Securing iOS and Android: Navigating Modern Mobile Threats

JAMF NATION LIVE

Milind Patel

Director, Product Management
Jamf

Agenda

1 | Mobile security in the modern era

How the ever-evolving digital landscape is changing the face of mobile security

2 | Understanding mobiles

How mobile devices are being used today and the security measures that come built-in to modern OSes

3 | Attack vectors & exploits

Common techniques used by malicious actors to target and compromise mobile devices

4 | Addressing mobile security

Prioritising and implementing the right security strategies to protect iOS and Android devices

Mobile security in the modern era

Work is increasing on mobile

Reduced Oversight

61%

of workers allowed friends or family to use work devices

2021 Mobile Security Index, Verizon

Ubiquitous Connectivity

432.5m

Public Wi-Fi hotspots

Global public Wi-Fi hotspots 2016-2022, Statista

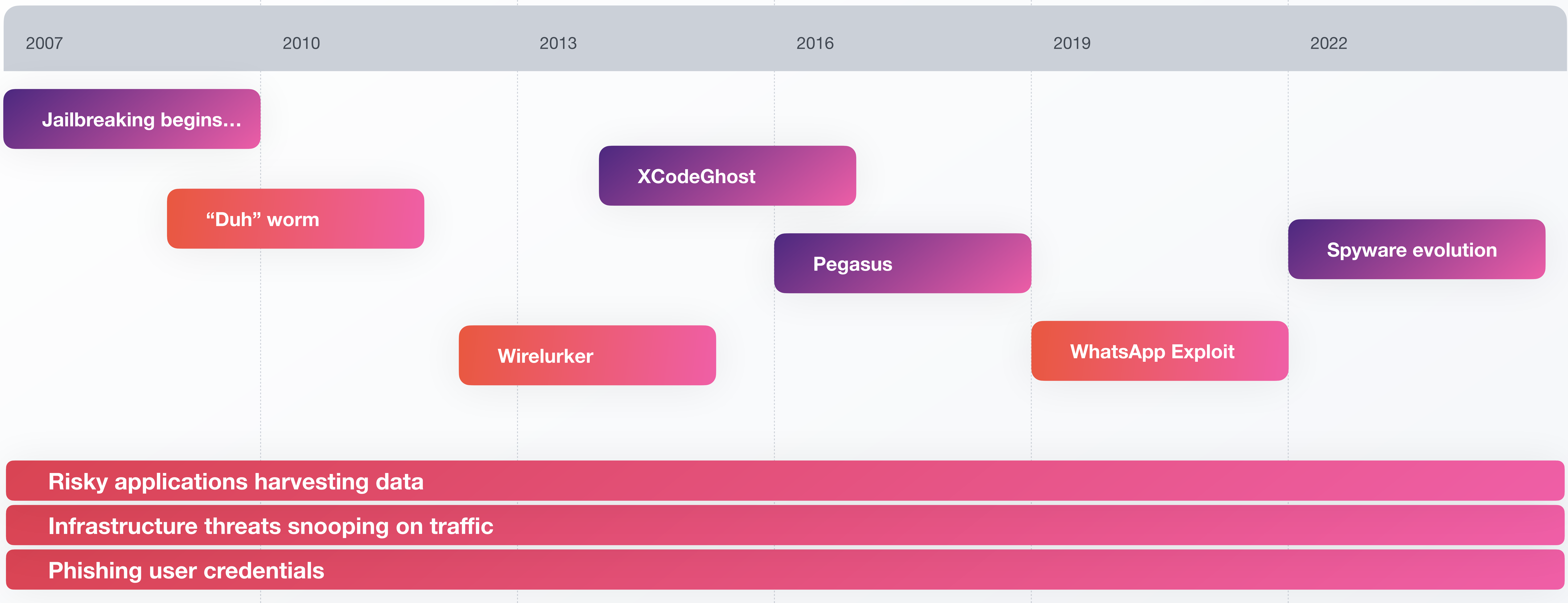
