This presentation contains forward-looking statements that reflect our current views with respect to, among other things, the operations and financial performance of JFrog Ltd. and its subsidiaries (collectively, “JFrog,” “we,” “us,” or “our”). All statements other than statements of historical facts contained in this presentation, including statements regarding matters such as our industry, business strategy, goals, and expectations concerning our market position, future operations, margins, profitability, capital expenditures, liquidity and capital resources and other financial and operating information, may be forward-looking statements. We may, in some cases, use words such as “outlook,” “believes,” “expects,” “potential,” “continues,” “may,” “will,” “should,” “could,” “seeks,” “predicts,” “intends,” “trends,” “plans,” “estimates,” “anticipates,” or the negative version of these words or other comparable words that convey uncertainty of future events or outcomes, to identify forward-looking statements in this presentation. The forward-looking statements contained in this presentation are based on management’s current expectations and are subject to uncertainty and changes in circumstances. Although we believe that the assumptions underlying the forward-looking statements are reasonable, there can be no assurance that management’s expectations, beliefs, and projections will result or be achieved. There are a number of factors, many of which are beyond our control, that could cause actual results to differ materially from the results anticipated by these forward-looking statements, including, among others: larger well-funded companies shifting their existing business models to become more competitive with us; our ability to provide or adapt our platform for changes in laws and regulations or public perception, or changes in the enforcement of such laws, including relating to data privacy; the effects of companies more effectively catering to our customers by offering more tailored products or platforms at lower costs; adverse general economic and market conditions reducing spending on sales and marketing; the effects of declining demand for sales and marketing subscription platforms; our ability to improve our technology and keep up with new processes for data collection, organization, and cleansing; our ability to provide a highly accurate, reliable, and comprehensive platform moving forward; our reliance on third-party systems that we do not control to integrate with our system and our potential inability to continue to support integration; our ability to successfully integrate technology from recent acquisitions; our ability to adequately fund research and development potentially limiting introduction of new features, integrations, and enhancements; our ability to attract new customers and expand the existing subscriptions; a decrease in participation in our contributory network or increased opt-out rates impacting the depth, breadth, and accuracy of our platform; and our failure to protect and maintain our brand and our ability to attract and retain customers. Should one or more of these risks or uncertainties materialize, or should any of our assumptions prove incorrect, our actual results may vary in material respects from those projected in these forward-looking statements. Factors or events that could cause our actual results to differ may emerge from time to time, and it is not possible for us to predict all of them. Furthermore, many of the foregoing risks and uncertainties are, and will be, exacerbated by the COVID-19 pandemic and any worsening of the global business and economic environment as a result. Our forward-looking statements do not reflect the potential impact of any future acquisitions, mergers, dispositions, joint ventures, investments, or other strategic transactions we may make. We may not actually achieve the plans, intentions or expectations disclosed in our forward-looking statements, and you should not place undue reliance on our forward-looking statements. Any forward-looking statement made by us in this presentation speaks only as of the date of this presentation. We undertake no obligation to publicly update or review any forward-looking statement, whether as a result of new information, future developments, or otherwise, except as required by law.

This presentation includes certain financial measures not presented in accordance with generally accepted accounting principles in the United States (“GAAP”), including Non-GAAP Gross Margin, Non-GAAP Operating Income, Non-GAAP Operating Margin, Free Cash Flow, and Free Cash Flow Margin, which are used by management in making operating decisions, allocating financial resources, and internal planning and forecasting, and for business strategy purposes, and which have certain limitations, and should not be construed as alternatives to financial measures determined in accordance with GAAP. The non-GAAP measures as defined by us may not be comparable to similar non-GAAP measures presented by other companies. Our presentation of such measures, which may include adjustments to exclude unusual or non-recurring items, should not be construed as an inference that our future results will be unaffected by other unusual or non-recurring items.

This presentation includes market and industry data and forecasts that we have derived from independent consultant reports, publicly available information, various industry publications, other published industry sources, and our internal data and estimates. Independent consultant reports, industry publications, and other published industry sources generally indicate that the information contained therein was obtained from sources believed to be reliable. The inclusion of market estimations, rankings, and industry data in this presentation is based upon such reports, publications, and other sources and our internal data and estimates and our understanding of industry conditions. Although we believe that such information is reliable, we have not had this information verified by any independent sources. You are cautioned not to give undue weight to such estimates. All trademarks, service marks, and trade names appearing in this presentation are the property of their respective holders.
THE FROG LEAPS FORWARD

