Utilise Jamf's security solutions to enhance your Device Compliance or Google BeyondCorp workflows

JAMF NATION LIVE

Alexander Dove

Senior Sales Engineer
Security
Jamf

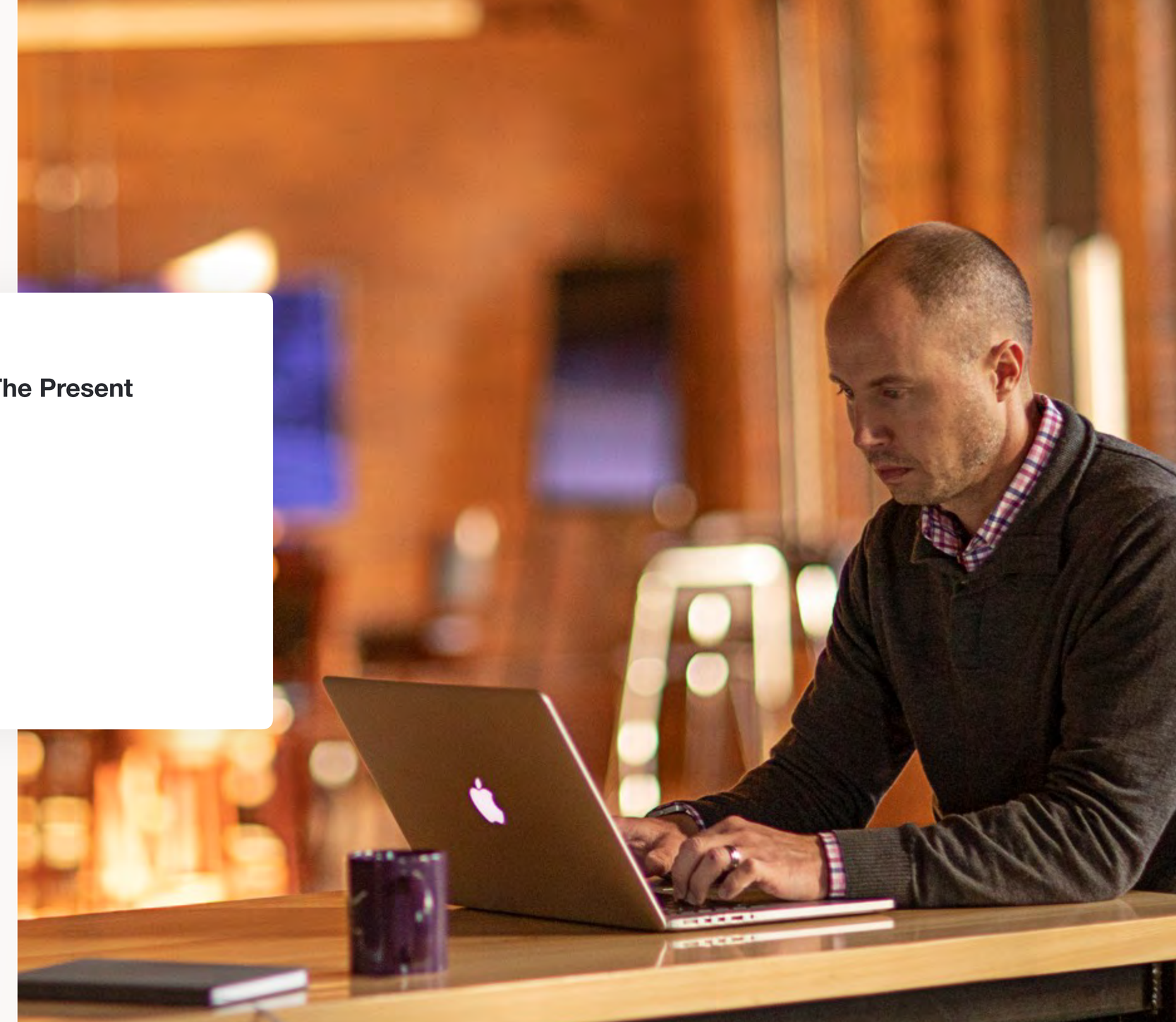
Agenda

1 | Jamf Security – The Past and The Present

2 | Jamf Compliance Workflows

3 | Demo

4 | Q&A



JAMF NATION LIVE

Jamf Security

The Past and The Present

JAMF NATION LIVE

Jamf Security — The present

Jamf Protect Portal

macOS endpoint protection

macOS Security Portal

RADAR Portal

Content Filtering

Threat Defence

Zero Trust Access

Jamf Security Cloud Portal