Rise of Remote Work

46%

Remote users

The State of Security 2022, Splunk

A brief timeline of iOS security challenges



2007

2010

2013

2016

2019

2022

Jailbreaking begins…

“Duh” worm

XCodeGhost

Pegasus

Spyware evolution

Wirelurker

WhatsApp Exploit

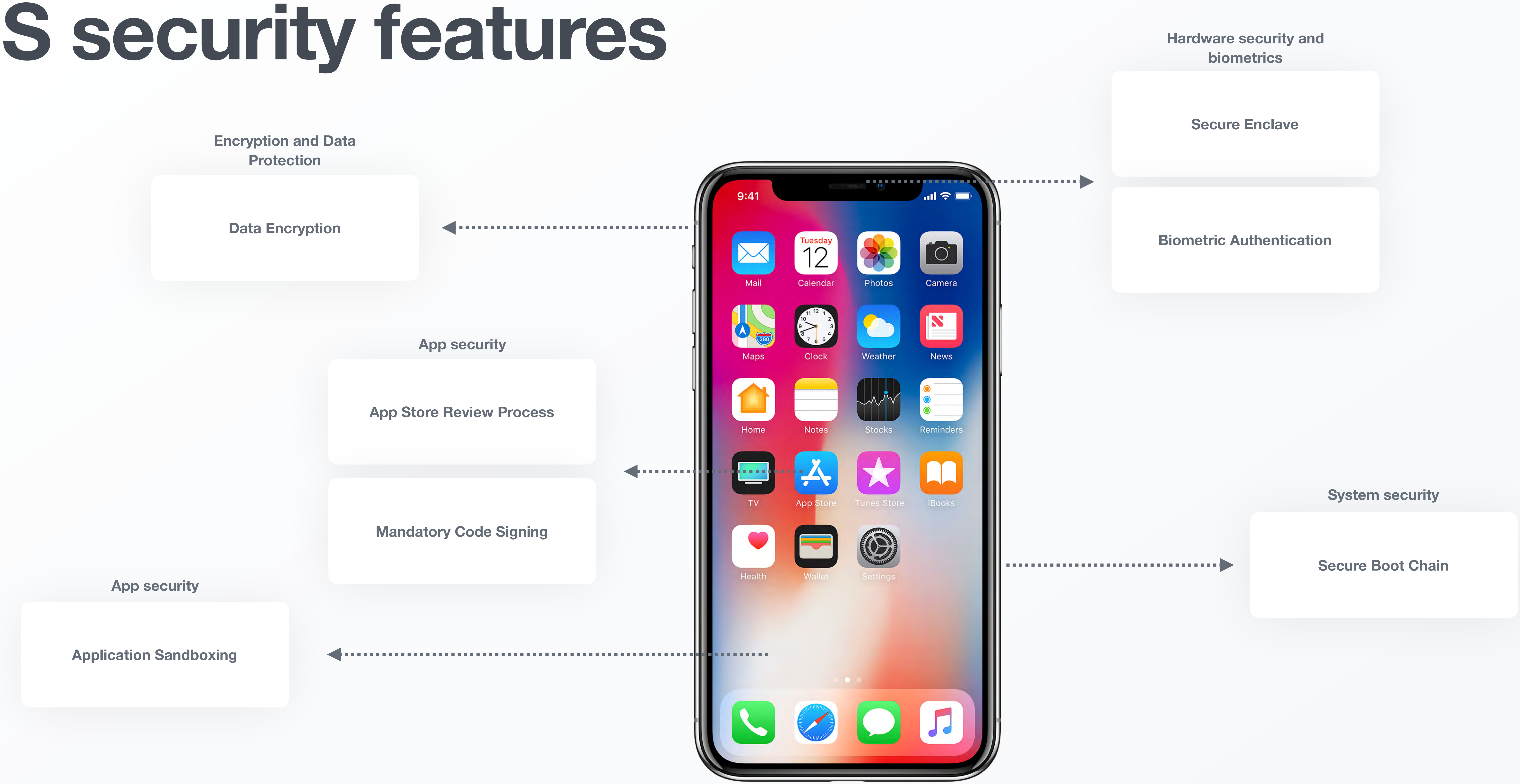
Risky applications harvesting data

Infrastructure threats snooping on traffic

Phishing user credentials

Understanding mobiles

iOS security features



Encryption and Data Protection

Data Encryption

App security

App Store Review Process

Mandatory Code Signing

App security

Application Sandboxing

Hardware security and biometrics

Secure Enclave

Biometric Authentication

System security

Secure Boot Chain

How does Android deviate from this?

App Store Ecosystem

Fragmentation

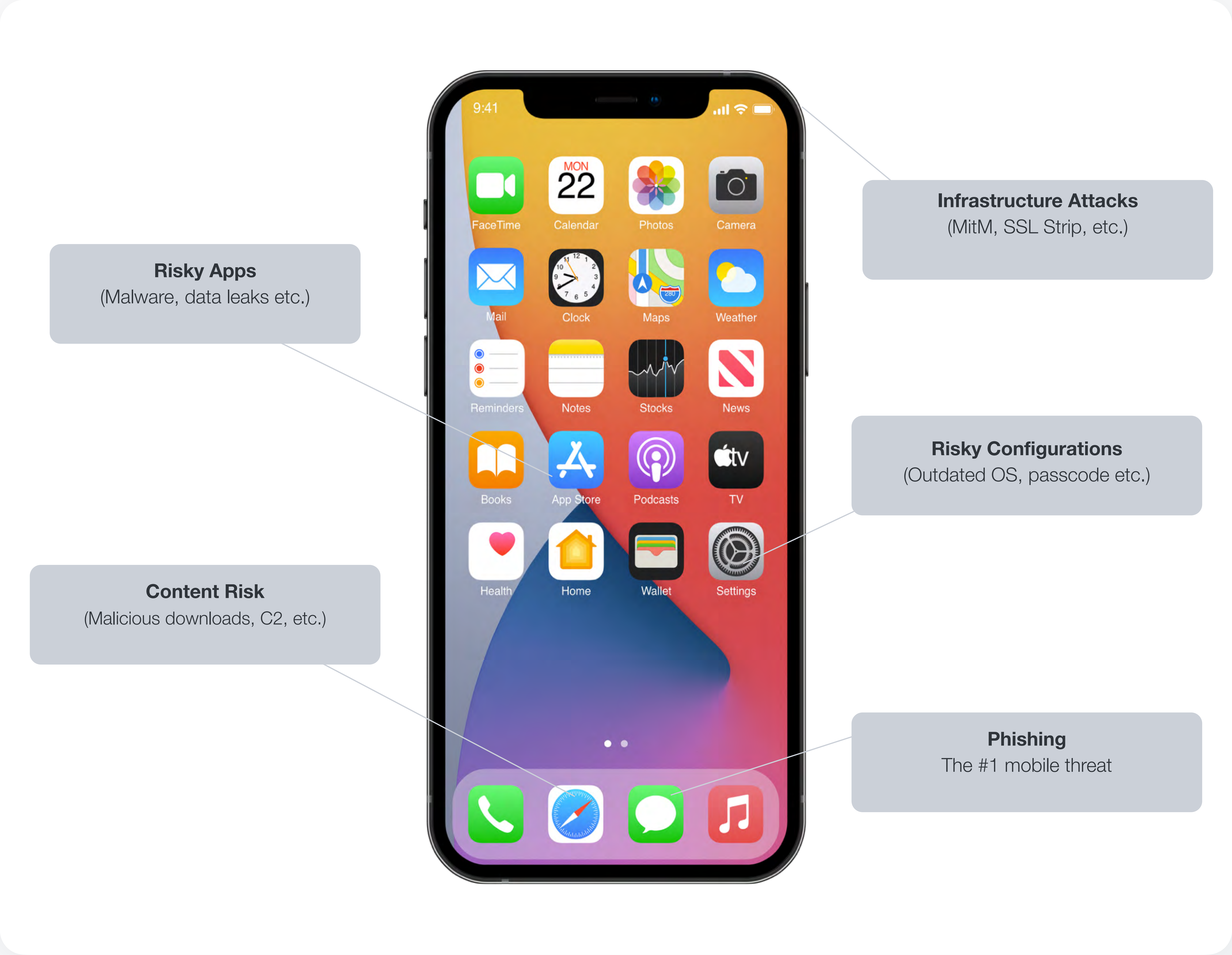
Permissions Model

Open Source

Customisability

Attack vectors & exploits

Common attack vectors



Risky Apps
(Malware, data leaks etc.)

