JAMF NATION LIVE

# Effective Incident Response Workflows with Jamf


**Stijn Brattinga**

**System Engineer**
Jamf

**Elmo Kuisma**

**System Engineer**
Jamf


**Rene Stiel**

**Senior System Engineer**
Jamf

# Agenda

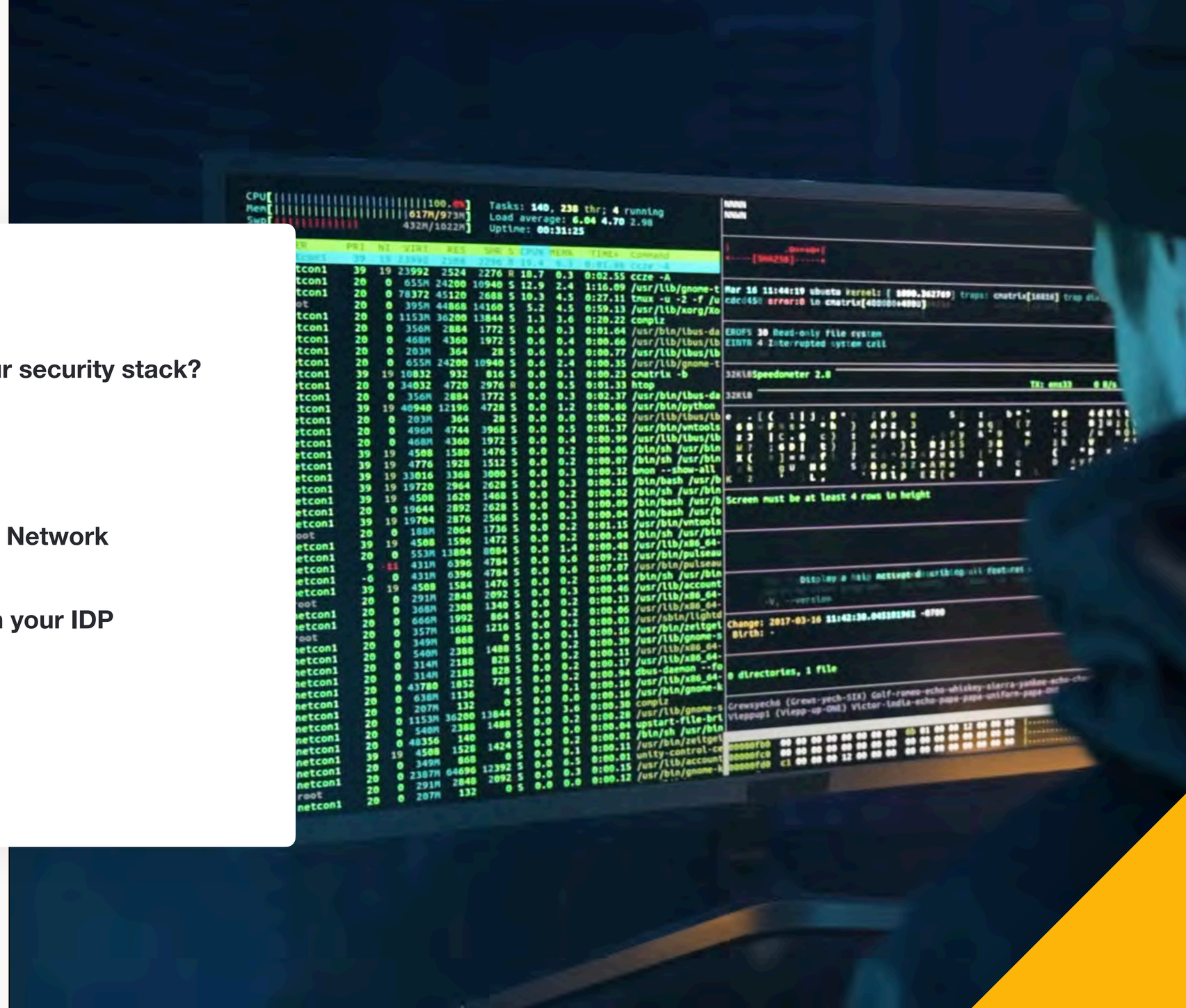
1 | Why add automation to your security stack?

2 | Automated Remediation

3 | Isolating Devices from your Network

4 | Integrating Risk Levels with your IDP

5 | D~~o~~n’t Do this at home!



# Let’s start with the basics

“Incident Response enables security teams to limit or prevent damage from cyberattacks or security breaches”

IBM.com

# Why automate your security workflows?

Save time (& resources) when it really matters

Integrating best in class software

Evolving Threat Landscape

# Who is already using automated incident response workflows?

# Examples of **Automated Incident Response**



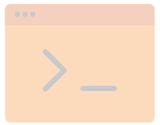
Block access from insecure BYOD mobile devices

Deny physical access if device is compromised



Monitor vulnerability of Installed applications

Gather forensic data after malware detection



Automatically block malicious content

Lock user account after DLP notification

**And many more..**

Workflow

# Automated Remediation

JAMF NATION LIVE

# Jamf Protect automated workflow

# Jamf Protect automated workflow

## Remediation

- Jamf Protect detects screenshot being taken
- Populates Extension Attribute to Jamf Pro
- SmartGroup membership change triggers a Policy
- Policy deletes associated screenshot

# Workflow Take-Away

## Analytics

Monitor for activity specific to your security needs. Create your own custom analytic to trigger these automated workflows.

