DevSecOps advocate with a profound understanding of the intricacies of software delivery and security. He is passionate about cloud security and threat detection and works tirelessly to integrate robust security measures throughout the software development lifecycle.

Currently, as the Senior Director of Solution Engineering at JFrog for the APAC region, Yash is instrumental in driving JFrog's mission to transform software security and resilience across the APAC landscape, ensuring organisations can confidently navigate the complexities of modern software development.
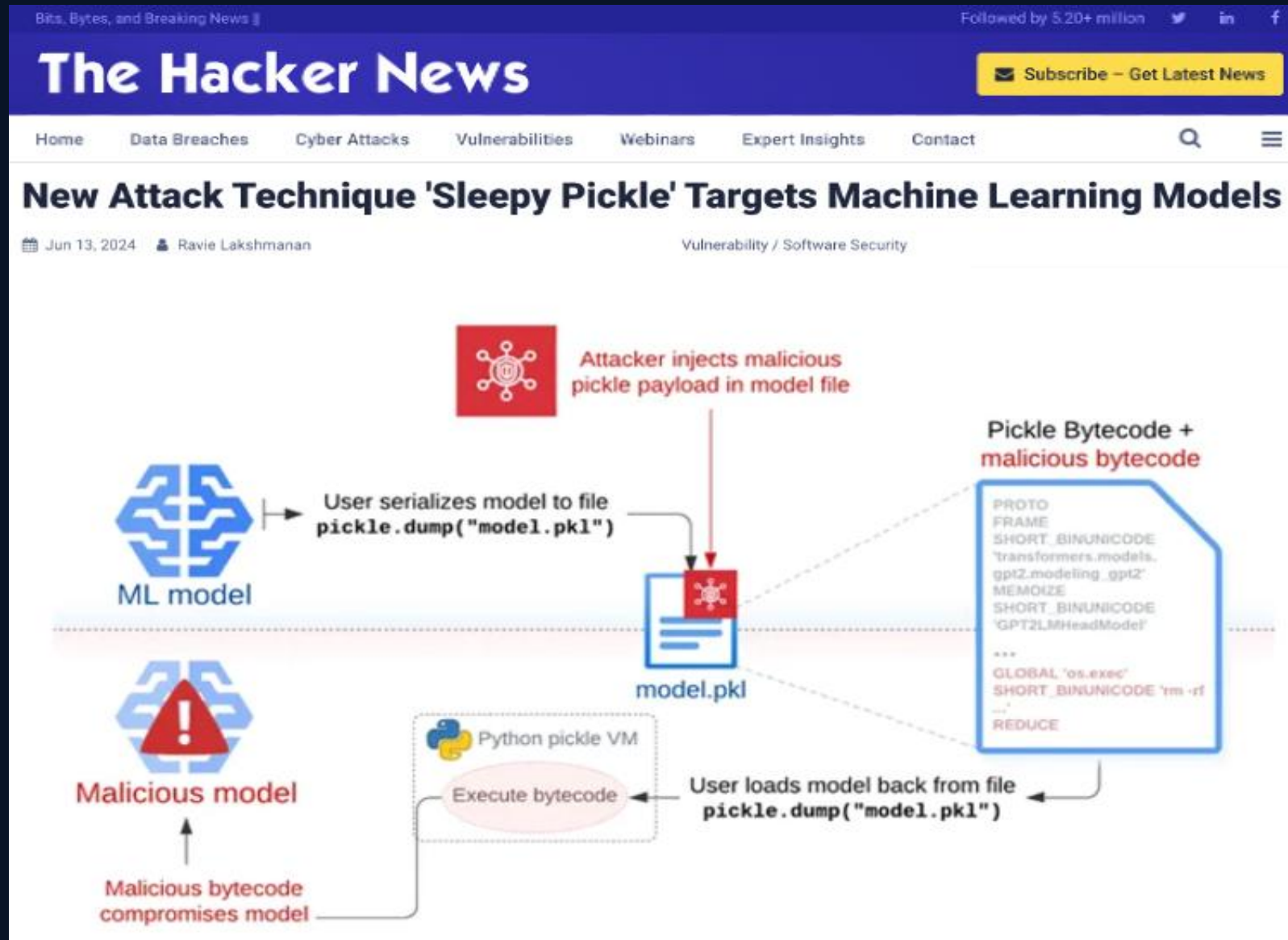
Let's Dive In

What's Making News?