Jamf Security — The present

macOS endpoint protection

Content Filtering

Threat Defence

Jamf Protect Licence

Zero Trust Access

Cloud idP based Account creation

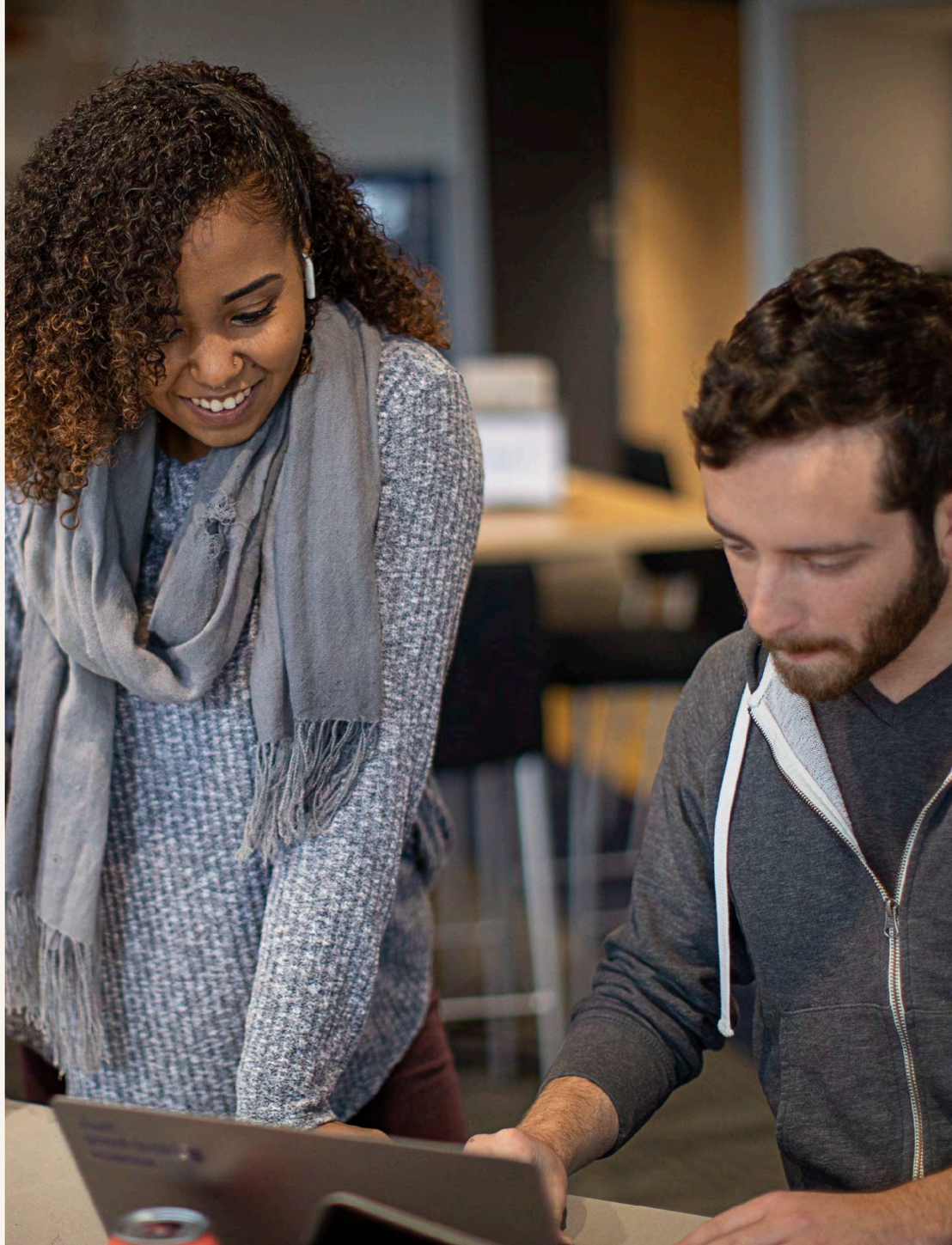
Jamf Connect Licence

Jamf Compliance Workflows

JAMF NATION LIVE

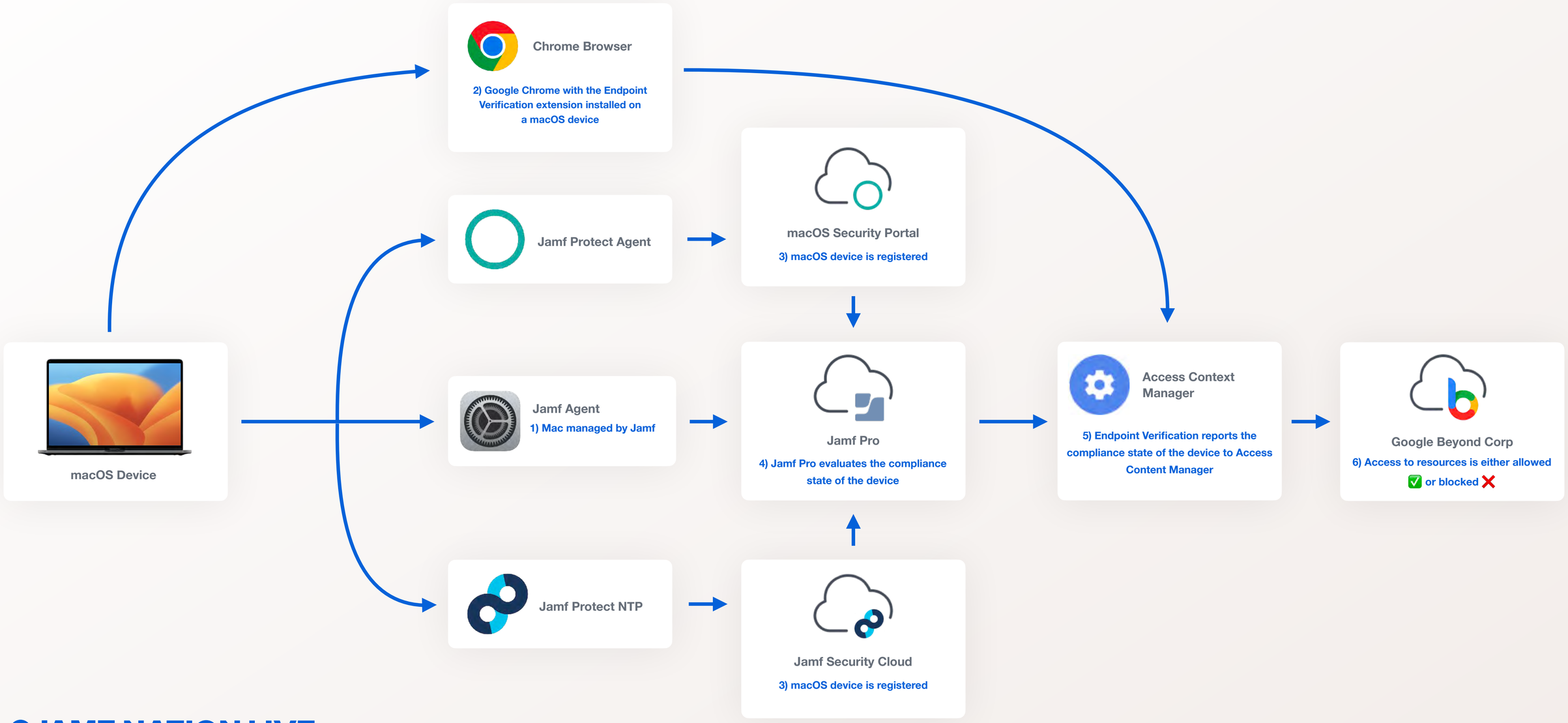
Why **Device Compliance?**

- Allowing best of breed solutions to determine compliance
- Devices can only access corporate data where the user is authorised, and the device is risk-free
- Continuous risk evaluation
- Allows organisations to move towards a true zero-trust model