## Editable End User Prompts

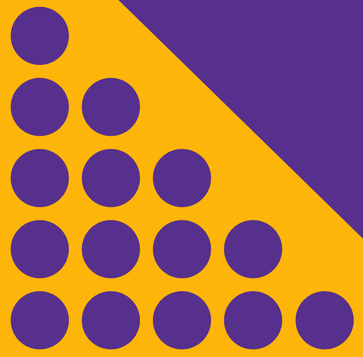
Leverage custom Jamf Helper, or SwiftDialog prompts via Jamf Pro to alert and inform end users of security events occurring on their device.

## Alerts & Logging

In Jamf Protect, alerts created by these events can be searched for and filtered by Alert Actions such as “SmartGroup”.

Workflow

# Limiting access to resources & websites



JAMF NATION LIVE

# What do we want?

- Restrict access to pre-defined destinations
- Inform the end user
- Keep connectivity to MDM & other tools
- Restore access after remediation

# Jamf Security Cloud

Block Malicious
Web Content

Connect with your
Identity Provider,
UEM, Office
building access

Manage Cellular
Data Usage

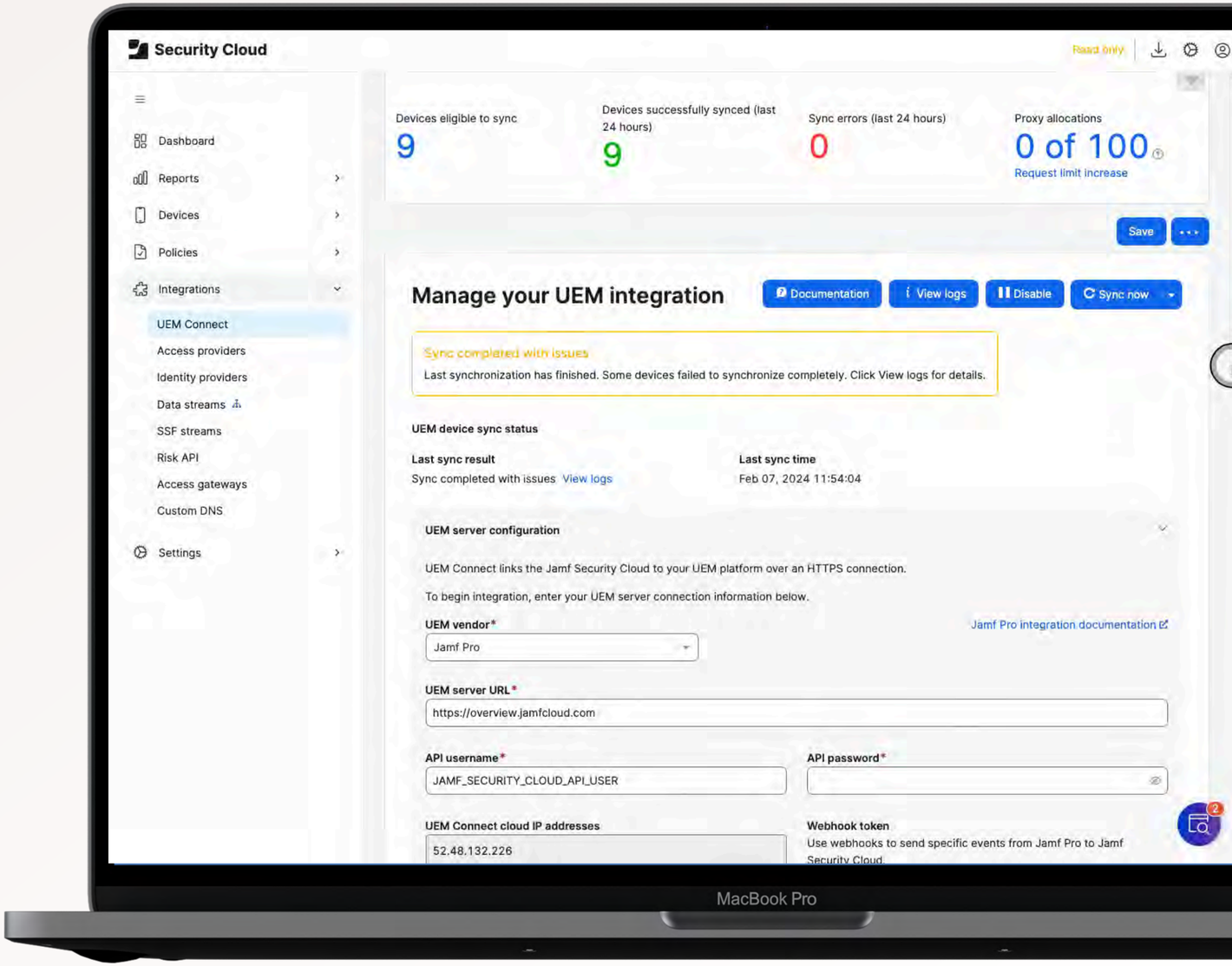
Create Acceptable
Content Policies

ZTNA policies to access
company resources

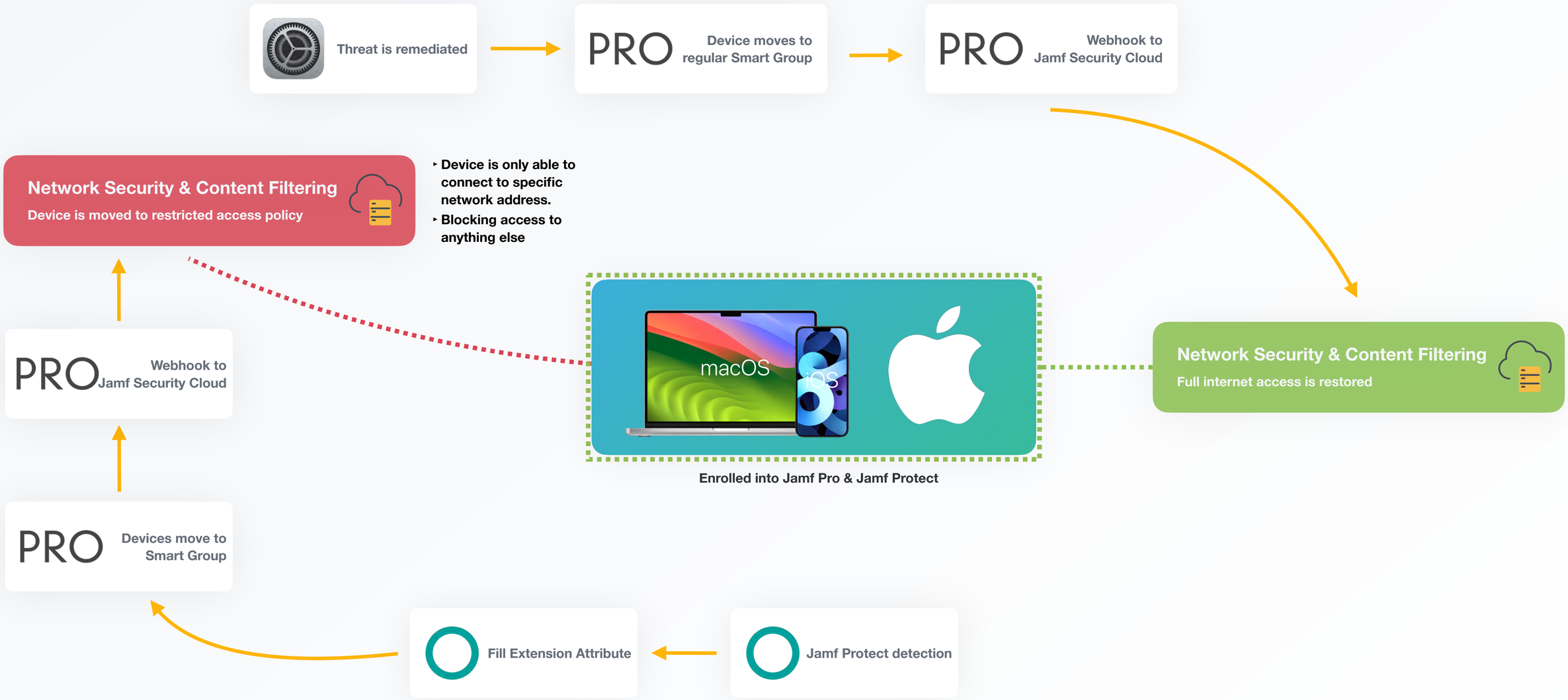
# Jamf Pro Webhook Remediations

Released in January, 2024

- **Enhanced UEM Connect integration** allows ad-hoc sync from Jamf Pro to Jamf Security Cloud
- **Trigger real-time workflows** based on **events in Jamf Pro**

