

# Under the hood of the Jamf Protect Agent



# Matteo Bolognini

Jamf - Senior Technical Support Engineer

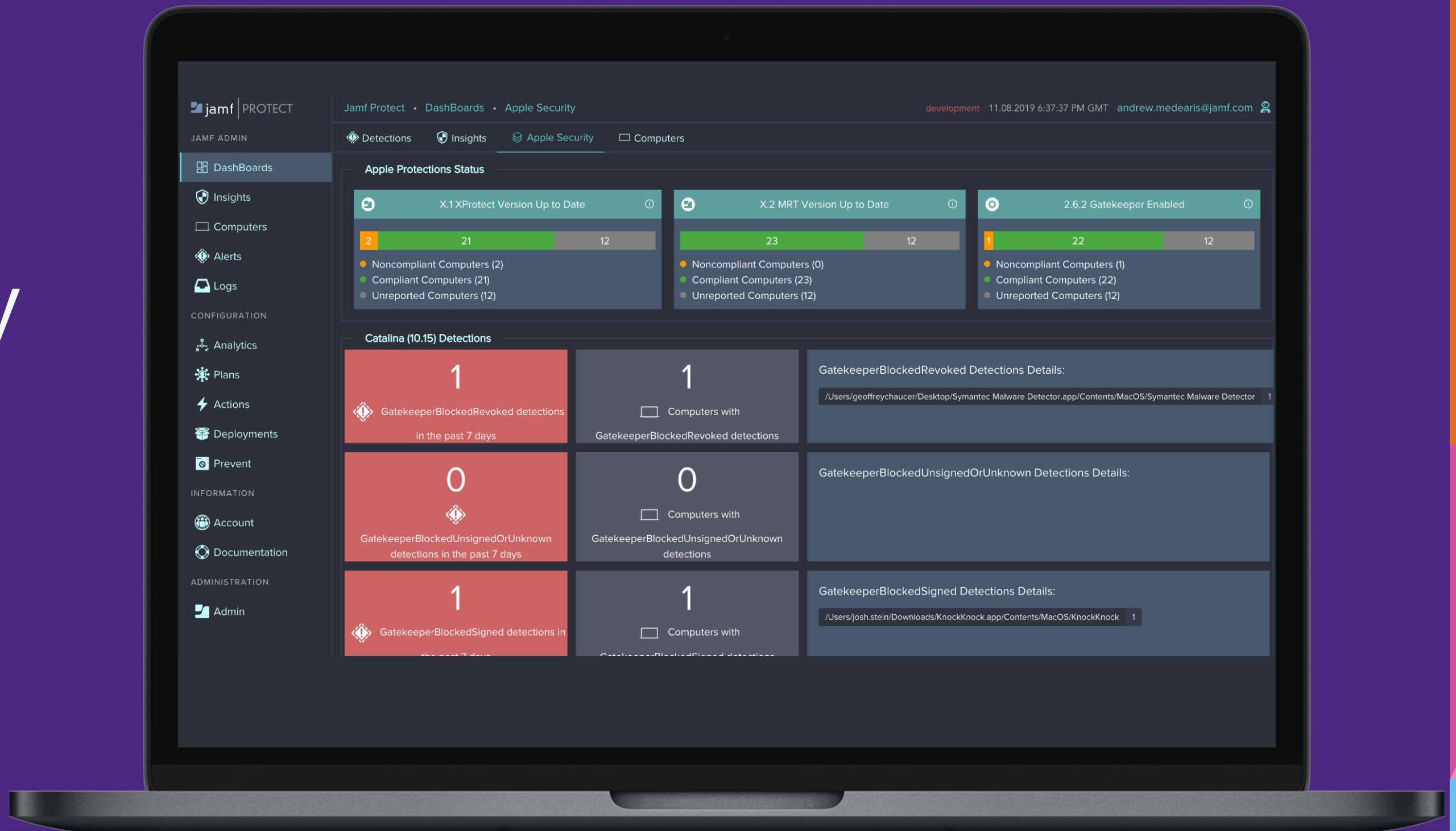


# Melwin Moeskops

Jamf - Enterprise Support Engineer



“Jamf Protect is an enterprise endpoint security solution for the Mac. “



# Jamf Protect in a nutshell

Jamf Protect Agent

Jamf Protect Web App

Jamf Protect Plans

# Jamf Protect Agent

Audit security settings

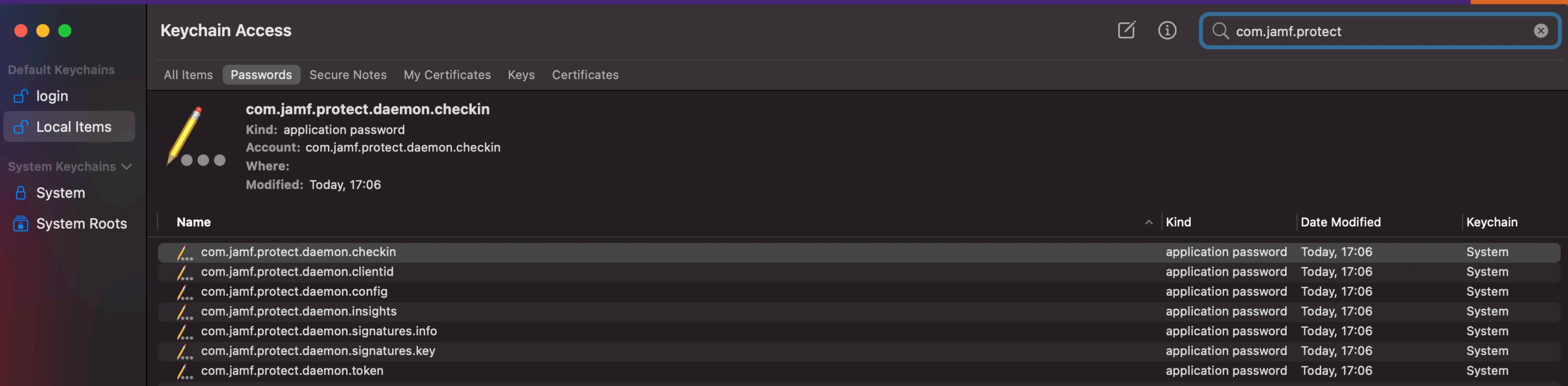
Monitor real-time event-driven activity

macOS 10.13 - 10.15 with System Extension

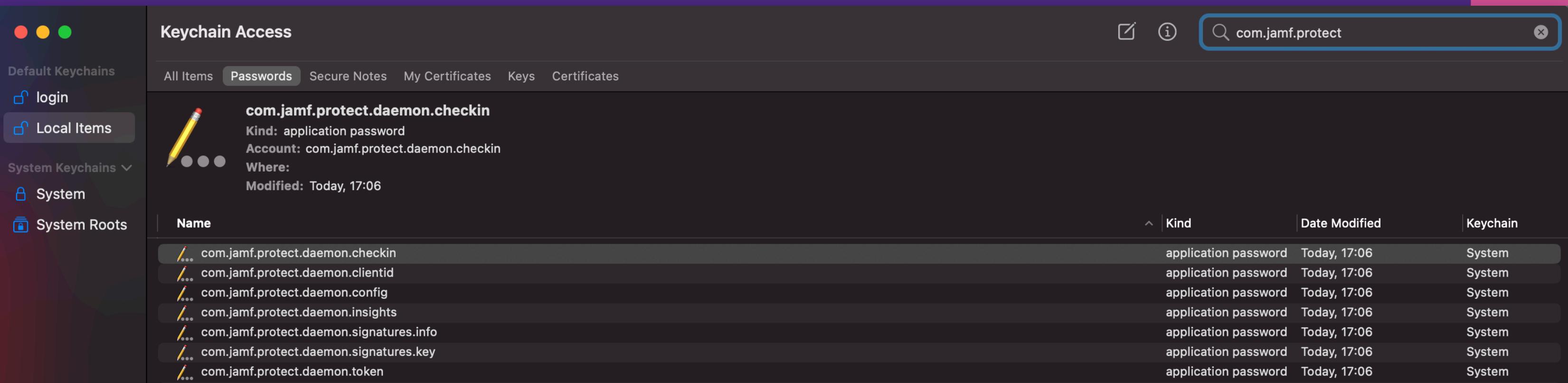
# Jamf Protect Keychain Items

The following additional data points are secured in the keychain and used to control the behaviour of Jamf Protect.

# Last check-in time of the agent



# ClientID of the agent



# Last check-in time of the agent

# ClientID of the agent

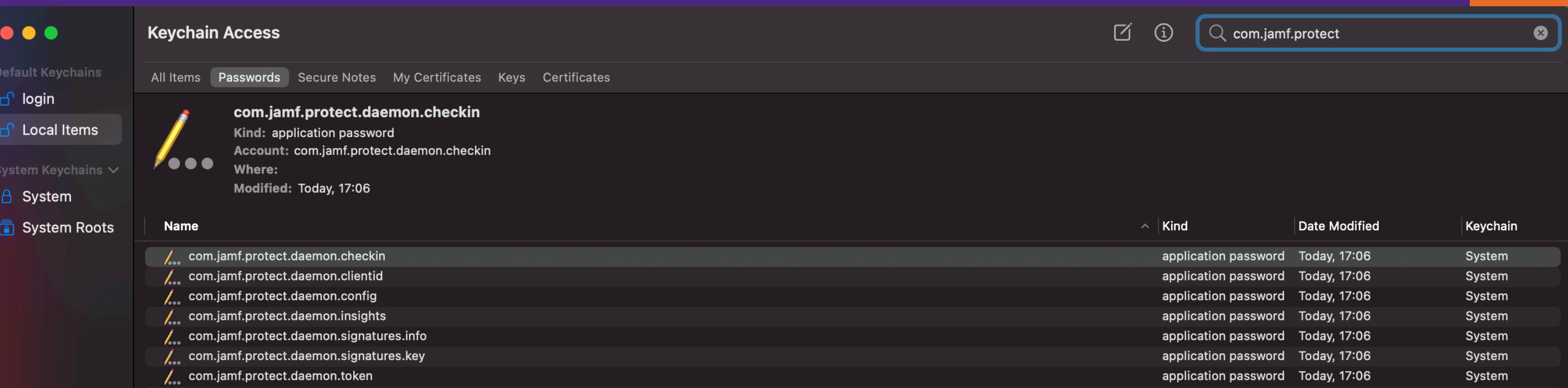
The screenshot shows the Jamf Pro interface. In the foreground, a modal window titled "com.jamf.protect.daemon.checkin" is open, showing an "Attributes" tab. The "Name" field contains "com.jamf.protect.daemon.checkin". The "Kind" field is set to "application password". The "Account" field is also "com.jamf.protect.daemon.checkin". Below these fields are "Where:", "Comments:", and "Show password:" checkboxes. A "Save Changes" button is at the bottom right. In the background, a search results table lists multiple entries for "application password" with the same account name, all modified "Today, 17:06".

Kind	Date Modified	Key
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys

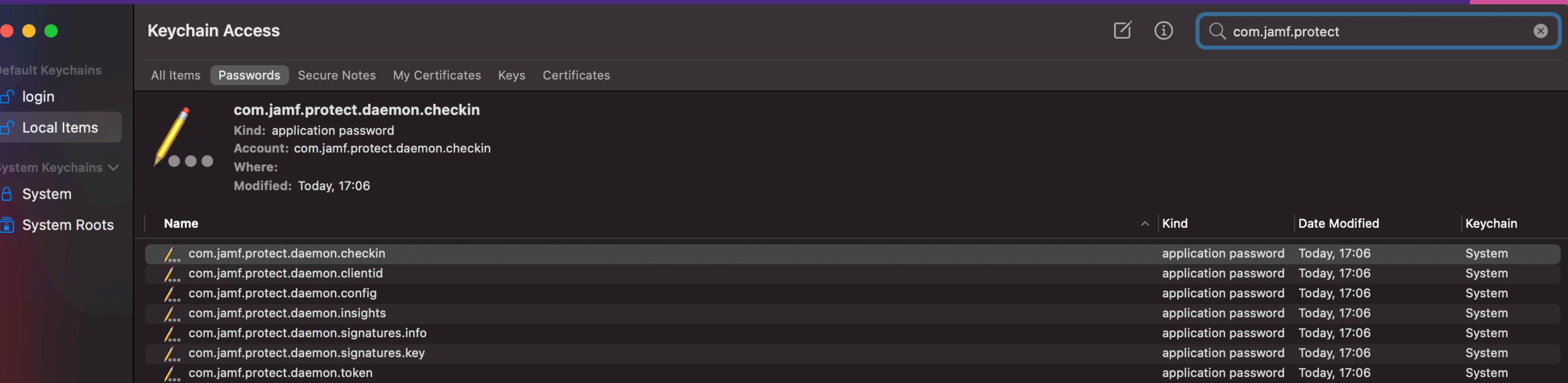
The screenshot shows the Jamf Pro interface. In the foreground, a modal window titled "com.jamf.protect.daemon.clientid" is open, showing an "Attributes" tab. The "Name" field contains "com.jamf.protect.daemon.clientid". The "Kind" field is set to "application password". The "Account" field is also "com.jamf.protect.daemon.clientid". Below these fields are "Where:", "Comments:", and "Show password:" checkboxes. A "Save Changes" button is at the bottom right. In the background, a search results table lists multiple entries for "application password" with the same account name, all modified "Today, 17:06".

