SALLE SÉCURITÉ

JAMF NATION LIVE

Securing iOS and Android: Navigating Modern Mobile Threats

Milind Patel Product Management Director, Jamf

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

JAMF NATION LIVE

Work is increasing on mobile

Rise of Remote Work

46%

Remote users

The State of Security 2022, Splunk

Work is increasing on mobile

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

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

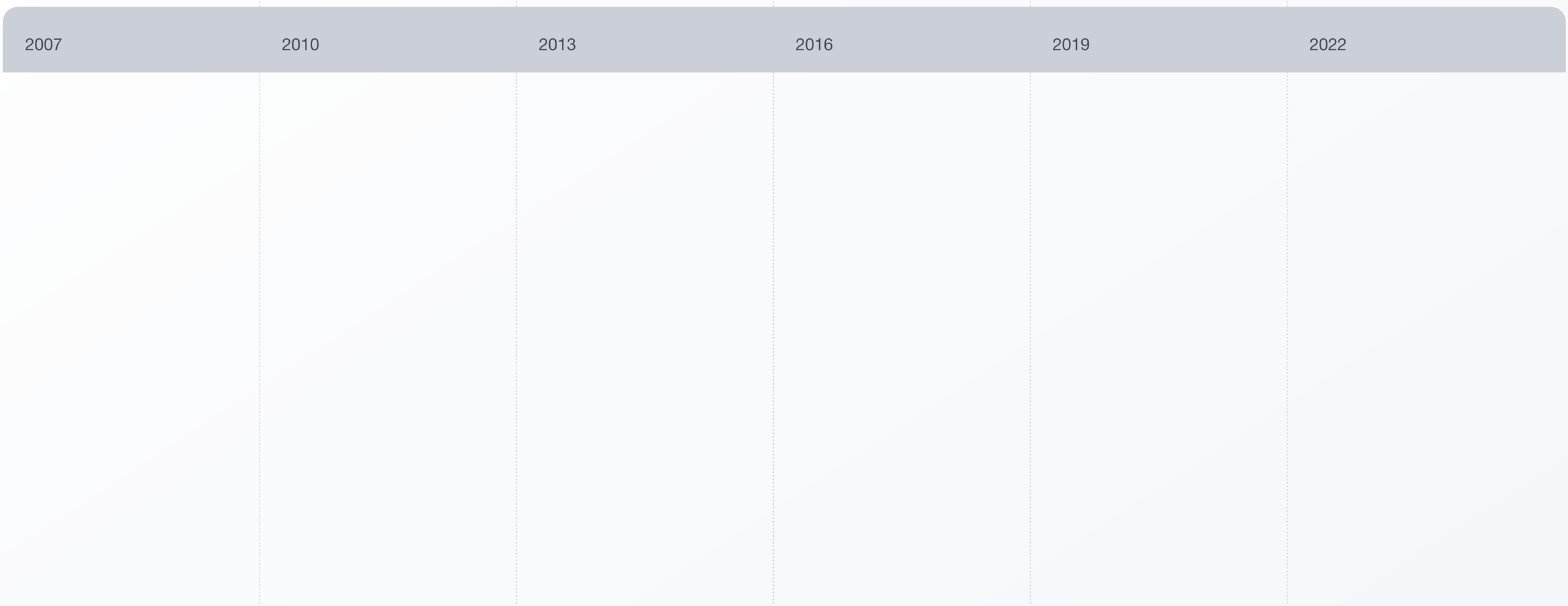
Global public Wi-Fi hotspots 2016-2022, Statista