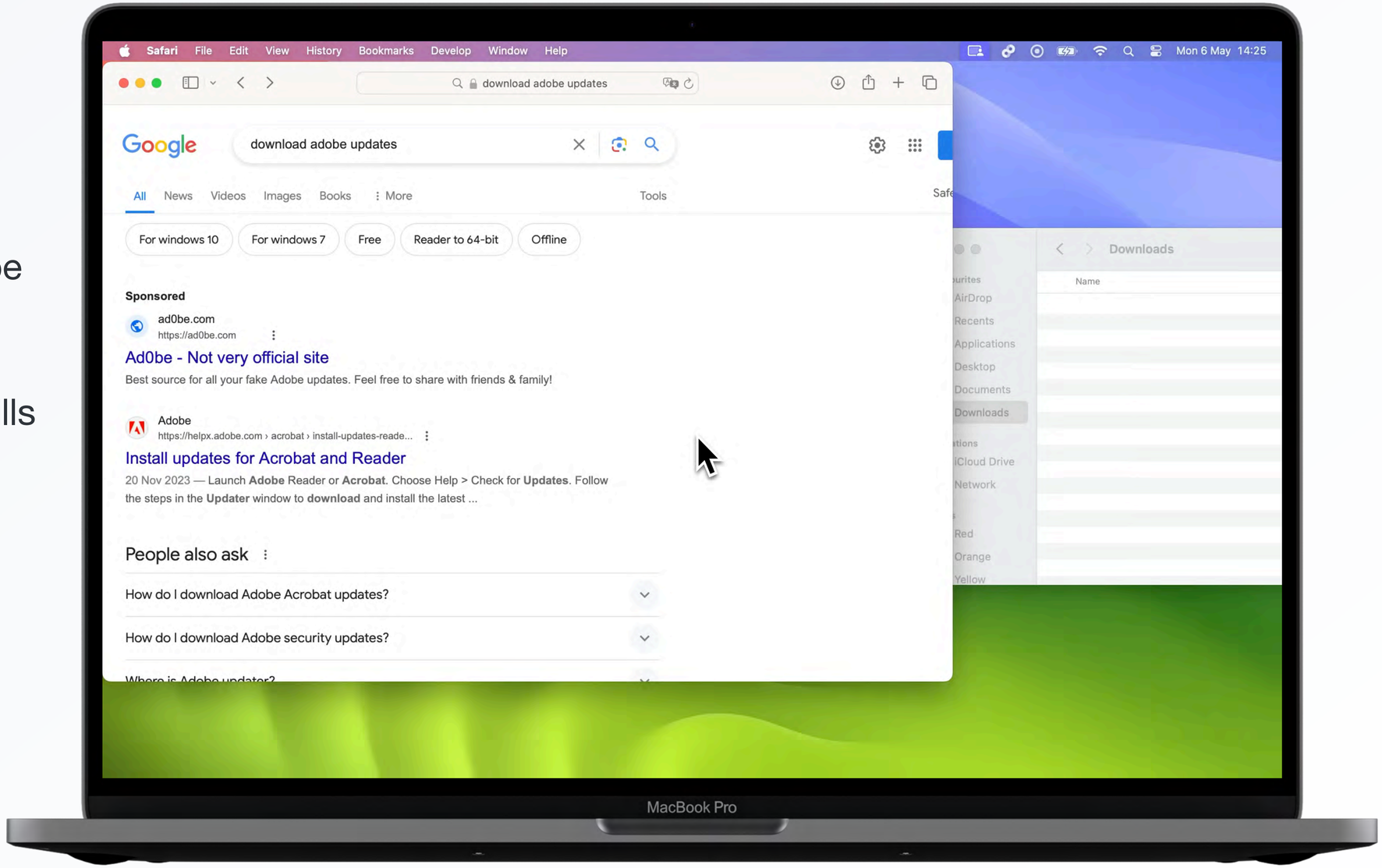


# Network Isolation workflow



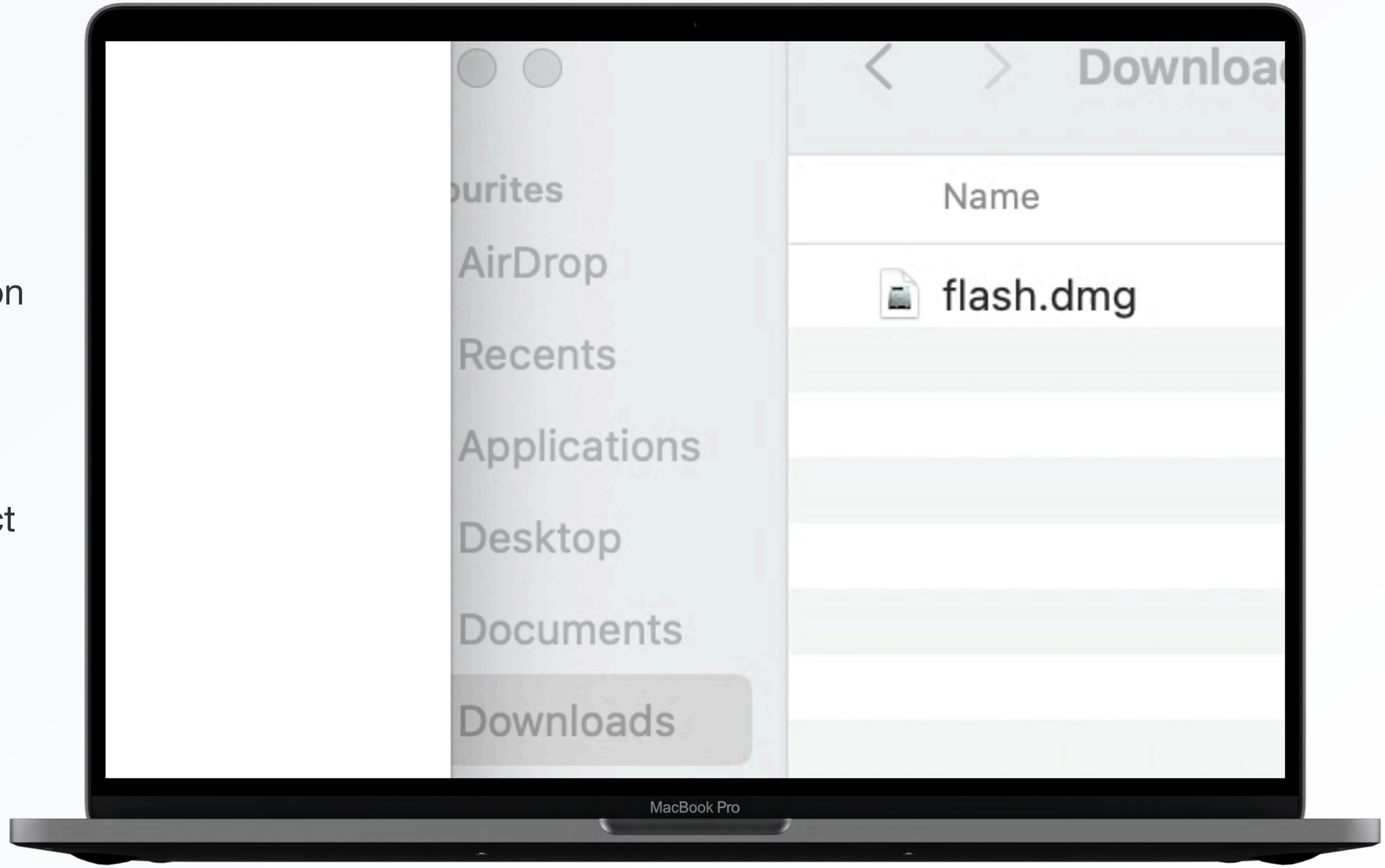
# Network Isolation: Threat Simulation

- User downloads fake Adobe update via Malvertising
- Jamf Protect detects and fills Extension Attribute