Content Risk
(Malicious downloads, C2, etc.)

Infrastructure Attacks
(MitM, SSL Strip, etc.)

Risky Configurations
(Outdated OS, passcode etc.)

Phishing
The #1 mobile threat

ON-DEVICE RISK

OS vulnerabilities, Risky Configurations

APP RISK

Malicious, Leaky, and Vulnerable apps

INFRASTRUCTURE RISK

MitM, SSL strip, Protocol attacks

CONTENT RISK

Phishing, Data Exfiltration, C2

Device Threats	
Jailbreak / Rooted Devices	High
Vulnerable OS	High
Risky iOS Profile	Med
Dangerous Certificates	Med
Out-of-date OS	Low

Configuration Vulnerabilities	
Android security patches …	High
Device Encryption Disabled	Med
Lock Screen Disabled	Med
Device Admin Apps Installed	Med
Third-Party App Store Installed	Low
Developer Mode Enabled	Low
Unknown App Sources Enabled	Low
USB App Verification Disabled	Low
USB Debugging Enabled	Low

ON-DEVICE RISK
OS vulnerabilities, Risky Configurations

APP RISK
Malicious, Leaky, and Vulnerable apps

INFRASTRUCTURE RISK
MitM, SSL strip, Protocol attacks

CONTENT RISK
Phishing, Data Exfiltration, C2

Malware	
Malicious apps	High
Sideloaded apps	High
Vulnerable apps	Med
Potentially Unwanted apps	Med

Data Leaks	
App Data Leak: Credit Card	High
Web Data Leak: Credit Card	
App Data Leak: Password	Med
Web Data Leak: Password	
App Data Leak: Email	Low
Web Data Leak: Email	
App Data Leak: Location	Low
Web Data Leak: Location	

