The mobile threat landscape

JAMF NATION LIVE

Agenda

1 | Why is mobile at risk?

Why are mobile devices being targeted, and who's targeting them?

2 | Mobile threats in detail

What sorts of mobile threats are there, and what risks do they pose?

3 | How to stay protected

Introducing Jamf Threat Defense, MI:RIAM and the Jamf Trust app

Why is mobile at risk?

Why are mobile devices being targeted, and who's targeting them?

Mobile threats are the **modern reality**

2.5 million

mobile users downloaded multiple malware apps last year.

6.5%

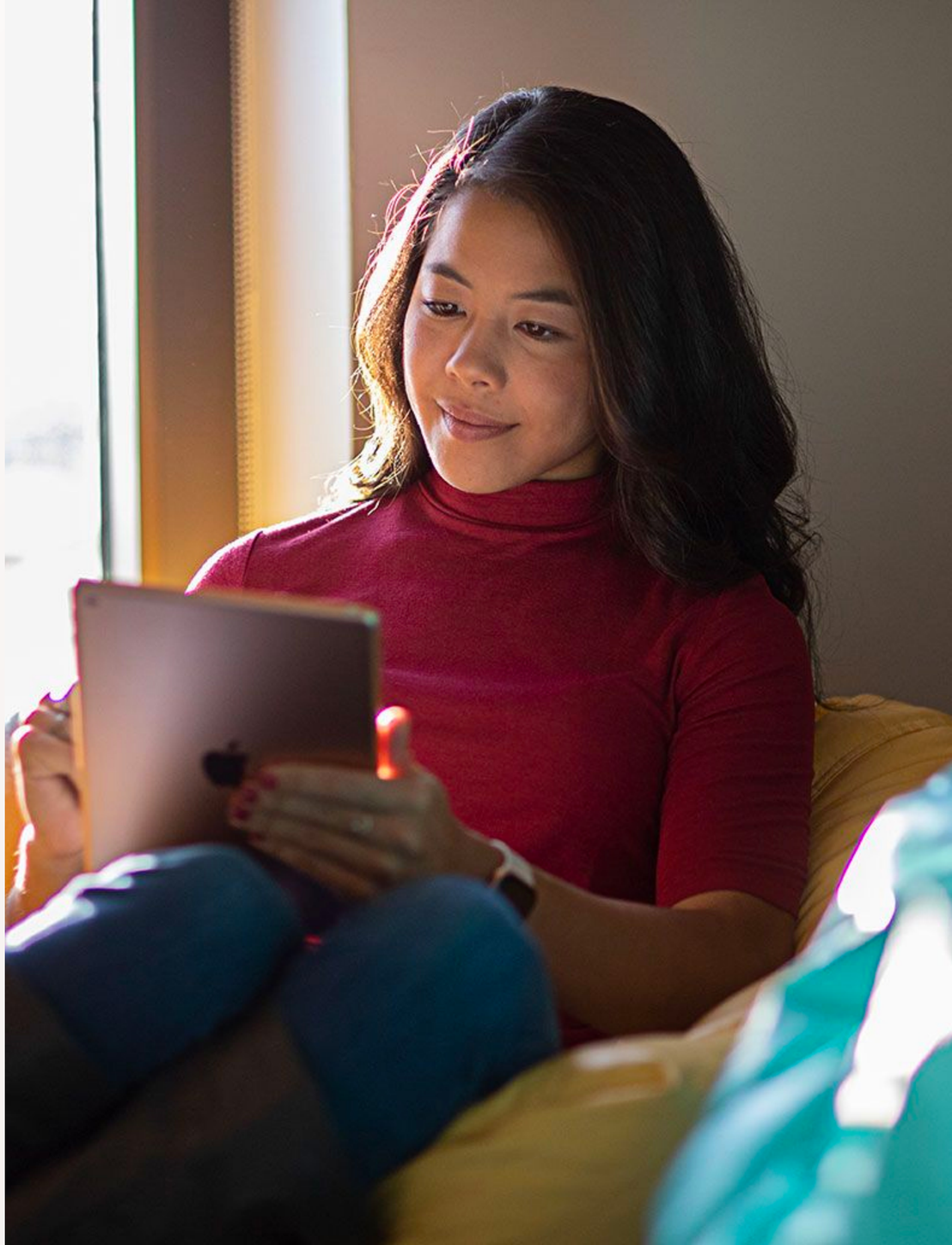
of all mobile devices are running an out-of-date or vulnerable OS.

85%

of mobile apps are unsecured and leak data.

25%

of all data breaches involve phishing.



Why is mobile being **targeted**?

The footprint of **mobile in business continues to grow**

71%

of organisations rate mobile 8/10 or above in terms of being crucial to their business.

Mobile is becoming increasingly critical in business

24%

sacrificed the security of mobile devices to facilitate their response to the pandemic and its restrictions.

Expansion of the attack surface

In **2021**

1 in 10

users fell victim to a **mobile phishing attack**.

39%

of organisations were regularly utilising an operating system **with a known security vulnerability**.

6%

of organisations encountered **malware installed on a remote device**.

Making the **headlines**

Spanish prime minister's mobile phone infected by Pegasus spyware, government says

Reuters

MADRID, May 2 (Reuters) - Spanish authorities have detected "Pegasus" spyware in the mobile phones of Prime Minister Pedro Sanchez and Defence Minister Margarita Robles, the government minister for the presidency, Felix Bolanos, said on Monday.