Kind	Date Modified	Key
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys

# Configuration of the agent



# The last Insights time of the agent



# Configuration of the agent

com.jamf.protect.daemon.config

Attributes Access Control

Name: com.jamf.protect.daemon.config

Kind: application password

Account: com.jamf.protect.daemon.config

Where:

Comments:

Show password:

Save Changes

Certificates

Kind	Date Modified	Key
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys

The last Insights time of the agent

com.jamf.protect.daemon.insights

Attributes Access Control

Name: com.jamf.protect.daemon.insights

Kind: application password

Account: com.jamf.protect.daemon.insights

Where:

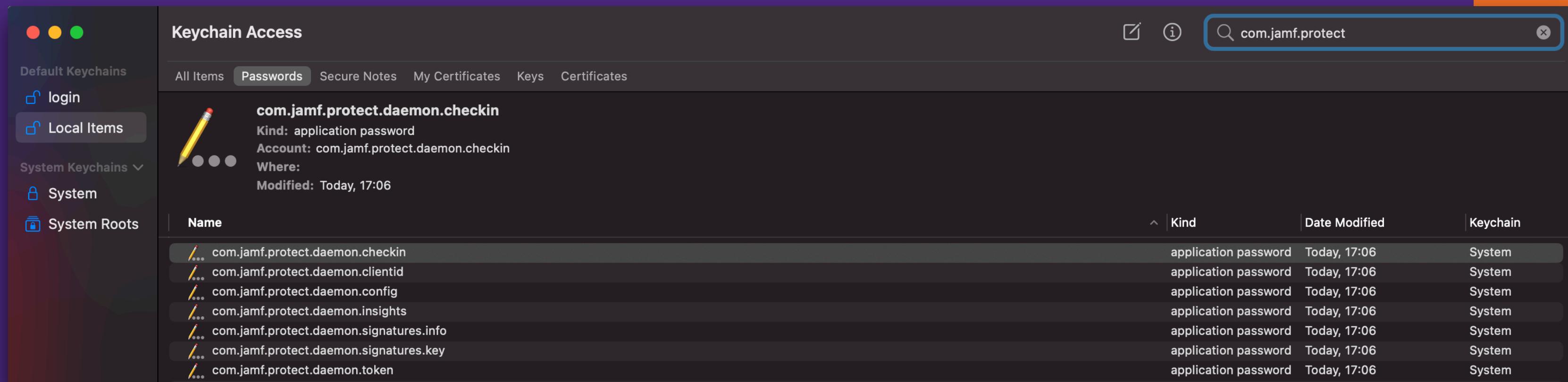
Comments:

Show password:

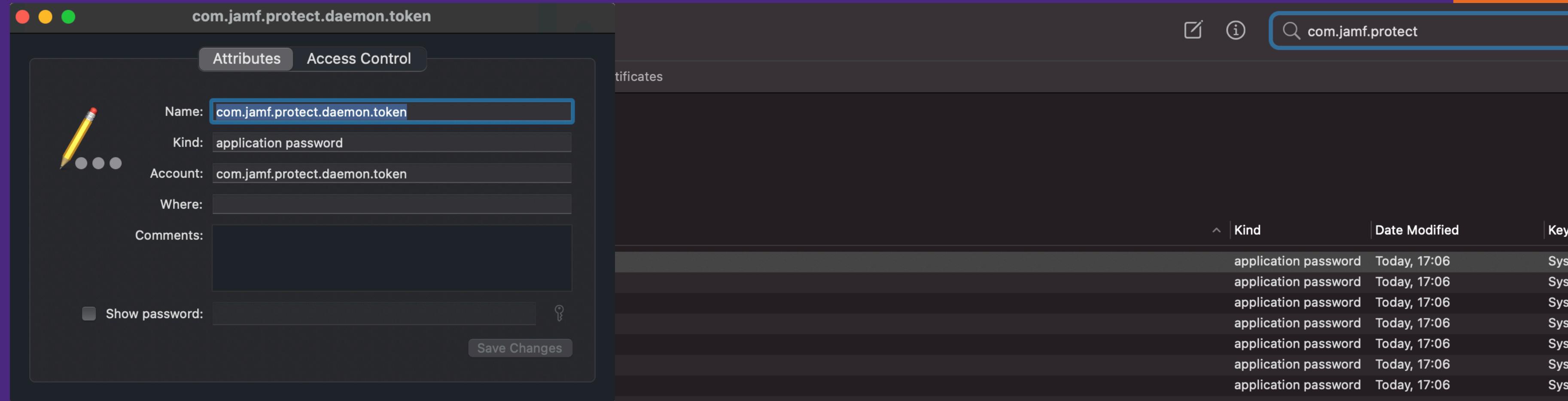
Save Changes

Certificates

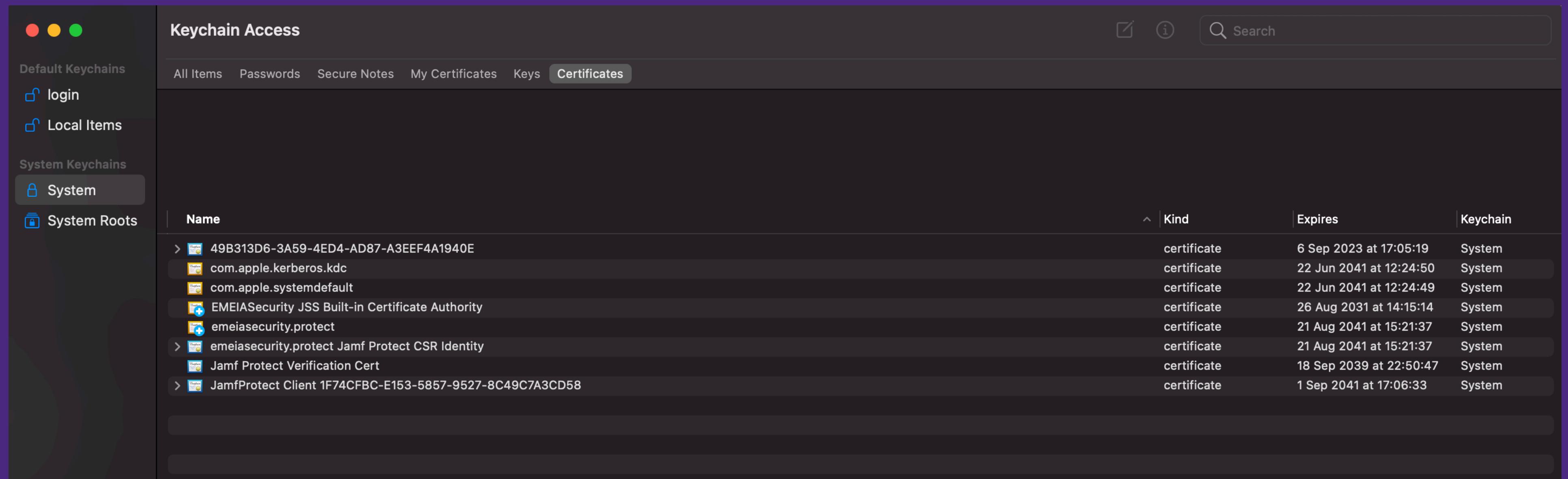
Kind	Date Modified	Key
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys
application password	Today, 17:06	Sys



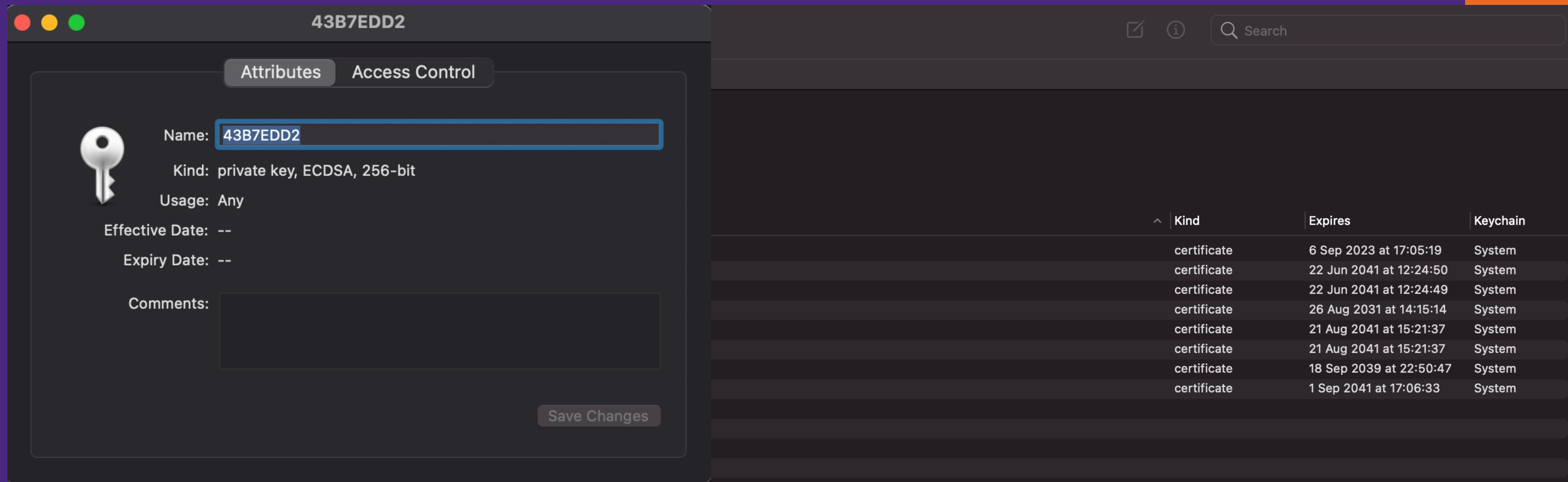
# Bootstrap information for initial communication and configuration



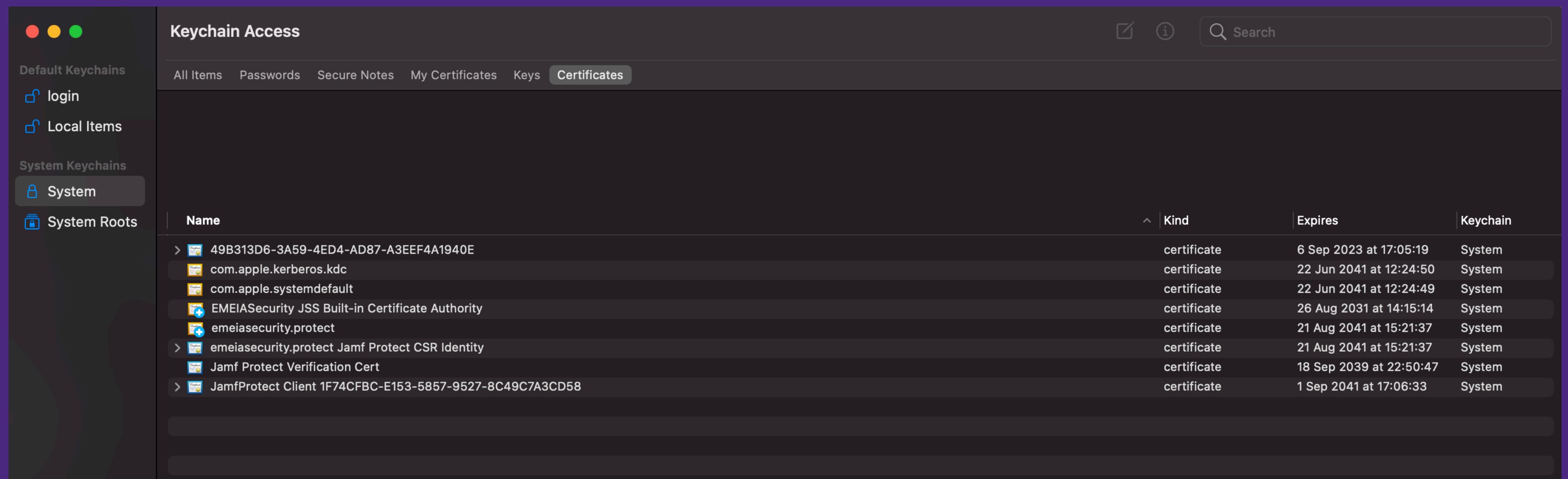
# Bootstrap information for initial communication and configuration