Cost of SSC Attacks – Real-World Examples

Attack	Year	Exploit Path	Supply Chain Impact	Estimated Cost/Impact
SolarWinds (SUNBURST)	2020	Trojanised Software Update	Backdoor in government and enterprise networks	$100M+ in damages
Kaseya VSA Ransomware	2021	Remote Exploitation of Update Mechanism	Ransomware spread via IT management software	$70M+ in ransom demands
Codecov Bash Uploader	2021	Compromised Open-Source Script	Stolen credentials from thousands of CI/CD pipelines	Undisclosed financial losses
Apache Log4j (Log4Shell)	2021	Vulnerable Open-Source Library	RCE attack vector across millions of applications	$10+ billion in mitigation costs
3CX VoIP Attack	2023	Backdoor in Official Installer	Trojanized version affecting 600,000+ companies	Unknown financial impact

JFrog

OSS PACKAGES

99% FORTUNE 500
USE OPEN SOURCE

MODERN SOFTWARE IS
85-90% OPEN SOURCE

CVE GROWTH RATE
57% INCREASE FROM 2020

Your Code

Open Source

Containers

OS

IaC

JFrog

Software Supply Chain Attacks
Costs Rising from $46B in 2023 to $138B by 2031!

Gartner ®

Curate	Create	Package	Promote	Distribute	Deploy	Run

Inject	*Discover*	*Exploit*	*Steal*	*Abuse*	*Tamper*	*Attack*
Malicious Packages	0-Days	CVEs	Secrets	Misconfigs	Binaries	Production

Growing Attack Surface

Gartner: *Leader's Guide to Software Supply Chain Security* (June '24)

JFrog

If You Can't **Control** It

CODE

BINARIES

Curate

Create

Package

Promote

Distribute

Deploy

Run

You Can't **Secure** It

JFrog
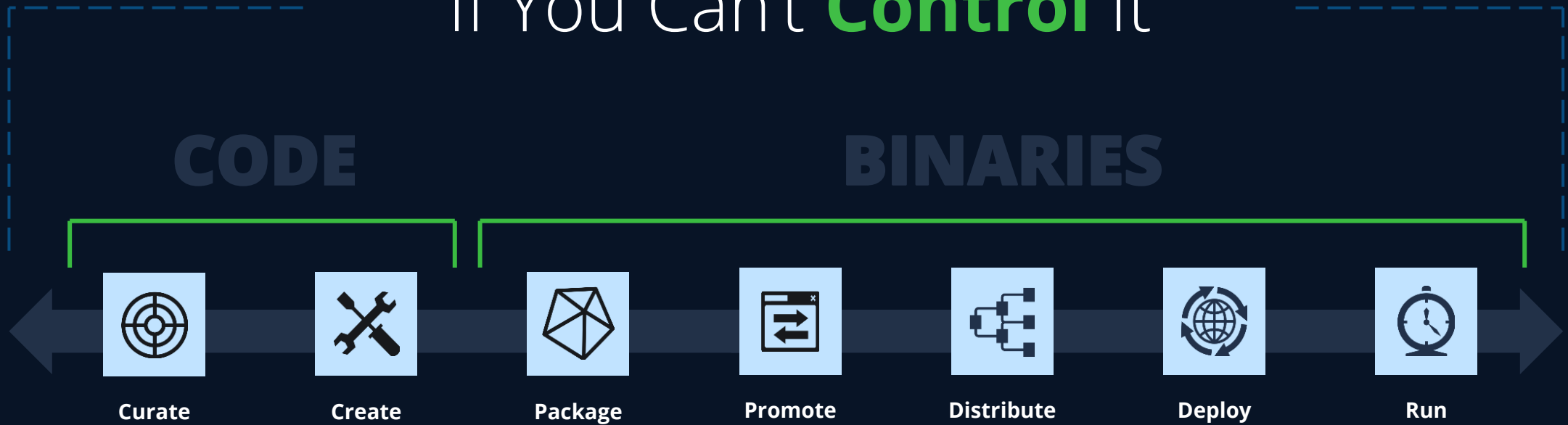
Software Supply Chain Attack Vectors

Compromised Dependencies

Build Server Compromise

Malicious Code in the Pipeline

Software Package Repositories

Code Signing Abuse

Malicious Software Update

Artifact Tampering

Compromised Development Tools

JFrog

Who's Responsible?

Security/DevSecOps Team

Development Team

Operations Team

Supply Chain/Procurement Team

Compliance Team

Product Management Team

JFrog

What do **Reports Say?**

Surveyed:

Global devs, dev team leaders/managers, and product owners that use DevSecOps about the time spent on security-related activities in their daily work

To Understand:

- Business impact of security tasks on dev time
- Tools and tasks taking the most time
- Value of developer time spent on DevSecOps
- Impact on dev flow & satisfaction

ORGANIZATION SIZE

1,000–2,499	2,500–4,999	5,000–9,999	10,000+
32%	29%	23%	16%

ROLE

Development Manager (multiple teams reporting)	Senior Developer (5+ years experience)	Product Owner (1–2 development teams)	Development Team Leader (1 team reporting)
37%	25%	20%	18%