Rise of Remote Work

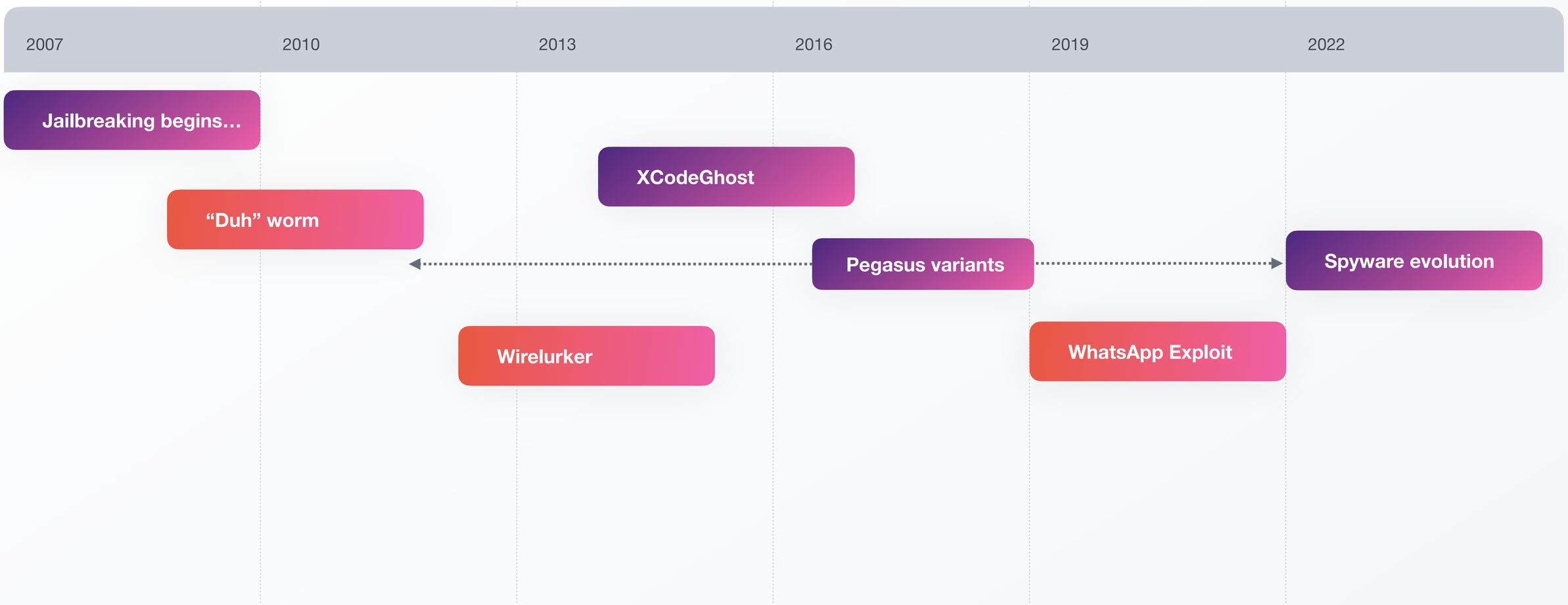
46%
Remote users

The State of Security 2022, Splunk

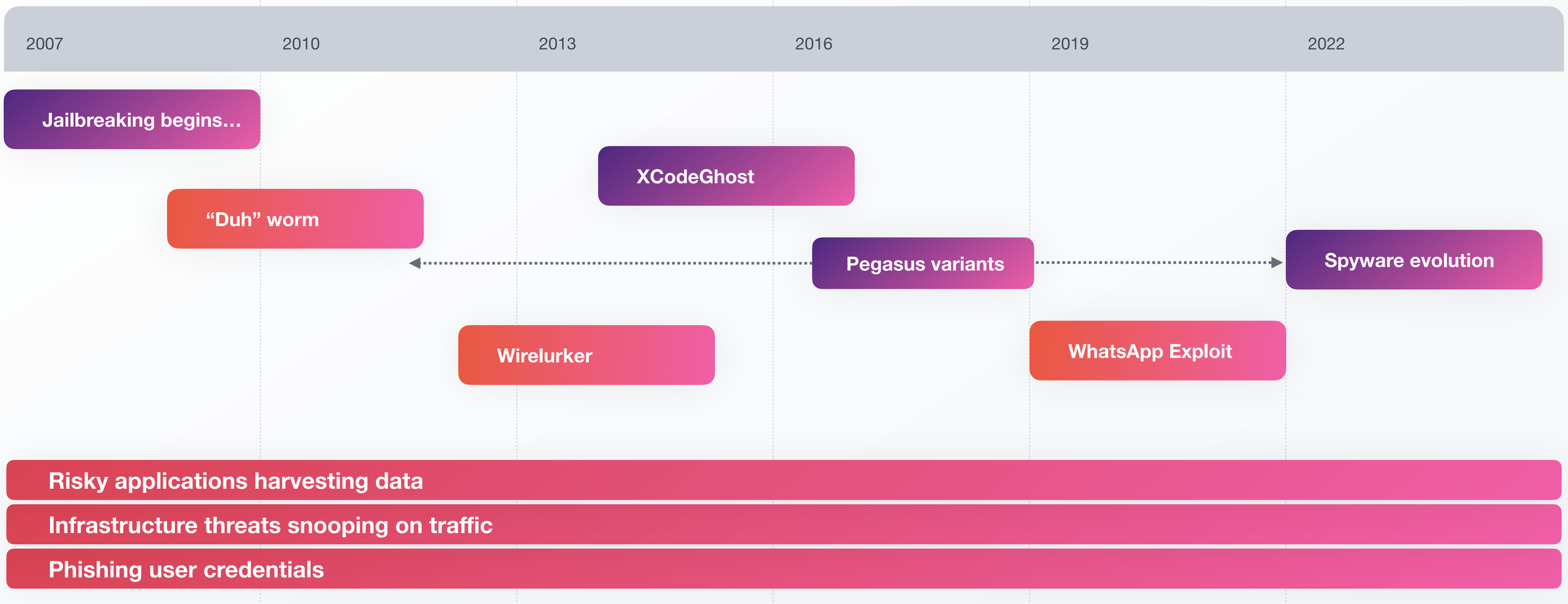
A brief timeline of iOS security challenges