Bolanos told a news conference Sanchez's phone was infected in May 2021 and at least one data leak occurred then. He did not say who could have been spying on the premier or whether foreign or Spanish groups were suspected of being behind it.

REUTERS

A Gift for Paying Your Mobile Bill? Don't Click That Link: It's a Scam

Group texts: Great for scammers, bad for everyone else, as the New Jersey Cybersecurity & Communications Integration Cell is warning T-Mobile customers.

By Nathaniel Mott 18 Apr 2022, 2:37 p.m.

Have you received text messages thanking you for paying your mobile bill, which include a link to a special gift? Don't click; it's a scam, the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) is warning T-Mobile customers.

"Similar to a recent SMiShing campaign targeting Verizon Wireless customers," NJCCIC says, "the message thanks the recipient for paying their bill and includes a malicious link to accept a free gift. The message, however, is sent via group text that includes a number of random recipients and was sent to the targets dozens of times over the course of three days. Customers were unable to block the unwanted messages since they were sent via group text."

PC PCMAG.COM

LaLiga fined $280K for soccer app's privacy-violating spy mode

Natasha Lomas @riptari / 11:15 AM GMT+1 • June 12, 2019

Comment

Spanish soccer's premier league, LaLiga, has netted itself a €250,000 (~$280k) fine for privacy violations of Europe's General Data Protection Regulation (GDPR) related to its official app.

As we reported a year ago, users of the LaLiga app were outraged to discover the smartphone software does rather more than show minute-by-minute commentary of football matches — but can use the microphone and GPS of fans' phones to record their surroundings in a bid to identify bars which are unofficially streaming games instead of coughing up for broadcasting rights.

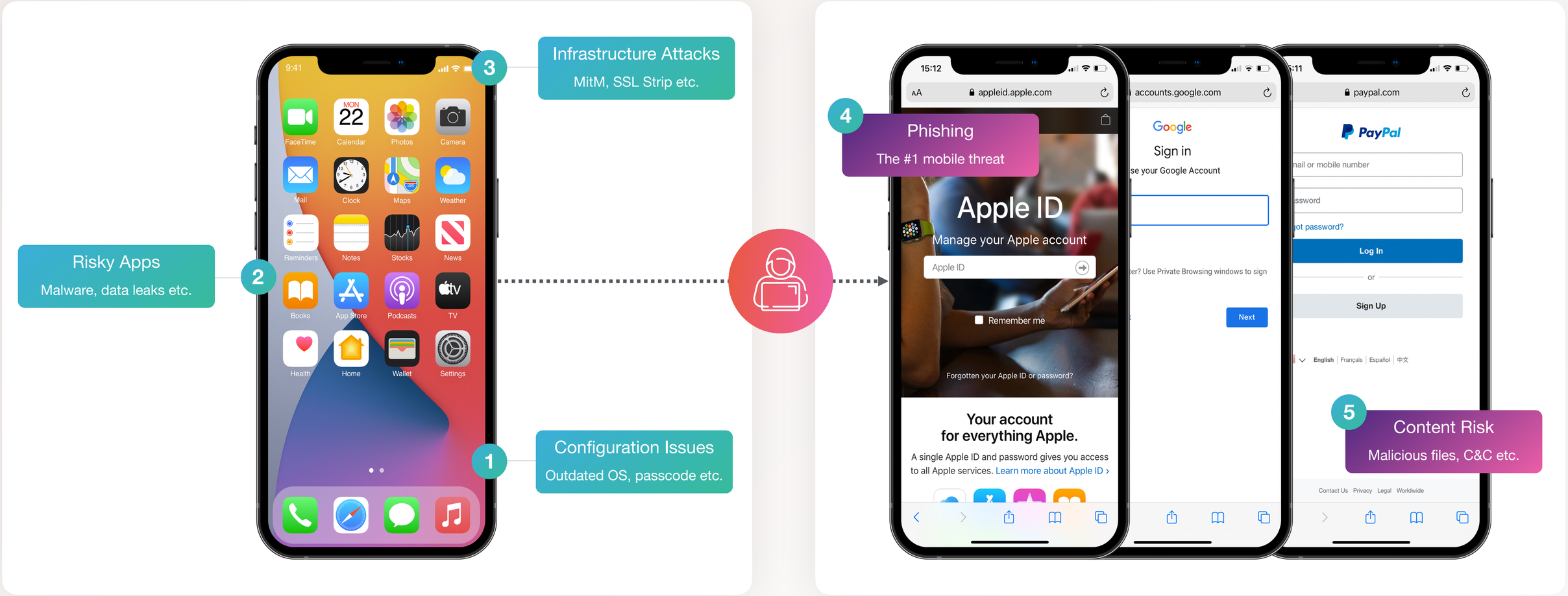
Unwitting fans who hadn't read the tea leaves of opaque app permissions took to social media to vent their anger at finding they'd been co-opted into an unofficial LaLiga piracy police force as the app repurposed their smartphone sensors to rat out their favorite local bars.

TechCrunch

Mobile threats **in detail**

What sorts of mobile threats are there, and what risks do they pose?

What sorts of mobile threats are there?