# WELCOME TO JFROG’S INVESTOR DAY

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
</table>
| 12:30 PM | Market Overview, JFrog Values & Vision  
Shlomi Ben Haim, CEO |
| 12:50 PM | Product Strategy & Differentiation  
Yoav Landman, CTO |
| 1:15 PM | Securing the Software Supply Chain  
Nati Davidi, SVP & Head of JFrog Security |
| 1:40 PM | Break |
| 1:50 PM | Voice of the Customer:  
Fidelity - Gerard McMahon - VP of Architecture, Head of Tools & Platforms  
Broadcom - Bill Morton - SBO, Head of DevOps Platform |
| 2:15 PM | Driving Growth at Scale  
Micheline Nijmeh, CMO |
| 2:40 PM | JFrog’s G2M Strategy, Hybrid Growth  
Tali Notman, CRO |
| 3:05 PM | Financials & Outlook  
Jacob Shulman, CFO |
| 3:30 PM | Open Q&A  
All Frogs |
| 3:45 PM | Program Concludes |
EVERYONE WANTS A PIECE OF DEVOPS
THE KEY RESULTS

THE MARKET IS ASKING FOR

- Automation – speed and secure flow
- Control and trust in software
- One platform that grows with market needs
- Modern software supply chain management
WHAT I SHARED WITH YOU 2 YEARS AGO...

Top software failures in recent history

The biggest software failures in recent history including ransomware attacks, IT outages and data leakages that have affected some of the biggest companies and millions of customers around the world.

By: Computerworld.com | February 01, 2020

Technology, you can’t live with it, you can’t live without it. Unfortunately, millions of users around the world have come to realize the latter over recent years due to a series of spectacular and thoroughly unwelcome, failures.

System Failure: The Boeing Crashes

How did aviation regulators allow the industry to reach this critical point? Investigating the factors that led to the tragedy.

Mobile bank goes dark for millions of customers as it seeks $5 billion valuation
BINARIES: THE CROSSROAD OF DEVOPS

Developers

Automation

Security

Monitoring

Observability

Runtime

Enterprise

Ops

BINARIES
BINARIES

(aka Software Packages, Artifacts, Containers, Images...)

have become the center of gravity for the modern Software Supply Chain
ONE LEAP
AT A TIME
2021: A YEAR OF INVESTMENT

- **29%** R&D
- **>200** TECH RELEASES
- **38%** SALES & MARKETING
- **~400** NEW EMPLOYEES
- **>300** COMMUNITY EVENTS
- **$300M+** M&A SPEND
2021: A YEAR OF RESULTS

1,000+ EMPLOYEES

$207M ANNUAL REVENUE

6,650 CUSTOMERS

39% YoY GROWTH RATE*

130% NDR*

>84% GROSS MARGIN

*Based on Q4 results
THE JFROG DEVOPS PLATFORM

JFrog MISSION CONTROL
Monitoring, Configuring, Admin Dashboard

JFrog ARTIFACTORY
Store and manage all binary software packages & container images

VCS
Source Code Repository

JFrog XRAY
Clear security & compliance issues

SECURE

DISTRIBUTE

JFrog DISTRIBUTION
Distribute to any data center production environment

Public Cloud Platforms
On-premise and Hybrid
Regional Clouds

DISTRIBUTE SECURE

JFrog CONNECT
Deploy, operate and monitor software in Edge/IoT devices

Distributed Edge
IOT Devices

JFrog PIPELINES
End-to-end CI/CD automation and orchestration

The Liquid Software Company

INVESTOR DAY
THE JFROG DEVOPS PLATFORM

DevOps

>$40B
RND & DevOps

DevSecOps

$17B
Security

Dev to IoT

$XXXB
Product Lead
STANDARDIZING ACROSS INDUSTRIES

9/10 TOP HEALTHCARE
8/10 TOP RETAIL
10/10 TOP FINANCE
10/10 TOP TECHNOLOGY
8/10 TOP TRANSPORTATION

Google  EMC²  Fidelity  Daimler  Walgreens  Games  University of San Diego  PennState

AMERICAN EXPRESS  Amazon  TomTom  Airbus  Chef  Adidas  RBC  Workday  Netflix  Yale

Bosch  GE  Costco  Snapchat  Hewlett Packard Enterprise  PayPal  Mercedes-Benz  Bose  Macy’s  FICO  Volkswagen

Airbnb  Berkeley Lab  Tableau  ASU  Arizona State University  Barclays  ING  Audi  Cloudera Broadcom

Verizon  Bank of England  Stanford University  Intuit  VMware  BT  Ohio University  United Airlines  Adobe

Microsoft  PagerDuty  Dell  Intel  Uber  Ansys  BMW  Kroger  1box  Deutsche Bank
LIQUID SOFTWARE WILL TOUCH EVERY ORGANIZATION

SOFTWARE IS EATING THE WORLD

EMPOWER developers & engineers
Automate for speed and security

DIGITIZE everything
To build competitive advantages

CONNECT & update
Liquid experiences to delight customers
LIQUID SOFTWARE WILL TOUCH EVERY ORGANIZATION

THE WORLD IS EATING SOFTWARE

EMPOWER developers & engineers
Automate for speed and security

DIGITIZE everything
To build competitive advantages

CONNECT & update
Liquid experiences to delight customers
## WHY CUSTOMERS CHOOSE JFROG

<table>
<thead>
<tr>
<th>EXISTING OFFERINGS</th>
<th>WHY JFROG WINS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOME-GROWN &amp; IN-HOUSE SOLUTIONS</td>
<td>Enterprise-level scale</td>
</tr>
<tr>
<td>DEVOPS &amp; DEVSECOPS FOCUSED COMPANIES</td>
<td>Binary-centric</td>
</tr>
<tr>
<td>CLOUD PROVIDERS</td>
<td>Breadth &amp; depth of functionality</td>
</tr>
<tr>
<td>DIVERSIFIED VENDORS</td>
<td>End-to-end platform</td>
</tr>
</tbody>
</table>
Can speed be achieved without automation?

