digital.ai™

2023 APPLICATION SECURITY THREAT REPORT

Security Threats for Apps “In the Wild”

Quantifying the risks for applications that operate outside a firewall

Contents

digital.ai

Introduction and Key Findings

The term “in the wild,” made popular by the American TV series *Silicon Valley*, depicts software set free into the world and is no longer under the author’s control. That applies to applications, and of course it also applies to the malware and viruses created to compromise apps and penetrate firewalls.

Unfortunately, the vast majority of cybersecurity research examines threats to apps operating inside a firewall (“in the zoo”). But with a staggering 100 billion mobile apps downloaded in 2021 alone[1], it has become clear that apps in the wild are pervasive, and the dearth of monitoring and research of apps in the wild only exacerbates the security risk.

Therefore, this study aims to help security professionals safeguard their apps and users from malicious activities by illuminating and quantifying the threats to applications in the wild.

Key Findings

01 **Attack Probability:** The study found that 57% of monitored apps experienced at least one attack.

02 **Industry Vulnerability:** Gaming and financial services (FinServ) apps face the highest risk of attack (63% and 62%, respectively). The likelihood of attacks in other industries is slightly lower (54%) but remains a significant concern.

03 **Android vs. iPhone:** Android apps are more likely to be targeted than iPhone apps (76% vs. 55%, respectively); however, the difference in the likelihood of attack was smaller than predicted.

04 **Attack Vector and Outcome:** The popularity of an app is not correlated with the likelihood of attack on an app: In many cases, less popular apps were attacked more often than popular apps.

[1]https://www.businessofapps.com/data/app-statistics/

Terminology

Application or App: One discrete executable that runs on a mobile operating system, in a browser, or on a desktop/server operating system.

Consumer: The end-user of applications created by the organization that protects the apps they create.

Instance: One discrete executable on a single consumer's phone.

Attack: Any action taken on a mobile/web/desktop app that violates the EULA (End User License Agreement) of the organization creating the app and/or the App Store/Play Store.

Guard: A protection added to an application to frustrate reverse engineering attempts.

FinServ App: Any consumer-facing application created by a bank, insurance company, credit card issuer, or payments platform.

Gaming App: Any web, mobile, or desktop app used to play games, exclusive of apps used to place bets or to gamble.

All Other Verticals: An application made by an organization in any industry other than the gaming or FinServ industry — for instance, medical devices, manufacturing, online retail, etc.

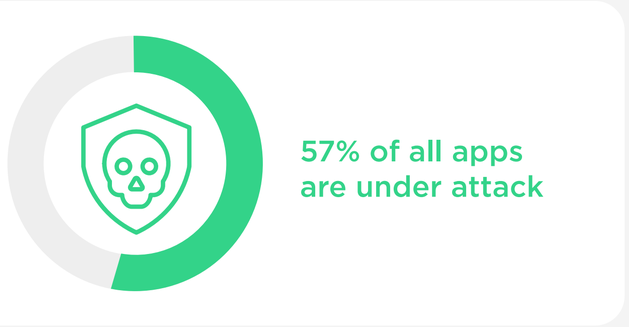
digital.ai™

How at Risk Is Your App?

The study captures a point-in-time baseline of current threats to apps. This benchmark makes it easier for stakeholders to measure and analyze future changes in the threat landscape.

Overall Threat Level

Based on 20 years of closely observing threat actors, recent risk trends, and preliminary data, the study's authors initially hypothesized that the likelihood of any app running in an unsafe environment would be greater than 50%. The actual figure was significantly higher: 57%.



57% of all apps are under attack

The confluence of several factors helps to explain the high likelihood of attack in 2023:

- **The pace of tool democratization** among threat actors has accelerated. Reverse-engineering tools such as Ghidra and dynamic instrumentation toolkits such as Frida have recently become more sophisticated and popular.
- **The advent of cryptocurrencies** and even Venmo make it much easier for threat actors to "cash out" of schemes, particularly if ransomware is involved.
- **The nationalization of attacks** has opened up enormous resources for threat actors.