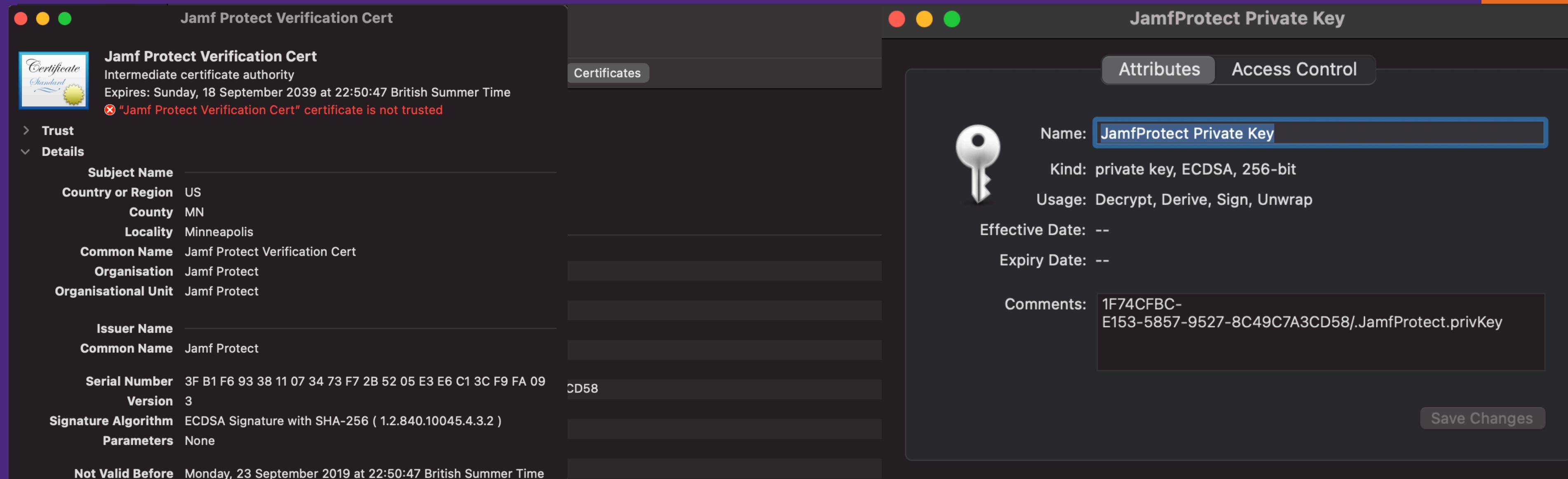
# Jamf Protect Public Key



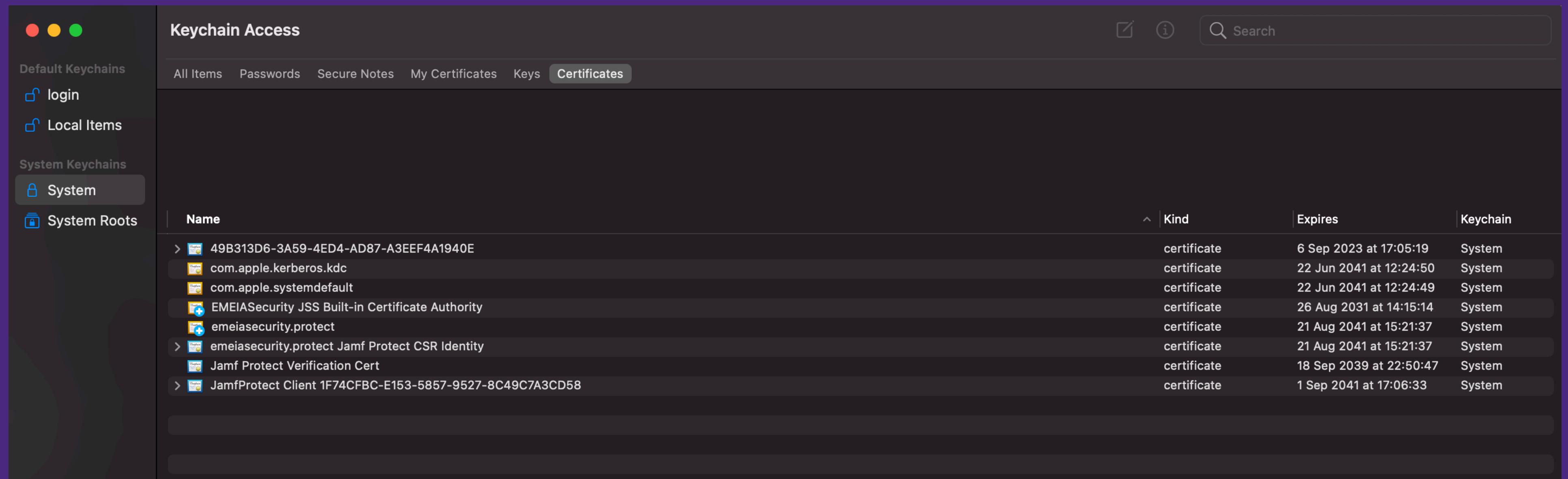
# Jamf Protect Public Key



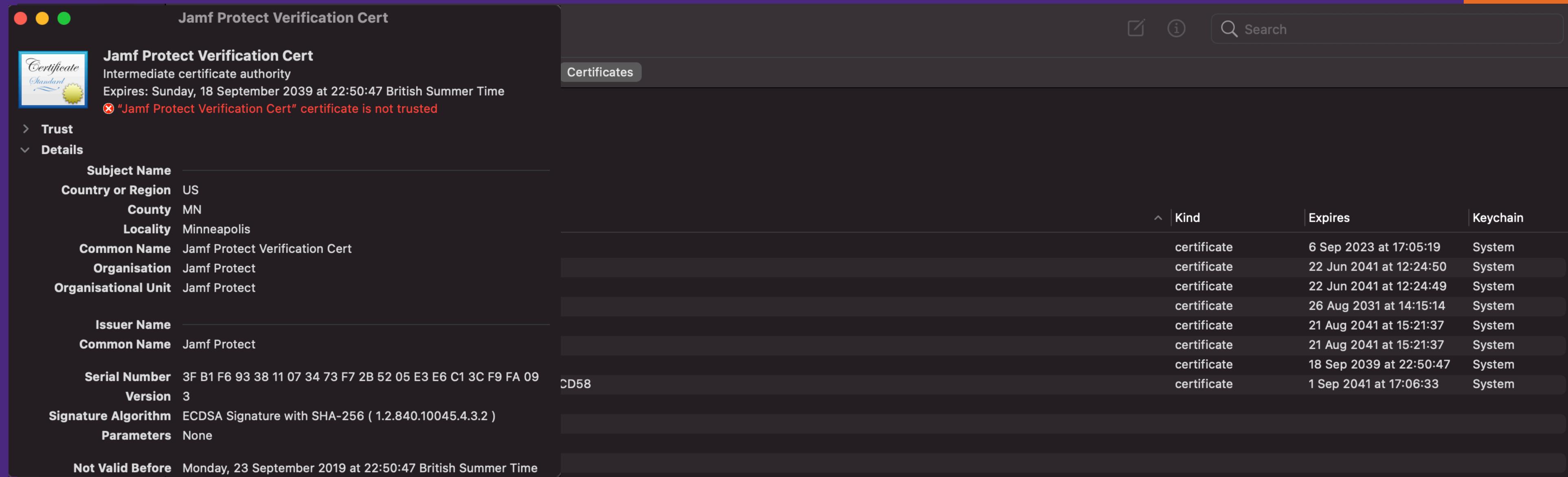
# JamfProtect client certificate (JamfProtect Client <UUID>) Jamf Protect Private Key