A brief timeline of iOS security challenges



A brief timeline of iOS security challenges



Understanding mobiles

iOS security features

iOS security features

Hardware security and biometrics

Secure Enclave

Biometric Authentication

iOS security features

Hardware security and biometrics

Secure Enclave

Biometric Authentication

System security

Secure Boot Chain

iOS security features

Hardware security and biometrics

Secure Enclave

Biometric Authentication

System security

Secure Boot Chain

App security

Application Sandboxing

iOS security features

Hardware security and biometrics

Secure Enclave

Biometric Authentication

App security

App Store Review Process

Mandatory Code Signing

System security

Secure Boot Chain

App security

Application Sandboxing

iOS security features

Hardware security and biometrics

Secure Enclave

Biometric Authentication

Encryption and Data Protection

Data Encryption

App security

App Store Review Process

Mandatory Code Signing

System security

Secure Boot Chain

App security

Application Sandboxing

How does Android deviate from this?

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
AitM, 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

“An unknown security flaw in software that is exploited by attackers before the developer has a chance to fix it”

Threat Actors taking a bite of the Apple vulnerabilities

456

Apple product vulnerabilities were added to CVE database, **down 23% from 2021**

*continuation of downward trend since 2015

9

zero-day vulnerabilities were known to have be exploited

JAMF NATION LIVE

Sources: CVE Database, CISA KEV, Mandiant, Qualys

Threat Actors taking a bite of the Apple vulnerabilities

456

Apple product vulnerabilities were added to CVE database, **down 23% from 2021**

*continuation of downward trend since 2015

9

zero-day vulnerabilities were known to have be exploited

known vulnerabilities actively exploited **increased from 2021**

Known vuln. exploits are almost always **cheaper** to buy, **easier to find or create** and often **just as effective** as a zero-day

The countdown begins **the second vulnerabilities become known**

JAMF NATION LIVE

Sources: CVE Database, CISA KEV, Mandiant, Qualys

Threat Actors taking a bite of the Apple vulnerabilities

456

Apple product vulnerabilities were added to CVE database, **down 23% from 2021**

*continuation of downward trend since 2015

9

zero-day vulnerabilities were known to have be exploited

known vulnerabilities actively exploited **increased from 2021**

Known vuln. exploits are almost always **cheaper** to buy, **easier to find or create** and often **just as effective** as a zero-day

The countdown begins **the second vulnerabilities become known**

Apple's new **Rapid Security Response** updates **significantly shorten** the mean time to patch **(MTTP)** for high-risk vulnerabilities

JAMF NATION LIVE

Sources: CVE Database, CISA KEV, Mandiant, Qualys

Zero-day vulnerabilities

Zero-day vulnerabilities

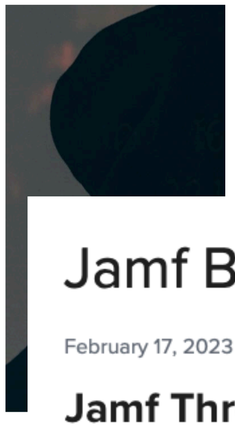
Jamf Blog

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.

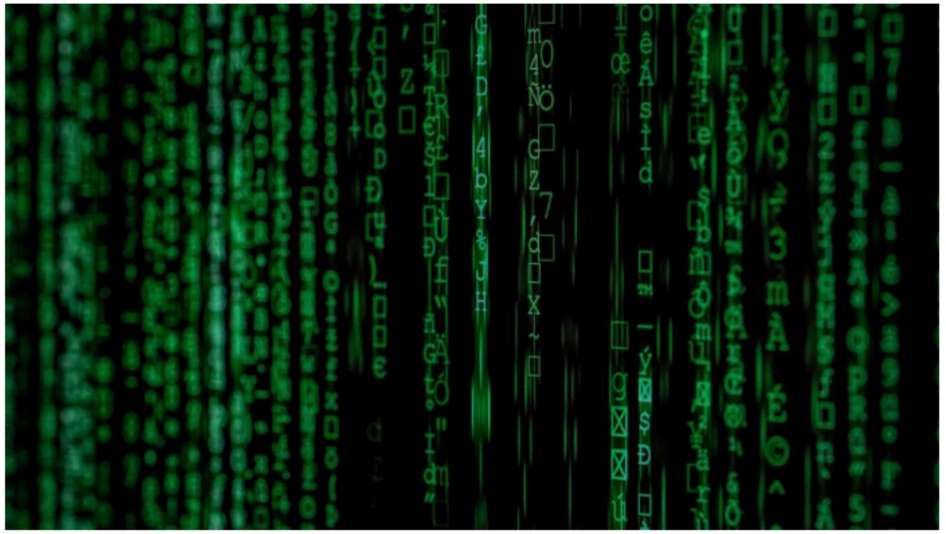
Jamf Blog

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.