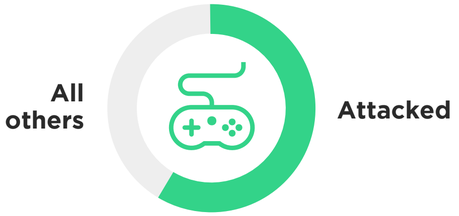
Risk to Apps By Industry

Financial Services and Gaming Industries

After analyzing results from multiple industry sectors, the study found that gaming apps and FinServ apps are the most likely to be attacked.

Likelihood of a Gaming app being attacked: 63%

Gaming Apps Under Attack



Likelihood of FinServ app being attacked: 62%

FinServ Apps Under Attack

The factors that cause the number of attacks to be higher in FinServ are perhaps obvious:

- That's where the money is!
- For geopolitical actors, disruptions in economies are equivalent to disruptions in national defense[2]

Several factors cause the risks to be higher in gaming:

- **There is money to be made.** Selling pirated games in grey-market app stores such as Cydia can give hackers direct income. In addition, money can be made in the micro-economies that popular games create and foster. For example, Fortnite, a game that arguably peaked in popularity in 2018, still hosts more than a quarter of a billion of monthly active users in 2023, and 68% of those users have spent money on "extras" such as emotes, harvesting tools, gliders, and outfits. And, with users trading so much real money for "game-bucks," there is a growing incentive to steal the credit card or PII that makes it easier to steal real money—which in turn creates an incentive for criminal organizations to launder money.
- **"Street cred" from hacking games**. Some of the most active Reddit communities and forums revolve around "cracking" or reverse engineering games. For example, the *PiratedGames* subreddit has 450k global members and is dedicated to discussing "pirated games and cracks." While most users are just consumers of cracks and cheats, those who can crack the most protected games are regularly hailed in comments and enjoy a kind of celebrity within the community.

[2]https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989

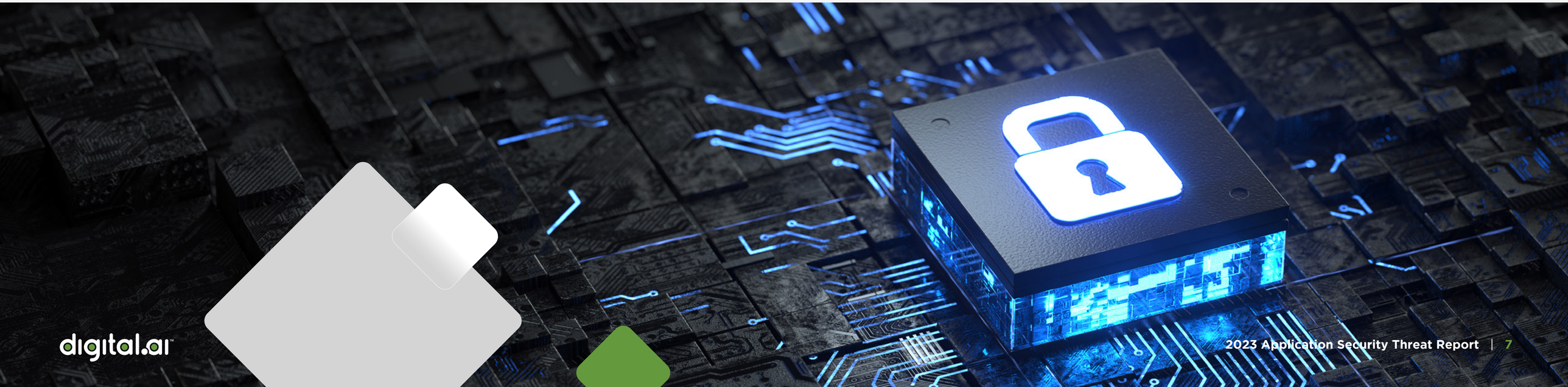
Risks to App By Industry *(cont.)*

- **Apps outside of FinServ and gaming** still have a 54% chance of being attacked. The motivations to attack such apps are myriad and increasing. For example:

- **Implantable medical devices** interface with the patients' phone apps as well as clinicians' phones and tablets. The incentives to hack those applications range from a curious patient wanting to experiment with a drug delivery system to a truly malicious actor looking to inflict bodily harm on another human.