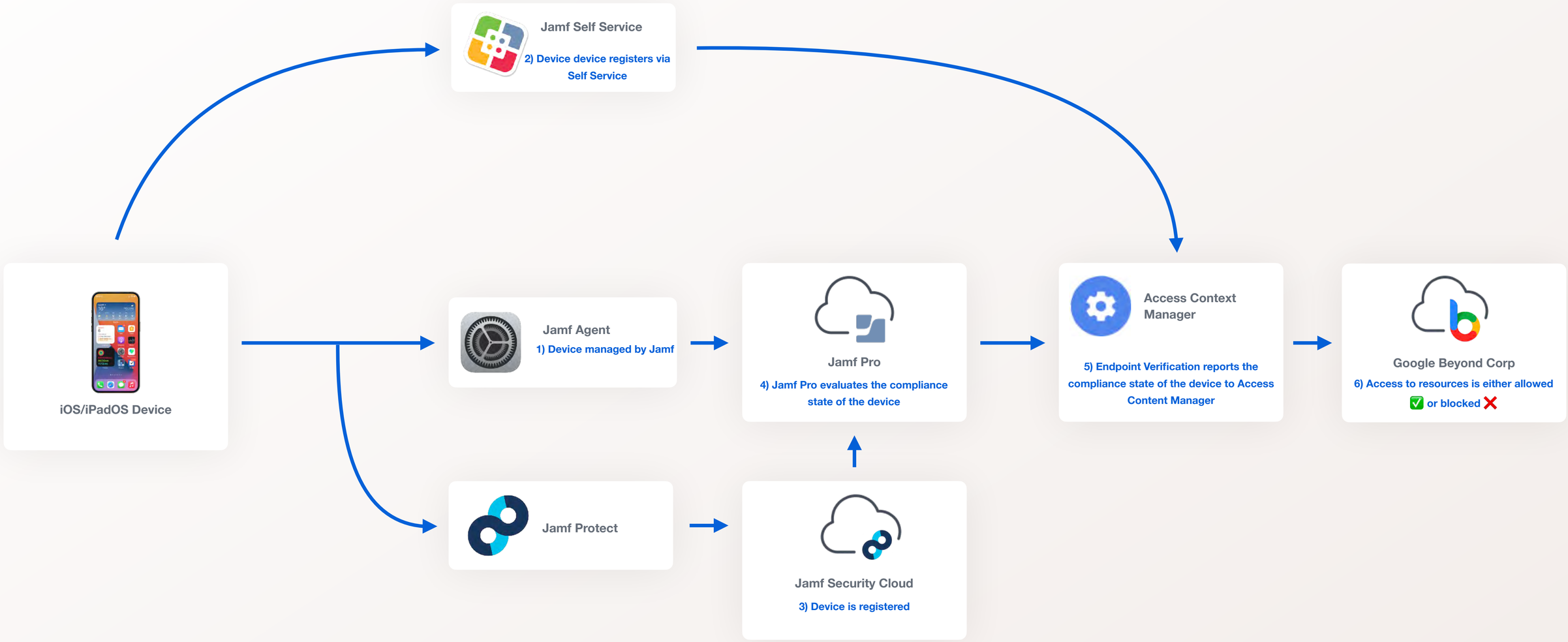


Google Compliance workflows

BeyondCorp Integration for macOS

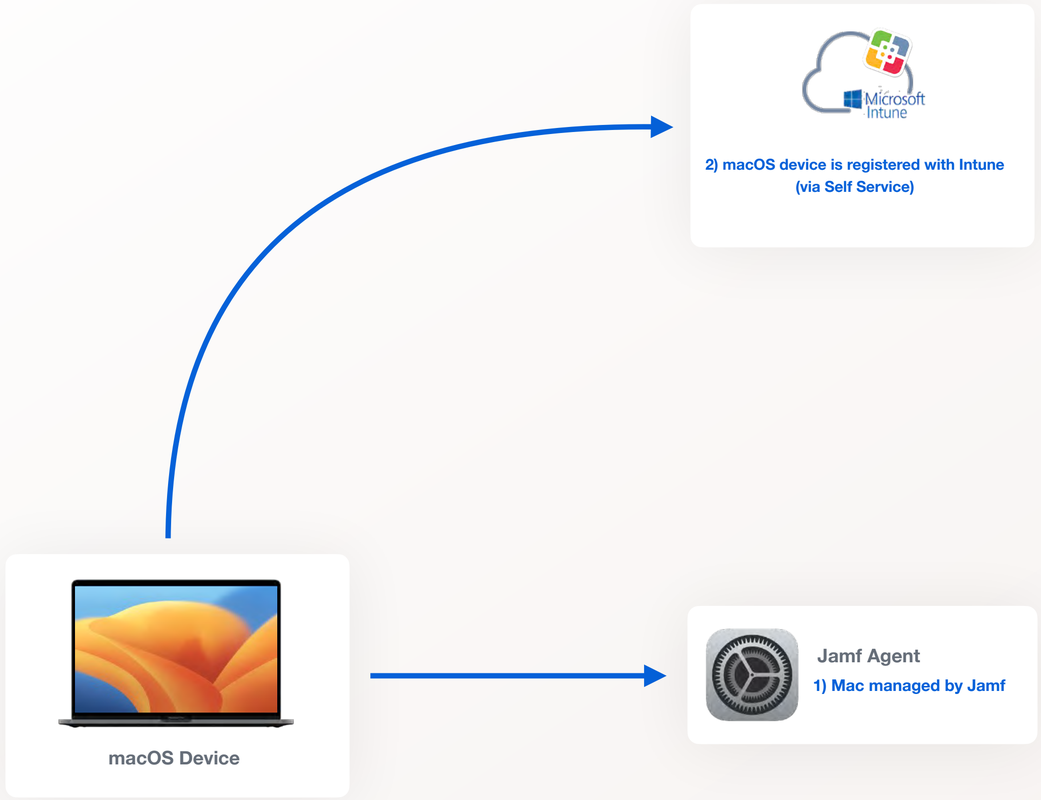


BeyondCorp Integration for Mobile

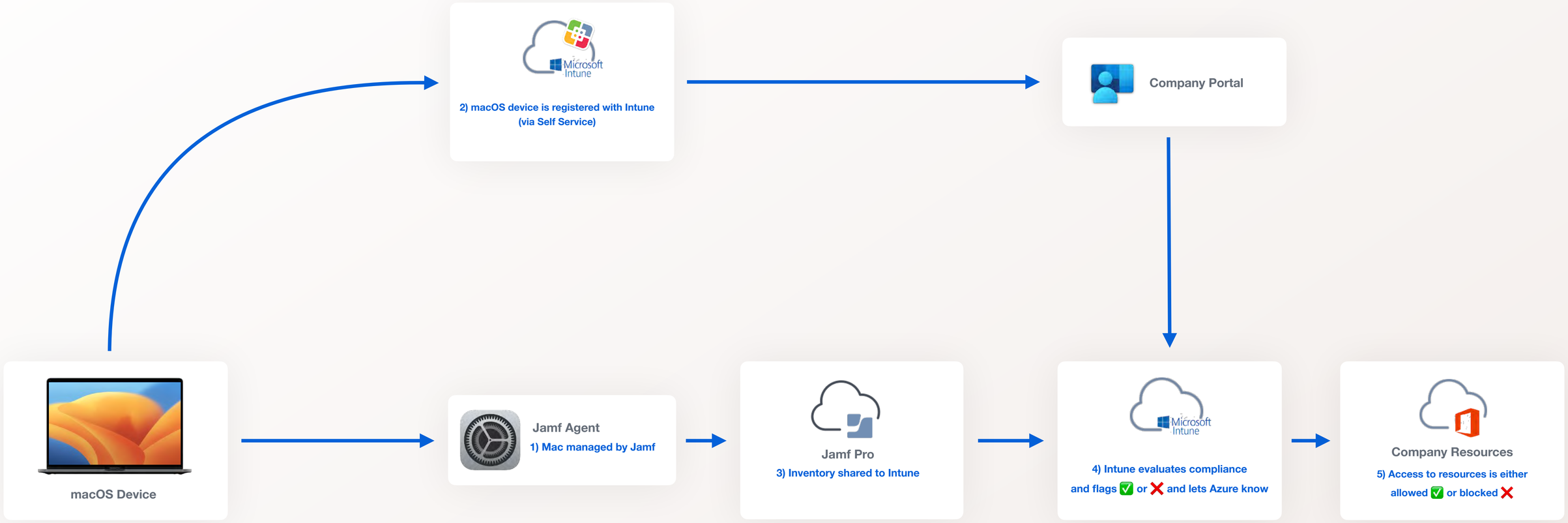


Microsoft Compliance workflows

Conditional Access for macOS



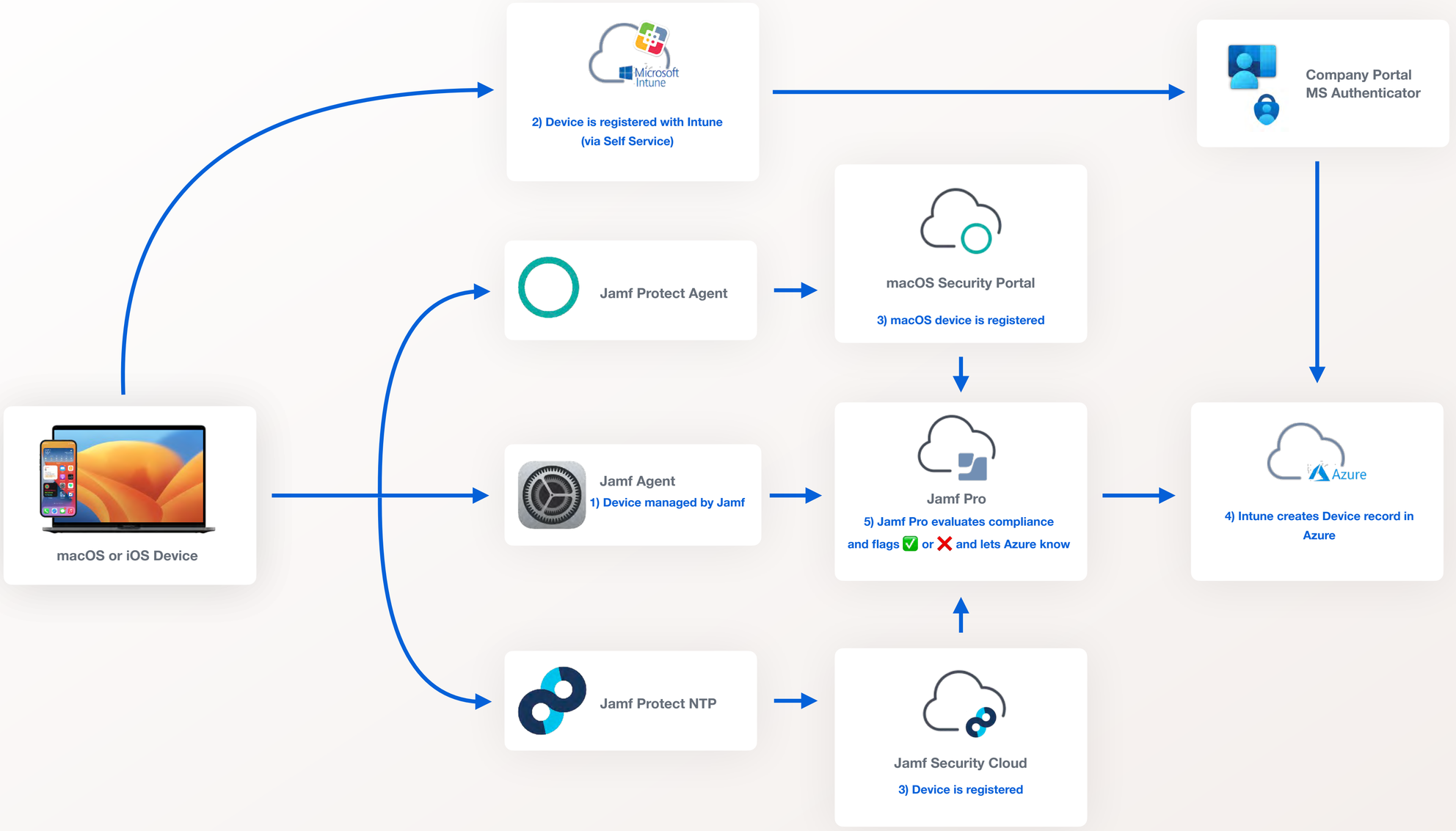
Conditional Access for macOS



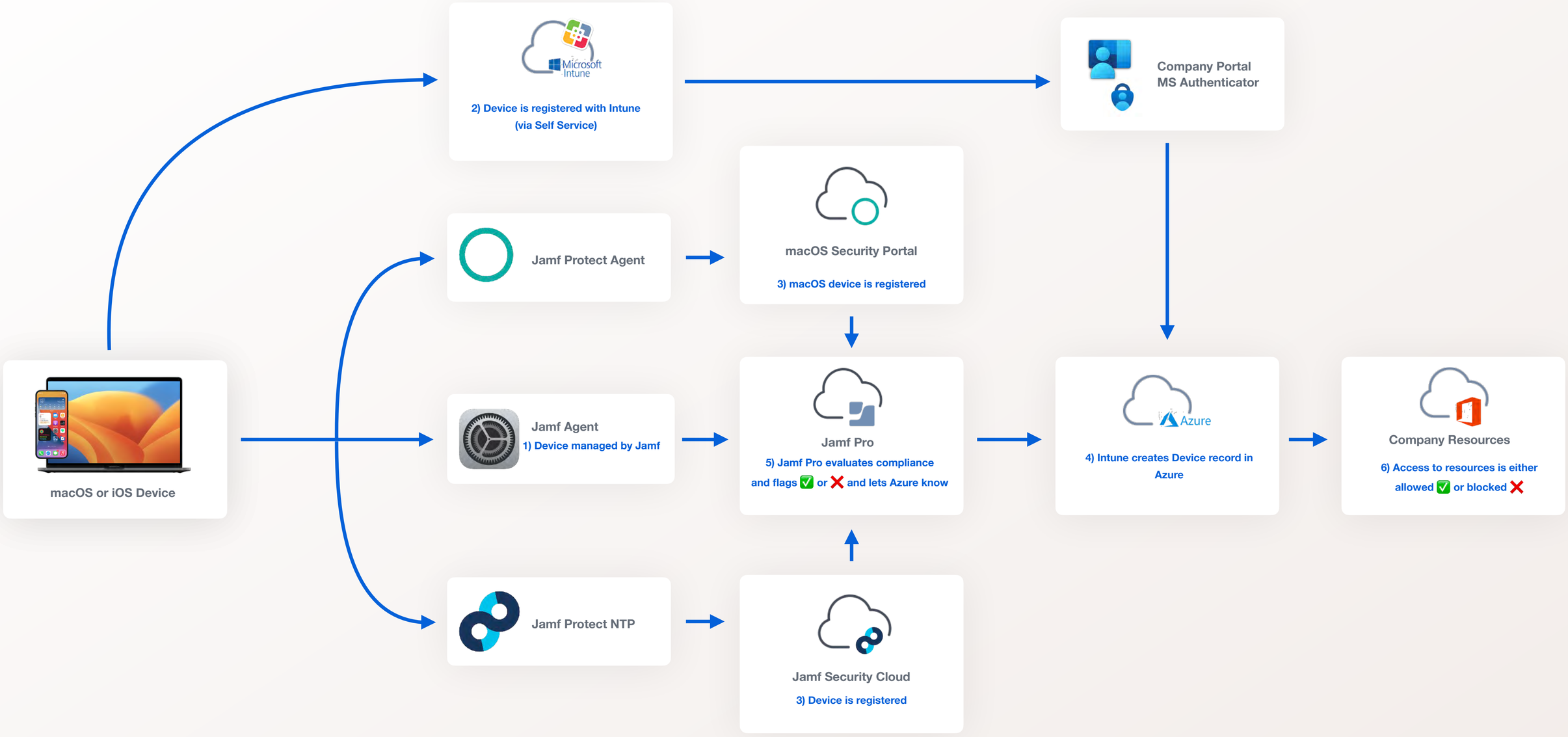
Conditional Access Criteria

Attribute	Example Data Sent to Microsoft Intune	Used in Compliance
OS Version	10.12.4 10.10.3	Yes
Password Requiered	TURE FALSE	Yes
# of previous password to prevent reuse	1 5 NotEnforced	Yes
Minimum # of character sets	2 NotEnforced	Yes
Password expiration (days)	30 NotEnforced	Yes
Password Type	Simple AlphaNumeric NotEnforced	Yes
Required Passcode Length	10 NotEnforced	Yes
Encrypted (FileVault 2)	TRUE FALSE	Yes
Firewall Enabled	TURE FALSE	Yes