DEVSECOPS ISN'T FREE

Companies Spend **$28,100** Per Developer Yearly on Software Security

Developers Estimate Spending **19%** of Their Weekly Work Hours on Security-Related Tasks
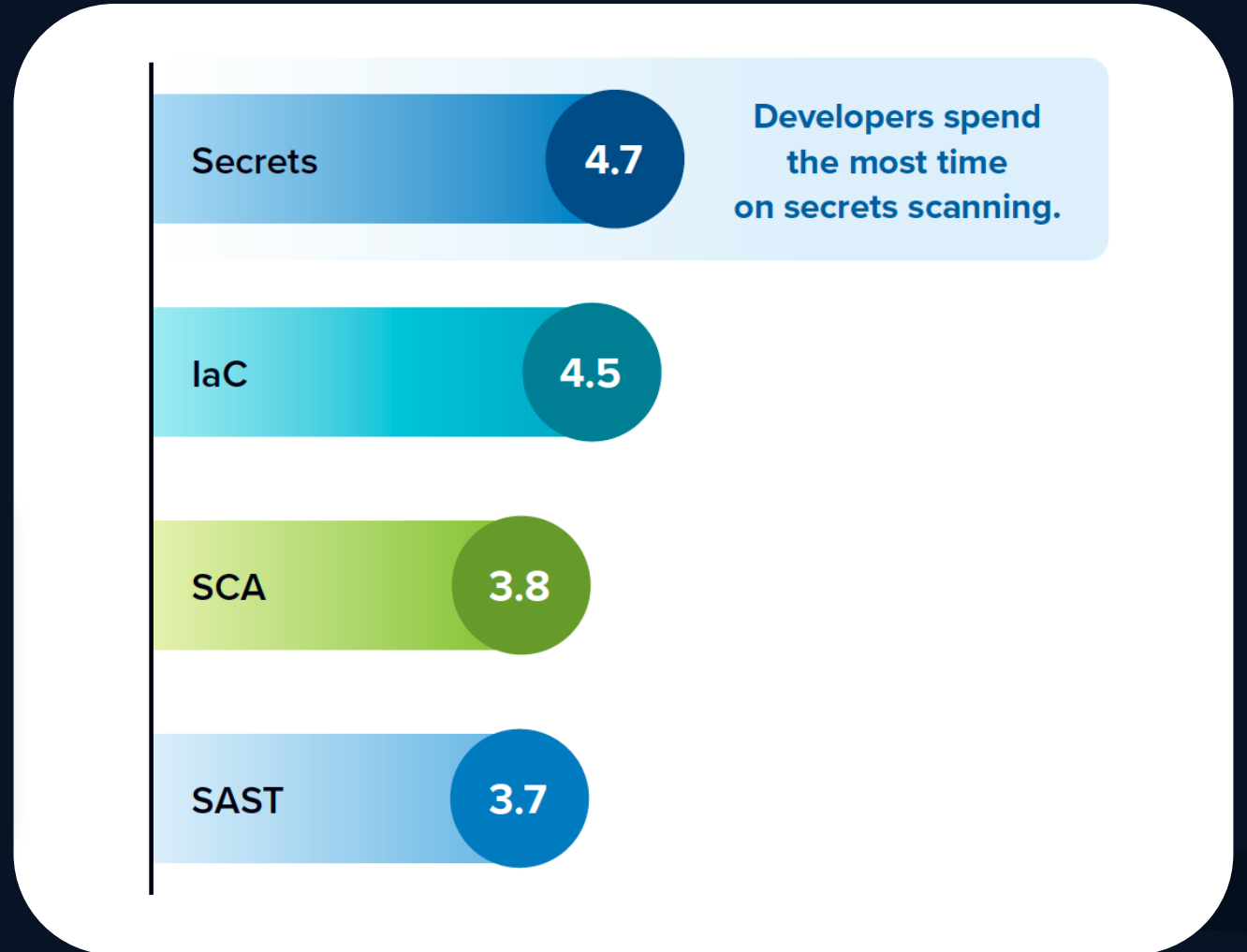
IMPACT BREAKDOWN

Big Picture:

Developers are spending an average of 3-5 hours per week on essential DevSecOps security scans

Where & What:

- Secrets - Interpreting results
- IaC - Every code change
- SCA - <60% code, binaries repos
- SAST - Just before prod deployment
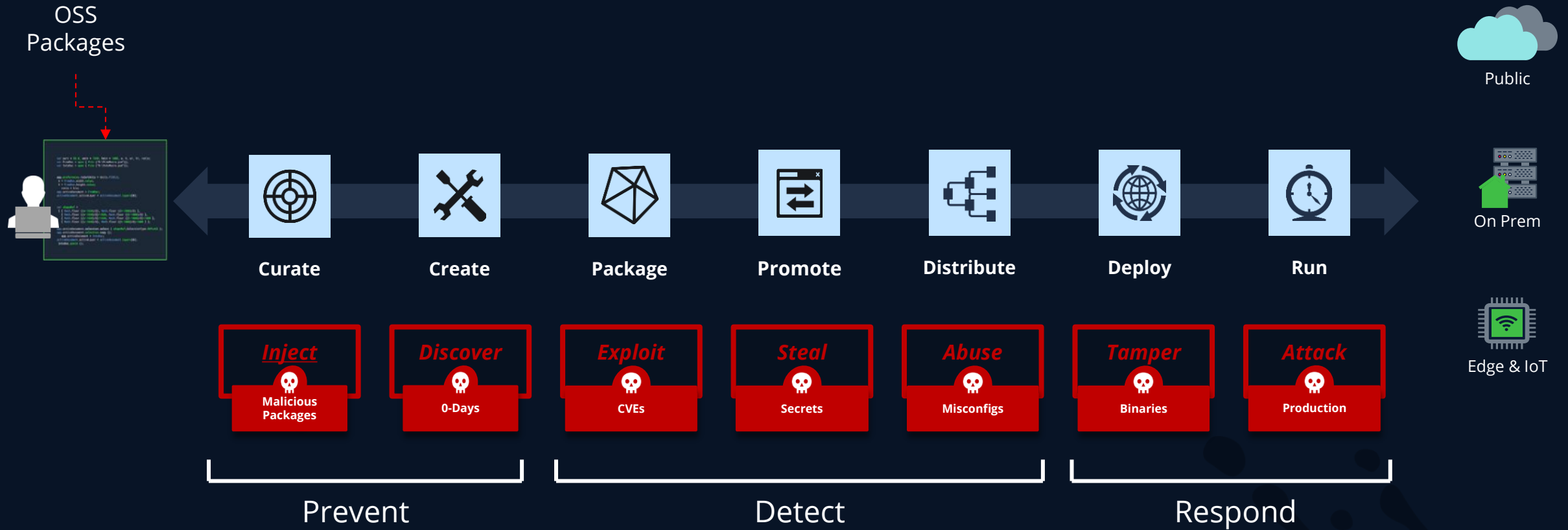
Secrets	4.7

Developers spend the most time on secrets scanning.

IaC	4.5
SCA	3.8
SAST	3.7

JFrog

DEVELOPERS
ARE THE CLEAR
TARGETS

BUT THEY ARE
TIRED OF SECURITY

Software Supply Chain Threats

OSS Packages

Public

On Prem

Edge & IoT

Curate	Create	Package	Promote	Distribute	Deploy	Run

Inject	*Discover*	*Exploit*	*Steal*	*Abuse*	*Tamper*	*Attack*
Malicious Packages	0-Days	CVEs	Secrets	Misconfigs	Binaries	Production

Prevent

Detect

Respond

JFrog

The JFrog Software Supply Chain Platform

Connect
Update, Control And
Manage Iot Fleets

IDE Plugin
SCA, Advanced
Security, SAST

JFrog Security
SCA, SBOM, Contextual Analysis,
Secrets, IaC, Misconfig Scans

Runtime
Impact & Integrity

Curation & Catalog
OSS package
curation & catalog

SAST
Source Code Scans

Public

Curate   Create   Package   Promote   Distribute   Deploy   Run

On Prem

Artifactory
Universal Binary
Management

Distribution
Distribute Releases
Across Endpoints

Frogbot
Scan Git repos
and Git pulls

Edge & IoT

SCM | Enterprise CI/CD | Pipelines | Release Lifecycle
Management | Monitoring | Binary and Identity Federation

JFrog CLI
Command Line
Interface

JFrog ML

Model Management | Serving | Monitoring |
Testing

JFrog

JFrog At A Glance

8000+
Customers as of FY24

83%
Fortune 100

1600
Employees

Nasdaq listed
FROG

The JFrog EveryOps Platform

DevOps

SecOps

MLOps

IOT

On Any Major Cloud (SAAS / Cloud /On-premises), Any Infra + Scales to Infinity

Cloud

Infra ENV

Integrated

HA, DR, 99.9%

Hybrid

Powering Industries

10/10	9/10	9/10	10/10	9/10
Top Finance	Top Retail	Top Healthcare	Top Technology	Top Transportation

A chain is only as **strong** as its weakest link!

Thomas Reid

Conclusion

- It's important to **consolidate** DevOps, Security & AI/ML toolsets

- Security is **everyone's** responsibility

- Automation of promotion is key to building pipeline **confidence**

- EveryOps is not one tool, not one approach... it's a need, it's the **future**

- **Come meet us at our booth #11**

Start for Free to learn more

JFrog