JAMF NATION LIVE

Uncovering iOS spyware

Uncovering iOS spyware

- System logs
- Kernel logs
- Certificates
- Crash info
- Software metadata

Uncovering iOS spyware

Process: libtouchregd

com.apple.CrashReporter.plist:

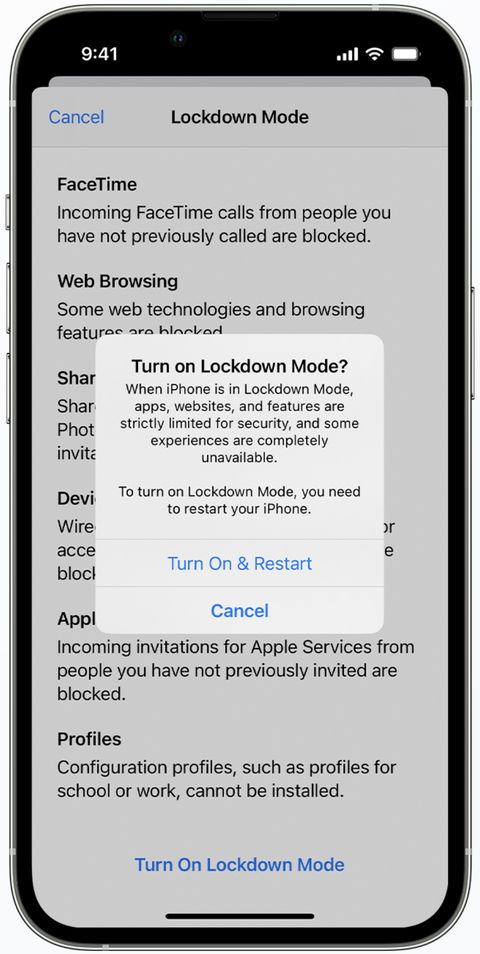
```
{
    "urgentSubmissionCount": 5,
    "urgentSubmissionDay": 19425
}
```