# JamfProtect client certificate (JamfProtect Client <UUID>) Jamf Protect Private Key



# Jamf Protect Verification Cert



# Jamf Protect Verification Cert

# Jamf Protect WebApp

Overview

Chain of Trust

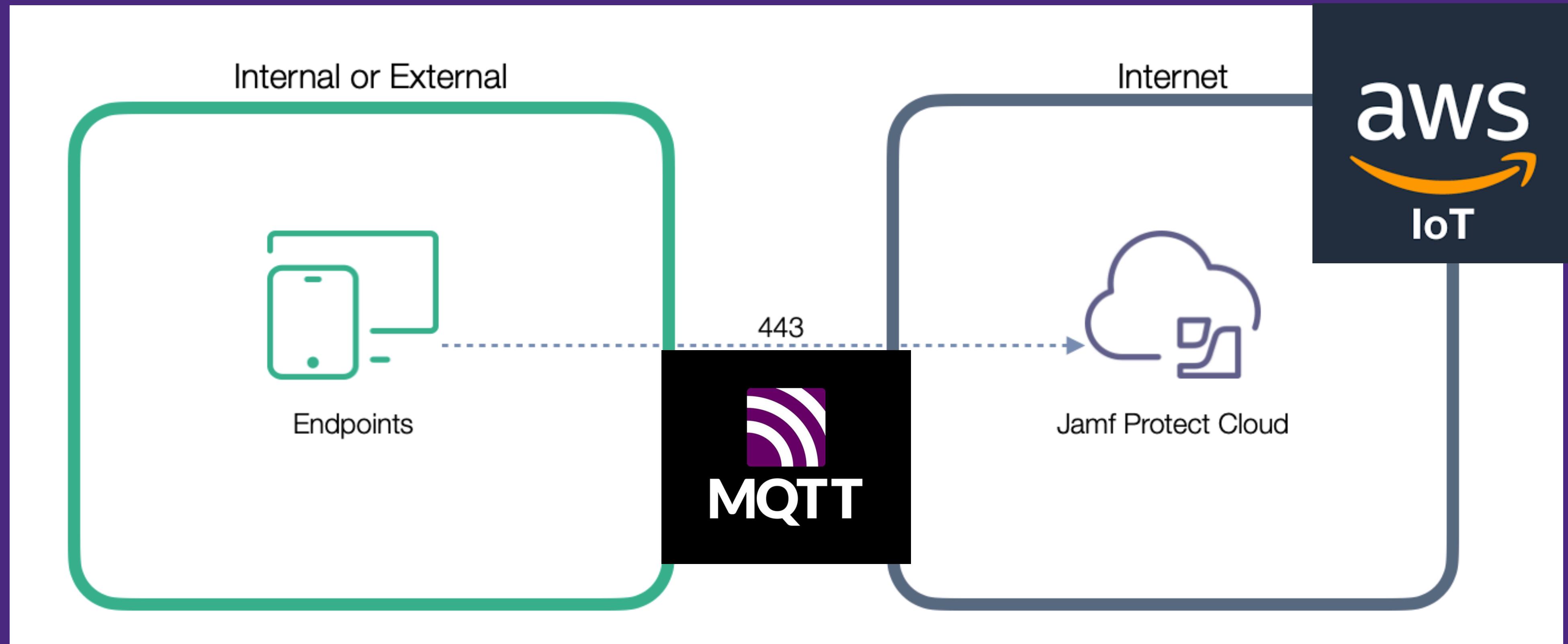
Authentication

# Network protocols

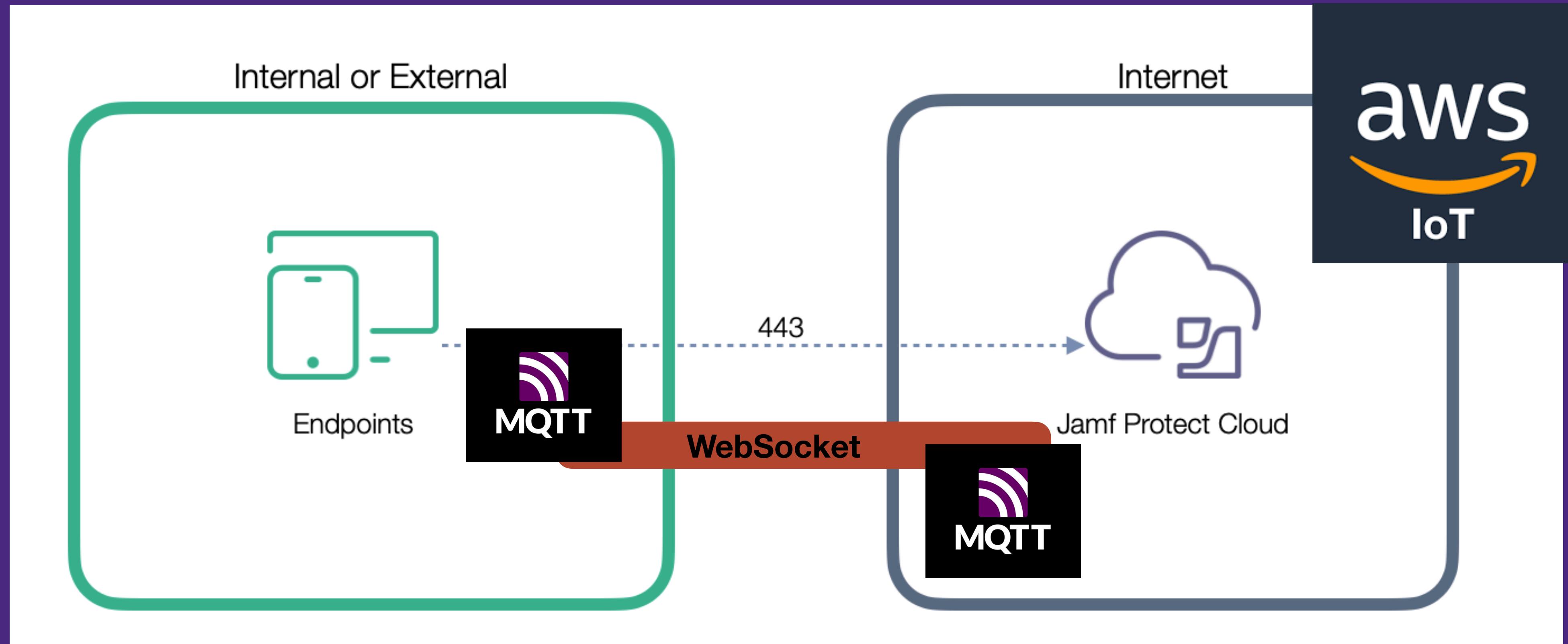
MQTT

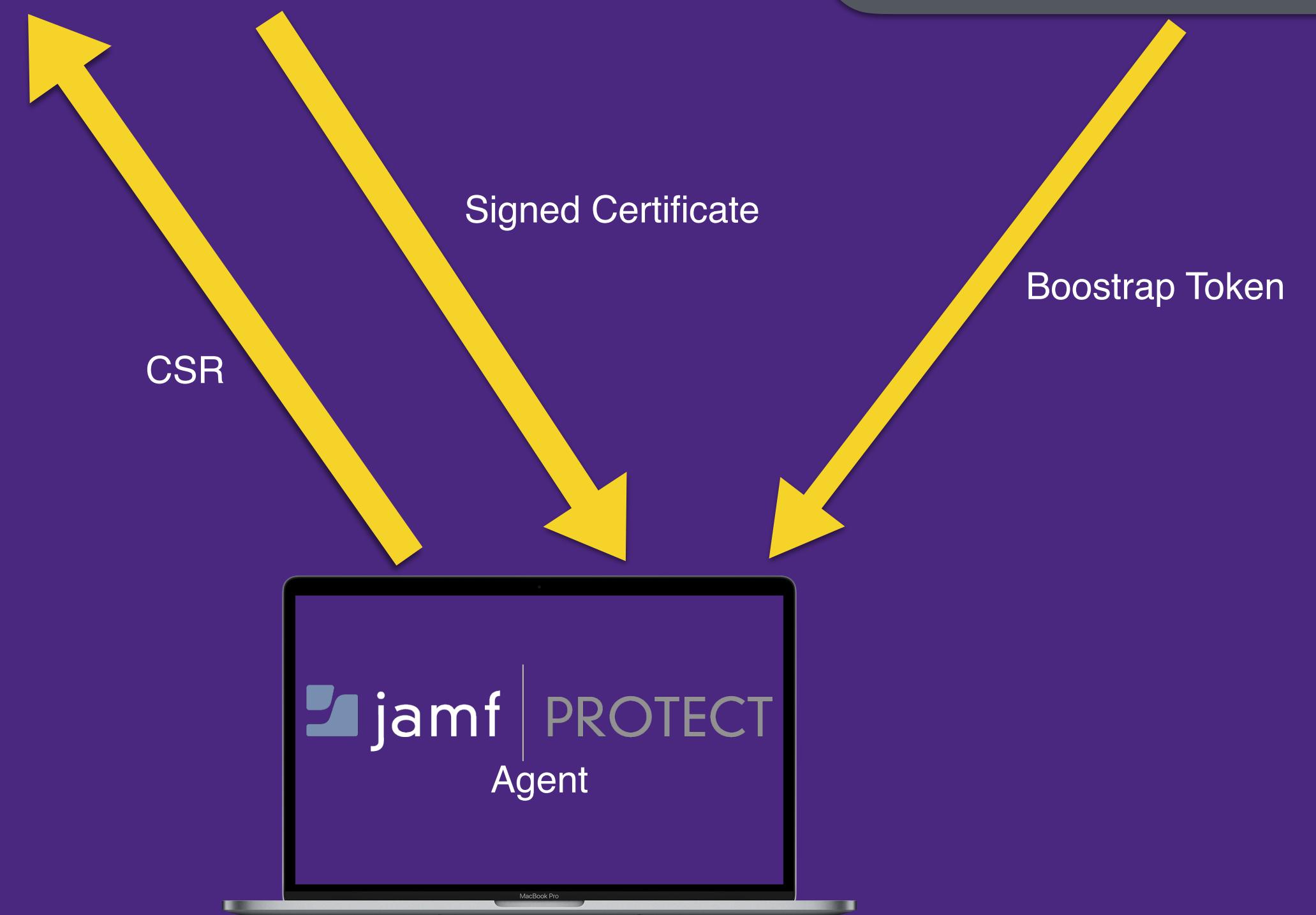
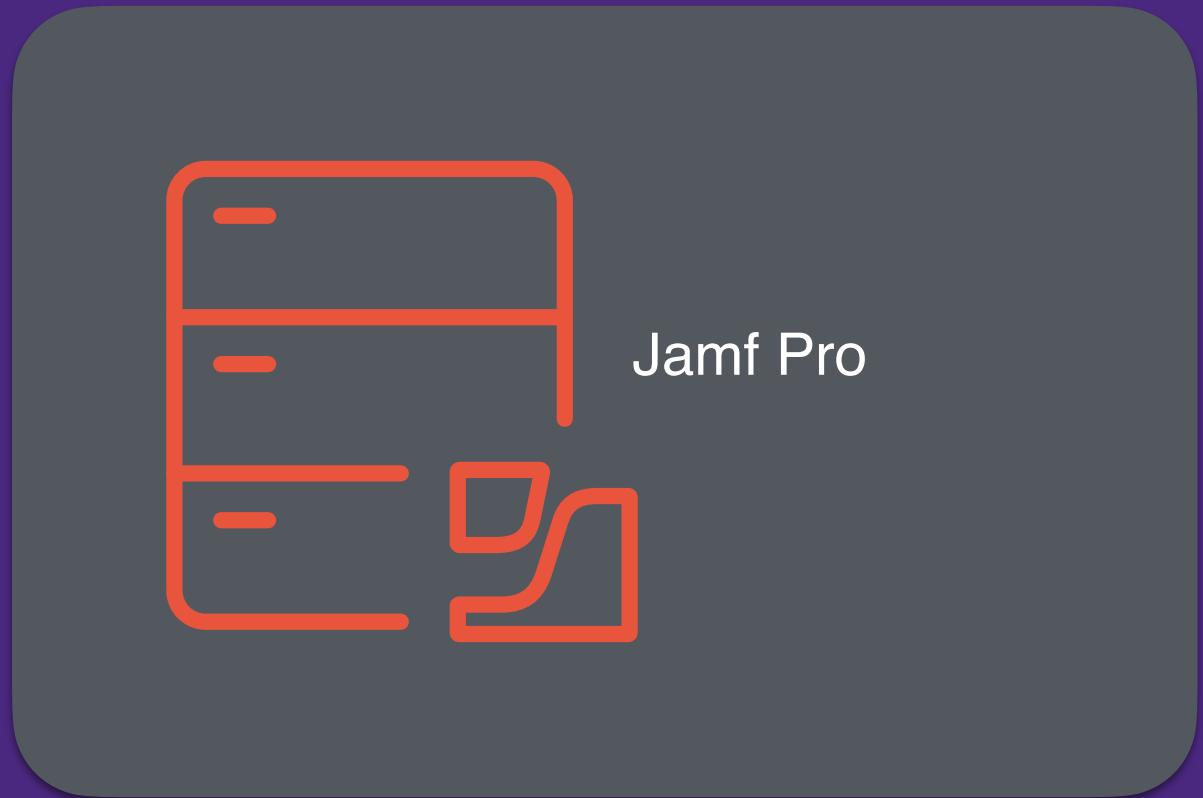
WebSocket