ON-DEVICE RISK

OS vulnerabilities, Risky Configurations

APP RISK

Malicious, Leaky, and Vulnerable apps

INFRASTRUCTURE RISK

MitM, SSL strip, Protocol attacks

CONTENT RISK

Phishing, Data Exfiltration, C2

Infrastructure Threats	
Adversary-in-the-Middle	High
Risky Hotspot	Med

ON-DEVICE RISK

OS vulnerabilities, Risky Configurations

APP RISK

Malicious, Leaky, and Vulnerable apps

INFRASTRUCTURE RISK

MitM, SSL strip, Protocol attacks

CONTENT RISK

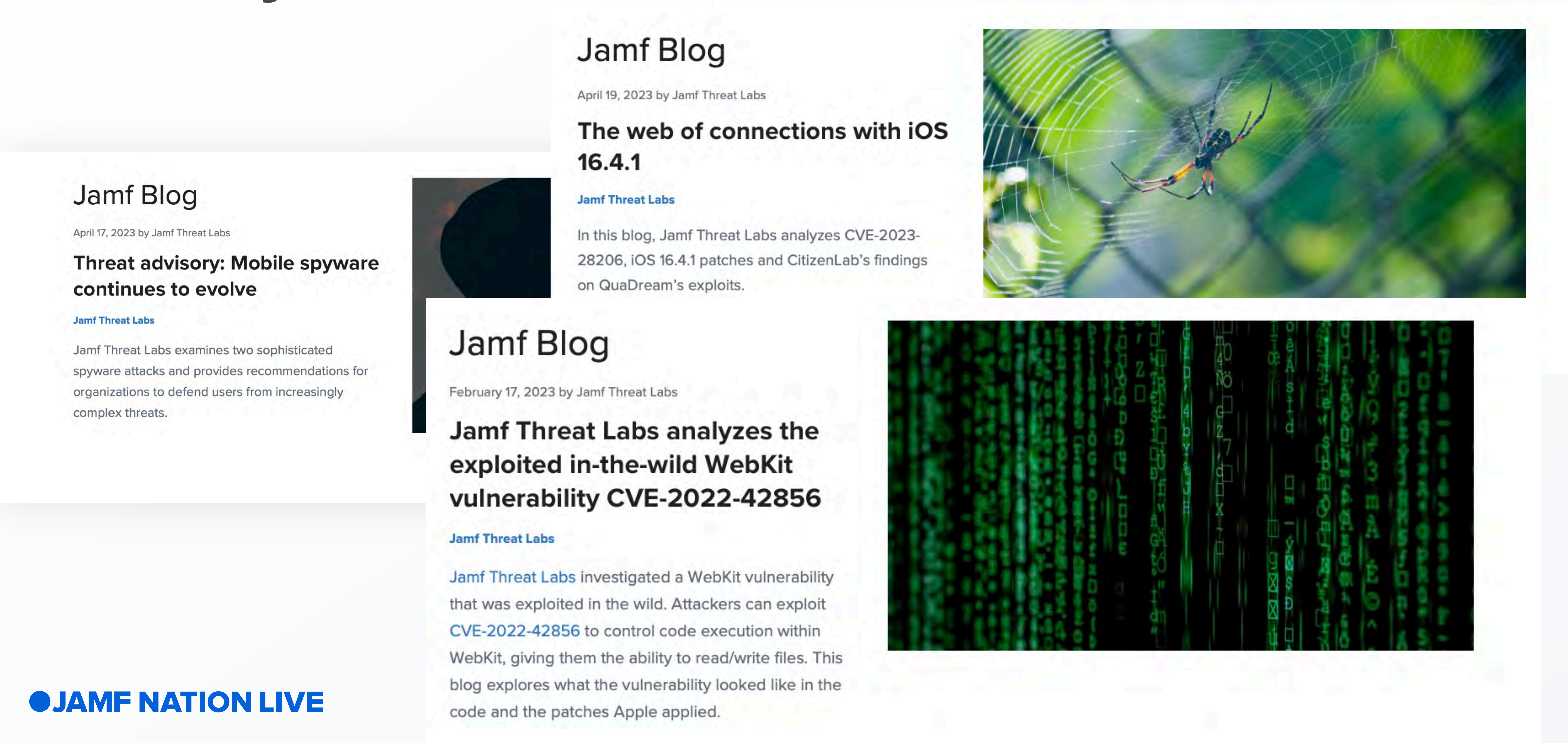
Phishing, Data Exfiltration, C2

Web / Content Threats	
Mobile Phishing	High
Malware Network Traffic	High
Cryptojacking	Med
Spam Websites	Med
3rd Party App Downloads	Low

Zero-day vulnerabilities

“A security flaw or weakness in a software or hardware system that is unknown to the vendor or developer, allowing attackers to exploit it before a patch or fix is available”

Zero-day vulnerabilities



Jamf Blog

April 17, 2023 by Jamf Threat Labs

Threat advisory: Mobile spyware continues to evolve

Jamf Threat Labs

Jamf Threat Labs examines two sophisticated spyware attacks and provides recommendations for organizations to defend users from increasingly complex threats.

Jamf Blog

April 19, 2023 by Jamf Threat Labs

The web of connections with iOS 16.4.1

Jamf Threat Labs

In this blog, Jamf Threat Labs analyzes CVE-2023-28206, iOS 16.4.1 patches and CitizenLab's findings on QuaDream's exploits.

Jamf Blog

February 17, 2023 by Jamf Threat Labs

Jamf Threat Labs analyzes the exploited in-the-wild WebKit vulnerability CVE-2022-42856

Jamf Threat Labs

Jamf Threat Labs investigated a WebKit vulnerability that was exploited in the wild. Attackers can exploit CVE-2022-42856 to control code execution within WebKit, giving them the ability to read/write files. This blog explores what the vulnerability looked like in the code and the patches Apple applied.

Apple platform vulnerability **disclosures** and **exploitation**

In 2022 there were..

456

Apple vulnerabilities added to CVE database, **23% less than 2021**

*continuation of downward trend since 2015

9

zero-day vulnerabilities actively exploited

17

known vulnerabilities actively exploited

Exploiting a known vulnerability is almost always **cheaper**, **more readily available** and often **just as effective** as a zero-day vulnerability.

The clock begins ticking upon first disclosure, with rapid security patching being crucial.

Sources: CVE Database, Mandiant

A look into iOS spyware

From a seamless onboarding experience to empowering users to get the most up-to-date resources needed to be productive, apps are the crux of every step in a user's journey.

