

● **JAMF NATION LIVE**

starts at **14:00**

Risky Business: Mobile App Security Unpacked



Elmo Kuisma

SALES ENGINEER III
CEE/MEA

**I currently know about vulnerabilities
on our mobile devices?**

**I currently have insights into mobile app
risks in our organisation?**

The Friday Afternoon Ping

“Are we affected by this?”

“How many devices?”

Don't know the CVE

Manual search of device inventory

No visibility of app permissions

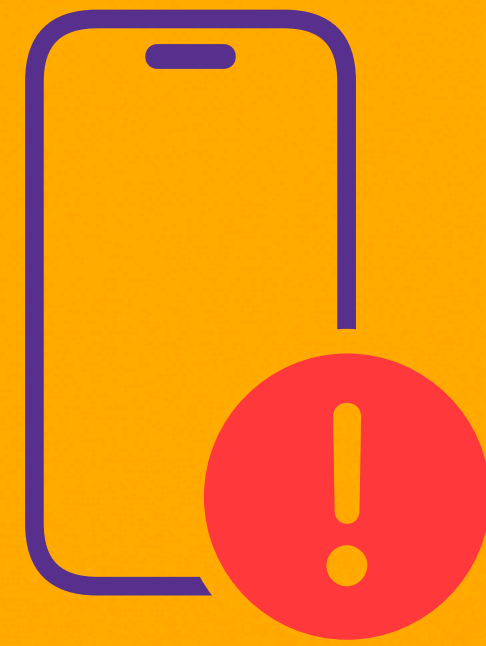
Can't block or control the network

“Can we take devices offline?”

“What's the main risk?”

The gap between finding a threat
and knowing your exposure, is the
problem.

Incident



Days/Weeks

Detection



Weeks/Months



Securing
Reporting

But wait....

what risks can a mobile app
really present?