# Network Communications

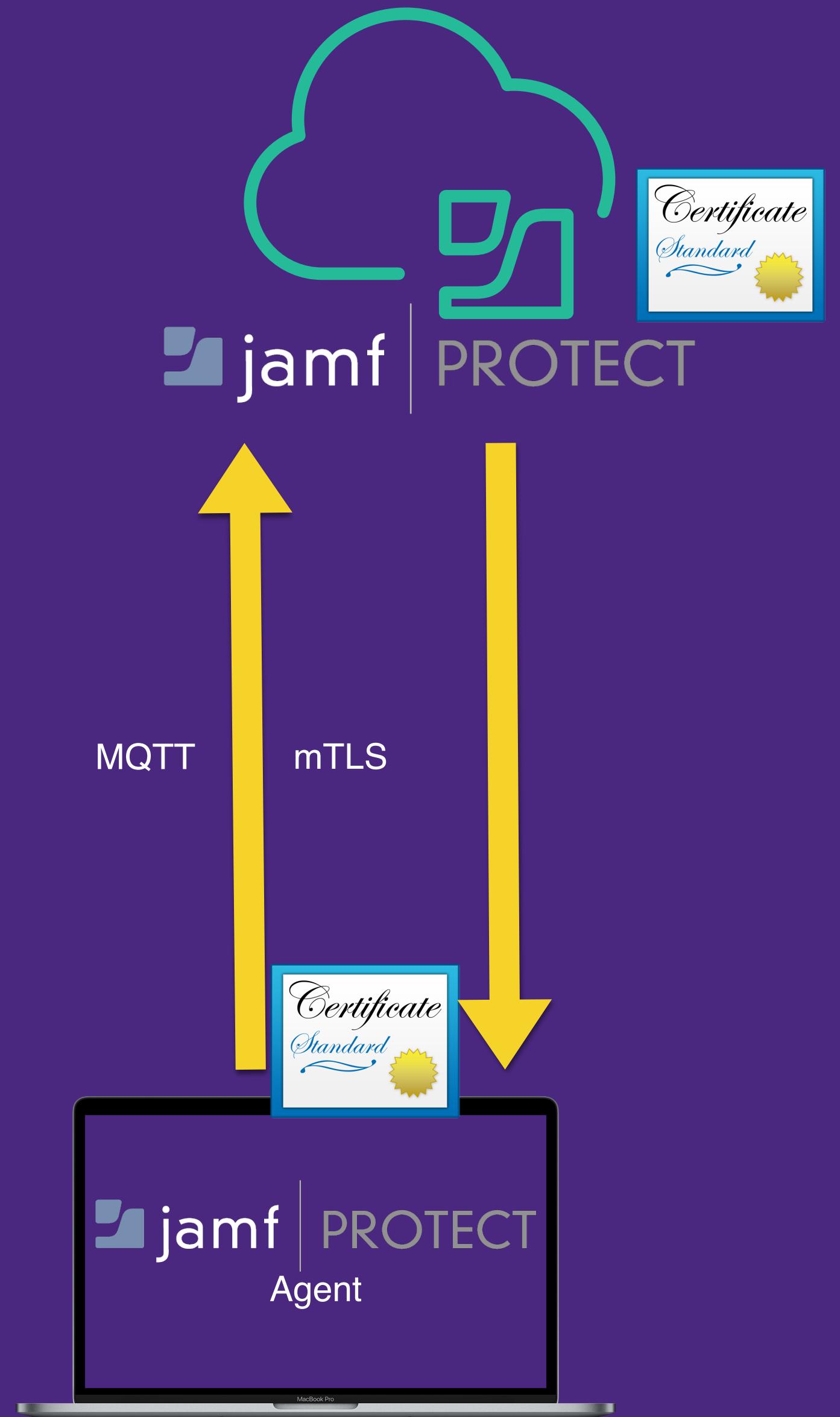


# Network Communications

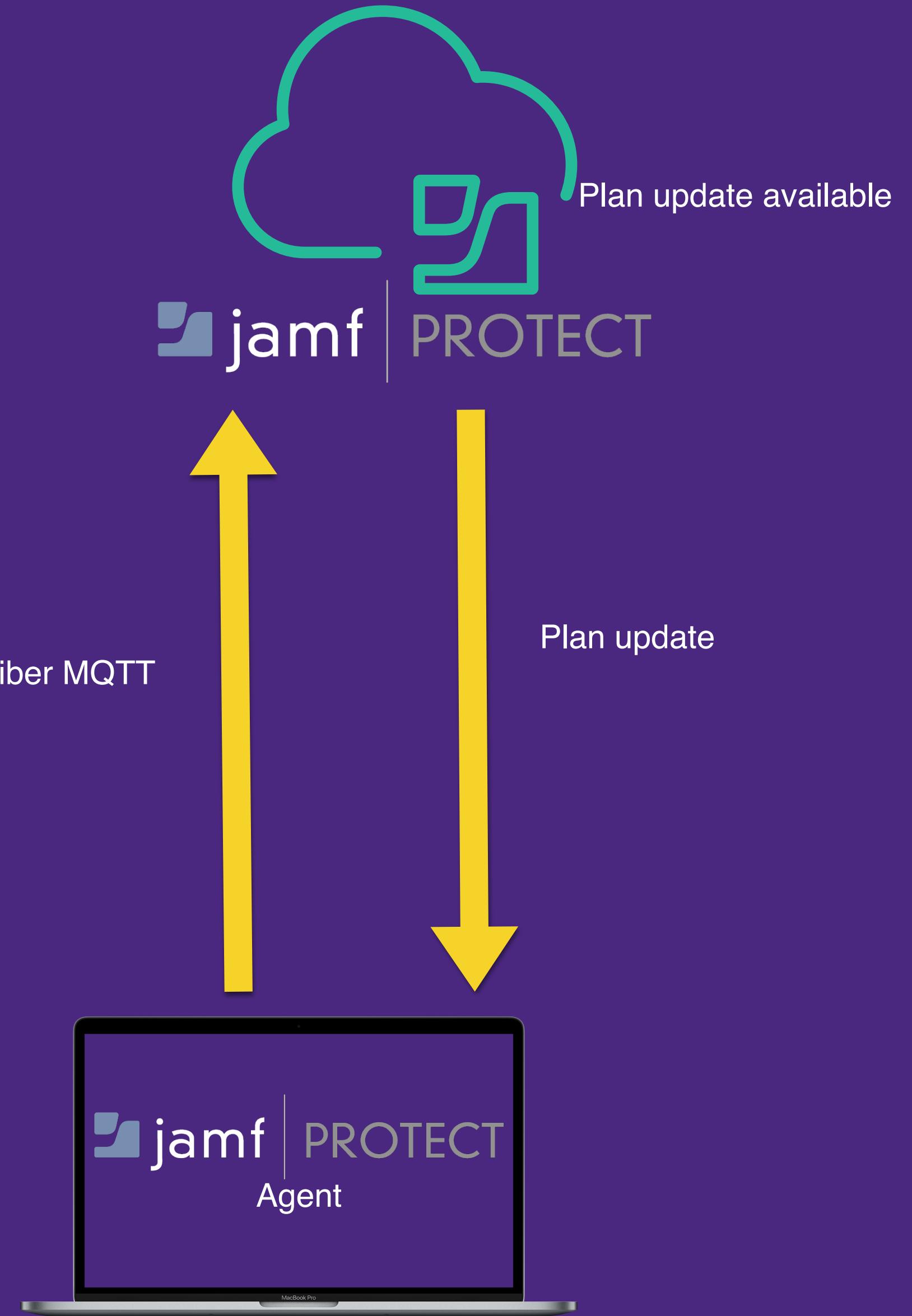




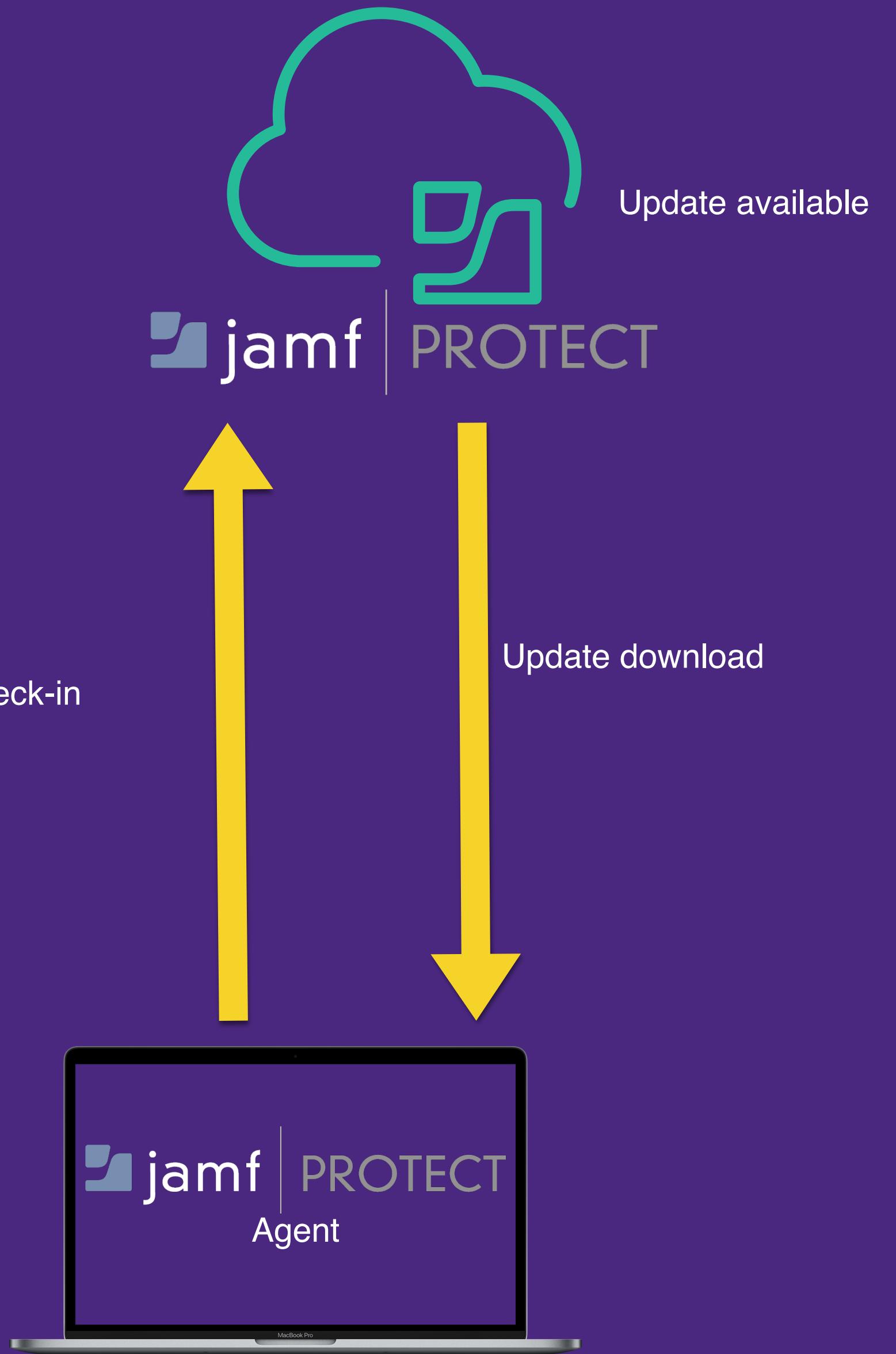
# Authentication



# Plan update



# Agent update



# Jamf Protect Plans

Configuration Profiles

Set of Analytics paired with Actions

# Agent Auto-Update

jamf PROTECT

TEST EMEA

- Overview
- Insights
- Computers
- Alerts
- Logs

CONFIGURATION

- Analytics
- Plans
- Actions
- Threat Prevention
- Unified Logging
- Administrative

Plans > Plan Summary

Edit Plan Save

Plan Name: JNUC Demo Plan

Description:

Action Configuration: JNUC Demo Action

Advanced Agent Configuration

Agent Update:  Enable AutoUpdate

Communications Protocol: Default option uses MQTT:8883 on macOS versions prior to 10.13.4

MQTT:443 (Default)

Built-in Threat Prevention Options:  Block & Report  Report Only  Disable

Log Level: Error

 Plan Name

JNUC Demo Plan

 Description

Description

 Action Configuration

JNUC Demo Action

 Advanced Agent ConfigurationAgent Update:  Enable AutoUpdate**Communications Protocol** Default option uses MQTT:8883 on macOS versions prior to 10.13.4

MQTT:443 (Default)

Built-in Threat Prevention Options:  Block & Report  Report Only  Disable Log Level

Error

## Advanced Agent Configuration

### Agent Update: Enable AutoUpdate

# Agent Auto-Update

# Agent protocol

jamf PROTECT

TEST EMEA

- Overview
- Insights
- Computers
- Alerts
- Logs

CONFIGURATION

- Analytics
- Plans
- Actions
- Threat Prevention
- Unified Logging
- Administrative

Plans > Plan Summary

Edit Plan Save

Plan Name: JNUC Demo Plan

Description:

Action Configuration: JNUC Demo Action

Advanced Agent Configuration

Agent Update:  Enable AutoUpdate

Communications Protocol: Default option uses MQTT:8883 on macOS versions prior to 10.13.4

MQTT:443 (Default)

Built-in Threat Prevention Options:  Block & Report  Report Only  Disable

Log Level: Error

Edit Plan **Plan Name**

JNUC Demo Plan

**Description**

Description

**Action Configuration**

JNUC Demo Action

**Advanced Agent Configuration**Agent Update:  Enable AutoUpdate**Communications Protocol** Default option uses MQTT:8883 on macOS versions prior to 10.13.4

MQTT:443 (Default)

Built-in Threat Prevention Options:  Block & Report  Report Only  Disable**Log Level**

Error

**Communications Protocol** Default option uses MQTT:8883 on macOS versions prior to 10.13.4MQTT:443 (Default) MQTT:443 (Default) 

WebSocket/MQTT:443

Error 

# Agent protocol

# Agent Log Verbosity

jamf PROTECT

TEST EMEA

- Overview
- Insights
- Computers
- Alerts
- Logs

CONFIGURATION

- Analytics
- Plans
- Actions
- Threat Prevention
- Unified Logging
- Administrative

Plans > Plan Summary

Summary Custom Profile Analytics Edit Delete

Edit Plan Save

Plan Name: JNUC Demo Plan

Description:

Action Configuration: JNUC Demo Action

Advanced Agent Configuration

Agent Update:  Enable AutoUpdate

Communications Protocol: Default option uses MQTT:8883 on macOS versions prior to 10.13.4

MQTT:443 (Default)

Built-in Threat Prevention Options:  Block & Report  Report Only  Disable

Log Level: Error

 Plan Name

JNUC Demo Plan

 Description

Description

 Action Configuration

JNUC Demo Action

 Advanced Agent ConfigurationAgent Update:  Enable AutoUpdate

Communications Protocol Default option uses MQTT:8883 on macOS versions prior to 10.13.4

MQTT:443 (Default)

Built-in Threat Prevention Options:  Block & Report  Report Only  Disable Log Level

Error

 Advanced Agent Configuration

Error

Warning

Info

Debug

Verbose

Error

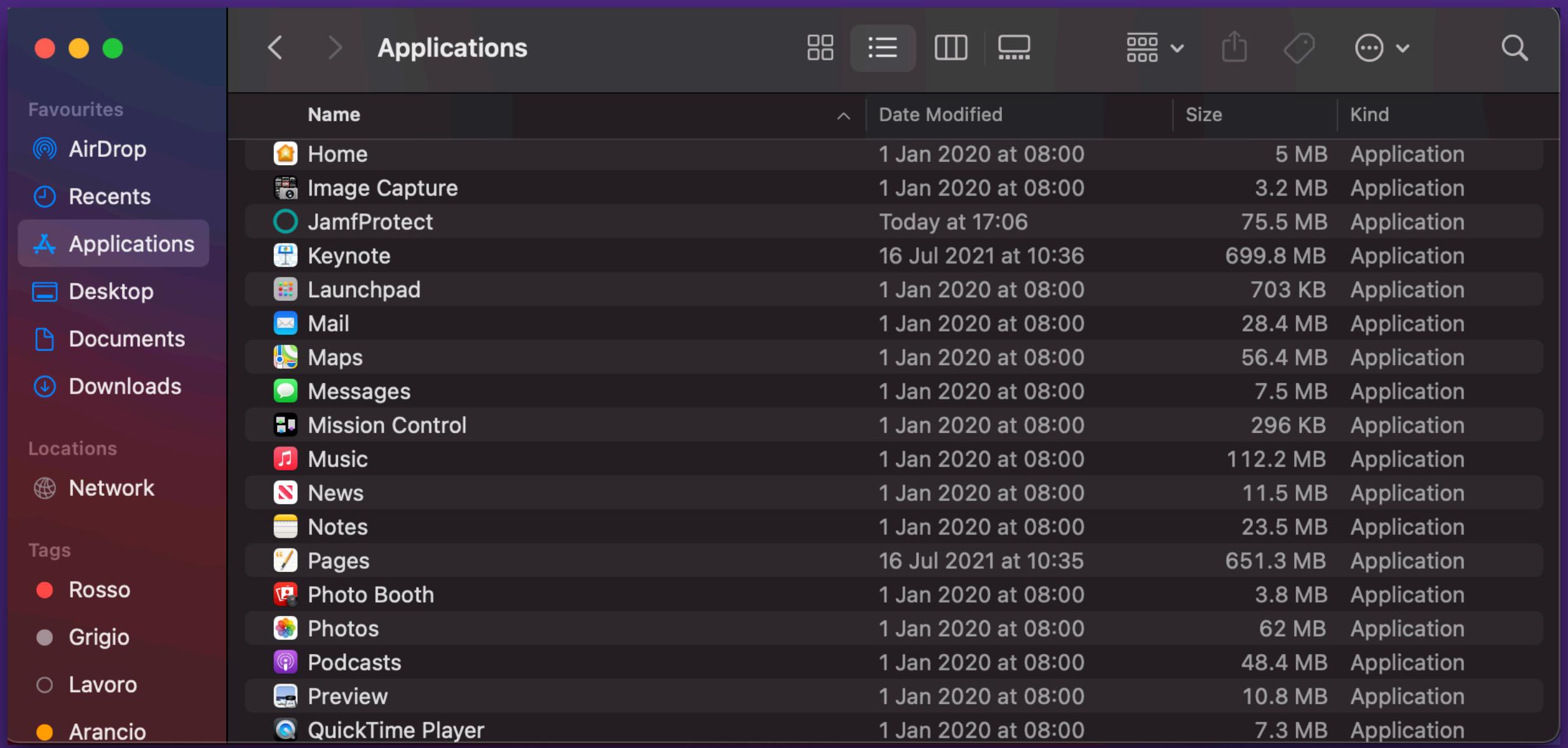
# Agent Log Verbosity

# Analytics

TEST EMEA							
	Summary	Custom Profile	Analytics	Edit	Delete		
	Save Plan Analytics Select or deselect analytics to make changes						
	Type	Owner	Modified	Name	Categories	Actions	Tags
Overview	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	AoboKeylogger	KnownMalware	Alert	Known Aobo_Keylogger
Insights	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	AppleJeusMalware	KnownMalware	Alert	Known AppleJeus
Computers	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	AppLoginItem	Persistence	Log	MITREattack Persistence LoginItems
Alerts	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	BlazingKeylogger	KnownMalware	Alert	Known BlazingKeylogger
Logs	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	BucaMalware	KnownMalware	Alert	Known Buca
CONFIGURATION	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	BundloreAdware	KnownMalware	Alert	Known Bundlore
Analytics	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	CallMeMalware	KnownMalware	Alert	Known CallMe
Plans	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	CaretoMalware	KnownMalware	Alert	Known Careto
Actions	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	CodecmAdware	KnownMalware	Alert	Known Codecm
Threat Prevention	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	ConduitMalware	KnownMalware	Alert	Known Conduit
Unified Logging	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	CronJob	Persistence	Log	MITREattack Persistence LocalJobScheduling
Administrative	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	CurlPipedToInterpreterLanguage	TTPIndicators	Log	TTPIndicators Tuning
	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	CustomURLHandlerCreation	Visibility	Log	Visibility
	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	DevilRobberMalware	KnownMalware	Alert	Known DevilRobber
	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	DisguisedExecutable	DefenseEvasion	Alert	MITREattack DefenseEvasion Masquerading Tuning
	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	DNSModification	Visibility	Log	Visibility DNS
	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	DocksterMalware	KnownMalware	Alert	Known Dockster
	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	DriveBy	InitialAccess	Log	MITREattack InitialAccess DriveByCompromise Tuning
	<input checked="" type="checkbox"/>		08/25/2021 9:02 PM GMT	DSStoreDirCreate	DefenseEvasion	Alert	Masquerading DefenseEvasion MITREattack Tuning