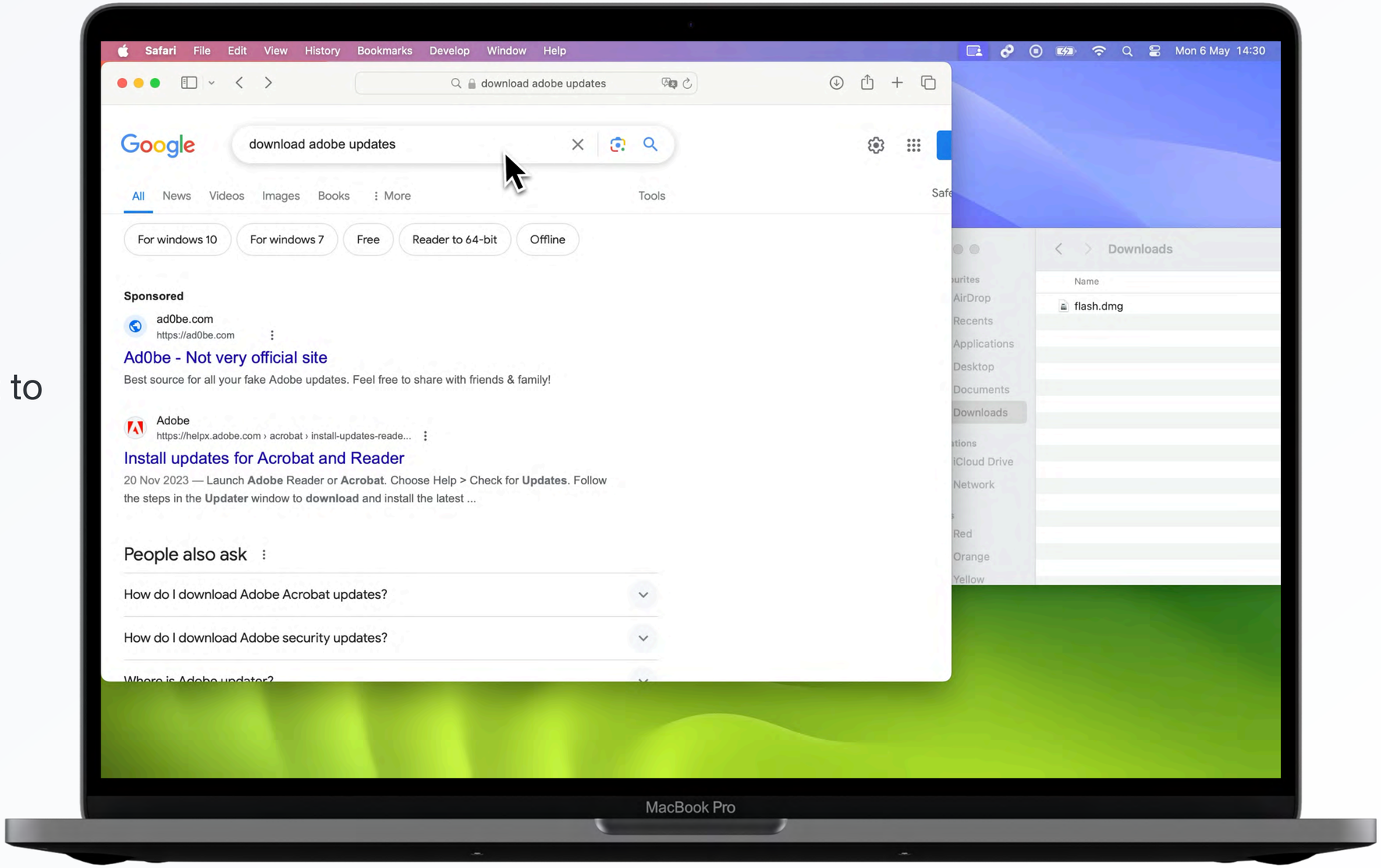
# Network Isolation: Remediation

- Smart Group triggers action
- User is notified
- Jamf Pro shares event information to Jamf Protect



# Network Isolation: Blocking

- Jamf Protect limits network access
- Endpoint is able to connect to allowed destinations



# Workflow Take-Away

## Security & Management Integration

With security and MDM working together automations are made easier and devices are kept more secure.

## Smart Group Webhook Triggers

Smart group membership changes trigger webhooks events. Both the trigger & event can be customised to create custom remediations.

## Network Security & Content Filtering

Risky devices are moved into a restricted access group, blocking access to network resources via content filtering.