- **Bluetooth-connected phone apps** that start our cars are increasingly available and are also obvious targets for threat actors looking to steal cars or, at the least, the goods stored inside them.

- **Dozens of other threat vectors** emerge in almost any industry—from apps used by oil prospectors, to apps used for computer-aided design, to apps used by your favorite retailer.



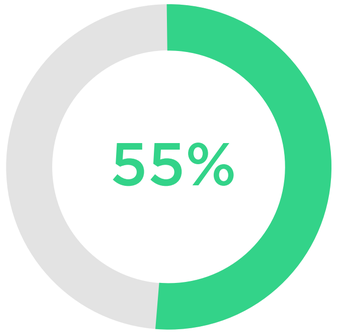
Risk to Apps By Device Type

iOS vs. Android

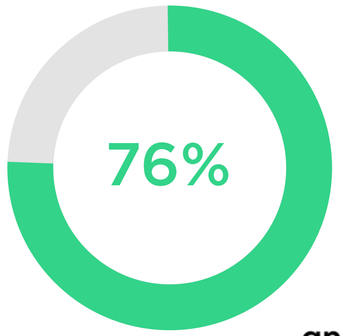
The popular notion is that iOS is more secure than Android because Apple is vocal about its commitment to privacy and has a legacy of running a “closed” environment. However, the reality is more complicated. IOS, like the Android OS, is an open platform, in the sense that 3rd party developers easily access application build tools. But since Apple controls the production of all iPhones, while Google licenses the Android OS to many different device makers, Android OS is more open and thus more accessible to threat actors.

Our data shows that Android apps are more likely to be put in unsafe environments, such as rooted phones, than iOS apps are likely to be run on jailbroken phones.

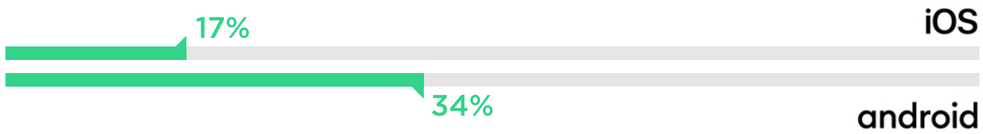
iOS likelihood of unsafe environment



Android likelihood of being put in an unsafe environment

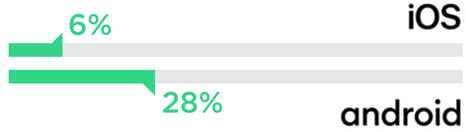


In addition, the study examined the relative likelihood of running with modified code — inclusive of running with a changed resource or signature. In this category, Android fell behind iOS by a 2:1 margin:



The margin is larger when we look JUST at the odds of running with modified code

Difference in likelihood of being run with modified code

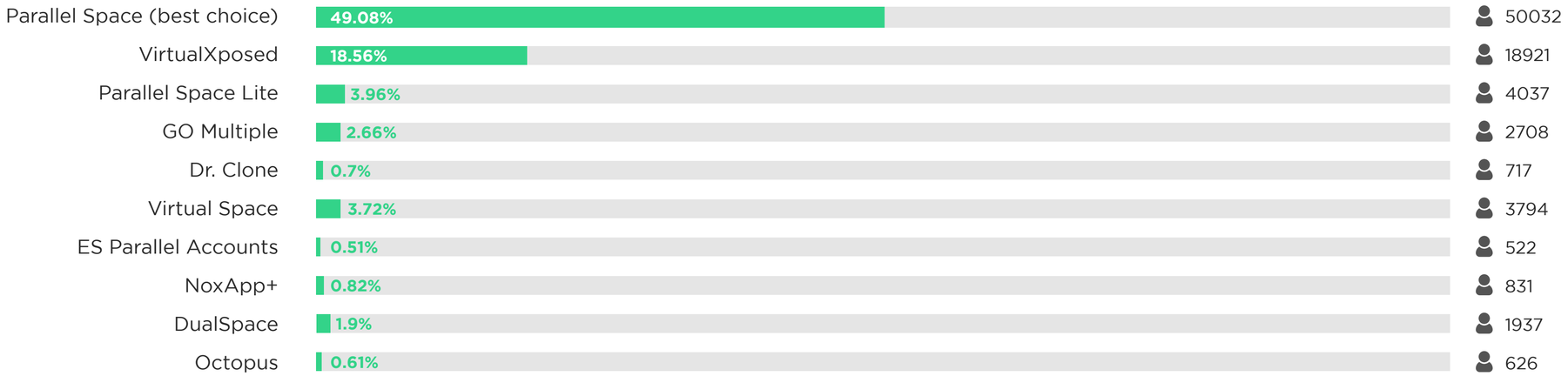


Does Risk Depend on App Popularity?

When fraudsters want to exploit the popularity of an app to do their dirty deeds, they often run the app in a virtualized environment and/or open multiple accounts on the same app. Catfishers on dating apps, for example, or gamers wishing to expand their presence on particular gaming sites, use virtualization spaces that allow them to virtualize their apps, as shown below.

Popularity of various types of virtualization spaces.

What virtual space do you use?



The study found that the probability that at least one instance of any given mobile app is put into a virtualized environment is 29%.

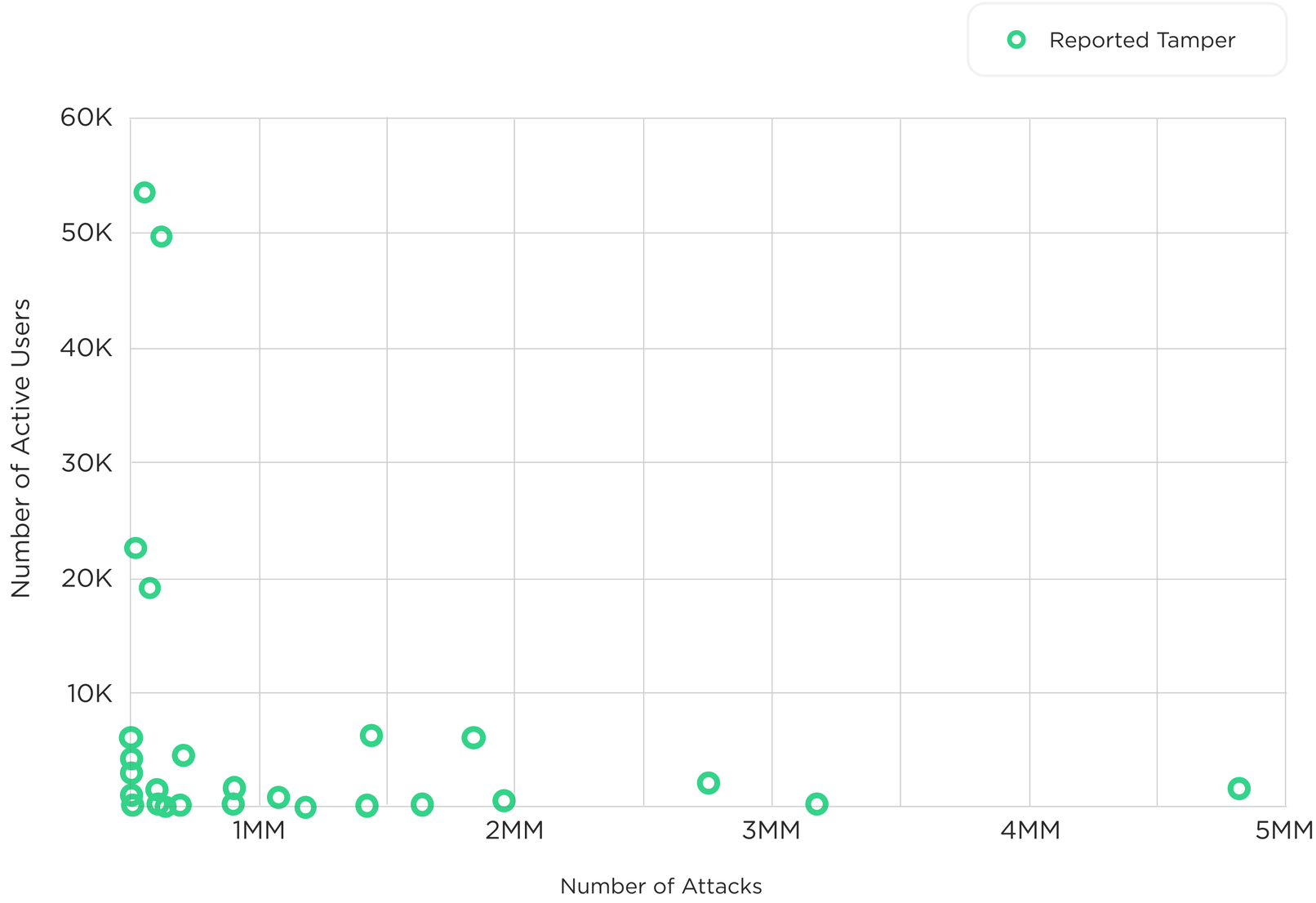
We discuss more of the reasons virtual spaces are popular, as well as the threat vectors that are opened up by the use of virtualization apps, in a blog post here.