Uncovering iOS spyware

Suspicious com.apple.CrashReporter.plist ⚠️

New IOC: /private/var/containers/appconduitd_helper ⚠️

Uncovering iOS spyware

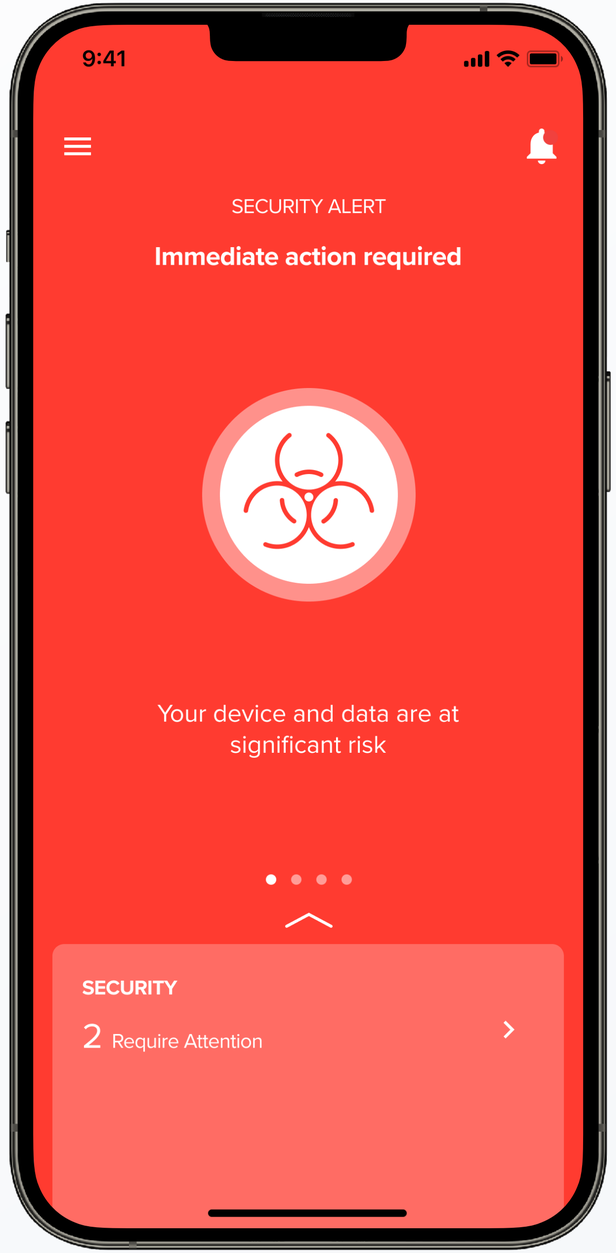


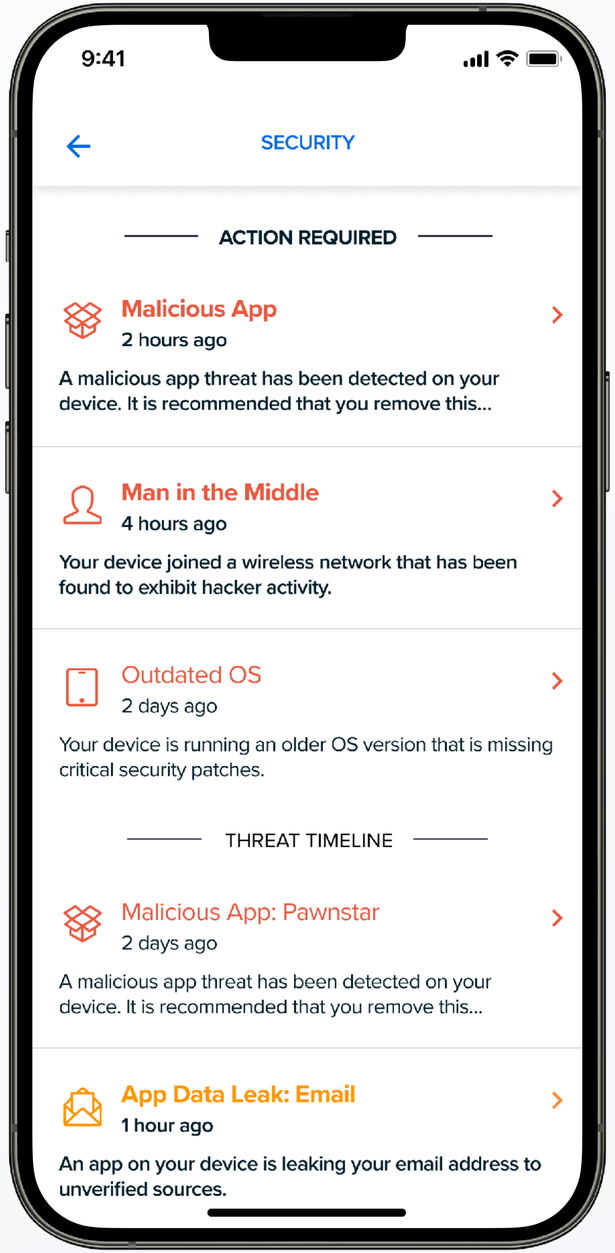
https://www.jamf.com/blog/threat-advisory-mobile-spyware-continues-to-evolve/