Addressing mobile security

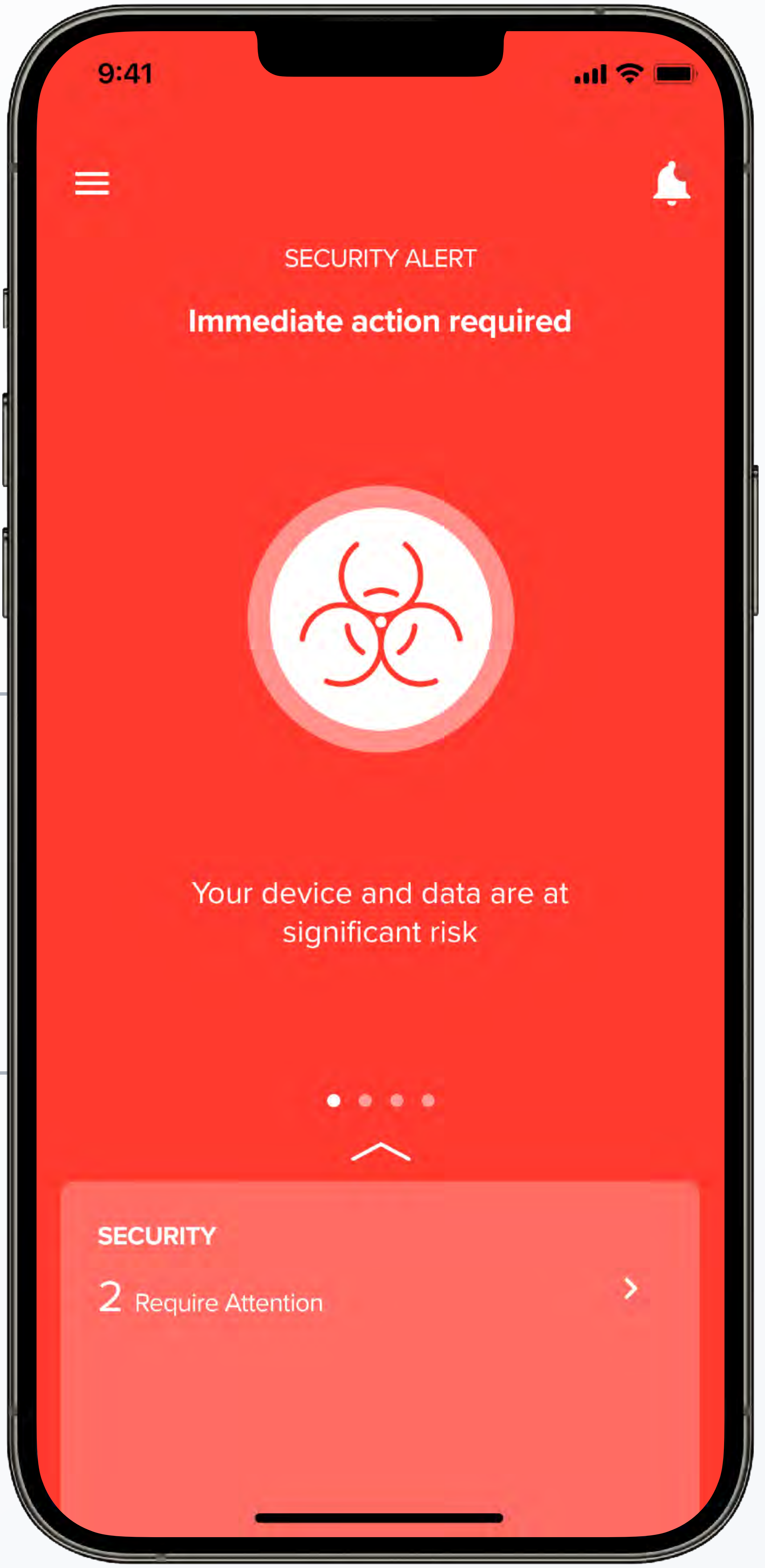
Mobile endpoint security

Device Security

Secure mobile devices against malware as well as highlighting device based vulnerabilities

Network Security

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



9:41

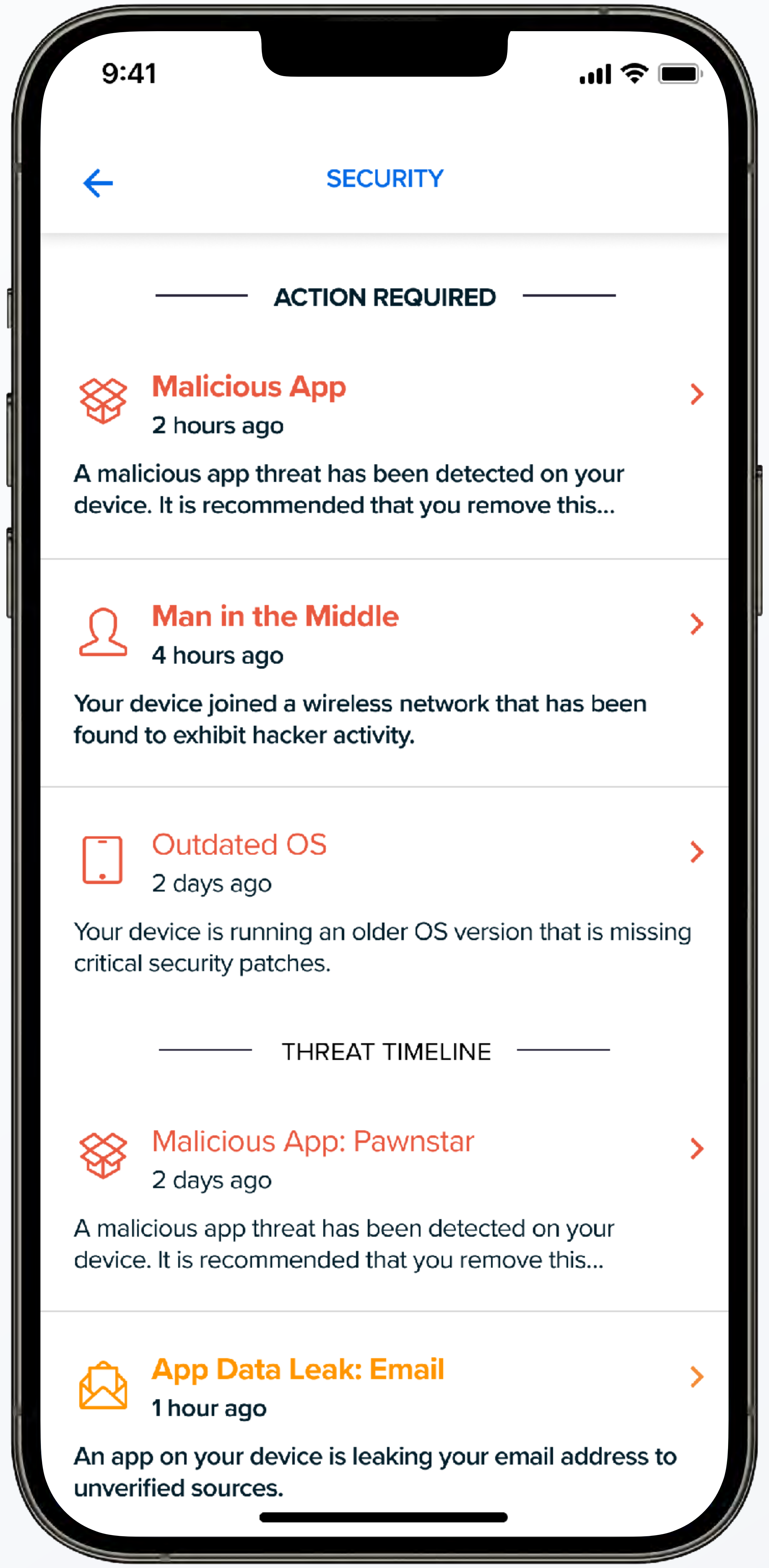
SECURITY ALERT

Immediate action required

Your device and data are at significant risk

SECURITY

2 Require Attention



9:41

SECURITY

ACTION REQUIRED

Malicious App
2 hours ago

A malicious app threat has been detected on your device. It is recommended that you remove this...

Man in the Middle
4 hours ago

Your device joined a wireless network that has been found to exhibit hacker activity.

Outdated OS
2 days ago

Your device is running an older OS version that is missing critical security patches.

THREAT TIMELINE

Malicious App: Pawnstar
2 days ago

A malicious app threat has been detected on your device. It is recommended that you remove this...