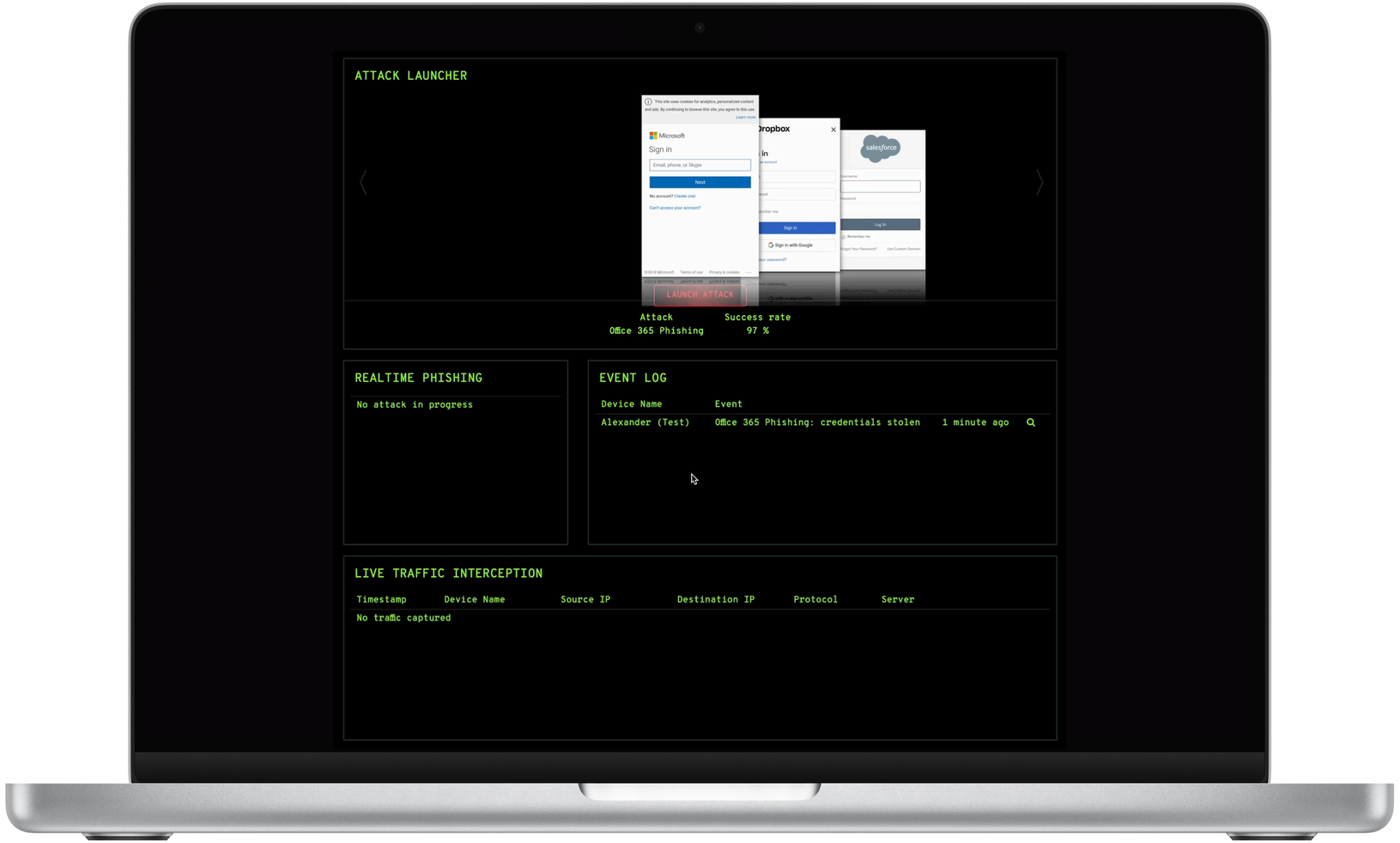


On-device threats

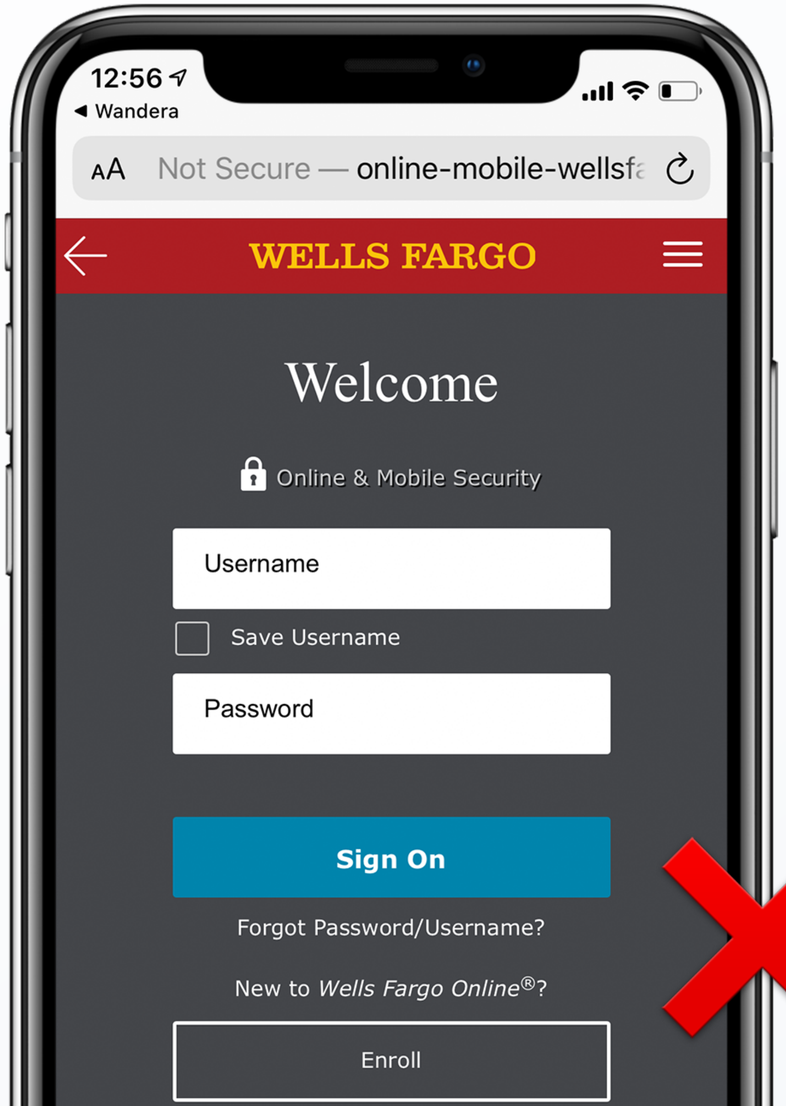
In-network threats

JAMF NATION LIVE

The #1 mobile threat vector: **Phishing**

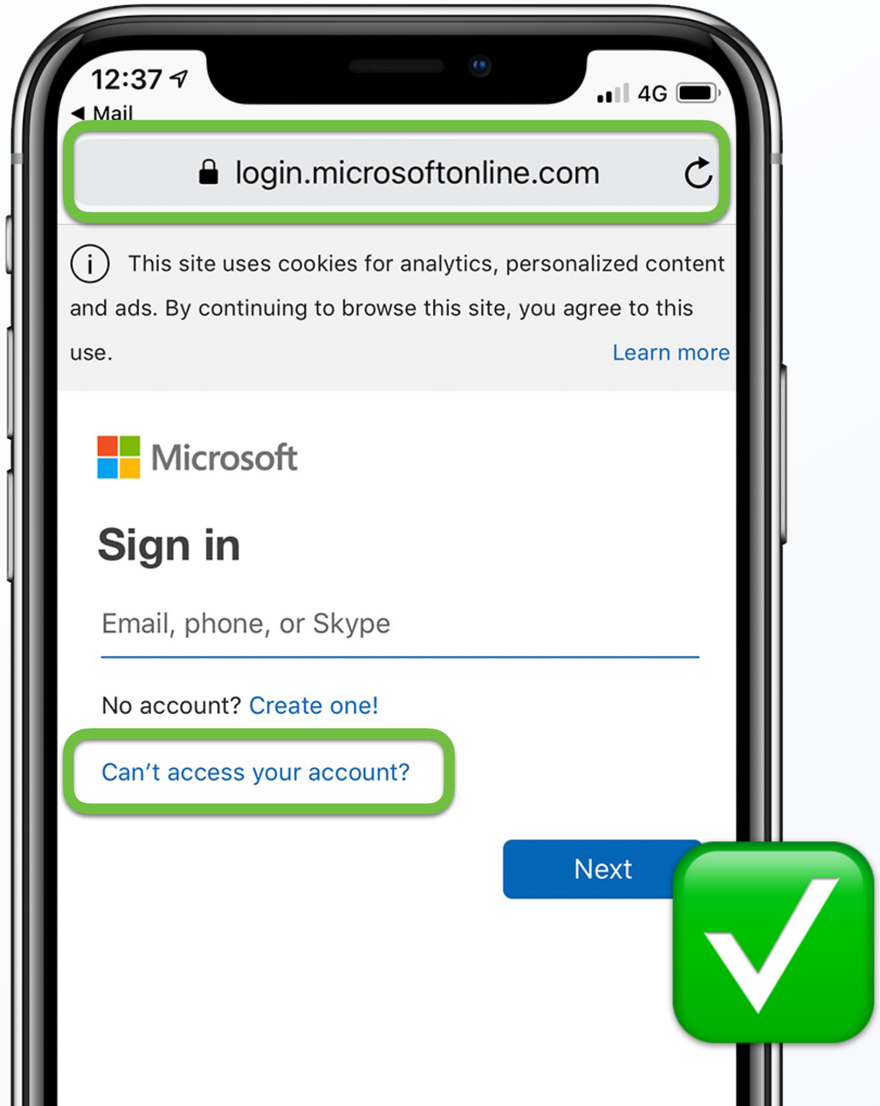


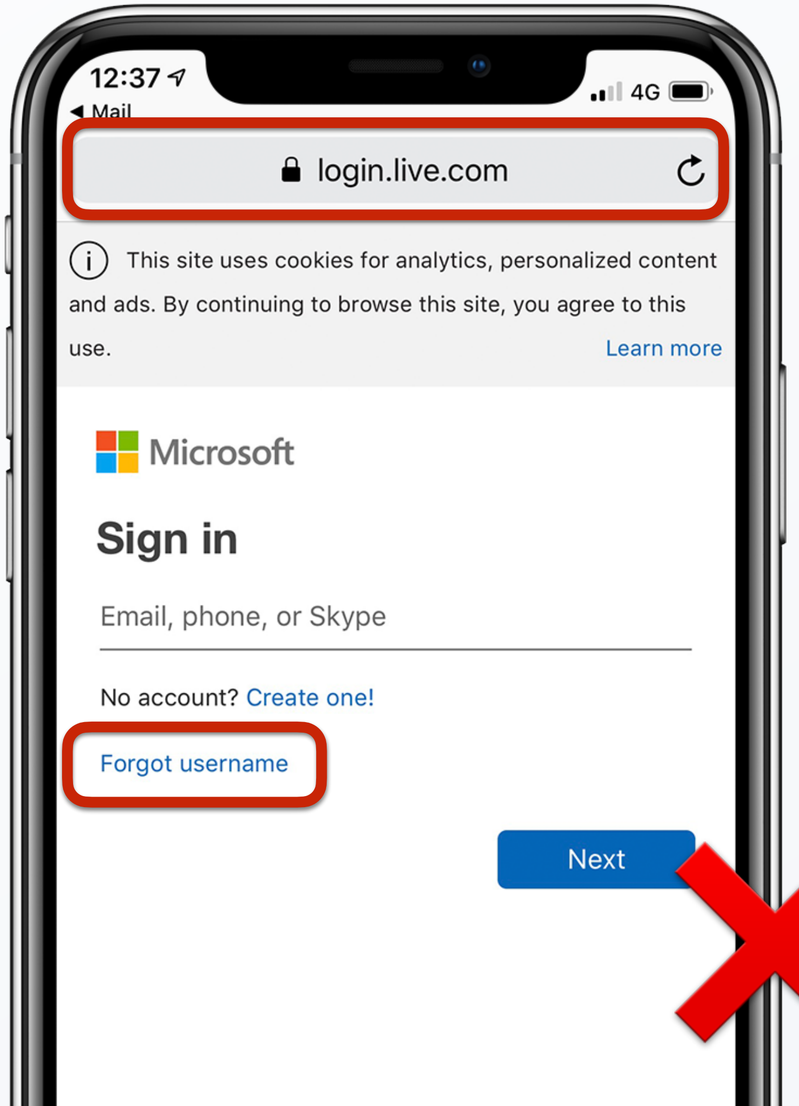
Which is the **real** banking site?



Green padlock icon indicates whether or not the connection is encrypted

Which is the **real** login page?





Different URLs

“Forgot username” - Different text, same URL

Near-identical design and layout

Expect the unexpected: **App risk**

Mobile apps are fraught with vulnerabilities,
even those we know and trust

1 in 4

mobile apps contains at least one high-risk security flaw.