Do companies know what’s being brought into their organizations?

Do companies know what’s in their runtime environments?

Is the world going hybrid? Multi-cloud? Updating at the edge?
THE FOUNDATIONS
OF OUR SUCCESS

Vision, Values & People

Technology & Innovation

Business & Customers
MAY THE FROG BE WITH YOU
PRODUCT STRATEGY & DIFFERENTIATION
WHAT’S IN A BINARY

OSS + OWN SOURCE CODE

- e.g., C, C++, C#, java, node.js, python, go

Compilation

BINARY FILE

- e.g., jar, zip, gzip, exe, dll, elf, so, rm, sh
- Compilation

Build & Packaging

Expensive and non-reproducible

APPLICATION “BINARY OF BINARIES”

- e.g., Container, firmware, android app (apk), iphone app (ipa), msi, zip, rar

Contains more than just code!
Code blueprints converted to executable format

Expensive and non-reproducible

Contains a full release
3rdp + inner sourcing

Servers

Web Service

IoT Device

Desktop/ Mobile

JFrog

The Liquid Software Company
UPDATING SOFTWARE: 10K FEET VIEW

- Developer writes source code
- Source is packaged to a managed binary format → software
- Software passes security and quality checks
- Software is distributed to where it can be accessed by the runtime
- Runtime gets a new software update
EVERY SOFTWARE UPDATE IS A FLOW OF BINARIES

- **JFrog MISSION CONTROL**
  - Monitoring, Configuring, Admin Dashboard

- **JFrog ARTIFACTORY**
  - Store and manage all binary software packages & container images

- **JFrog XRAY**
  - Clear security & compliance issues

- **JFrog DISTRIBUTION**
  - Distribute to any data center production environment

- **JFrog CONNECT**
  - Deploy, operate and monitor software in Edge/IoT devices

- **JFrog PIPELINES**
  - End-to-end CI/CD automation and orchestration

- **JFrog INSIGHT**
  - Analyzing Intelligence Metrics

- **Source Code Repository**
- **VCS**

- **Public Cloud Platforms**
  - AWS
  - Microsoft Azure
  - Google Cloud

- **On-premise and Hybrid Regional Clouds**

- **Distributed Edge**
  - IOT Devices
JFROG ARTIFACTORY: THE DATABASE OF DEVOPS

Maven

IMPORT

npm

DISTRIBUTE

JFrog ARTIFACTORY +30 TECHNOLOGIES
Unified DevOps Platform

Scale

Universal Tech

Too Integrated to fail

Hybrid, Multi-cloud, Multi-region
TRUSTED SOFTWARE
SINGLE SOURCE OF TRUTH

- Tracking the journey of your binaries to Runtime → Trust
- **SBOM** - what ends up in your software
- Antifactory keeps unique **SBOMs** to track the composition of applications:
  - BuildInfo
  - ReleaseInfo
  - PipeInfo
TRUST IS MAINLY BUILT ON BINARIES

Source: MITRE, Deliver uncompromised -- Securing critical software supply chains, January 2021
CENTRAL SECURITY THROUGH MANAGED BINARIES

ONE OF THE TOP 3 BANKS IN THE US:

All vulnerable production applications turn safe IN UNDER 12 HOURS
JFROG XRAY: HOLISTIC PRODUCT SECURITY APPROACH

- Strongly integrated with Artifactory to protect your binaries
- Unique graph database for impact analysis

Security Management & Policies
Granular, consistent policy enforcement
Informed decisions based on accurate data

SOFTWARE COMPOSITION ANALYSIS
Security & license compliance issues in third-party software

CONFIGURATION SECURITY
Software configuration issues and product security malpractices

ZERO-DAY VULNERABILITY DETECTION
Potential unknown vulnerabilities in proprietary code

Security Research
Continuous enrichment of security data & scanning technology
Vulnerability discovery - 400+ disclosures to date
JFROG DISTRIBUTION: ACCELERATING DELIVERY

INTERNAL DISTRIBUTION
- Sharing artifacts with remote global workforce

EXTERNAL DISTRIBUTION
- Sharing packages and APIs by customers/partners

RUNTIME DISTRIBUTION
- Private Distribution closer to runtime
- Handle update bursts
- Allow disconnected distribution

FEDERATED REPOS

ARTIFACTORY EDGE

PDN
DISTRIBUTING APPLICATIONS AT SCALE

LARGE INVESTMENT BANKING FIRM IMPLEMENTING THE DISTRIBUTION OF:

1,000s of signed applications, using 10s different technologies, developed by 10,000s of developers, distributed to 10s of different global locations
**JFROG CONNECT:** DEPLOYS FOR CONNECTED DEVICES

- **UPDATE** any Linux-based device
- **MANAGE** software supply-chain (SBOM)
- **KEEP TRACK** of software versions in large fleets
- **REMEDIANTE** failures remotely
- **MONITOR** devices behavior in the field
LOW CODE UPDATE FLOWS

- Use drag-and-drop interface for building complex update scenarios
- Deploy binary files, containers, VM images, configuration files
- Execute scripts and commands remotely
- Remediate errors with granular rollbacks
EXPANDING LEFT AND RIGHT

- Onboard developers at their desktop
- Binary curation into the organization
- Runtime tracking and protection
DEMO: E2E OVER THE AIR SOFTWARE UPDATE

NEW YORK DEVICES

DUBLIN DEVICES

APPLICATIONS + SBOM

BUILD
JFrog customers utilize a unique, automated E2E Solution for Managing the Flow of Binaries to the Runtime to achieve TRUSTED SOFTWARE UPDATES.
SECURING THE SOFTWARE SUPPLY CHAIN
THE BINARY FROM THE ATTACKER’S POV

Log4j, SolarWinds, BlueKeep, Heartbleed

Were all consumed, integrated, deployed and distributed as a binary, not as a source code

SOURCE CODE
- e.g., C, C++, C#, java, node.js, python, go

BINARY FILE
- e.g., exe, dll, elf, so, rm, sh

APPLICATION
- "BINARY OF BINARIES"
- Contains far more than just code!
  - 3rdp + inner sourcing

Binaries MUST be analyzed, monitored and protected
WHAT COULD THE ATTACKER EXPLOIT IN A BINARY FILE?

1. Known vulnerabilities in 3rd Party software (“CVEs”), OSS or Commercial

2. Malicious code pre-injected intentionally via supply chain

3. Unknown vulnerabilities in 1st and 3rd party code (“Zero-days”)

4. Non-code issues: misconfigurations, encryption, private keys, OS issues
THE NEXT GENERATION OF XRAY
END TO END SOFTWARE SUPPLY CHAIN SECURITY

- **Contextual SCA & CVE Applicability**
  - Enhanced research data and Applicability Scanners

- **Malicious Code Detection**
  - Malicious code pre-injected intentionally via supply chain

- **Contextual Security-Focused SAST**
  - 1st and 3rd party potential Zero-days

- **Configuration Security**
  - Misconfigurations e.g., bad encryption, OS issues, private keys & credentials

Role infographic:
- **Dev**
  - Engineering leader
  - DevOps
  - Automation engineer
  - Quality engineer

- **Sec**
  - CISO, CSO, CPSO
  - Product security leader
  - Security architect
  - Security engineer
  - AppSec leader
  - DevSecOps leader
  - Security champion in dev

JFrog connectors:
- **JFrog Artifactory**
- **JFrog Distribution**
- **JFrog Connect**
- **JFrog Pipelines**
APPROACH VS. COMPETITORS
“... we are approaching the point of convergence of source and binary analysis... in two cases static (binary) analyzers were even able to discover one vulnerability they could not find in the original source code...”

EUROCOM FRANCE AND ARIZONA UNIVERSITY, DARPA SUPPORTED FA875019C0003, FEB 2022

“The software of the connected device is evaluated by a test laboratory using automated binary analyzers.”

CSA SINGAPORE, NOV 2021

“...those requesting SBOM data should try to obtain it from the instance of the build...”

U.S. NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION (NTIA), JULY 2021
# FROM APPSEC TO E2E SW SUPPLY CHAIN SECURITY

<table>
<thead>
<tr>
<th>Common Approach</th>
<th>Modern, Comprehensive Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naïve SCA (commoditized)</td>
<td>Binary-based, contextual SCA via proprietary applicability scanners</td>
</tr>
<tr>
<td>SBOM data and licenses info only</td>
<td>Research data including malicious packages and zero-days early notice</td>
</tr>
<tr>
<td>Manual PT for non-code issues</td>
<td>Binary-based configuration security with special focus on containers and embedded</td>
</tr>
<tr>
<td>Source code base SAST/DAST</td>
<td>Binary &amp; source based analysis to protect your IP and reduce FP</td>
</tr>
<tr>
<td>Basic remediation info</td>
<td>Detailed mitigation and remediation instructions and automation</td>
</tr>
<tr>
<td>Separate container security</td>
<td>One universal solution for any kind of image or binary</td>
</tr>
<tr>
<td>Disconnected security solution</td>
<td>Part of a platform that guards all SW assets across the entire supply chain</td>
</tr>
<tr>
<td>Common Approach</td>
<td>Modern, Comprehensive Approach</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Naïve SCA (commoditized)</td>
<td>Binary-based, contextual SCA via proprietary applicability scanners</td>
</tr>
<tr>
<td>SBOM data and licenses info only</td>
<td>Research data including malicious packages and zero-days early notice</td>
</tr>
<tr>
<td>Manual PT for non-code issues</td>
<td>Binary-based configuration security with special focus on containers and embedded</td>
</tr>
<tr>
<td>Source code base SAST/DAST</td>
<td>Binary &amp; source based analysis to protect your IP and reduce FP</td>
</tr>
<tr>
<td>Basic remediation info</td>
<td>Detailed mitigation and remediation instructions and automation</td>
</tr>
<tr>
<td>Separate container security</td>
<td>One universal solution for any kind of image or binary</td>
</tr>
<tr>
<td>Disconnected security solution</td>
<td>Part of a platform that guards all SW assets across the entire supply chain</td>
</tr>
</tbody>
</table>
FROM APPSEC TO E2E SW SUPPLY CHAIN SECURITY