App Data Leak: Email
1 hour ago

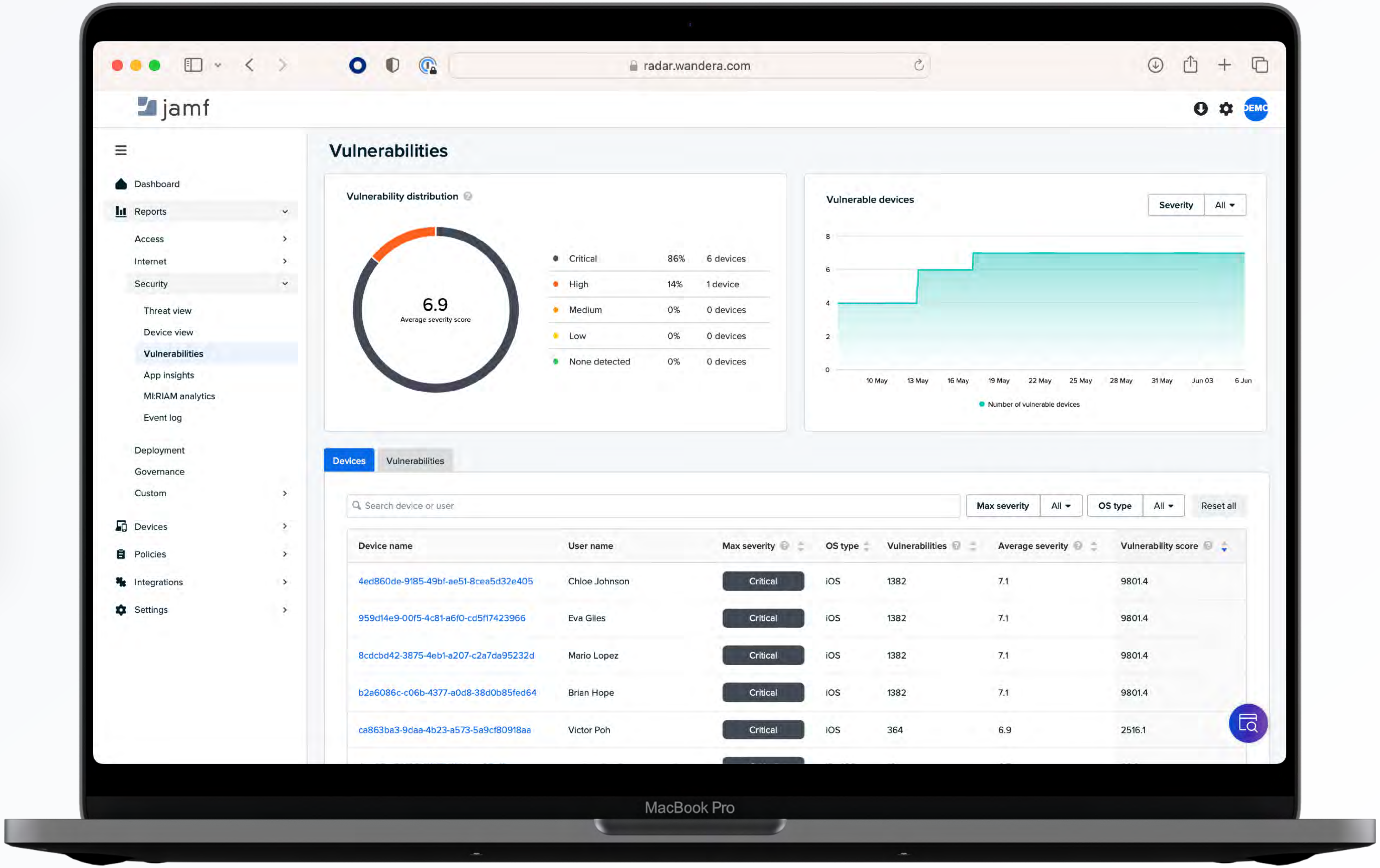
An app on your device is leaking your email address to unverified sources.