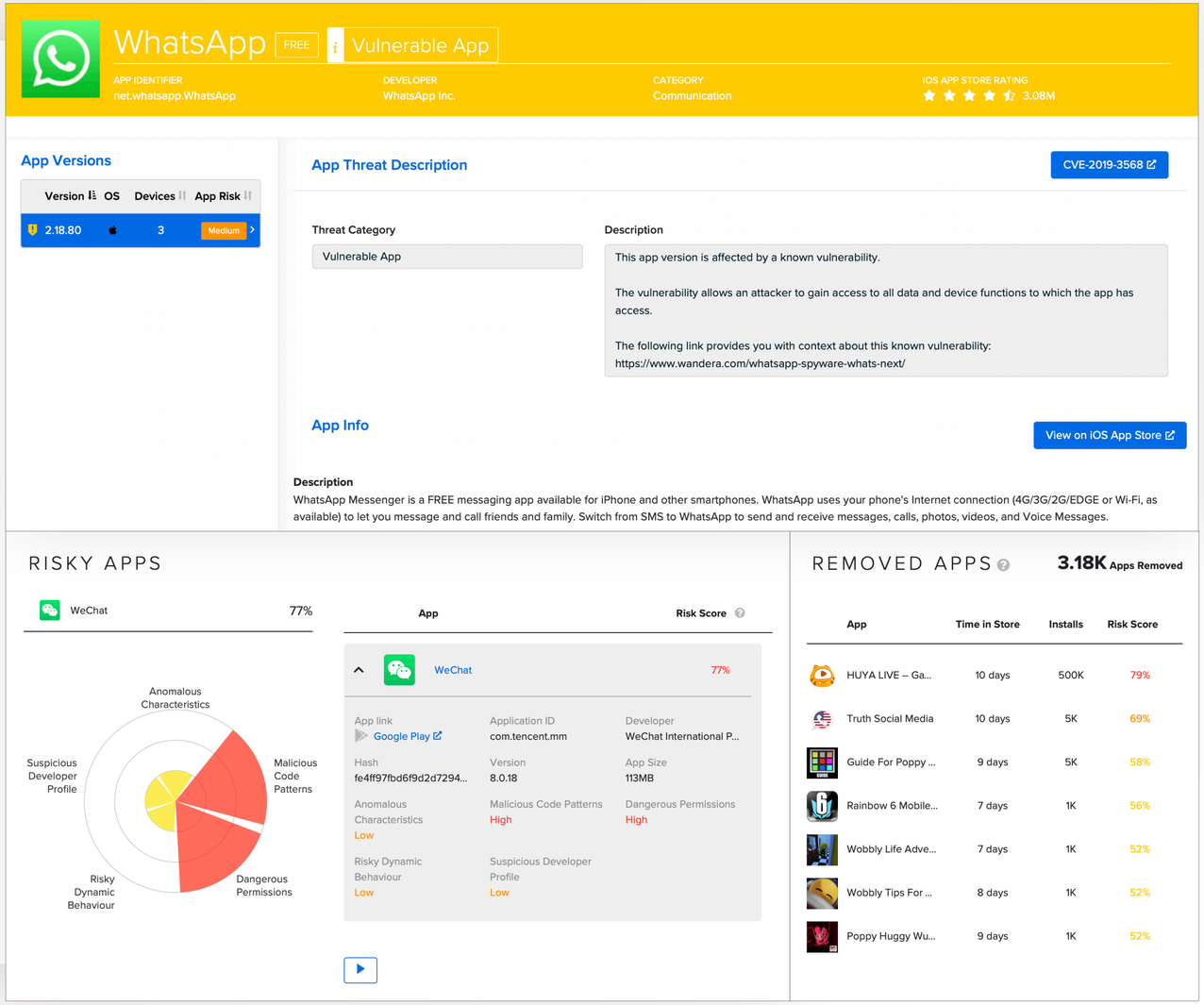
50%

of apps with five to ten million downloads include a security flaw.

3x

Business apps are three times more likely to leak login credentials.

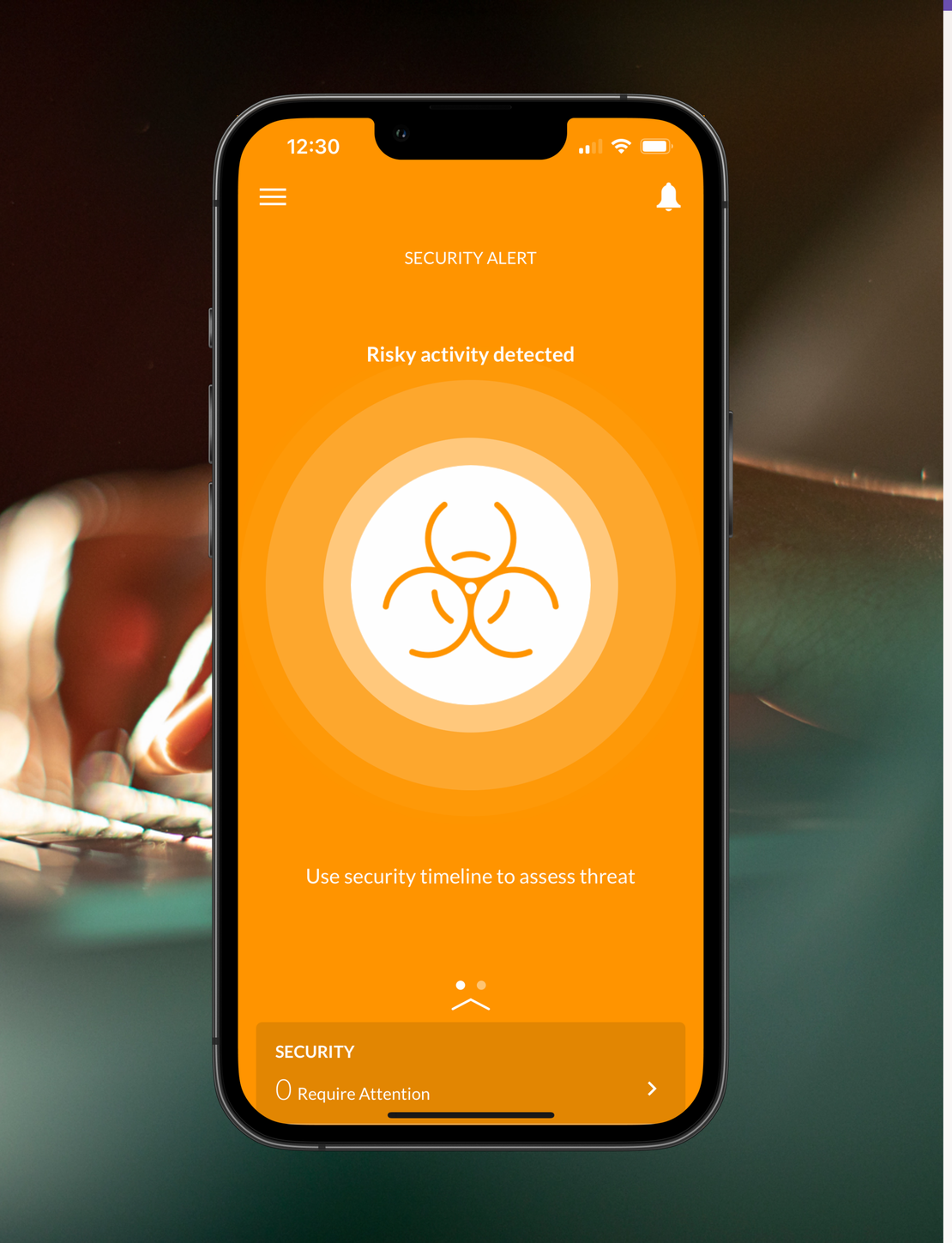
Encryption	Apps without encryption: easy data exfiltration
Permissions	Apps often request excessive permissions access
Vulnerable OSS	Hackers use apps to exploit OS loopholes
Reverse engineering	Apps are disassembled to exploit vulnerabilities
Side-loading	Side-loading of “BETA”, or pre-release apps