Addressing mobile security

JAMF NATION LIVE

Mobile endpoint security





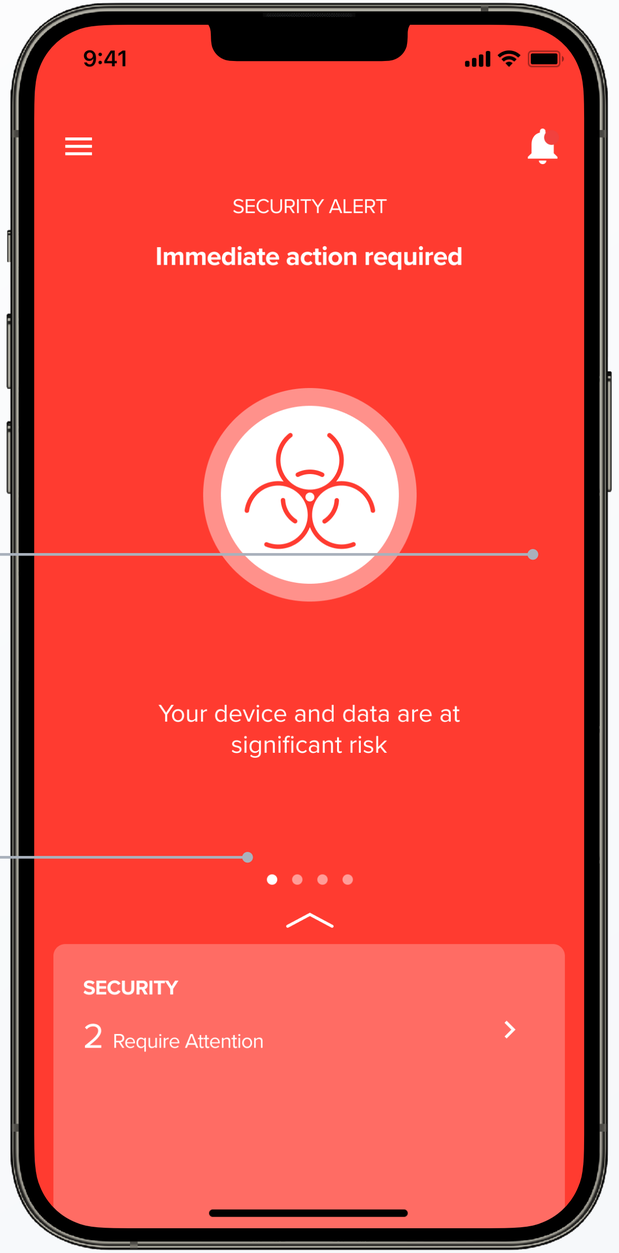
Mobile endpoint security

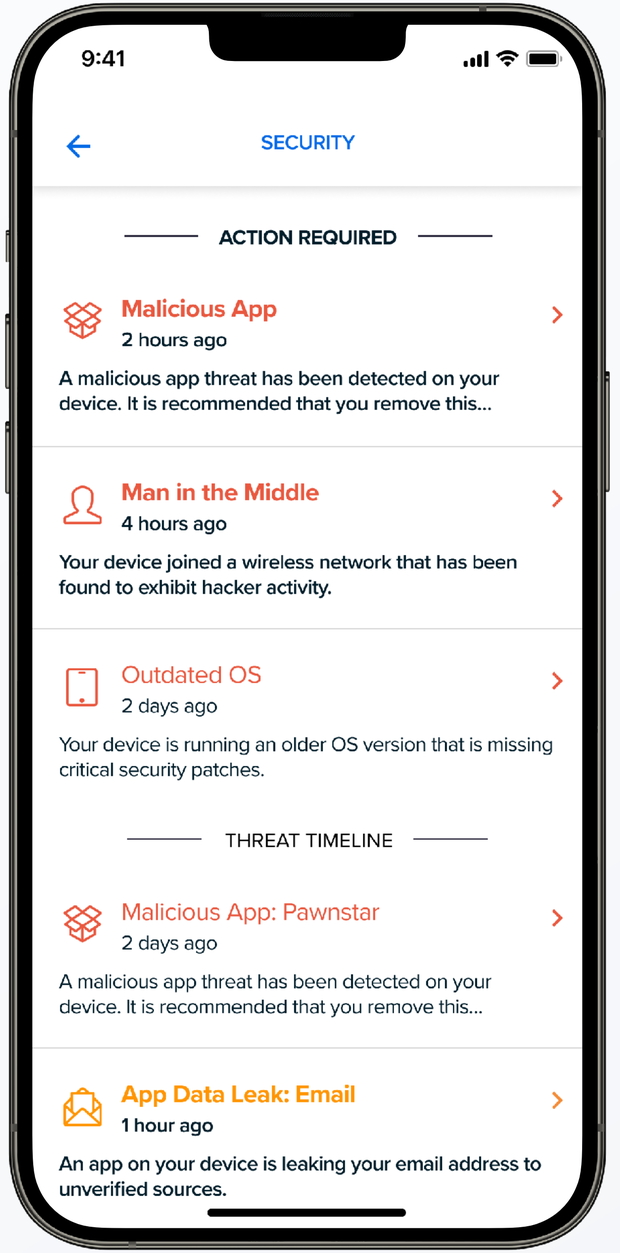
Device Security

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



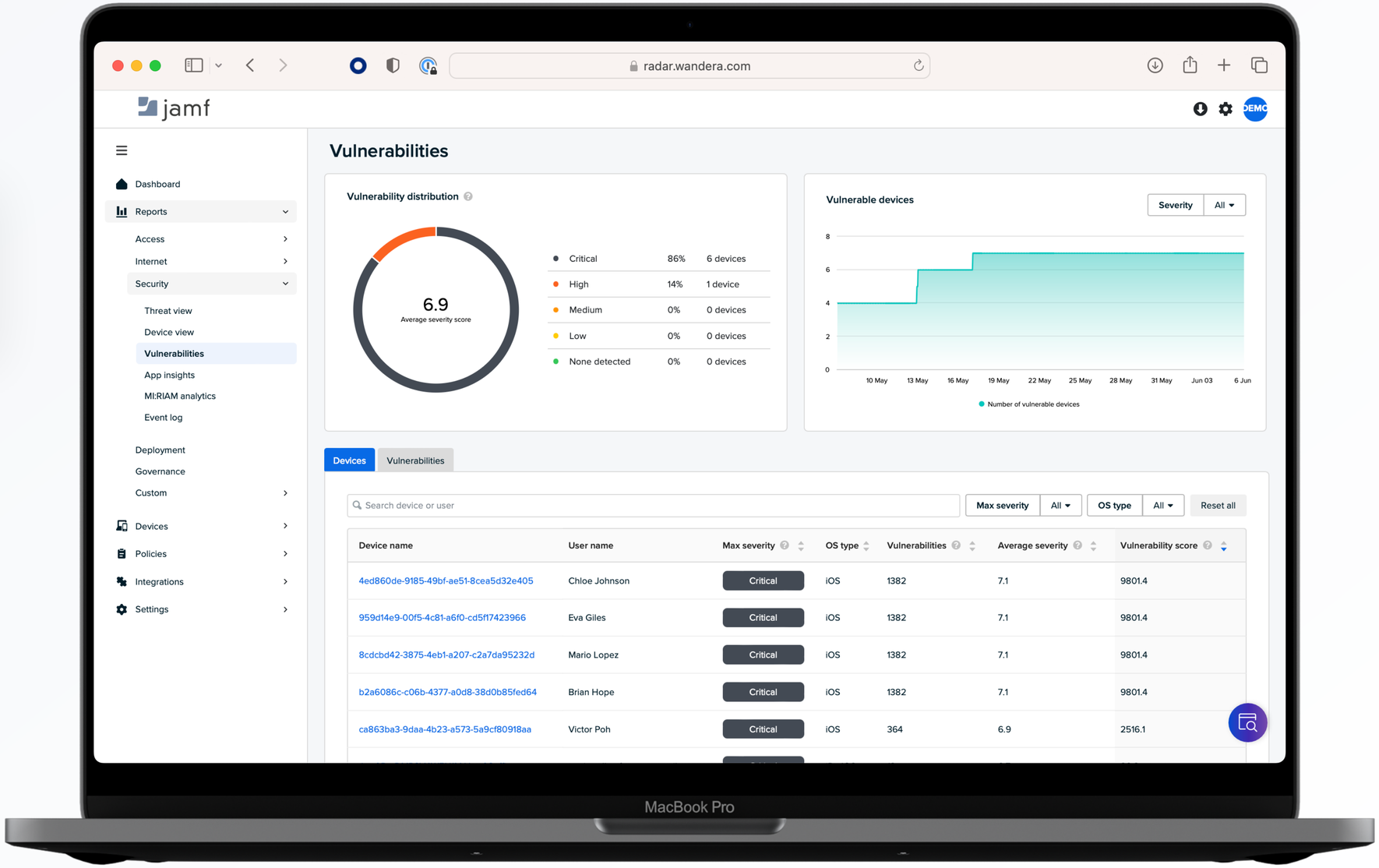


Vulnerability Management

Visibility

Vulnerability management

Visibility