Workflow

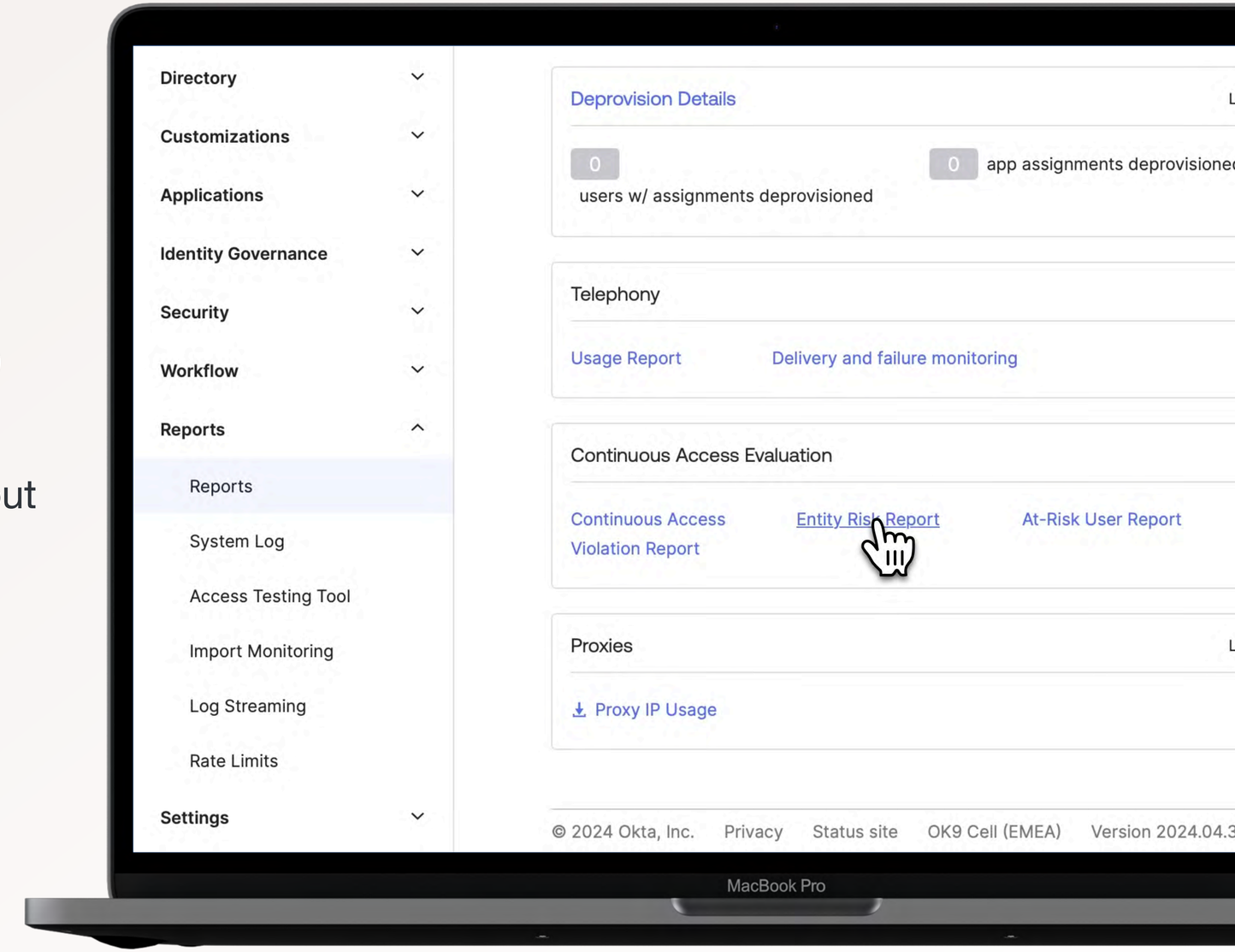
# Sharing risk levels with Identity Providers

JAMF NATION LIVE

# Shared Signal Framework integration

Released in January, 2024

- New Jamf Security Cloud integration support for establishing a **Shared Signals Framework (SSF)** stream with third party vendors like Okta
- It allows Jamf to **continuously share events** about device risk level changes
- Feature available in limited early access in Okta