How to stay **protected**

Introducing Jamf Threat Defense, MI:RIAM and the Jamf Trust app

JAMF NATION LIVE



Jamf
Threat Defense

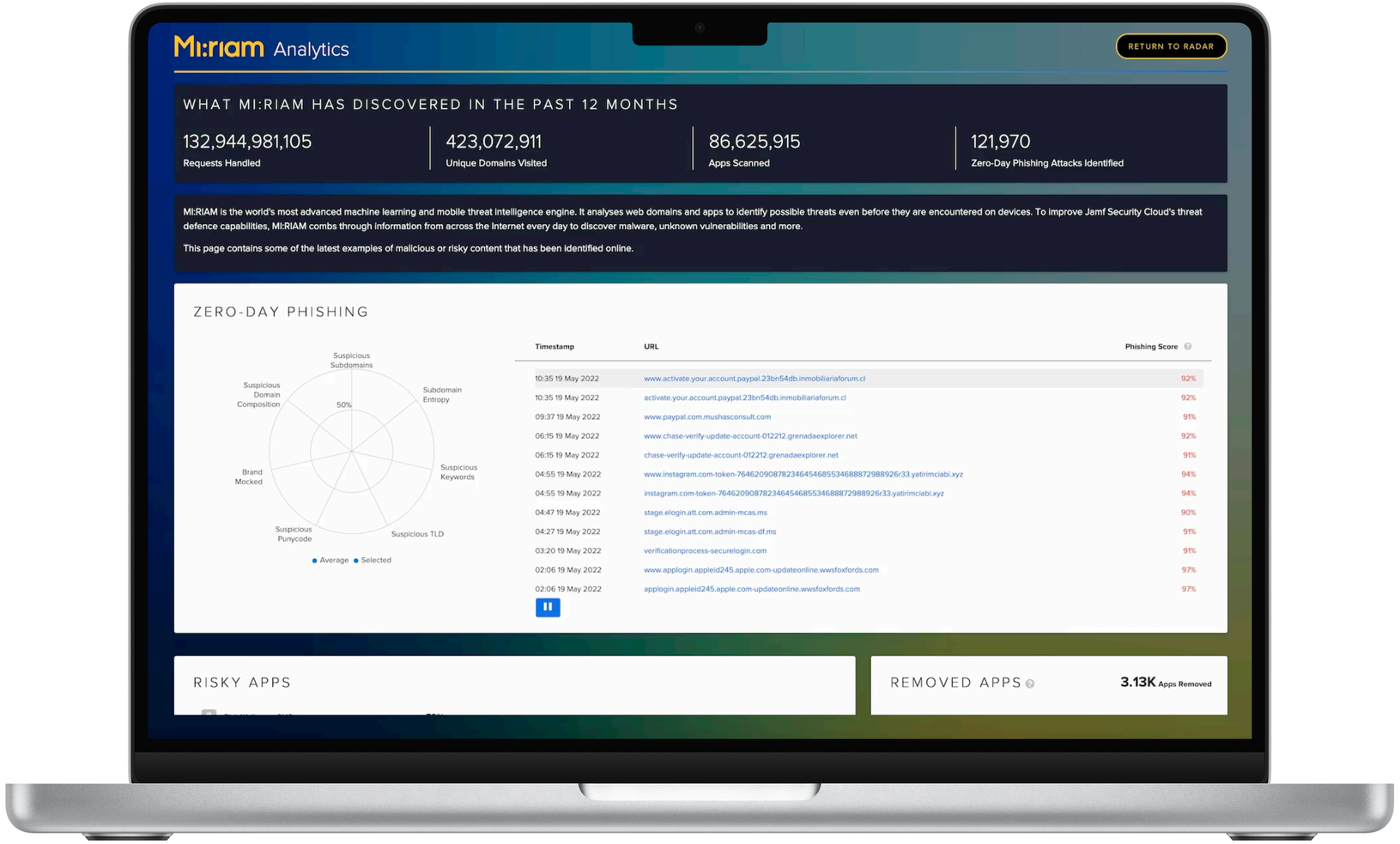
Leading **mobile threat defense** for iOS, iPadOS, and Android

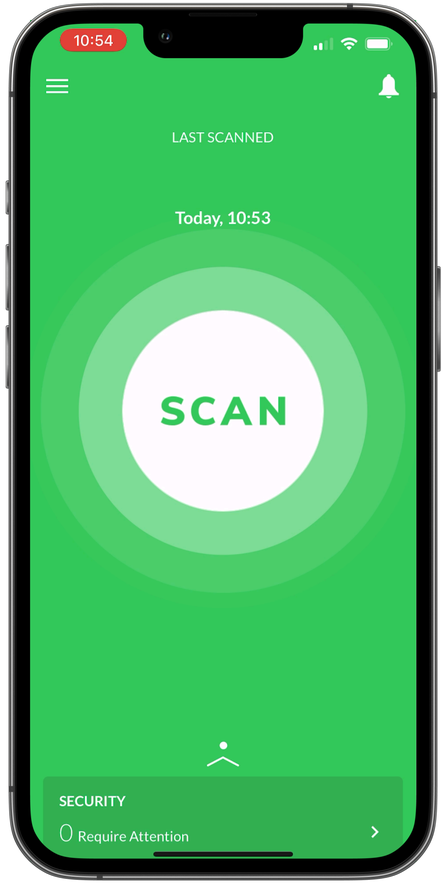
Mobile security for all your workers

- **Detect** configuration vulnerabilities
- **Protect** against malware & risky apps
- **Mitigate** malicious infrastructure
- **Prevent** incoming attacks
- **Gain** insights through analytics