# Components

LaunchDaemon vs System Extension

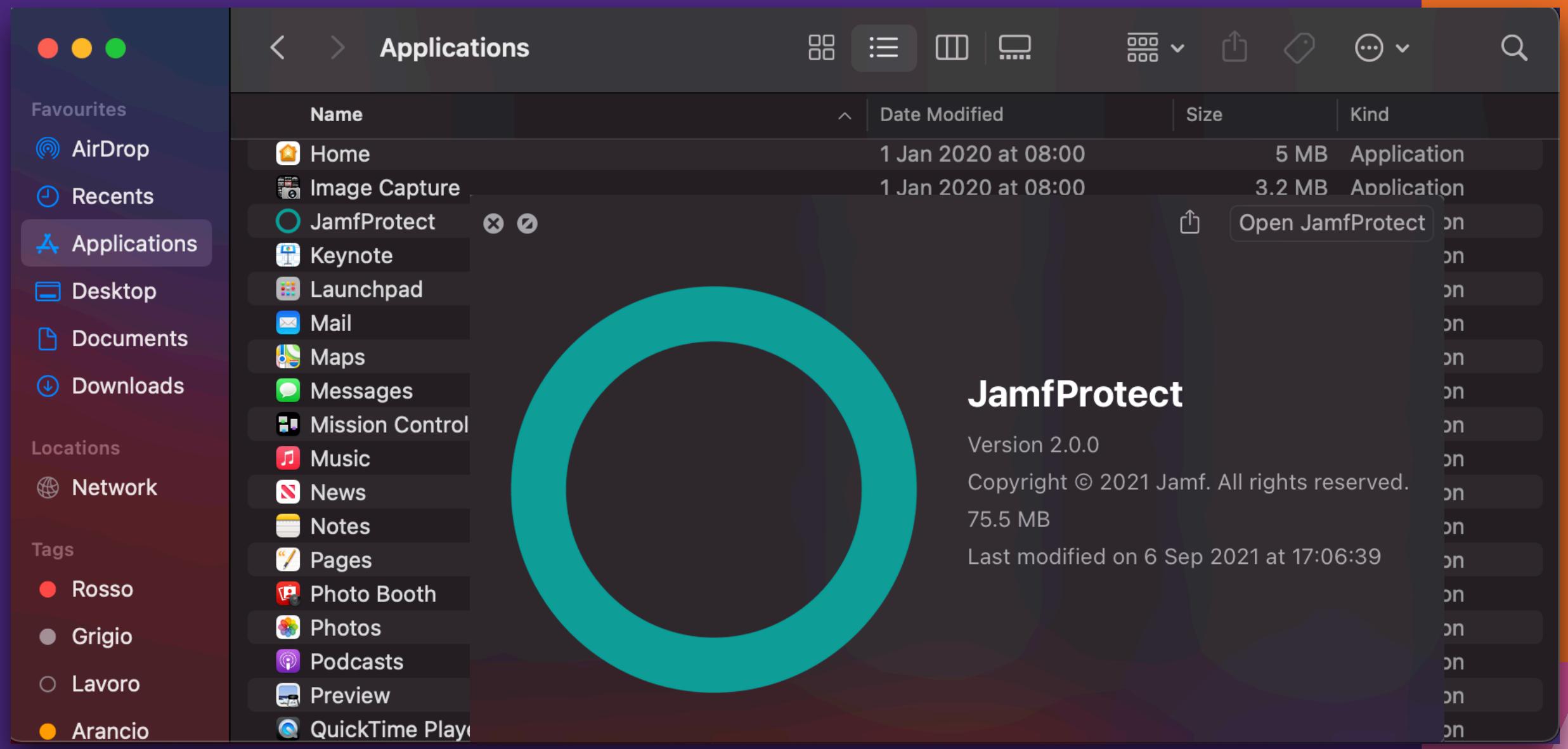


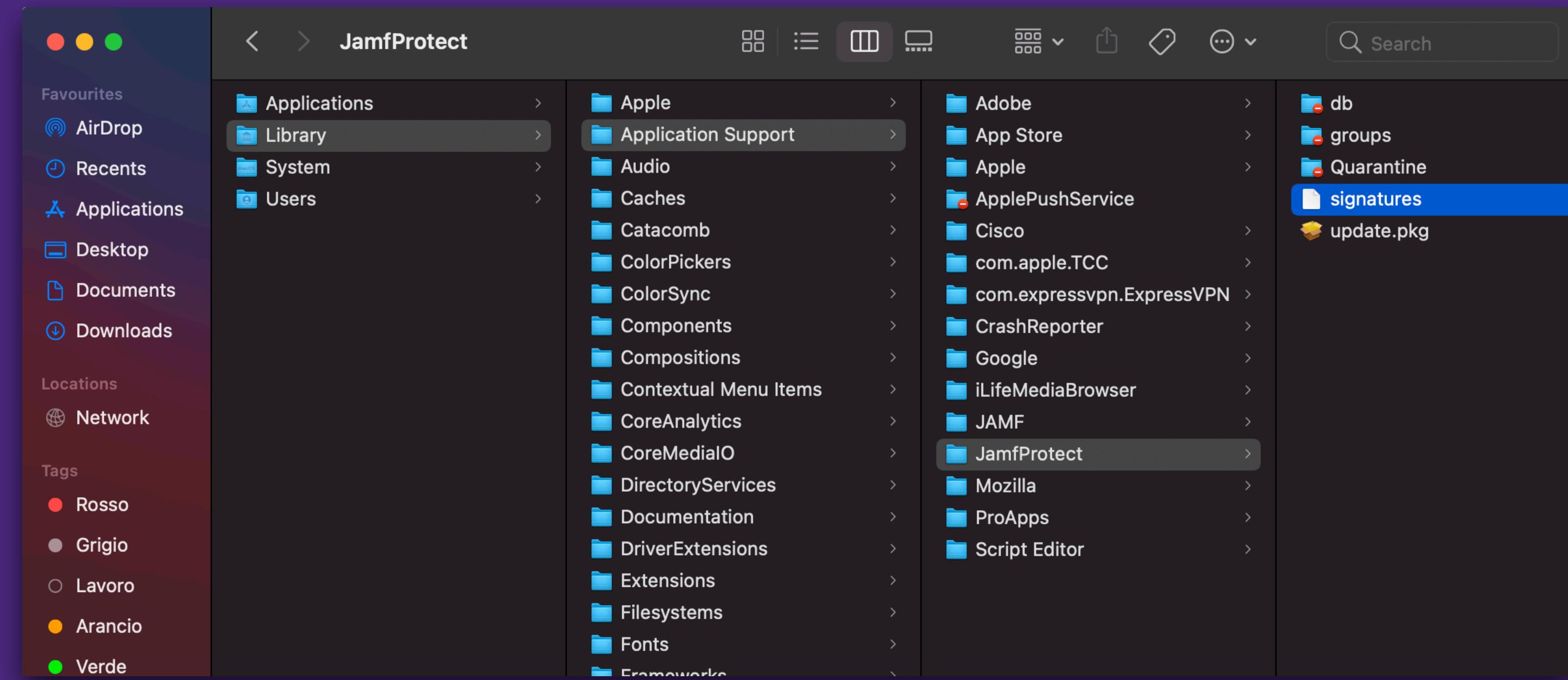
A screenshot of a Mac OS X desktop showing the Applications folder. The window title is "Applications". The table lists various applications with their names, last modified dates, sizes, and kinds. The "JamfProtect" application is listed at the top of the list.

Name	Date Modified	Size	Kind
Home	1 Jan 2020 at 08:00	5 MB	Application
Image Capture	1 Jan 2020 at 08:00	3.2 MB	Application
JamfProtect	Today at 17:06	75.5 MB	Application
Keynote	16 Jul 2021 at 10:36	699.8 MB	Application
Launchpad	1 Jan 2020 at 08:00	703 KB	Application
Mail	1 Jan 2020 at 08:00	28.4 MB	Application
Maps	1 Jan 2020 at 08:00	56.4 MB	Application
Messages	1 Jan 2020 at 08:00	7.5 MB	Application
Mission Control	1 Jan 2020 at 08:00	296 KB	Application
Music	1 Jan 2020 at 08:00	112.2 MB	Application
News	1 Jan 2020 at 08:00	11.5 MB	Application
Notes	1 Jan 2020 at 08:00	23.5 MB	Application
Pages	16 Jul 2021 at 10:35	651.3 MB	Application
Photo Booth	1 Jan 2020 at 08:00	3.8 MB	Application
Photos	1 Jan 2020 at 08:00	62 MB	Application
Podcasts	1 Jan 2020 at 08:00	48.4 MB	Application
Preview	1 Jan 2020 at 08:00	10.8 MB	Application
QuickTime Player	1 Jan 2020 at 08:00	7.3 MB	Application

# App bundle: /Applications/JamfProtect.app/

# App bundle: /Applications/JamfProtect.app/





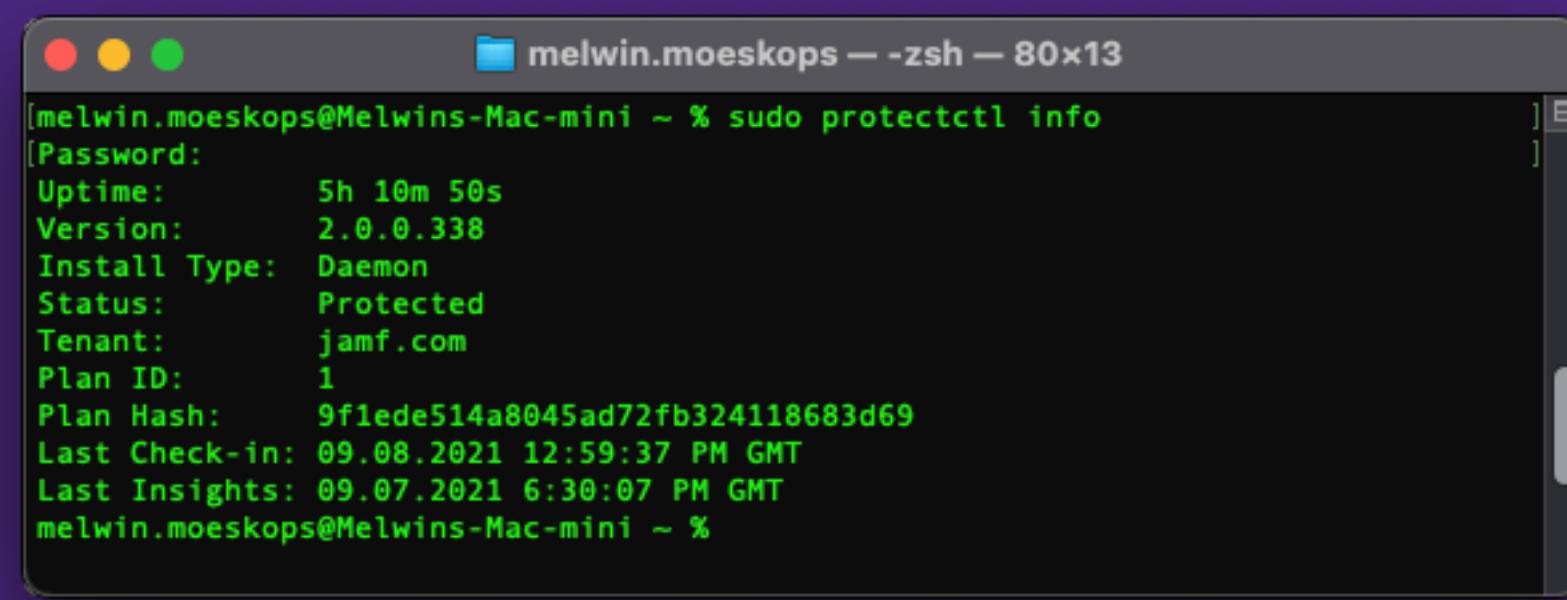
/Library/Application\ Support/JamfProtect/

# LaunchDaemons vs Systems Extensions

# protectctl command

- Repair - Finds and repairs issues that may occur during installation of the Jamf Protect agent
- Version - Prints the Jamf Protect agent version installed on computers
- Checkin - Forces a Jamf Protect agent check-in on computers. You can also use the --insights flag to force an insights check-in.
- Help - Prints help information about protectctl commands

- Info:



A terminal window titled "melwin.moeskops -- zsh -- 80x13" displaying the output of the "protectctl info" command. The output shows various system and Jamf Protect agent details:

```
[melwin.moeskops@Melwins-Mac-mini ~ % sudo protectctl info
[Password:
Uptime:      5h 10m 50s
Version:     2.0.0.338
Install Type: Daemon
Status:      Protected
Tenant:      jamf.com
Plan ID:     1
Plan Hash:   9f1ede514a8045ad72fb324118683d69
Last Check-in: 09.08.2021 12:59:37 PM GMT
Last Insights: 09.07.2021 6:30:07 PM GMT
melwin.moeskops@Melwins-Mac-mini ~ %]
```