Source-code-based Application Security Testing starts and end in the development phase

Repositories

Interim & Nightly
- Third-party code
- Proprietary code
- Config files & scripts

Release Gatekeeping

Open-source
Commercial
FROM APPSEC TO E2E SW SUPPLY CHAIN SECURITY

DEVELOP
- Repositories
  - Open-source
  - Commercial

BUILD
- Interim & Nightly
  - Third-party code
  - Proprietary code
  - Config files & scripts

DEPLOY & UPDATE
- Release Gatekeeping

- Secure Component Selection
- Automated Security in Build Process
- Security Validation for Release Approval
- Continuous Vulnerability Monitoring and Runtime Security

POST DEPLOYMENT
CASE STUDY SECURITY PERSONA AS AN ENTRY POINT

VENDOR CHARACTERISTIC

- Main division in a leading enterprise-network vendor
- Heavily regulated
- Use entire AppSec suite with all traditional AST tools
- Use case: software gatekeeper for new releases
- Concrete needs: (1) find vulnerabilities before the attackers do (2) Customers scan the vendors’ accessible binaries and introduce risk which does not exist

ENGAGEMENT FLOW

POC
- Flagship network enterprise product
- 14 zero-day vulnerabilities found in a single scan
- None of the AppSec tools found it
- Additional information on exploitability of known CVEs that reduced vendors’ overhead

Land
- 6 digits, 3 years commitment
- Persona: CTO of the organization and product security leader
- Full build scans of 3 flagship products’ software stack (yearly)

Expand
- Introduction of the entire platform
- Initiation of Artifactory POC for embedded software management
- Introduction to more personas and divisions in the org
THE SECURITY RESEARCH EXPERTISE

Spreading security knowledge & enabling automated analysis enhancements

- Discover and disclose new OSS vulnerabilities
- Respond promptly to any newly discovered vulnerabilities to feed the platform with up-to-date data
- Analyze novel attack methods and how to discover them automatically
- Help the community and the customers with advanced security challenges

Strengthen our brand, generate new leads and drives expansion with existing customers

100 SECURITY ENGINEERS & RESEARCHERS

450+ ZERO-DAY VULNERABILITIES DISCOVERED
LOG4J/LOG4SHELL JFROG SECURITY BEHIND THE SCENES

[A] Promptly **update** the platform (Artifactory and Xray) with detailed research data

[B] Release to the community open-source **tools** to look for Log4Shell vulnerabilities in binary JAR files

[C] **Research** further to detect hundreds of vulnerable packages that use Log4j and additional Log4j issues
The power of top-notch security research group

The power of the platform and its control over software assets

The power of binary analysis that enables contextual analysis
**RESEARCH CONTRIBUTION TO THE COMMUNITY**

Since July 2021

*Based on aggregation of articles published on the competing vendors websites and on CVEs attributed to their teams by 3rd party organizations*

<table>
<thead>
<tr>
<th></th>
<th>JFrog</th>
<th>Snyk</th>
<th>GitLab</th>
<th>Sonatype</th>
<th>WhiteSource</th>
</tr>
</thead>
<tbody>
<tr>
<td>High severity zero day vulnerabilities in OSS</td>
<td>22 (6)</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Low/Med severity zero day vulnerabilities in OSS</td>
<td>15 (9)</td>
<td>31</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Malicious Packages</td>
<td>39 (28)</td>
<td>3</td>
<td>0</td>
<td>19</td>
<td>15</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>76 (43)</strong></td>
<td><strong>39</strong></td>
<td><strong>0</strong></td>
<td><strong>19</strong></td>
<td><strong>16</strong></td>
</tr>
</tbody>
</table>

(Confirmed, unpublished)
JFROG SECURITY TEAM AND XRAY EVOLUTION

Q3 2021 DEV MILESTONE 1
- New 700+ High Profile CVE entries added to XUC DB
- Remediation & mitigation steps
- Gadgets infrastructure for rapid development of applicability scanners
- Jira integration

Q4 2021 DEV MILESTONE 2
- 170+ new applicability scanners
- CVE Contextual Analysis for containers
- Malicious packages detection
- Git dependency scanning
- On-demand scanning