Device Compliance for macOS and Mobile

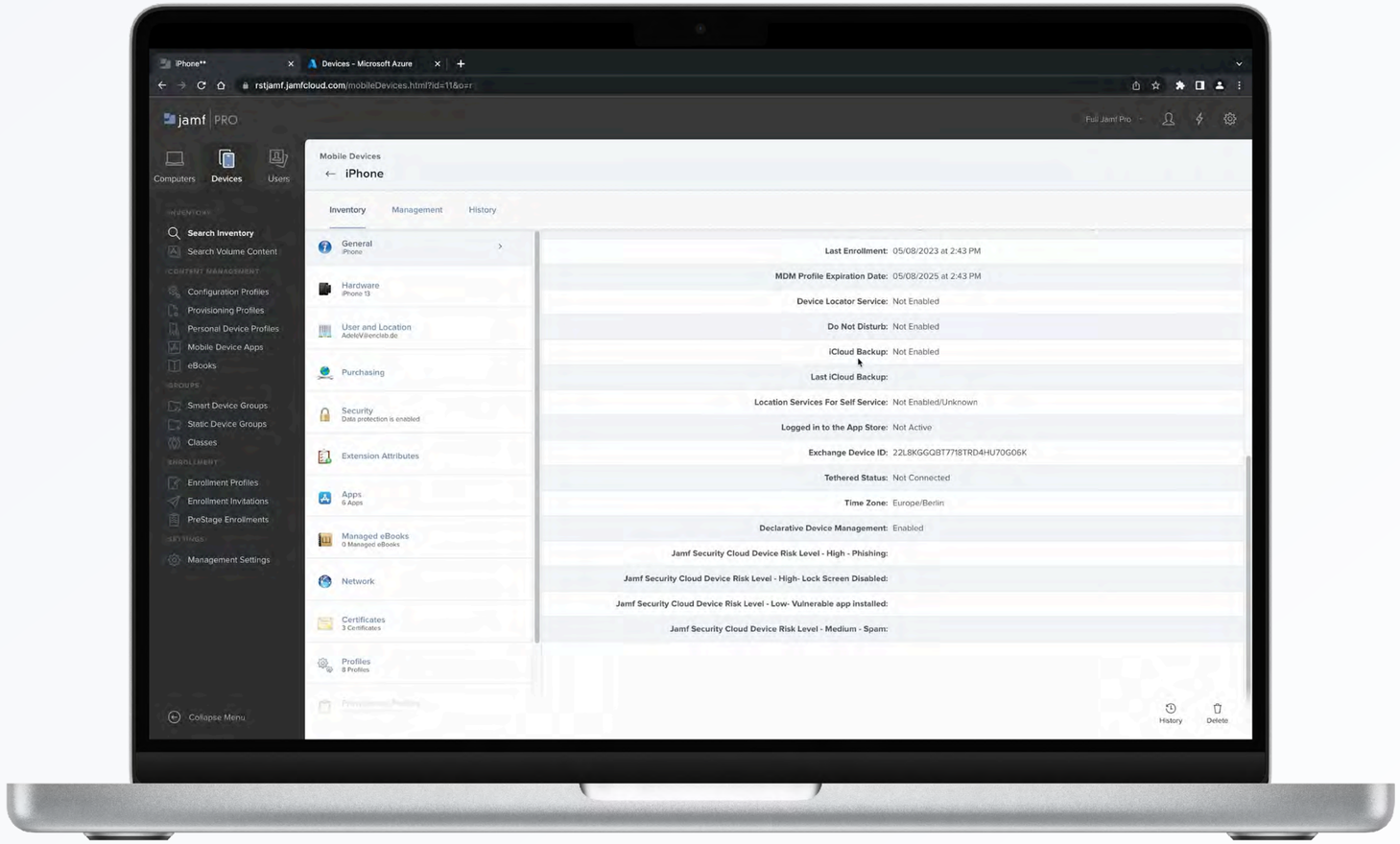


Device Compliance for macOS and Mobile

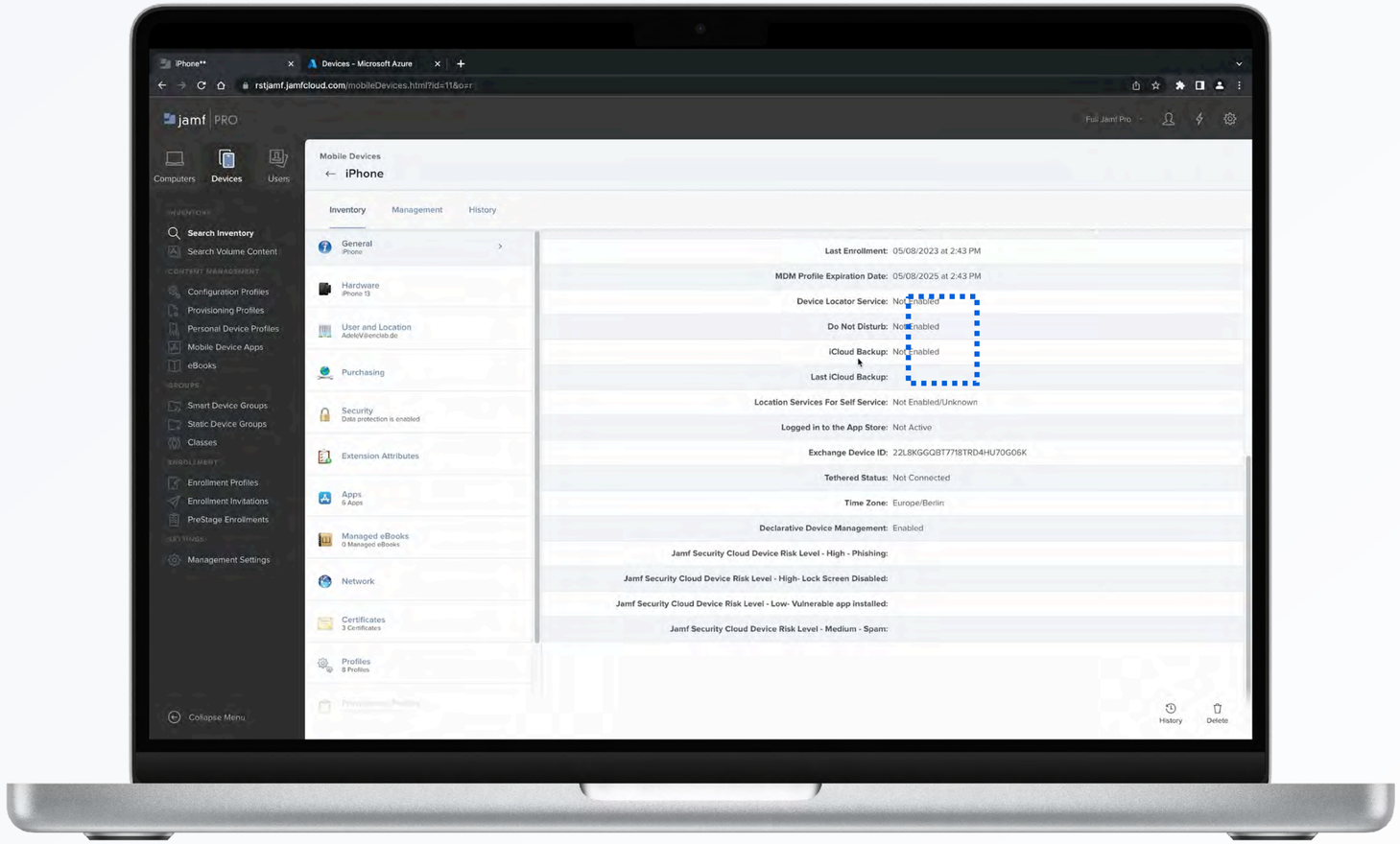


Workflow Demonstration

Compliant Device — Mobile



Compliant Device — Mobile

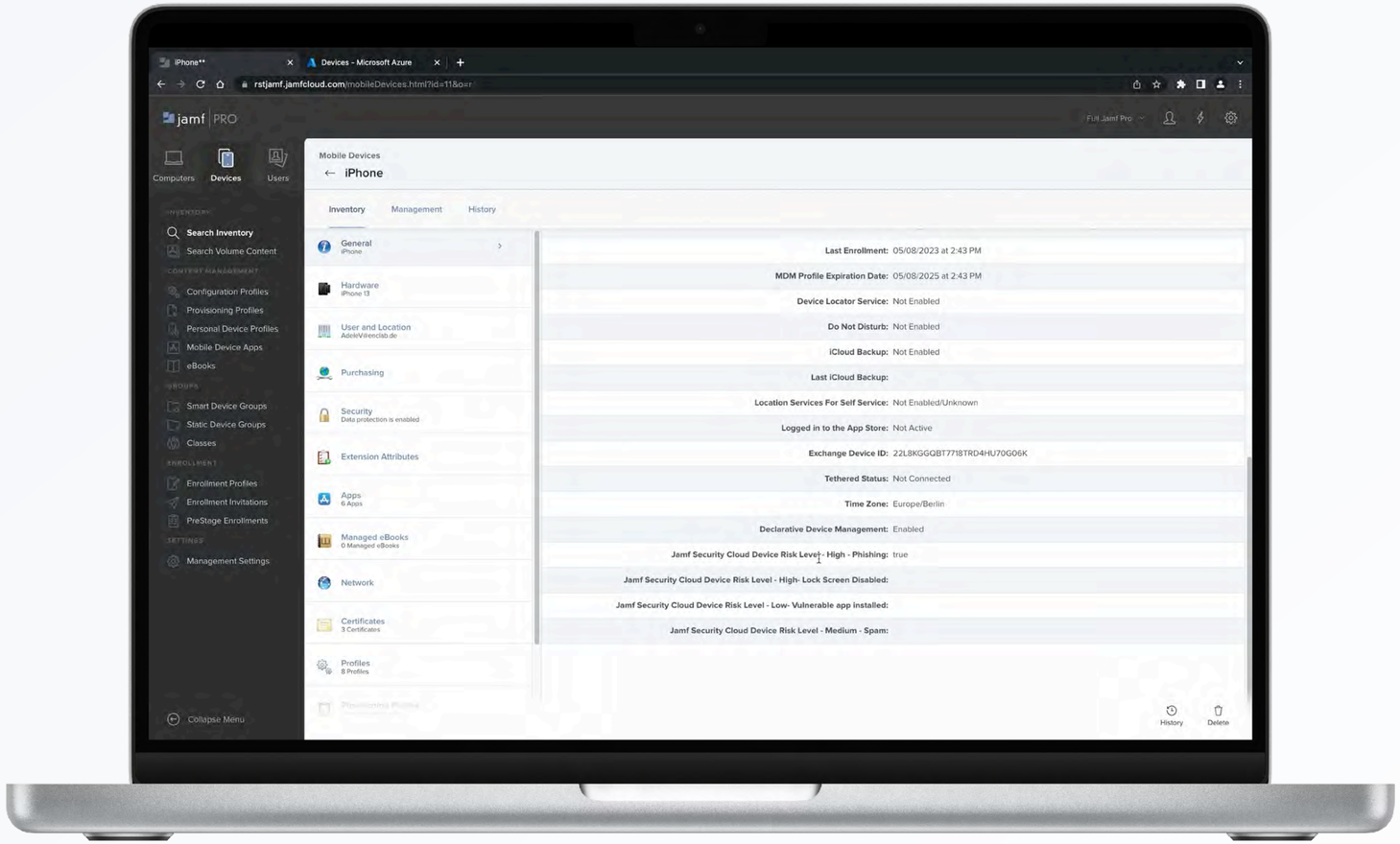


Threat Execution — Mobile

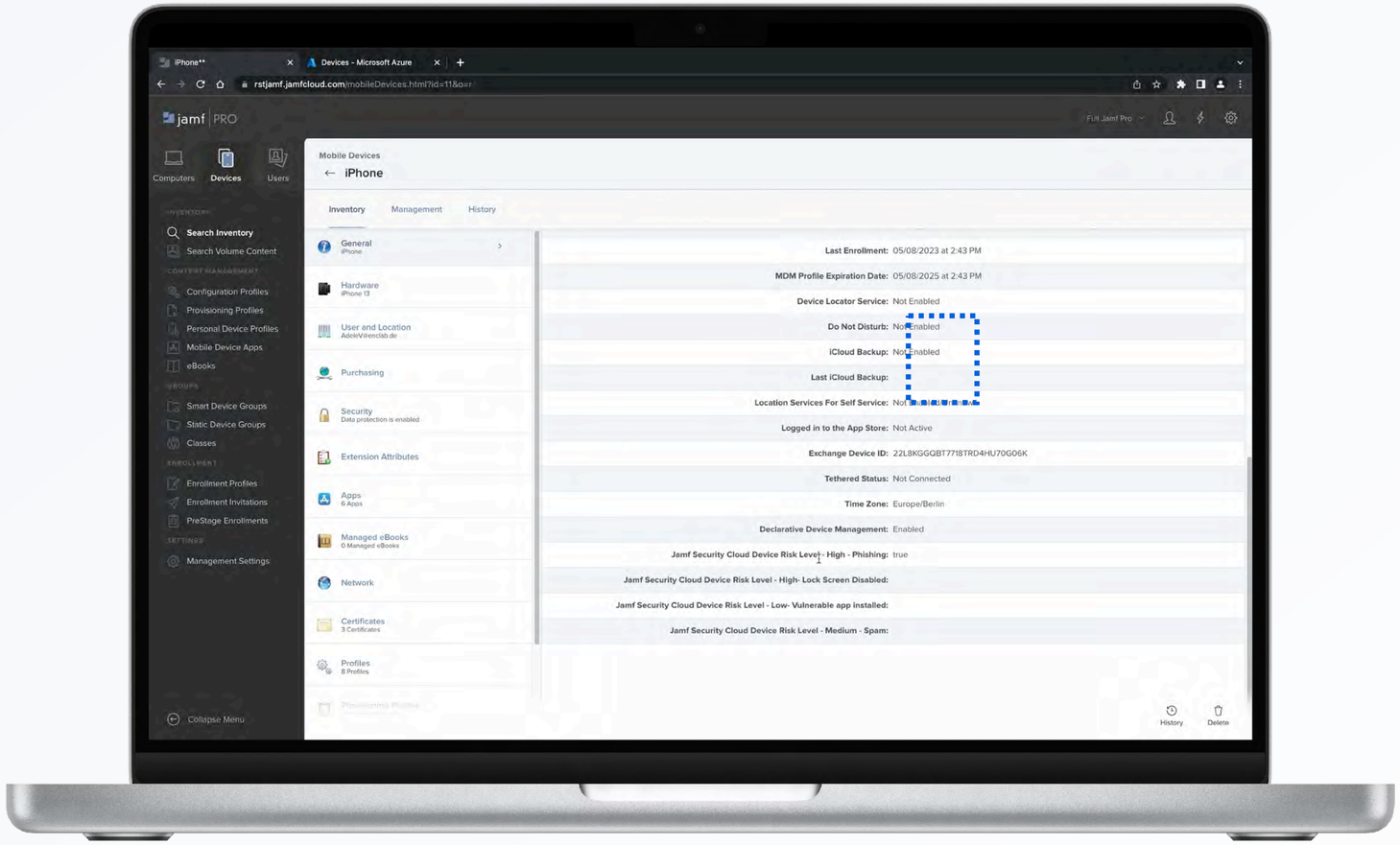
Network Threat

Device Threat

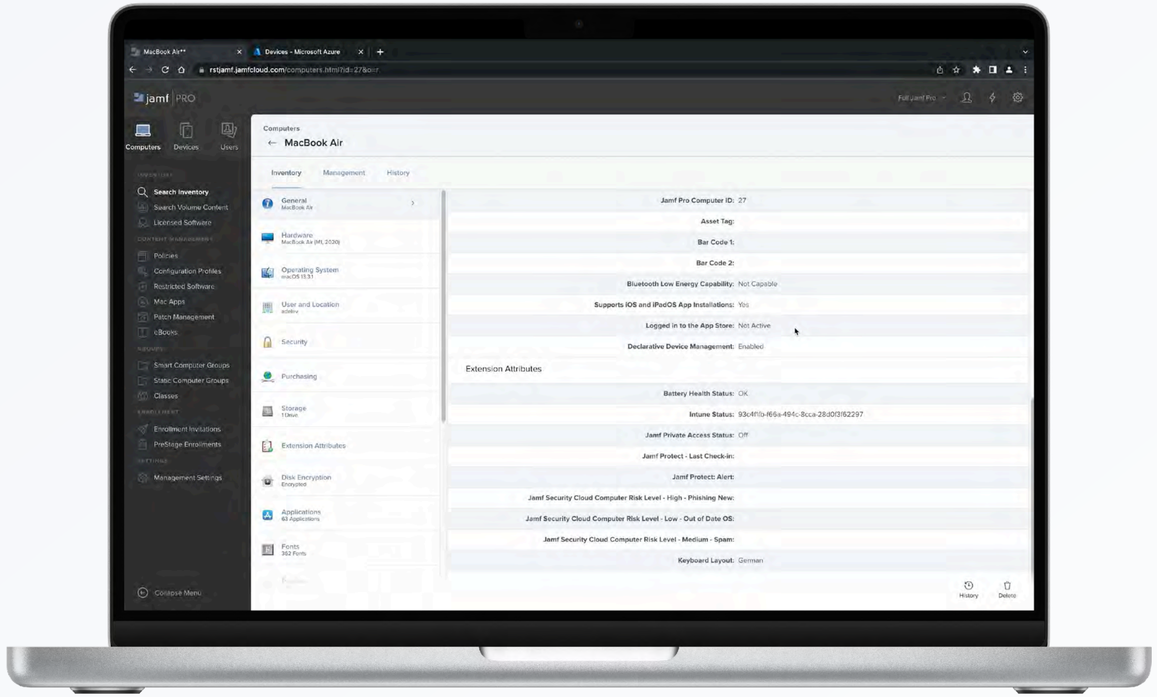
Non-Compliant Device — Mobile