The App Itself

Code

Network Traffic

User Configurations

Permissions

Access



The App Itself

Code

Network Traffic



Vulnerabilities
Network Behaviour
Third-party Libraries

User Configurations

Permissions

Access



The App Itself

Code

Network Traffic



Vulnerabilities
Network Behaviour
Third-party Libraries

User Configurations

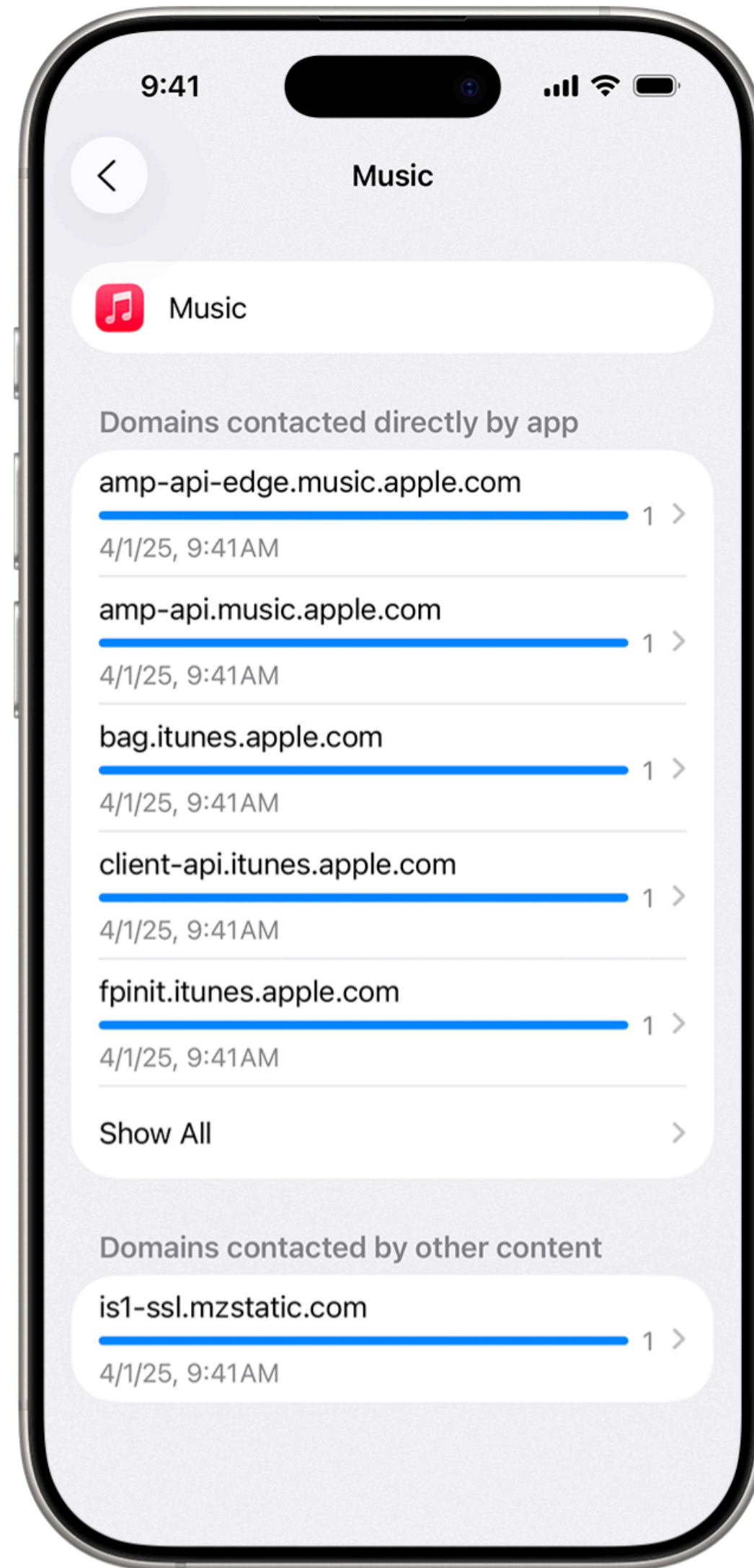
Permissions

Access

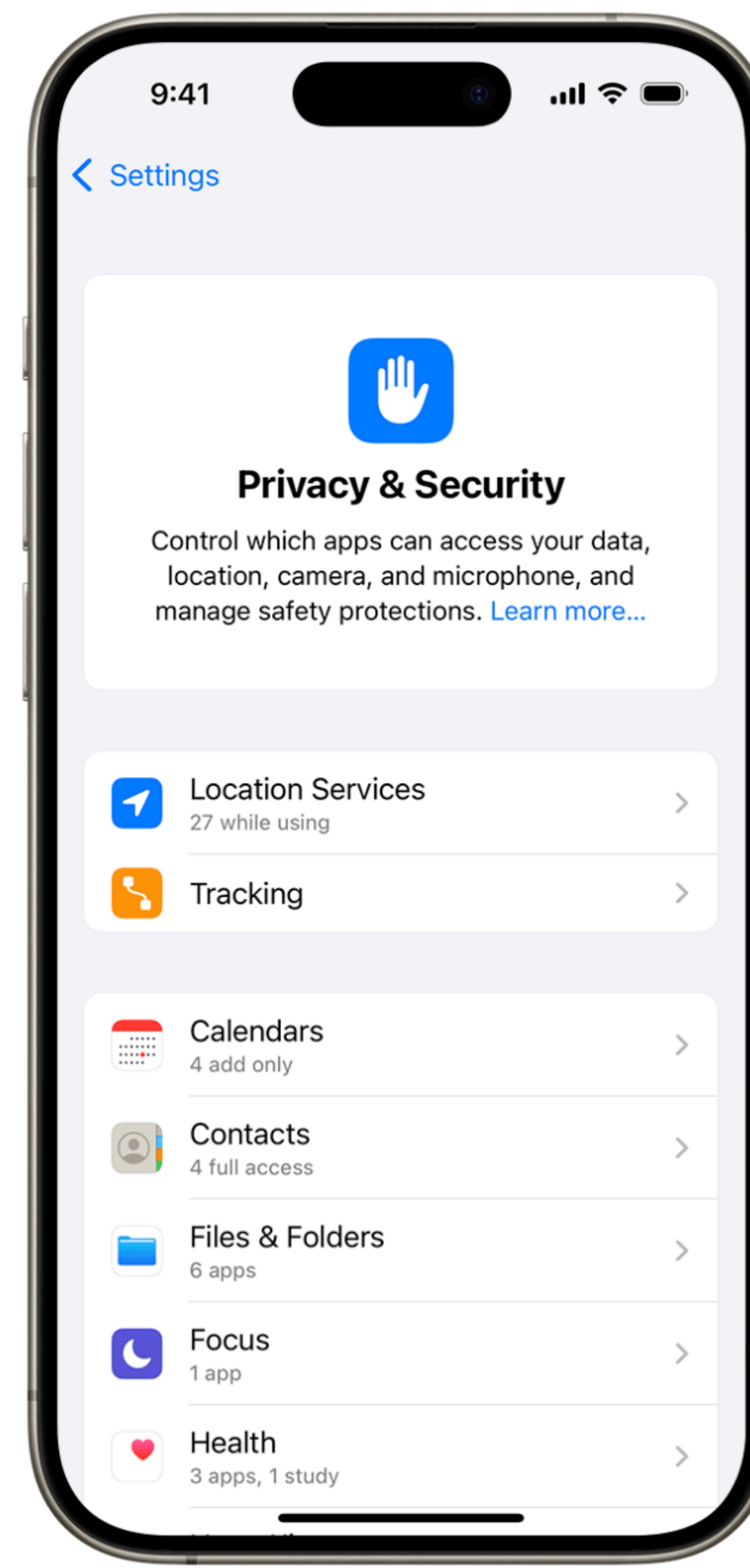


Data over-reach
Exfiltration
Access & Identity

The App Itself



User Configurations



Live Demo

APP VULNERABILITIES:

What does Jamf
tell you about the app
itself?

311 known vulnerabilities

Affected Devices

Exact Software Version

Chrome iOS 4 311

Q Search software version

Software version	Devices	Vulnerabilities	Max severity
125.6422.145	3	311	Critical

Q Search device or user

Device name	User name
iPhone	gerard.daugherty@jamfharbor.com
iPhone	sven.shanahan@jamfharbor.com
iPhone	gerard.daugherty@jamfharbor.com

APP VULNERABILITIES:

What does Jamf tell you about the vulnerabilities?

Severity

First Detection

CVE Description & Link

The screenshot displays the Jamf Vulnerabilities interface. At the top, there are navigation tabs for 'Devices', 'Vulnerabilities' (which is selected), and 'Software'. Below the navigation is a search bar containing 'CVE-2026-8580'. A table lists the vulnerability details:

Vulnerability	Severity ?	CVSS score	Exp
<input type="checkbox"/> CVE-2026-8580	Critical	9.6	No

Below the table, a detailed view for the selected vulnerability is shown:

Severity	Critical	Description
CVSS score	9.6	
Affected devices	24	Attribution
First detected	May 19, 2026	
Exploit code	No	

At the bottom, there is a search bar for 'Search device or user' and a table with columns for 'Device name' and 'User name ?':

Device name	User name ?
HARBOR-Z5Q6DXKGKP	gerard.daugherty@jamfharbor.com

APP VULNERABILITIES:

What does Jamf tell you about the vulnerabilities?