2022
- Embedded SW support
- Zero-day analysis
- Configuration Security
- Operational risk
- Product Security UX
- Security dashboard
JFROG SECURITY TEAM AND XRAY EVOLUTION

Announcing completion of 1st integration phase and the release of substantial enhancements:

1. **CVE research data & remediation alternatives** - SaaS and Self-Hosted
2. **Malicious packages data** - SaaS and Self-Hosted
3. **Contextual analysis for containers** - SaaS only (Self-Hosted later this year)
JFrog INVESTOR DAY LEAPING THROUGH 2022
Managing DevOps in a Digitally Transforming Enterprise at Scale

Gerard McMahon, Fidelity

February 15, 2021
Disclaimer

This presentation is a case study of the Fidelity Investments experience. It is not an endorsement or recommendation of any vendor, product or service.
About Me

• VP Architecture in Enterprise Cloud Computing (Head of ALM Tools & Platforms)
• Co-chair, Fidelity’s DevOps Council
• ~30 years’ experience in architecture, design, development
• At Fidelity since 2006
1946
Fidelity Management & Research Company Founded

1965
Fidelity Purchases First Computer

1995
Fidelity Becomes an Internet Pioneer with First Mutual Fund to Create a Home Page

1995

2016
Fidelity’s First Product Application Deployed to the Cloud

2019
Fidelity Launches Multi-Cloud & Hybrid Strategy

Today
4,600 Applications on Public Cloud

~55K Employees

~16k Technologists

More to transform…
## Enterprise Cloud Strategy

### Vision

Execute on an enterprise cloud platform strategy accelerating delivery of new capabilities, providing access to innovation and delivering value to our customers and for Fidelity.

### Objectives

- Efficiency through common architecture and standards
- Increased stability and controlled risk through production support model
- Financial accountability and effective resource utilization
- Unified focus brings improved productivity and collaboration
- Manage CSP dependencies and vendor concentration risk

### Focus Areas

<table>
<thead>
<tr>
<th>Cloud Computing</th>
<th>Unified Plan</th>
<th>Security</th>
<th>Accountability</th>
<th>Workforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable core AWS and Azure services and automate development pipelines</td>
<td>Develop and execute on a unified Fidelity plan and Firm Foundation initiatives (Cloud, API, Data)</td>
<td>Establish standards and automatic software updates to align with security best practices</td>
<td>Drive financial accountability through robust FinOps practice</td>
<td>Optimize workforce through training and change management</td>
</tr>
</tbody>
</table>

**Enterprise Cloud Computing (ECC)**

*One Unified Team*
Our Digital Transformation Journey: Securing the Software Supply Chain

~4600 cloud apps, ~16k developers

Software Supply Chain Continuous Security

Continuous Development
Continuous Integration
Continuous Testing
Continuous Delivery
Continuous Verification
MultiCloud Deployment

Code
Binaries

3rd Party & OSS
90% of our inventory
Software Business Operations (SBO) DevOps Platform Team

Supporting:

- Both Software and Hardware DevOps Platforms
- 23 Business Units (BUs) across Broadcom
- 5 BUs in Broadcom Software Group (BSG: CA Tech, Symantec)
- SaaS Platform Engineering and Services Teams
- All Acquisition Integration Projects (SW & Semiconductors) & Divestitures
- InfoSec, Legal, Compliance and Audit teams
- 100s of DevOps teams across Broadcom
- 16K+ Product Engineers
- CI/CD Pipeline for SaaS Applications
- 900+ DevOps Application Instances
- 30+ DevOps Applications
- 100+ Integrations
- 100+ Plugins (many are home grown)
DevOps Platform: Facilitating Product DevOps Teams across BSG

As an example working with 1BU: Symantec DevOps Teams
How DevOps Platform Standards are Established
Origins of Standard DevOps Stack for Software Business Operations (SBO)

- Broadcom-wide Evaluation/POC Process involving DevOps teams & SBO
- Tracking industry Trends and Standards
- Acquisitions
Artifactory Usage in Broadcom Software Group (BSG)
Universal Artifact/Binary Management System and Source of Truth for CI/CD

- 3rd party binary object dependencies
- Broadcom approved OS images
- Intra-product dependencies
- Various binary type registry and management (Docker, Helm, Maven, NPM, Python, RPM and many more)
- Build Information records
- Security and Vulnerability Scanning
- BSG Pipeline

Broadcom Software users: 6000+
BRCM Semiconductor users: 400+
Artifactory
Center of the CI/CD Pipeline: proxy, source of truth, deployment hub
Artifactory Analogy
Facilitating the Supply Chain

Continuous Integration (CI)
- OpenSource/Git
- Package Mgrs
- Proxy
  - Artifactory XRay
- Build

Continuous Deployment (CD)
- Package
- Binaries
- Deploy
- Artifactory

Sources
- Storage/Transport
- Ingredients
- Refrigerator
- Cook

Meal
- Package
- Smart Refrigerator
- Serve
Additional JFrog Platform Tools used @ Broadcom