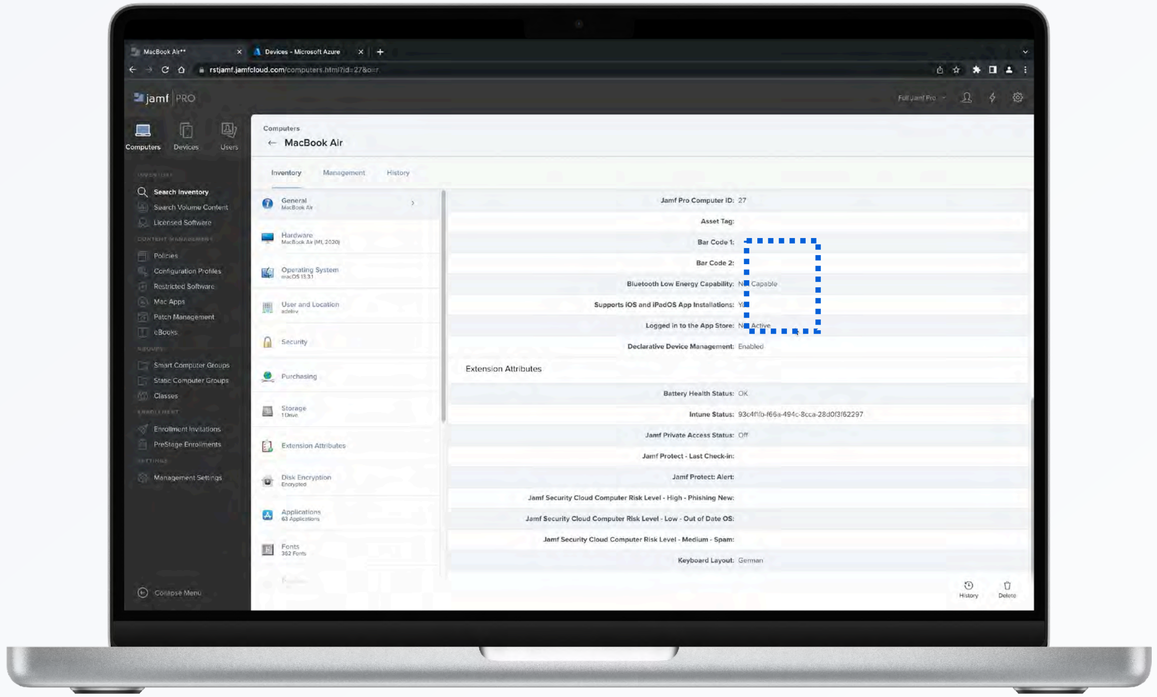
Non-Compliant Device — Mobile



Compliant Device — macOS

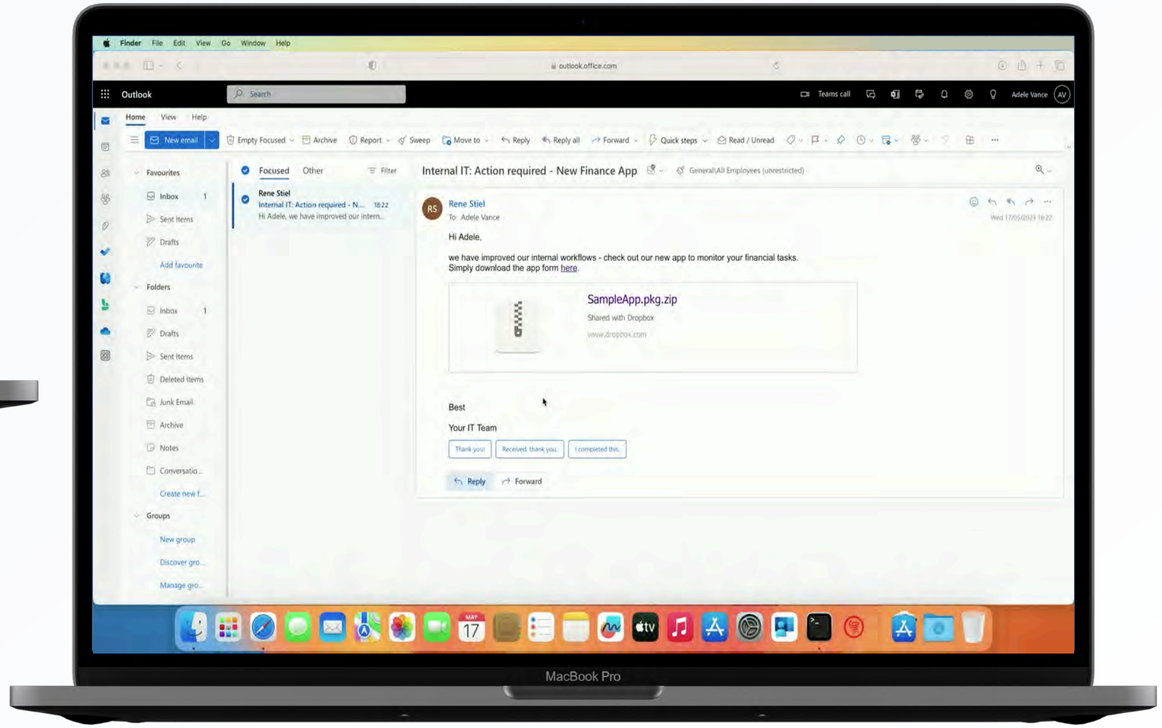


Compliant Device — macOS



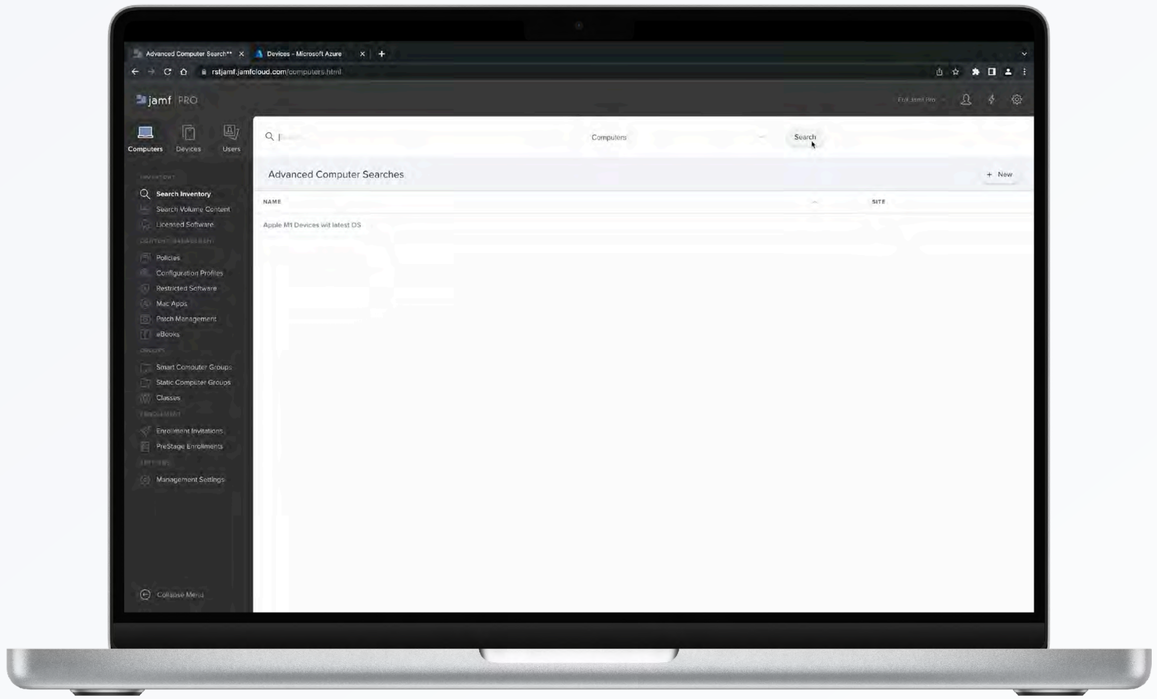
Threat Execution — macOS

Network Threat

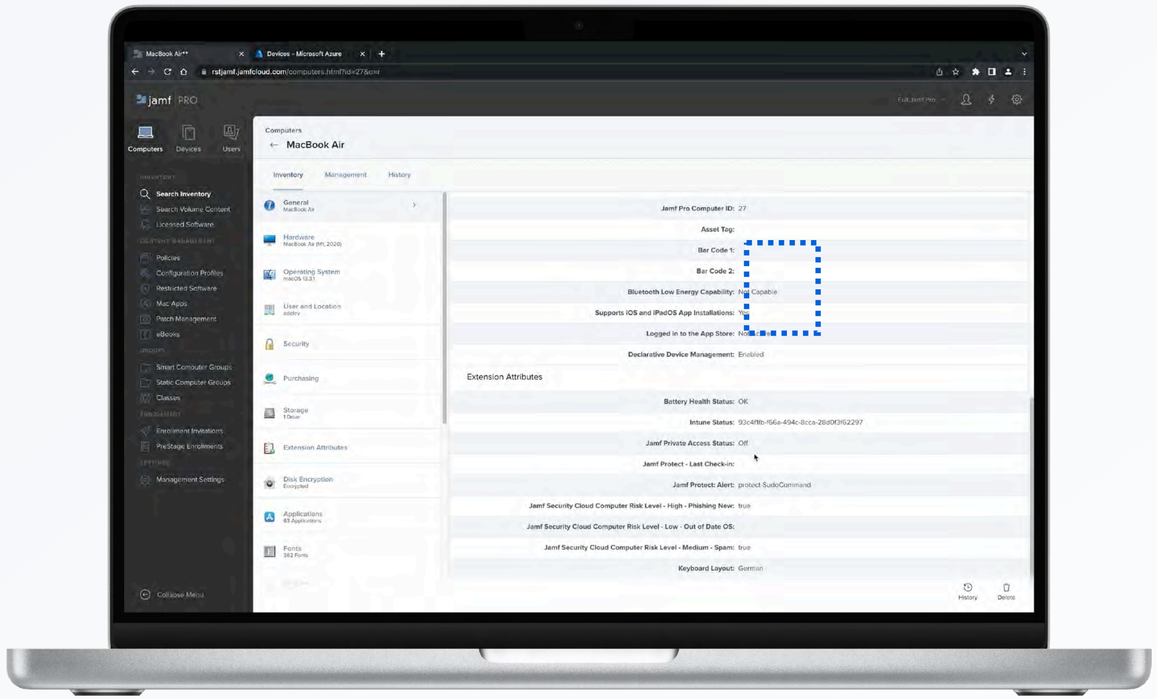


Device Threat

Non-Compliant Device — macOS

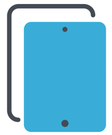


Non-Compliant Device — macOS



Just **one more** thing…

Jamf **ZTNA**



IP whitelisting

Have confidence that only devices that are managed and enrolled into Jamf Trust are able to reach apps/ services - perhaps even just the authentication page!

Encrypt traffic

Traffic is encrypted in per-app tunnels, securing connections for users anywhere in the world. Customers can choose to egress from specific datacenter locations

What about other services?

Jamf Security Cloud can support customers, whether they have apps/services that are; on-prem, hybrid or cloud native. Routed by hostname or directly using IP

Extra layer of defence

With the Jamf Security Cloud's built in conditional access controls, customers can add additional layers of security in front of any other service to enhance their security in real-time!

Device Compliance iOS

Google Beyond Corp

Device Compliance macOS

Jamf ZTNA for Beginners

JAMF NATION LIVE

Thank you