Severity

First Detection

CVE Description & Link

The screenshot shows a web interface for viewing vulnerability details. At the top, there are filters for Severity (All), Exploit code (All), and a Clear button. Below this is a table with columns for CVSS score, Exploit code, and Devices. The CVSS score is 9.6, Exploit code is No, and Devices is 24. The main content area has a Description: "Use after free in Mojo in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)". Below the description is an Attribution link: "Source page". At the bottom, there are filters for Software view (Device view is selected), Software OS (All), and a Clear button. The bottom row shows the user name "rd.daugherty@jamfharbor.com" and the Software OS "macOS 26.1.0".

CVSS score	Exploit code	Devices
9.6	No	24

Description: Use after free in Mojo in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

Attribution: [Source page](#)

Software view: **Device view** | Software OS: All

User name: rd.daugherty@jamfharbor.com | Software OS: macOS 26.1.0

APP INSIGHTS:

Current Risks & Application Forensics

Organisational Risk
Access to data

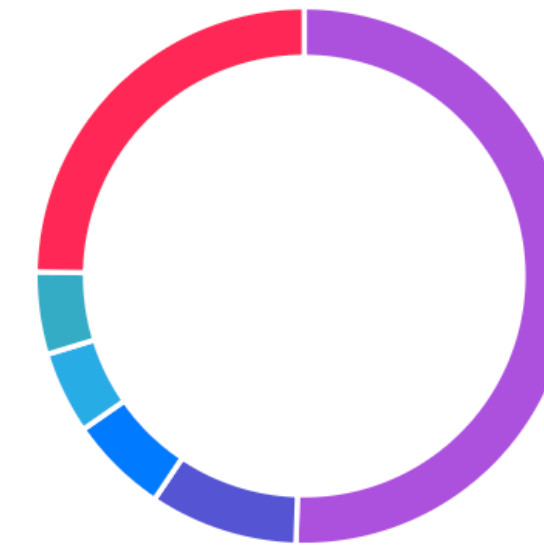
App insights

Apps installed in the last 7 days



No new apps this week

App installations by category







- Productivity 51%
- Business and industry 9%
- Office 365 6%
- Entertainment 5%
- Video and photo 5%
- Other 25%

Apps by risk level ⓘ

Apps	Installations
1 High	6
3 Medium	11
49 Low	256

Application list

Application ⓘ	OS	Versions	Category ⓘ	Installations ⓘ	Risk level ⓘ	
 AV Test App com.fsecure.eicar.antivirus.test 1 APP THREAT		1	Productivity	6	High	Detail view
 WhatsApp com.whatsapp 1 APP THREAT		1	Communication	3	Medium	Detail view
Booking.com						

APP INSIGHTS:

Current Risks & Application Forensics

Organisational Risk
Access to data

The screenshot displays the Google Play Store page for the Chrome app. At the top, the app name 'Chrome' is shown with a 'Free' label and a 'Vulnerable app installed' warning. Below this, the app identifier 'com.google.chrome.ios', developer 'Google', and category 'Productivity' are listed. The 'App versions' section contains a table with columns for Version, OS, Devices, and App risk. The current version, 125.6422.145, is highlighted in blue. The 'App info' section includes a description of the app, a 'Show full description' link, and fields for Version (125.6422.145) and App size (357MB). A risk assessment box indicates 'Low: 0% risk' with a brief explanation. The 'App watchlist management' section is partially visible at the bottom.

Version	OS	Devices	App risk
N/A	Apple	2	Low
149.7827.137	Apple	6	Low
149.7827.45	Apple	2	Low
144.7559.53	Apple	1	Low
132.6834.100	Apple	1	Low
131.6778.134	Apple	1	Low
125.6422.145	Apple	8	Low

App info

Description
Download the new Google Chrome for your iPhone and iPad. Now more simple, secure and faster than ever. Sync your bookmarks and passwords with Chrome on your laptop. Download the fast, secure browser.

NEW - You can now set Chrome as your default browser. Follow the in-app prompt or go to Settings > Default browser to set Chrome as your default browser. From now on, web links will automatically open in Chrome.