JAMF NATION LIVE

Vulnerability management

Visibility 🔍

Risk-based patching 🩹



Vulnerabilities

Vulnerability distribution

6.9
Average severity score

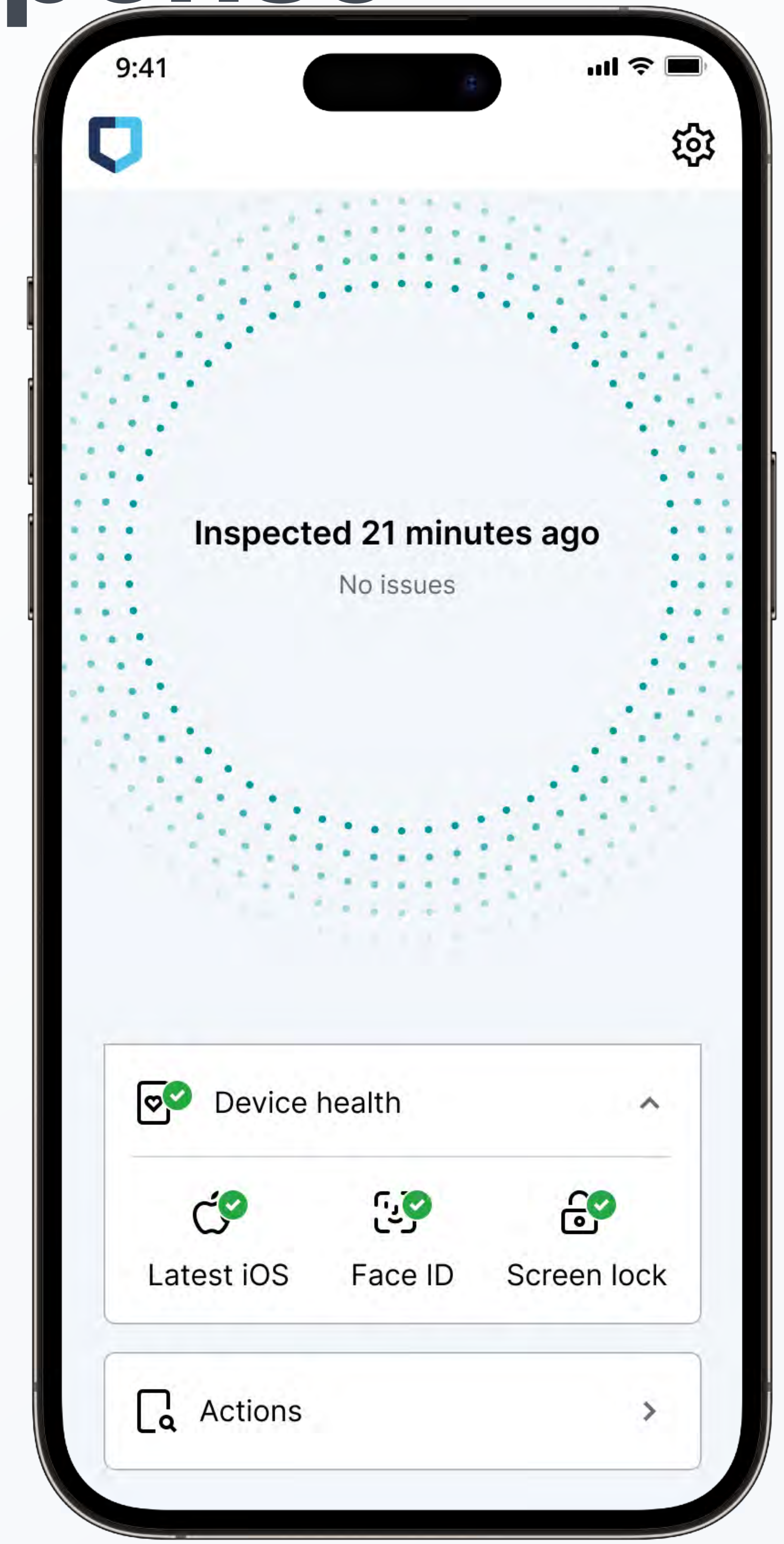
● Critical	86%	6 devices
● High	14%	1 device
● Medium	0%	0 devices
● Low	0%	0 devices
● None detected	0%	0 devices

Device name	User name	Max severity	OS type	Vulnerabilities	Average severity	Vulnerability score
4ed860de-9185-49bf-ae51-8cea5d32e405	Chloe Johnson	Critical	iOS	1382	7.1	9801.4
959d14e9-00f5-4c81-a6f0-cd5f17423966	Eva Giles	Critical	iOS	1382	7.1	9801.4
8cdcbd42-3875-4eb1-a207-c2a7da95232d	Mario Lopez	Critical	iOS	1382	7.1	9801.4
b2a6086c-c06b-4377-a0d8-38d0b85fed64	Brian Hope	Critical	iOS	1382	7.1	9801.4
ca863ba3-9daa-4b23-a573-5a9cf80918aa	Victor Poh	Critical	iOS	364	6.9	2516.1

JAMF NATION LIVE

Advanced detection and response

- Collect comprehensive mobile endpoint telemetry
- Detect indicators of compromise (IOC)
- Remediate advanced persistent threats (APT) confidently
- Monitor to ensure device integrity