# SSF Workflow

IDP restricts access to gated resources

Threat is remediated
Compliance restored

PRO Device moves to regular Smart Group

Risk level reverts to Secure

SSF updates risk level with IDP

IDP restores access to gated Resources

PRO Devices Smart Group status changes

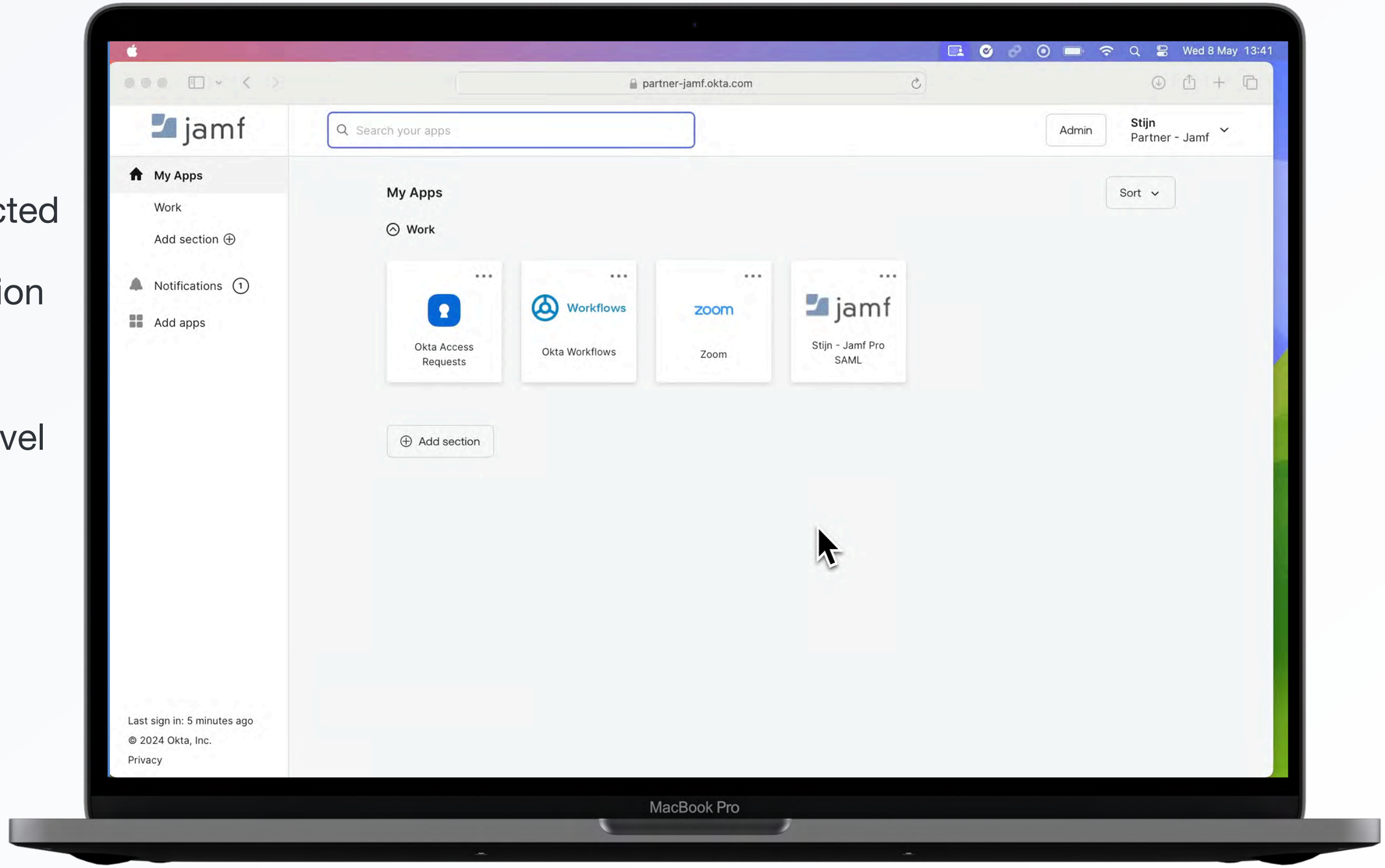
PRO Webhook to Jamf Security Cloud

Risk level is set in Jamf Security Cloud

SSF shares risk level with IDP

# **Shared Signal Framework** Enduser Experience

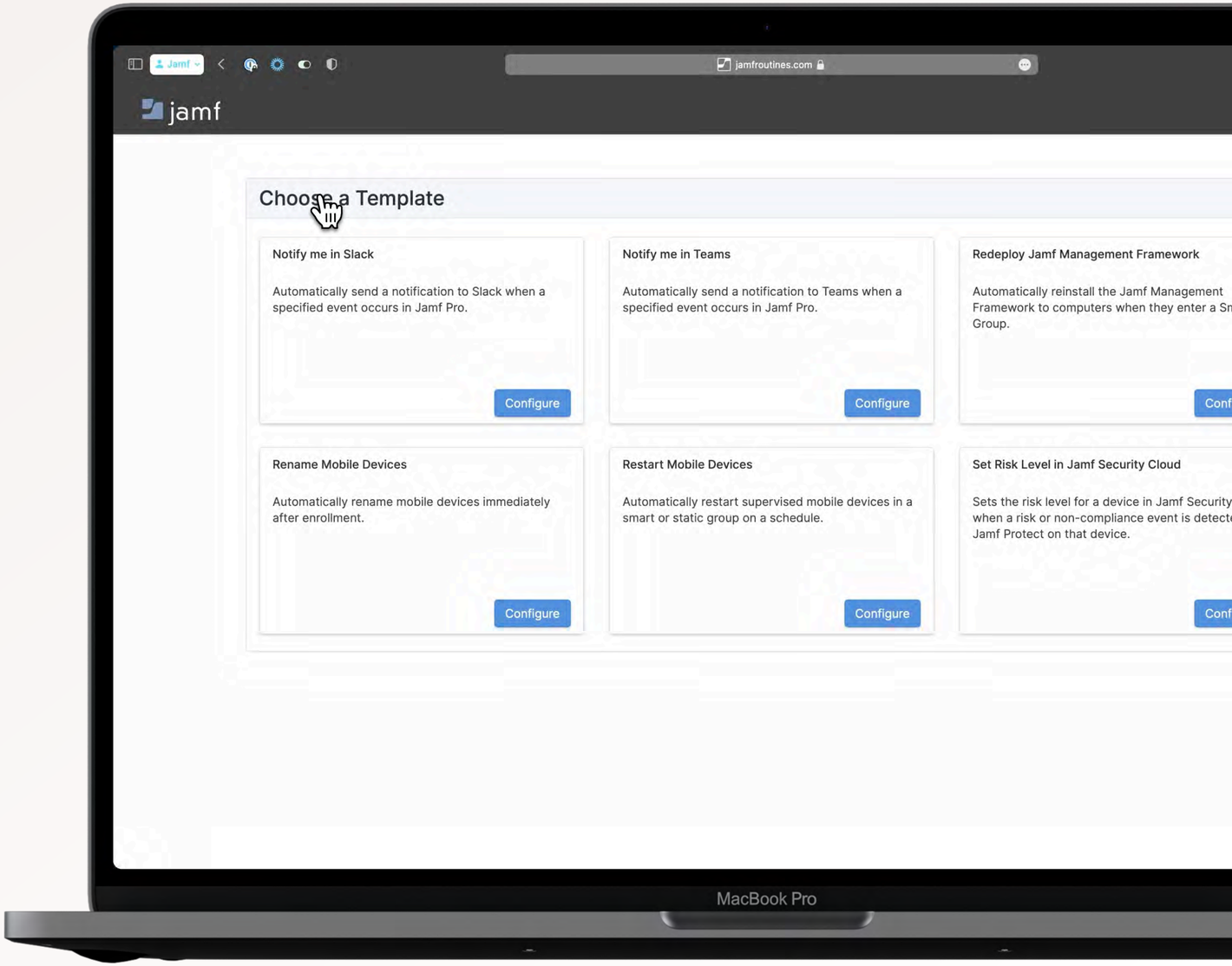
- Compliance change detected
- Webhook shares information to Security Cloud
- Jamf shares device risk level with Okta
- Users Okta access is restricted