Show full description

Version: 125.6422.145
App size: 357MB

App version risk level

Low: 0% risk
This app has been classified as "low risk" by our machine learning e...

App watchlist management

APP INSIGHTS:

Current Risks & Application Forensics

Organisational Risk
Access to data

Application forensics

Application transport security — 2

Global settings

- This app bypasses security best practices and allows communication over insecure network connections ⚠️
- This app does not require certificate transparency for any network communications ⚠️

Permissions — 7

Add or modify Calendar events ?

Add to Photo Library ?

Bluetooth Peripherals ?

Invoke Face ID ?

Precise location - when open (GPS and network-based) ?

Record audio ⚠️

Take pictures and videos ?

Third-party libraries — 2

com.google.chrome.ios.chromessoframework

com.google.chrome.ios.chromeframework

App

Vulnerabilities

Vs

Insights

The screenshot shows a search for 'Chrome' on 'iOS' with version '6' and 208 vulnerabilities. A table lists software versions and their associated vulnerabilities and severity levels.

Software version	Devices	Vulnerabilities	Max severity
125.6422.145	3	208	Critical
147.7727.99	2	3	High

Below the table, a search for 'vulnerabilities' shows a result for 'CVE-2026-7957' with a severity of 'High' and 2 affected devices.

The screenshot displays 'App versions' and 'App info' for Chrome. The app versions table shows the current version (125.6422.145) has a low risk level.

Version	OS	Devices	App risk
N/A	Apple	2	Low
149.7827.137	Apple	6	Low
149.7827.45	Apple	2	Low
144.7559.53	Apple	1	Low
132.6834.100	Apple	1	Low
131.6778.134	Apple	1	Low
125.6422.145	Apple	8	Low

The 'App info' section shows the current version is 125.6422.145 and the app size is 357MB. The 'App version risk level' is 'Low: 0% risk', with a note: 'This app has been classified as "low risk" by our machine learning e...'

We know the risk And the affected devices

What do we do with this information.