# Agent Detection

- What is Agent Detection

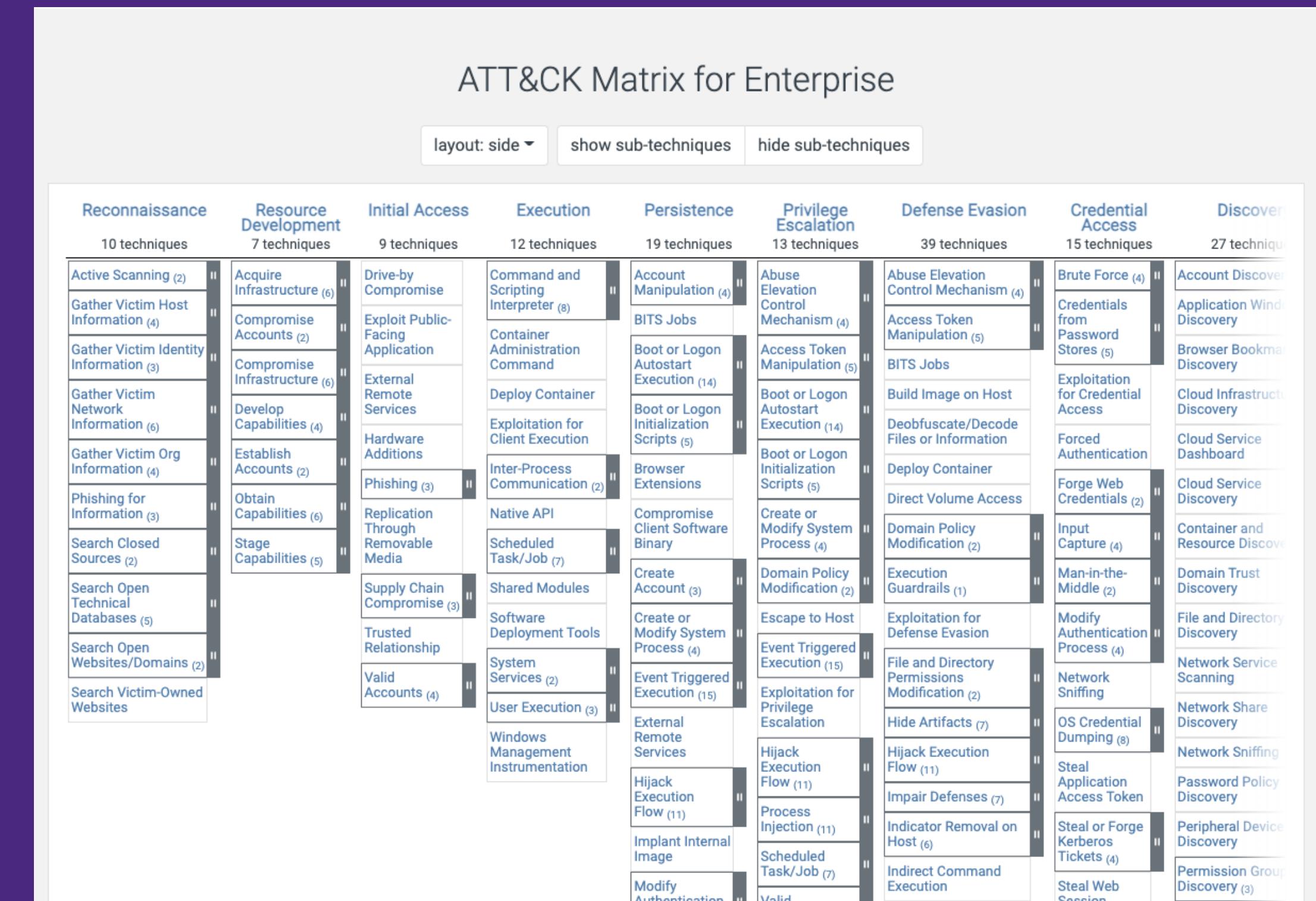
# Signature detection

- What is signature detection

# Behaviour detection

- What is behaviour detection
- Where will we be notified
- When does it decided there is a threat?

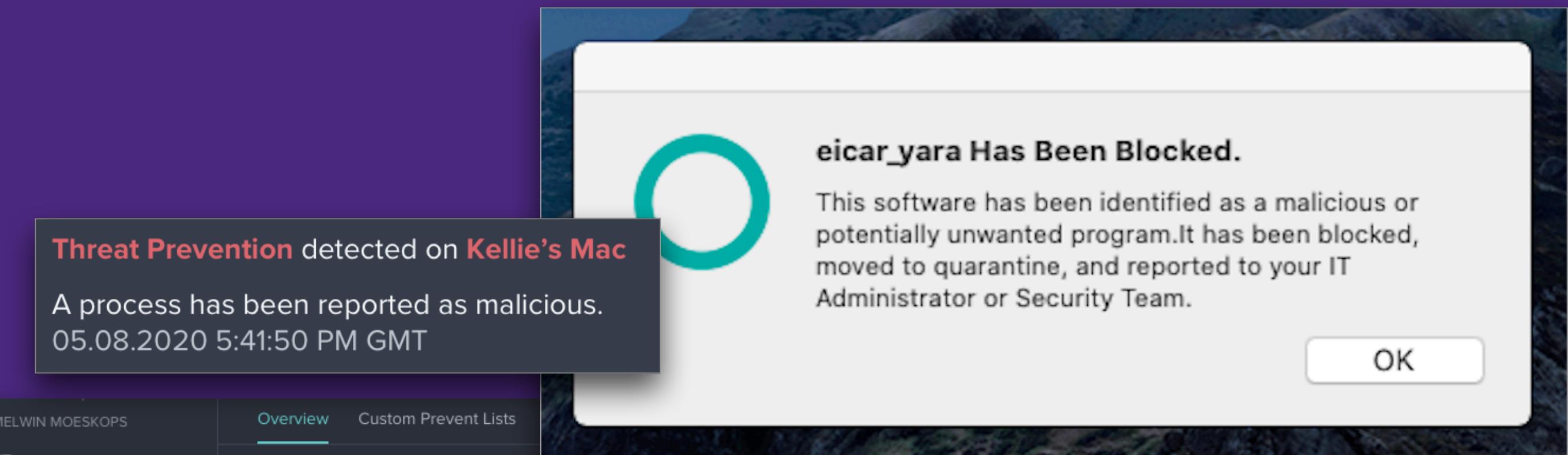
<https://attack.mitre.org/>



# Threat prevention

- Computers with macOS 10.15.0 or later
- Computers with version 1.1.0.124 or later of the Jamf Protect agent

The screenshot shows the 'Create Prevent List' page. At the top, there are tabs for 'Overview' and 'Custom Prevent Lists'. Below that, a 'Name' field is filled with 'Name'. Under 'Prevent Type', 'File Hash' is selected. There are also tabs for 'Signing Information' and 'Administrative'. At the bottom, there are buttons for 'Plain Text' and 'File Upload'.

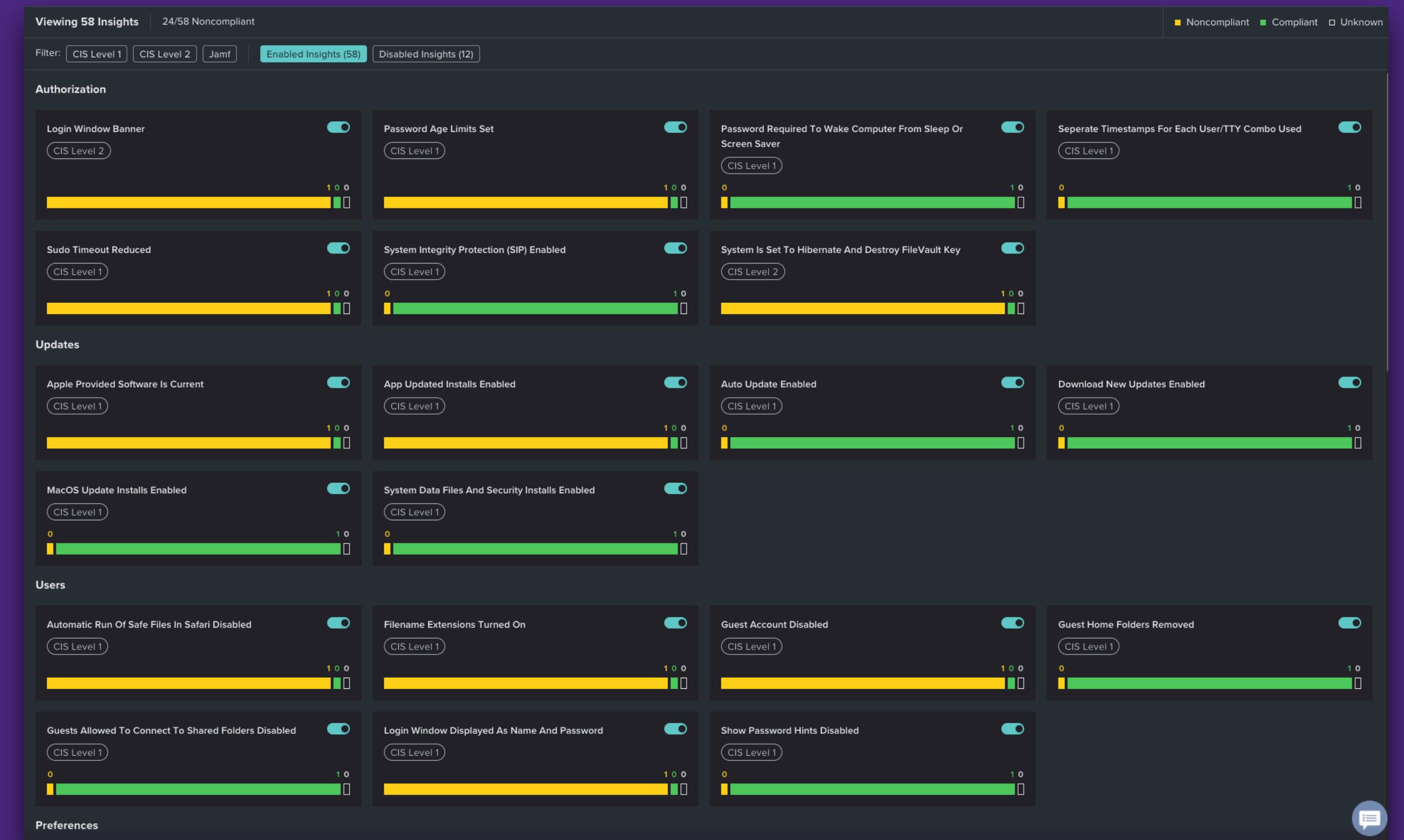


The screenshot shows the 'Threat Prevention' section. On the left, there is a sidebar with 'Overview', 'Insights', 'Computers', 'Alerts', 'Logs', 'Configuration', 'Analytics', 'Plans', 'Actions', 'Threat Prevention' (which is selected and highlighted in blue), 'Unified Logging', and 'Administrative'. The main area displays a table of 'Built-in Threat Prevention Version History'. The table has columns for 'Version', 'Created', and 'Last Modified'. The 'Latest' version is listed as 'Version 4440' created on '09/07/2021 4:08 PM GMT'. Below the table, a message states 'All computers are on the latest version'.

# Insights & Analytics

# Insights

- Insights only report computer settings and do not enforce settings and restrictions on computers.
- Jamf Protect still collects data for disabled insights during each check-in.
- Only the currently logged in user's computer settings are monitored and reported.