Xray & Vdoo
- Xray provides integrated Security & Vulnerability Scanning & Vdoo provides Zero Day detection
- Was used for log4j scanning and mitigation

Distribution Control
- Used for Product Releases and is integrated with BRCM Customer Support Portal (CSP)

Mission Control
- Single access point for managing multiple JFrog Platform Deployments
- Primarily used for ease of administration of multiple instances of JFrog instances across DCs

JFrog SaaS
- BinTray Replacement: Current usage of JFrog SaaS (BinTray replacement) is to provide released Docker images and certain other software packages to Broadcom’s external customers
DELIVERING VALUE TO COMMUNITY & CUSTOMERS

COMMUNITY MEMBERS
- Universal integrations for freedom of choice
- Open source communities
- Low barrier to entry to the JFrog Platform

SECURITY TEAMS
- Security as a Platform entry point
- Secure binary repository
- World class security experts & research

PRODUCT LEADERS
- Streamline, standardized Approach across entire SDLC
- Automation efficiencies
- DevOps modernization
GROWTH OPPORTUNITIES

PLATFORM ADOPTION
- Bottom-up
- Inbound
- Cloud & On Prem Free
- Community Events

ACCELERATING GROWTH IN THE ENTERPRISE
- Outbound
- Field Marketing
- Co-marketing/Cloud adoption

EXPAND IN KEY INTERNATIONAL MARKETS
- European and APAC region Investments Partnerships

PUBLIC SECTOR
- Iron Bank
- FedRamp
BUILD FOUNDATION FOR SCALE

MARKETING MOTION
- Product-led
- Inbound
- Outbound
- Cross-sell

GROWTH AVENUES
- Win the Hearts & Minds of Developer
- Accelerate Growth in the Enterprise
- Global expansion – EMEA/APAC
JFROG G2M
STRONGER FASTER
## THE FOUNDATION OF FUTURE GROWTH

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>ADOPTERS</th>
<th>JFROG SOLUTION</th>
<th>SALES MOTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agile Software Development</td>
<td>Individuals (Engineers)</td>
<td>Single Product</td>
<td>• Bottom-up</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Self serve</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Low touch</td>
</tr>
<tr>
<td>Software Supply Chain</td>
<td>Eng. teams &amp; Super DevOps</td>
<td>Integrated product</td>
<td>• Enterprise</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Inside sales</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Direct</td>
</tr>
<tr>
<td>Digital Transformation</td>
<td>Organizations</td>
<td>E2E Platform</td>
<td>• Top-down</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Strategic sales</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Indirect</td>
</tr>
</tbody>
</table>
E2E PLATFORM EXPANSION
WIRELESS NETWORK OPERATOR

2014-2015
Basic Binary MGMT capabilities (Pro) $30K

2016-2018
Team expansion and HA enhancement (Enterprise) $250K

2019
Adoption of XRay (EnterpriseX) $550K

2020
DevOps standardization of JFrog Platform (Enterprise+) $1,000K

2021
Distribution to Edge points (Enterprise+) $1,900K

5G Cellular Towers Update

Global Technology Services
TIERED, FOCUSED SALES STRUCTURE
DRIVING RAPID GROWTH

LOW-MID TOUCH INSIDE SALES

Exist:
- All size offering
- Solution & model based cross sell
- Ecosystem integrations

New:
- Outbound sales
- Security focus
- Hybrid sales team

HIGH-TOUCH STRATEGIC SALES

Exist:
- Established 2020
- Global team structure (AE, SE, ESL)
- Experienced leadership

New:
- Indirect sales: top GSIs, Cloud Partners
- Premium support
- Industry based expertise
$100K CLUB

- 2018: 131 customers, 38% of Total ARR
- 2019: 235 customers, 46% of Total ARR
- 2020: 352 customers, 51% of Total ARR
- 2021: 537 customers, 57% of Total ARR

Legend:
- Blue: # of Customers
- Green: % of Total ARR
NEW ROUTES TO REVENUES

CLOUD FIRST
- Cloud<>SH merged teams
- Cloud sales incentives
- Cloud partner co-sell

PARTNER & ALLIANCE
- Partner program: Targeting top GSIs
- Cloud Alliance transition

GEO EXPANSION
- APAC: JFrog direct
- Channel Partner
- Multi-cloud establishment

TECH INNOVATION
- SSC as an Ent scale driver
- Security entry point
- IOT green field
DELIVERING ON OUR GOALS
BUILDING DIVERSIFIED BUSINESS
LONG-TERM MODEL
DELIVERING ON OUR GOALS

BUILDING DIVERSIFIED BUSINESS

LONG-TERM MODEL
STRONG REVENUE GROWTH

ANNUAL REVENUE

($M)

<table>
<thead>
<tr>
<th>Year</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020</td>
<td>151</td>
</tr>
<tr>
<td>2021</td>
<td>207</td>
</tr>
</tbody>
</table>