Patch, Update

Or remove vulnerable apps

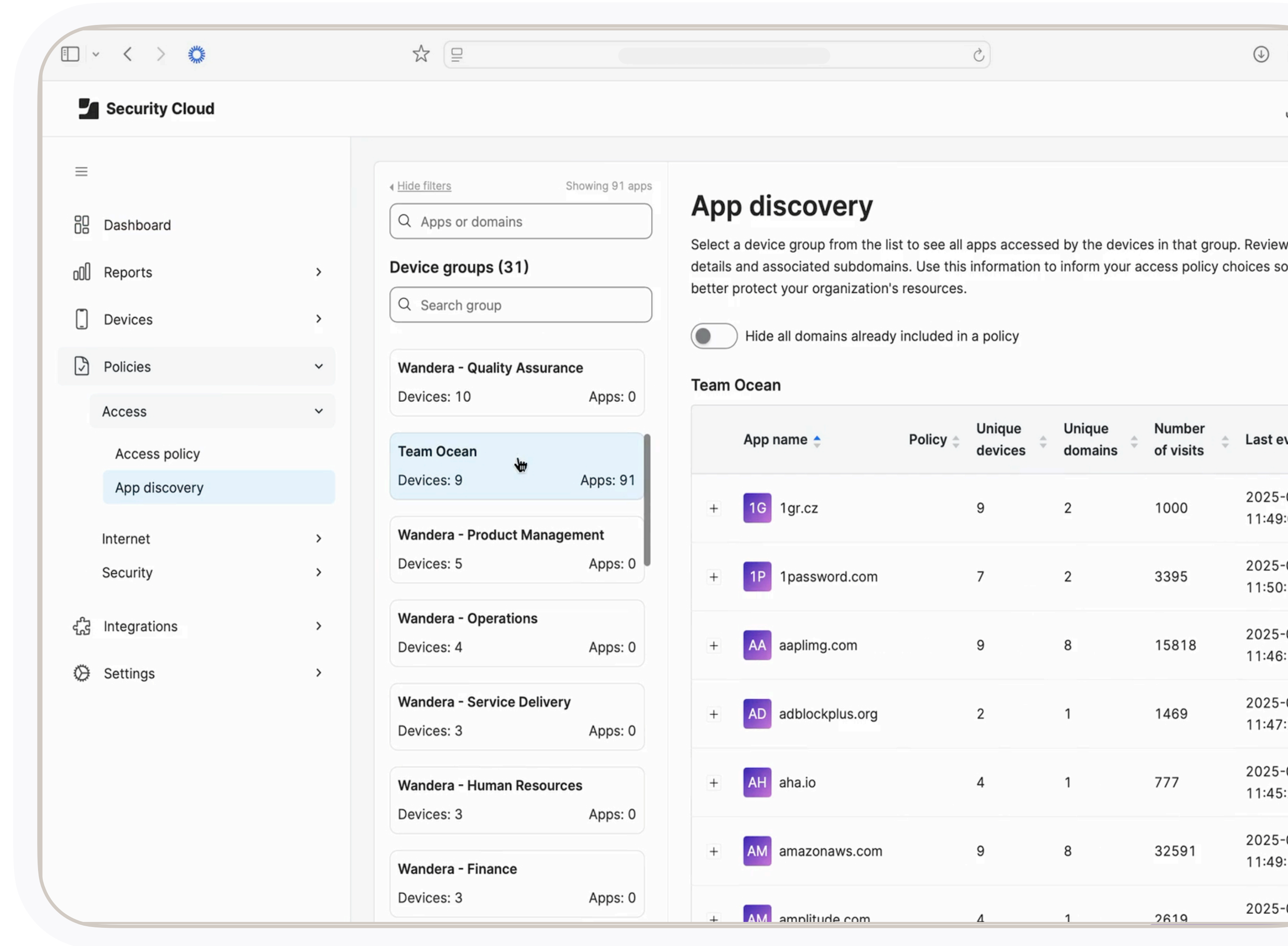
Secure network access
to apps your users actually use

How do I know what to secure?