JAMF NATION LIVE

Introducing **MI:RIAM**





Jamf
Threat Defense

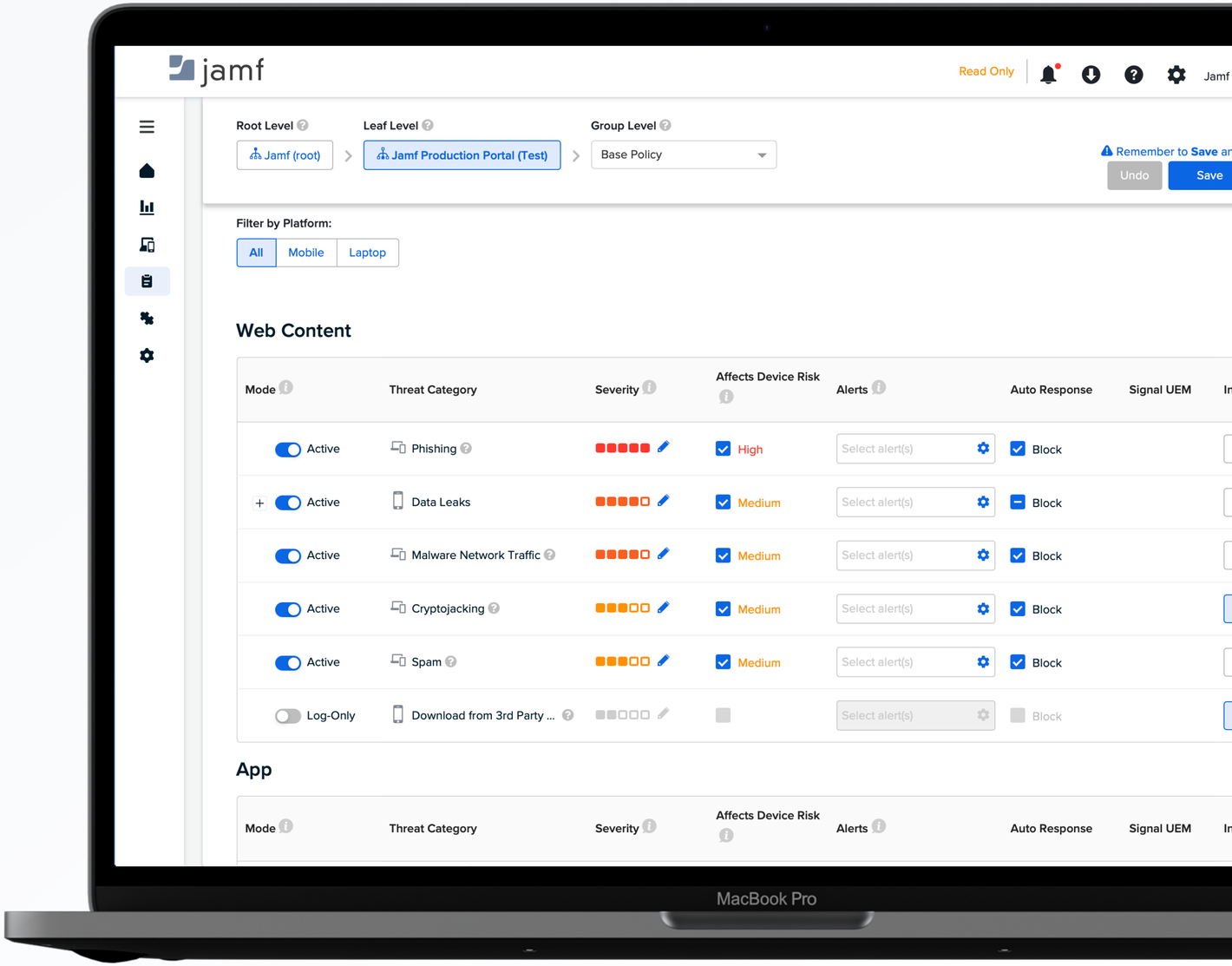
Leading **mobile threat defense** for iOS, iPadOS, and Android

Detailed analytics

- Cloud-based, easy-access reporting
- Comprehensive app vetting

Powerful integrations

- SIEM, SOAR etc.
- Zero-touch UEM deployment
- Conditional access and risk tagging



JAMF NATION LIVE

Jamf **Trust**

One consistent security experience across platforms

Jamf Threat Defense

Protect end users against malicious domains, phishing, data leaks and other network-based threats

Any ownership model

Whether BYOD, COPE or COBO, empowering all users in a way that protects the business

Thank you.

Questions?

Jamf
Threat Labs

Jamf
Threat Defense