37% Growth

| Territory         | Revenue
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>75%</td>
</tr>
<tr>
<td>Rest of World</td>
<td>25%</td>
</tr>
</tbody>
</table>

REVENUE BY TERRITORY*

QUARTERLY REVENUE TREND

($M)

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1'20</td>
<td>33</td>
</tr>
<tr>
<td>Q2'20</td>
<td>36</td>
</tr>
<tr>
<td>Q3'20</td>
<td>39</td>
</tr>
<tr>
<td>Q4'20</td>
<td>43</td>
</tr>
<tr>
<td>Q1'21</td>
<td>45</td>
</tr>
<tr>
<td>Q2'21</td>
<td>49</td>
</tr>
<tr>
<td>Q3'21</td>
<td>54</td>
</tr>
<tr>
<td>Q4'21</td>
<td>59</td>
</tr>
</tbody>
</table>

75% Self-Managed
25% SaaS

REVENUE BY SUBSCRIPTION TYPE*

* Represents actual results in Q4'21
CONTINUED GROWTH

SAAS REVENUE GROWTH
- Q4'20: $33M, 52% Growth
- Q4'21: $50M

>$100K CUSTOMERS
- Q4'20: 352
- Q4'21: 537, 53% Growth

>$1M CUSTOMERS
- Q4'20: 10
- Q4'21: 15, 50% Growth

TRAILING 4 QUARTER NDR TREND
- Q4'20: 133%
- Q1'21: 130%
- Q2'21: 129%
- Q3'21: 129%
- Q4'21: 130%
* One-time payment related to holdback agreements associated with acquisitions
DELIVERING ON OUR GOALS

BUILDING DIVERSIFIED BUSINESS

LONG-TERM MODEL
SUSTAINABLE GROWTH WITHIN CUSTOMER BASE

85% of Fortune 100\(^{(1)}\)

45% of Fortune 500\(^{(1)}\)

30%+ of Global 2000\(^{(1)}\)

(1) As of 12/31/2021

FORTUNE 500 ACCELERATED GROWTH

- 2019: 26%
- 2020: 38%
- 2021: 38%

(1) As of 12/31/2021
INCREASING ADOPTION

REVENUE BY SUBSCRIPTION

Q1'20  Q2'20  Q3'20  Q4'20  Q1'21  Q2'21  Q3'21  Q4'21

E+  Enterprise  Pro & Pro X

CUSTOMER COUNT BY SUBSCRIPTION

Q1'20  Q2'20  Q3'20  Q4'20  Q1'21  Q2'21  Q3'21  Q4'21

E+  Enterprise  Pro & Pro X
>2X IN 3 YEARS
NEW CUSTOMER TRENDS

2020

- 40% Self Managed
- 60% SaaS

ASP - $10K

2021

- 58% Self Managed
- 42% SaaS

ASP - $11K
DELIVERING ON OUR GOALS
BUILDING DIVERSIFIED BUSINESS
LONG-TERM MODEL
Q1’22 & FY2022 GUIDANCE

Q1’22
- Revenue: $60.8M - $61.8M
  (36% growth at mid-point)
- Operating Income: $(0.5M) - $0.5M
- EPS: $(0.01) - $0.01

FY2022
- Revenue: $273M - $275M
  (33% growth at mid-point)
- Operating Income: $(1.0M) - $1.0M
- EPS: $(0.01) - $0.01
R&D INVESTMENTS

INNOVATION
PRODUCTS
INFRASTRUCTURE
GLOBAL SCALE

Non-GAAP R&D % of Revenue

Q1'20 Q2'20 Q3'20 Q4'20 Q1'21 Q2'21 Q3'21 Q4'21

- $8M
- $9M
- $10M
- $12M
- $14M
- $16M
- $18M

25% 23% 23% 24% 26% 28% 30% 30%

INVESTMENTS
S&M INVESTMENTS

Non-GAAP R&D % of Revenue

COMMUNITY
GLOBAL EXPANSION
STRATEGIC
CHANNELS
PARTNERSHIPS
## LONG-TERM MODEL

<table>
<thead>
<tr>
<th>% of Revenue</th>
<th>FY'21</th>
<th>LONG-TERM TARGET MODEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gross Margin</td>
<td>84%</td>
<td>80%</td>
</tr>
<tr>
<td>Research &amp; Development</td>
<td>29%</td>
<td>21%</td>
</tr>
<tr>
<td>Sales &amp; Marketing</td>
<td>38%</td>
<td>27%</td>
</tr>
<tr>
<td>General &amp; Administrative</td>
<td>16%</td>
<td>9%</td>
</tr>
<tr>
<td>Operating Margin</td>
<td>2%</td>
<td>23%</td>
</tr>
<tr>
<td>Free Cash Flow Margin (1)</td>
<td>21%</td>
<td>30%</td>
</tr>
</tbody>
</table>

(1) Normalized for $19.0 million one-time payment related to holdback agreements associated with acquisitions.
30%+ GROWTH FOR THE FORESEEABLE FUTURE