Discovery most used apps

Create access policies

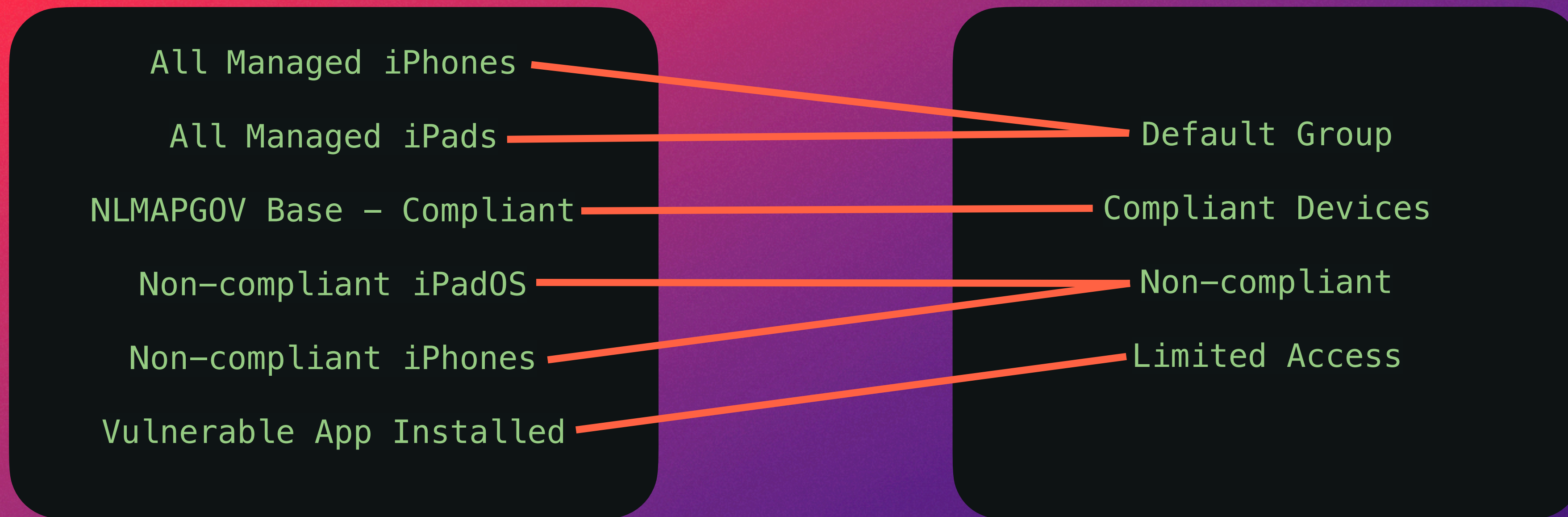
Secure & limit access

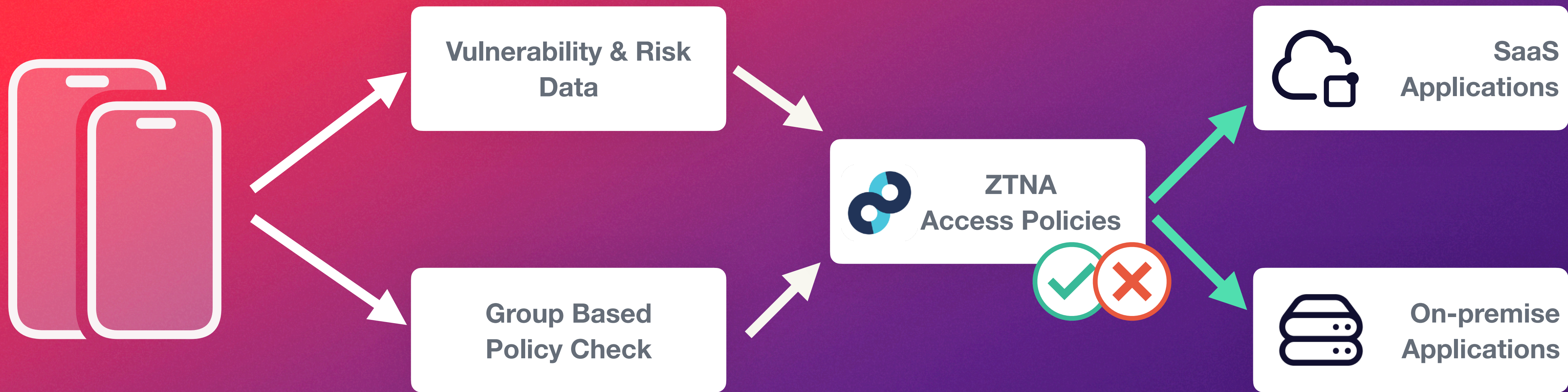


Group Based Access

Jamf Pro

Jamf Security Cloud





The Friday Afternoon Ping

“Are we affected by this”

372 Devices with Chrome

27 running a vulnerable version

11 updates pending

27 devices network access restricted



Mobile
Forensics

Compliance
Benchmarks



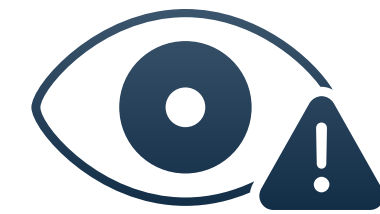
iOS
Android

SIEM
Integration



Zero Trust
Network Access

Vulnerability
Management



CVE
Reporting

Data
Usage



Risk Based
Access

Network
Security



Custom
Remediations

Threat Labs
Research



App
Intelligence



On-Device
Content Filtering



Admin
Alerts

App
Discovery