9:41

Inspected 21 minutes ago

No issues

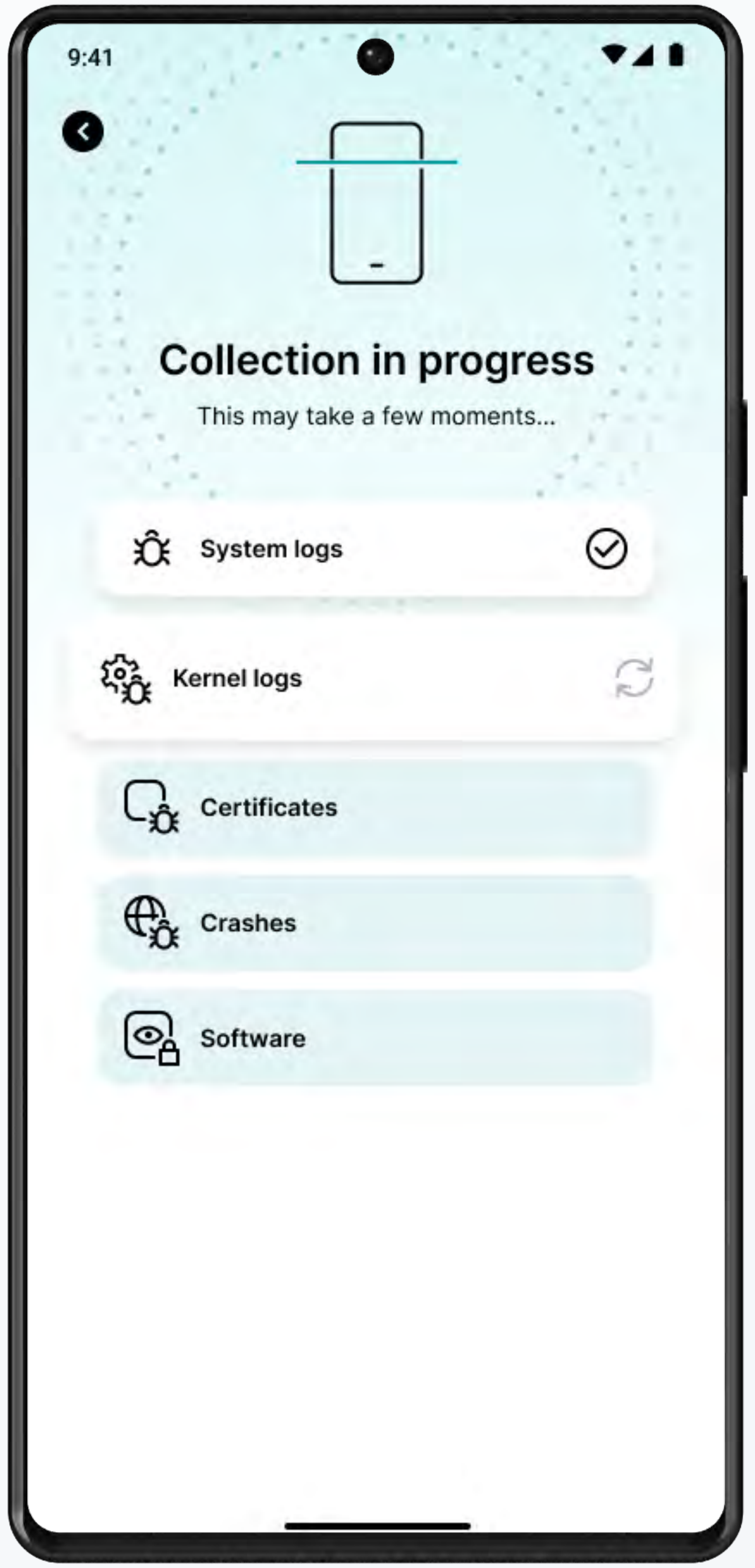
Device health

Latest iOS

Face ID

Screen lock

Actions



9:41

Collection in progress

This may take a few moments...

System logs

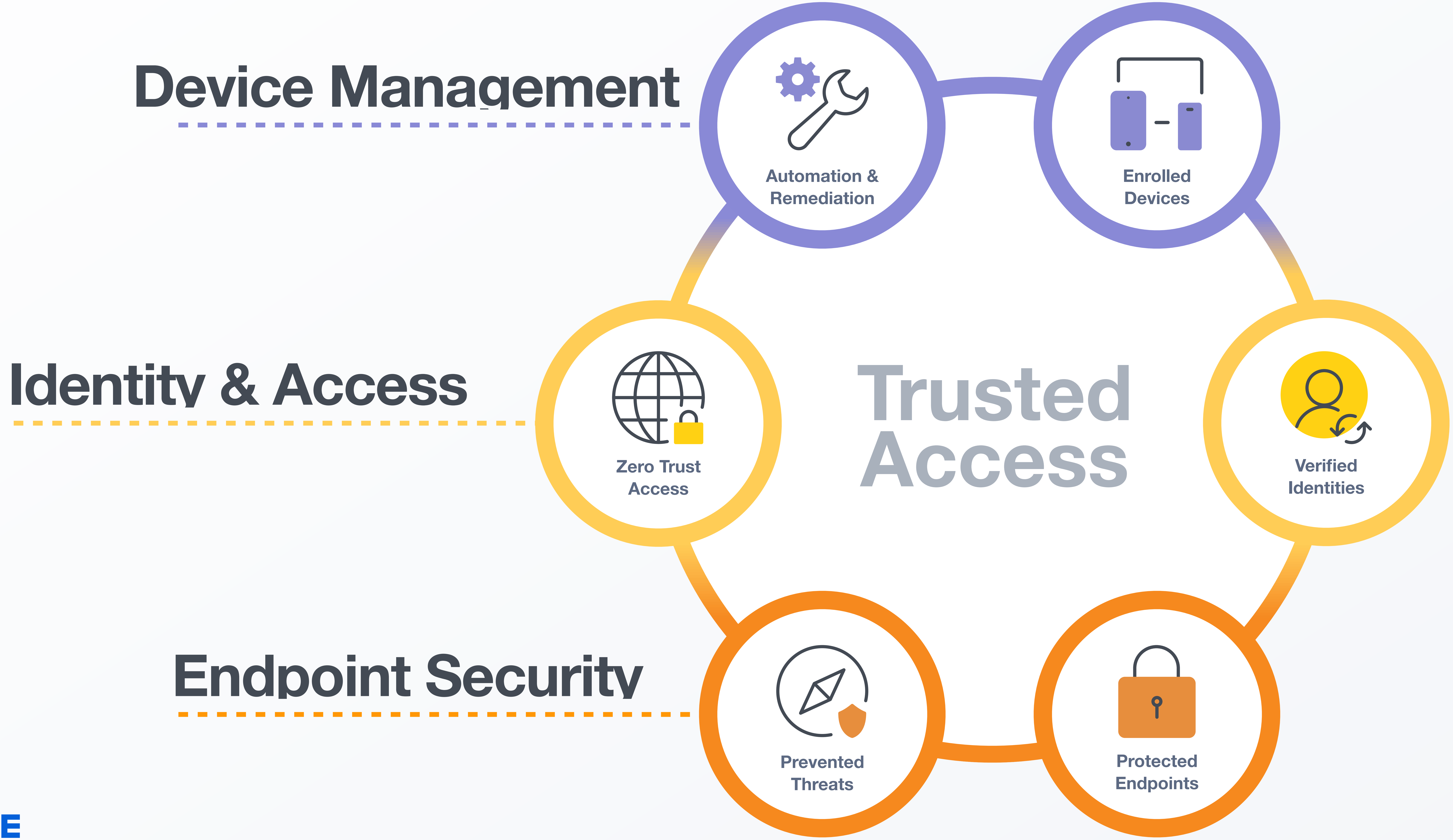
Kernel logs

Certificates

Crashes

Software

JAMF NATION LIVE



Device Management
Identity & Access
Endpoint Security
Automation & Remediation
Enrolled Devices
Zero Trust Access
Trusted Access
Verified Identities
Prevented Threats
Protected Endpoints

only **Authorized Users**

on **Enrolled Devices**

that are **Secure & Compliant**

can **Access Sensitive Data**

Trusted Access

Thank You!