# Jamf Routines: Setup Automation

Released in April, 2024

- Create **automated workflows** by connecting Jamf Pro to third-party tools
- **6 templates** available
- Open to **Business and Enterprise plan** customers




JAMF NATION LIVE

Try it on **www.jamfroutines.com**

# Workflow Take-Away

## IDP Integration

Establish shared signal frameworks with 3rd party IDP providers from Jamf Security Cloud.

## Risk Level Sharing

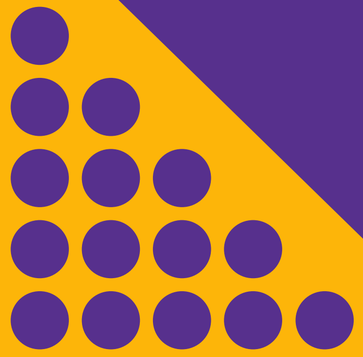
Automate the setting of devices risk levels through Jamf Routines. Device risk levels can then be shared with your IDP through the SSF.

## Compliance

Restrict IDP resources in real time from non-compliant devices. Outline compliance using Jamf Pro Smart Groups.

Workflow

# Gathering post-attack data



JAMF NATION LIVE


Open source

# Incident Response Framework

jamf

# How can Aftermath help?

- Gather post-incident forensics
- Provides a complete storyline
- Easily deployed from Jamf Pro
- Scripts & Playbooks available

PRO Jamf Pro Policy

PRO Devices move to Smart Group

Fill Extension Attribute

Jamf Protect detection

macOS

Enrolled into Jamf Pro & Jamf Protect

## Jamf Aftermath

Internet Browser history
Shell history
LaunchDaemons
System Extensions
Unified Logs
& more

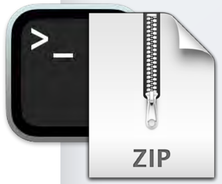
ZIP

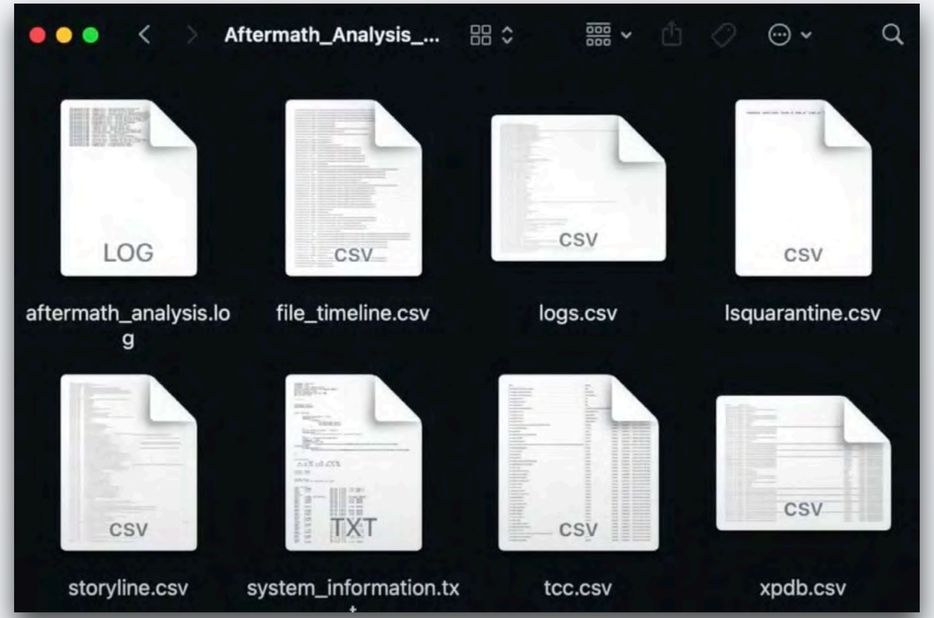
aws | S3

JAMF NATION LIVE

## Jamf Aftermath

Internet Browser history
Shell history
LaunchDaemons
System Extensions
Unified Logs
& more




# What can you bring home?

Custom Workflows

Post Incident Response

Endpoint & Network Security

SIEM

Risk Level

Isolation

Content Filtering

Aftermath

Zero Trust Network Access

Jamf Routines

Threat Prevention

Jamf Protect

Security Cloud

Jamf Connect

Custom Analytic Remediations

Shared Signal Framework

Compliance Baselines

Jamf Pro

Jamf Security Cloud

Smart Group Actions

Compliance Editor

Routines

Unified Logs

Jamf Threat Labs

Extension Attributes

Workflows

Okta

Risk Levels

# All the resources you need to start testing in your own environment

JAMF NATION LIVE

# Thank you