Risk and Popularity *(cont.)*

Scatterplot of data from Digital.ai App Aware

The study also found no correlation between the likelihood of being attacked and the app's popularity. This scatterplot shows that many popular apps are put into untrusted environments less frequently than unpopular apps.

While the lack of correlation between the popularity of an app and the likelihood of it being attacked might be illogical to a casual observer, we know from experience that the reasons and motivations for attacking any particular app are varied. As a result our customers have determined that building security into their apps is the simplest and best way to prevent attacks on their apps.



Protecting Your Apps in the Wild

Application owners know all too well the pressures of creating more applications faster. This often leads to short-shrifting security—either not including it in the DevOps process, seeing it as an impediment, or simply not knowing where to start.

Digital.ai has hundreds of application security customers worldwide who protect over 1 billion instances of applications. Many of those customers contributed anonymized data that led to the findings of this study. If you are an existing Digital.ai Application Security customer and would like to contribute data to future studies, contact us at https://digital.ai/why-digital-ai/contact/

For all of our existing and new customers, we offer application security solutions that build in security in multiple ways:

Embedding security into the application development process

- Obfuscate code to prevent reverse-engineering
- Prevent tampering by detecting unsafe environments and code changes
- Configure customized or automated protections on-premises or in the cloud

Providing visibility into at-risk apps

- Produce stand-alone reports or integrate with existing Security Operations Center tools
- Create searchable logs
- See which guards and protections are activated

Automatically responding to threats

- Force step-up authentication
- Alter app features
- Shut down applications that are under attack

Get more information about our Digital.ai Application Security solution and it's capabilities by accessing the resource below. Then contact us to get started on your journey.

Read more about our Application Security solution.

CONTACT US

Appendix: Methodology

This study was conducted using data gathered with permission from Digital.ai application security customers around the globe. Two types of data were collected and analyzed:

Telemetry data, which includes the types of guards that are used for a particular app but does not contain information on whether or not a guard has been “tripped” or fired.

App Aware data from customers’ Digital.ai threat monitoring system. Customers who use App Aware have data on the number and locations of app instances they have in production, as well as information on when and where each of those apps is either modified or placed in an unsafe environment. The study gathered information from App Aware with permission from customers and anonymized and aggregated the data.

The data in this report was collected over a 4 week period from February 1 to February 28 2023.

About Digital.ai

Digital.ai is an industry-leading technology company dedicated to helping Global 5000 enterprises achieve digital transformation goals. The company's AI-powered DevSecOps platform unifies, secures, and generates predictive insights across the software lifecycle. Digital.ai empowers organizations to scale software development teams, continuously deliver software with greater quality and security while uncovering new market opportunities and enhancing business value through smarter software investments.

Additional information about Digital.ai can be found at **digital.ai/** and on **Twitter**, **LinkedIn**, and **Facebook**.