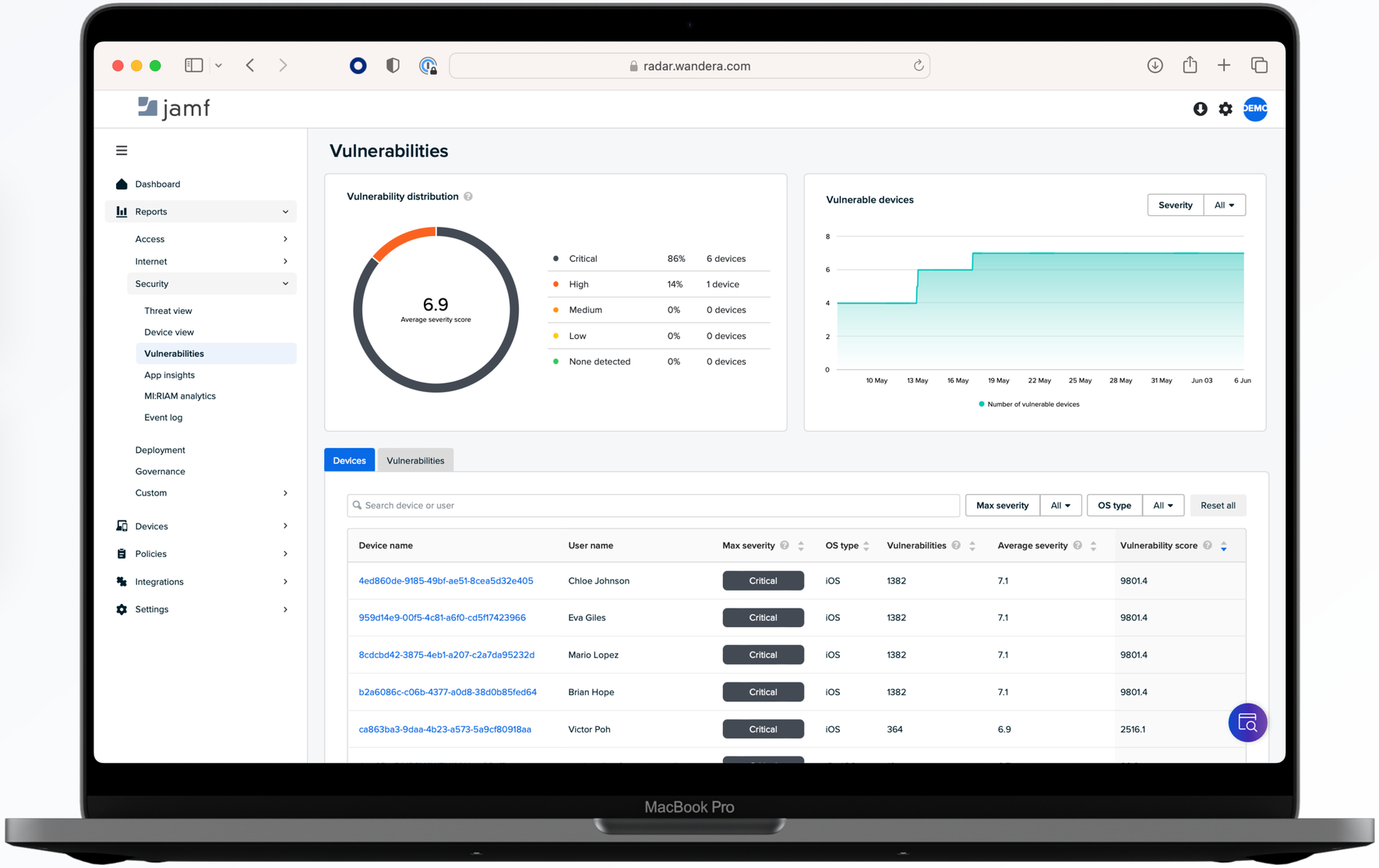


JAMF NATION LIVE

Vulnerability management

Visibility

Risk-based patching

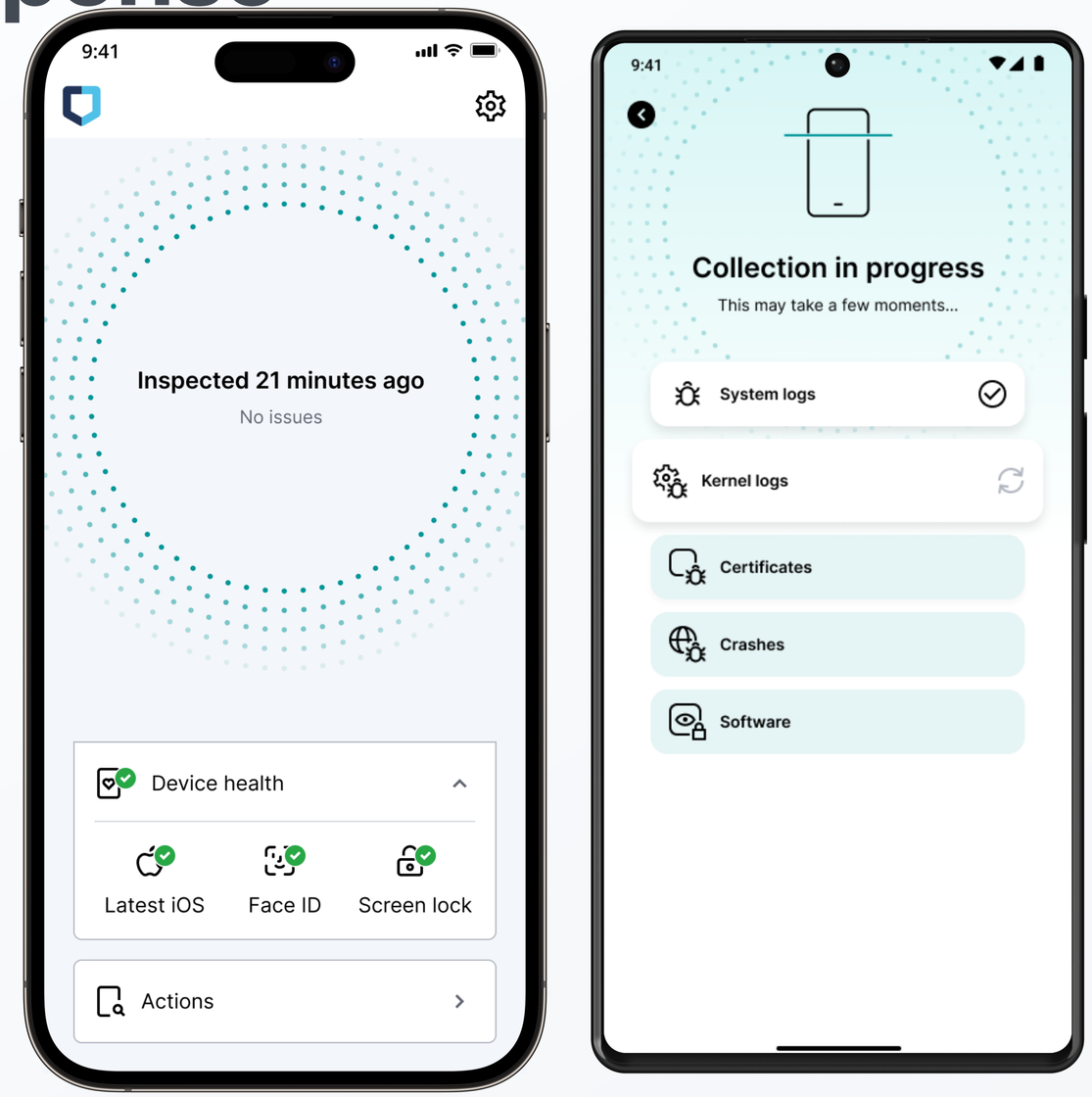


Advanced detection and response

- Collect mobile endpoint telemetry regularly
- Look out for indicators of compromise (IOC)
- Use appropriate tools to remediate advanced persistent threats (APT)

Advanced detection and response

- Collect mobile endpoint telemetry regularly
- Look out for indicators of compromise (IOC)
- Use appropriate tools to remediate advanced persistent threats (APT)



Device Management

Identity & Access

Endpoint Security

Trusted Access

only **Authorized Users**

on **Enrolled Devices**

that are **Secure & Compliant**

can **Access Sensitive Data**

Trusted Access

Thank You!