Viewing 58 Insights

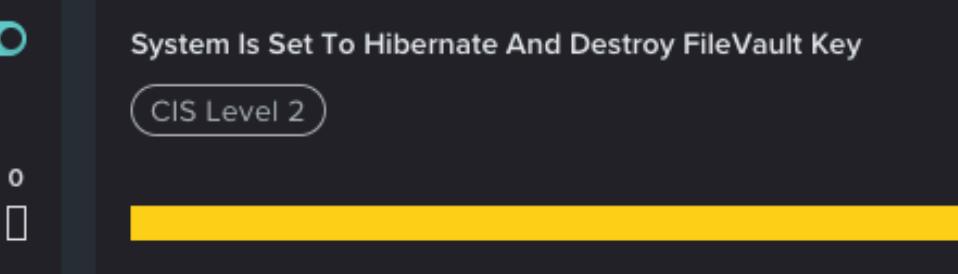
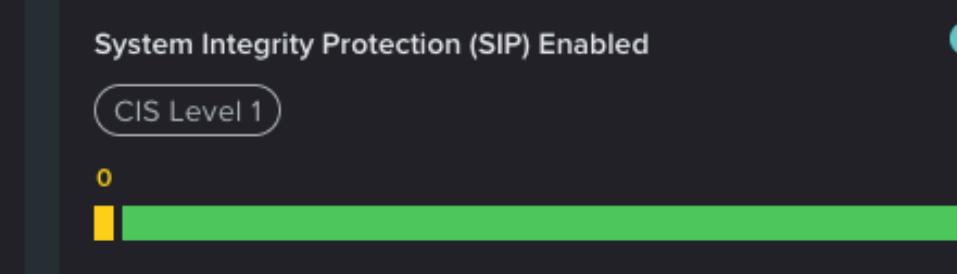
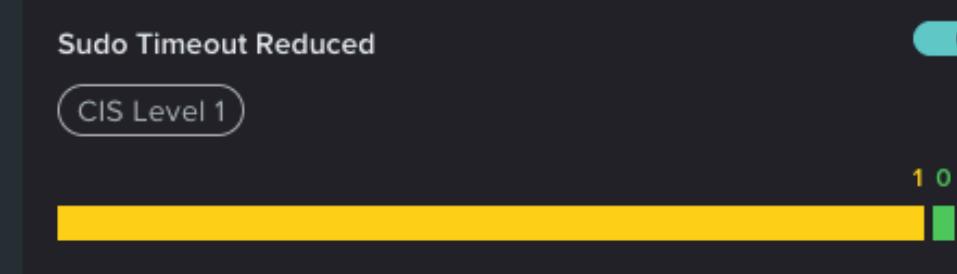
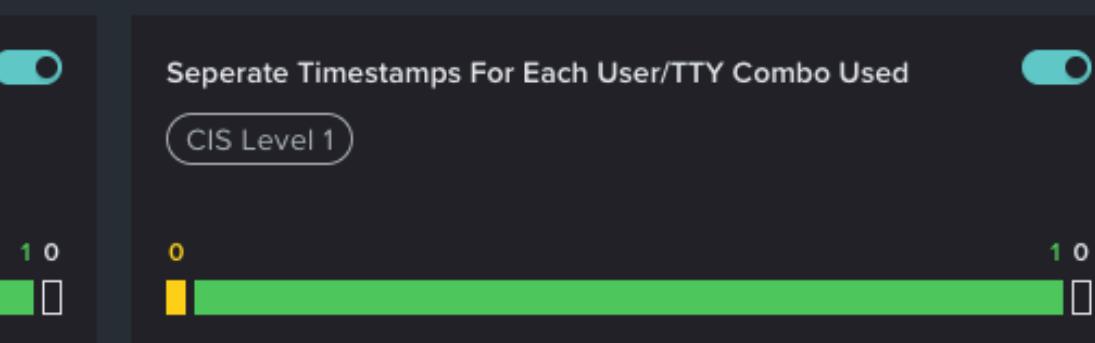
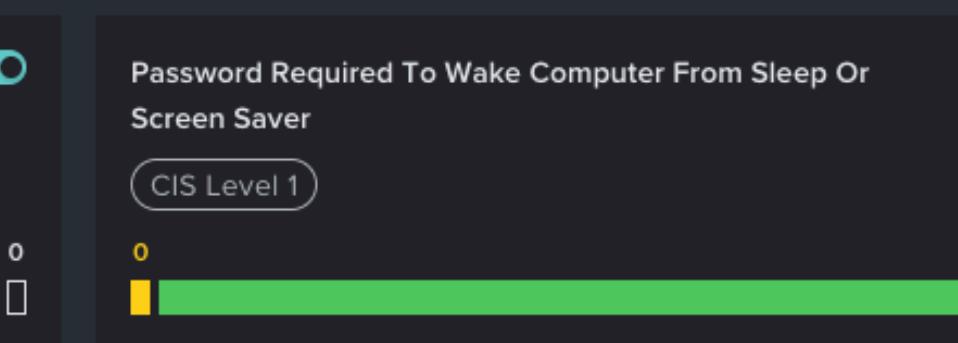
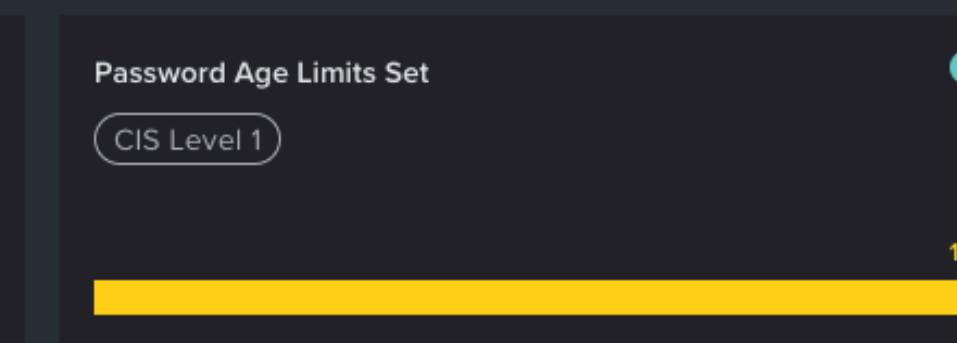
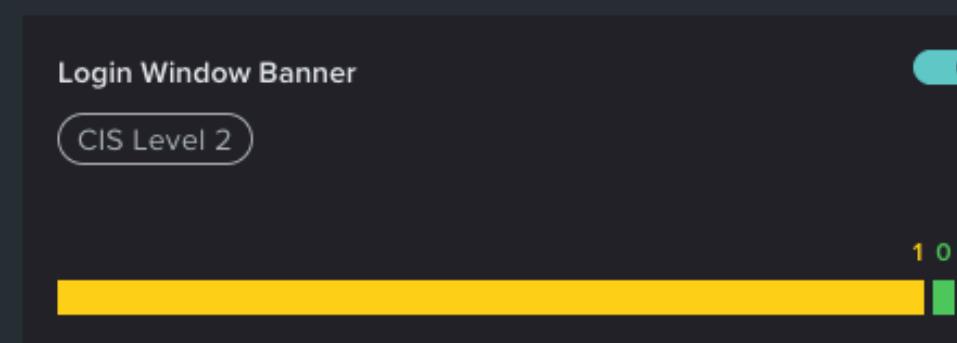
24/58 Noncompliant

■ Noncompliant ■ Compliant ■ Unknown

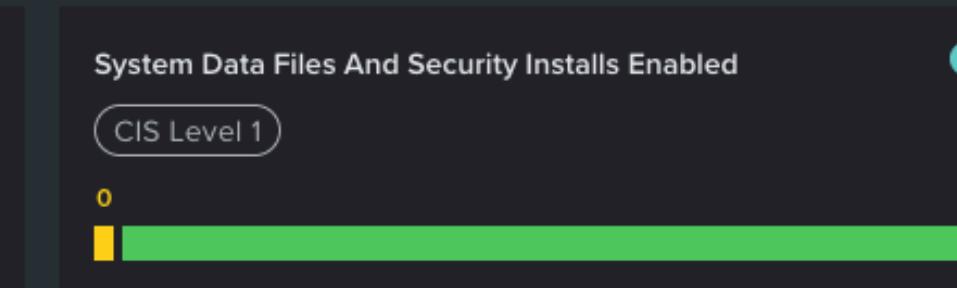
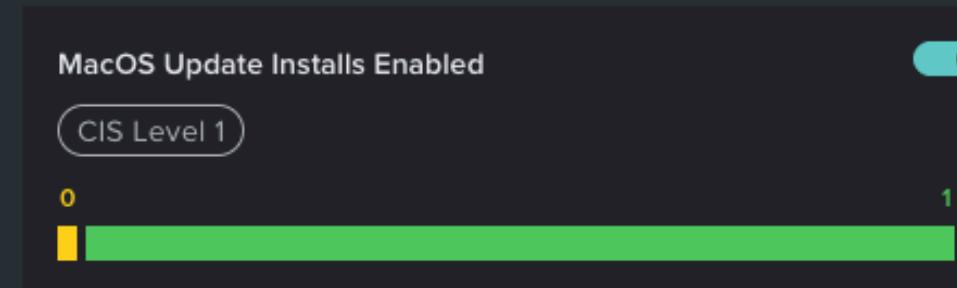
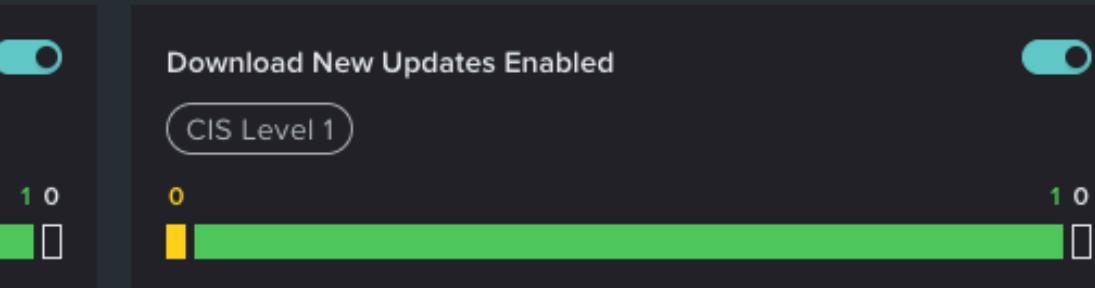
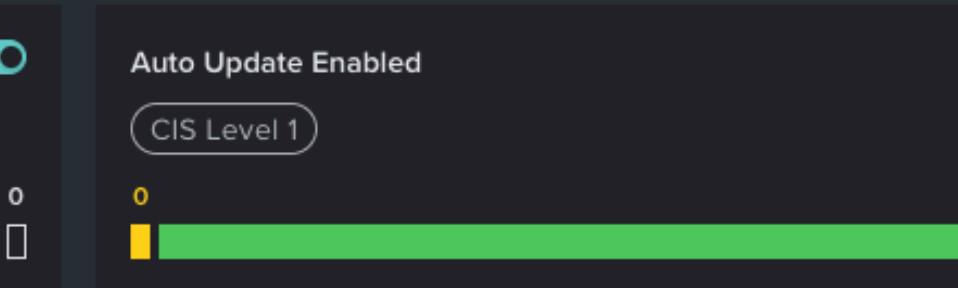
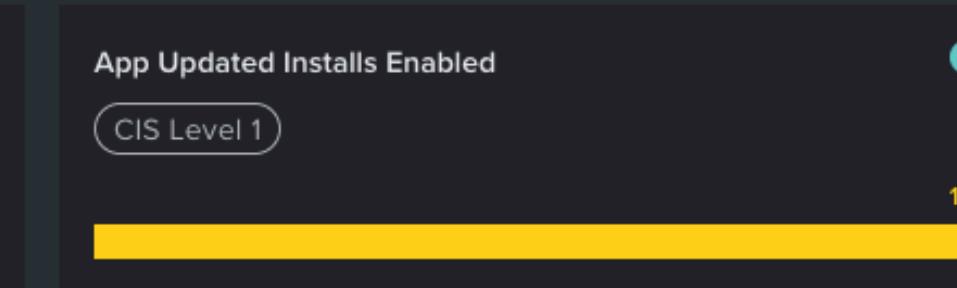
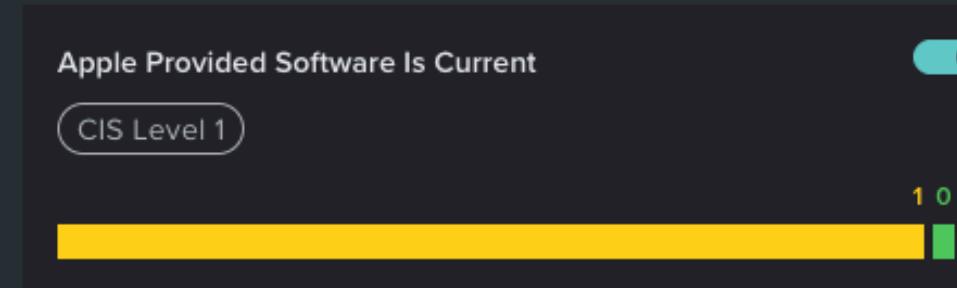
Filter: CIS Level 1 CIS Level 2 Jamf

Enabled Insights (58) Disabled Insights (12)

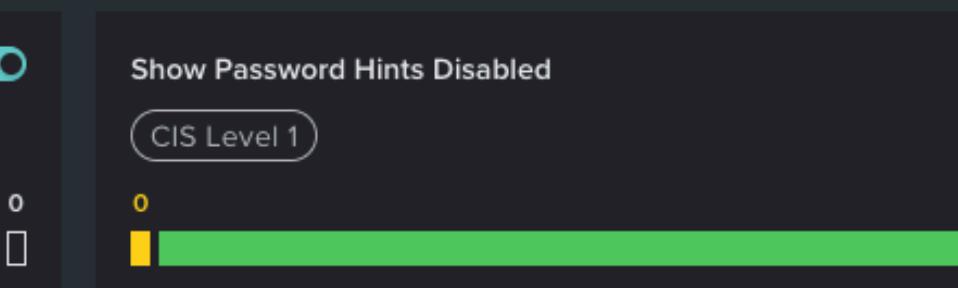
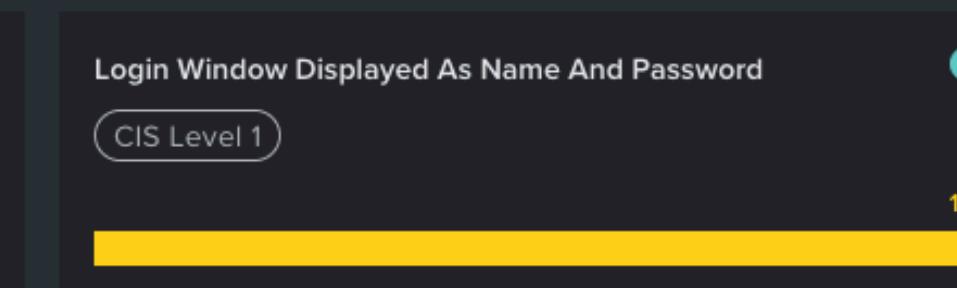
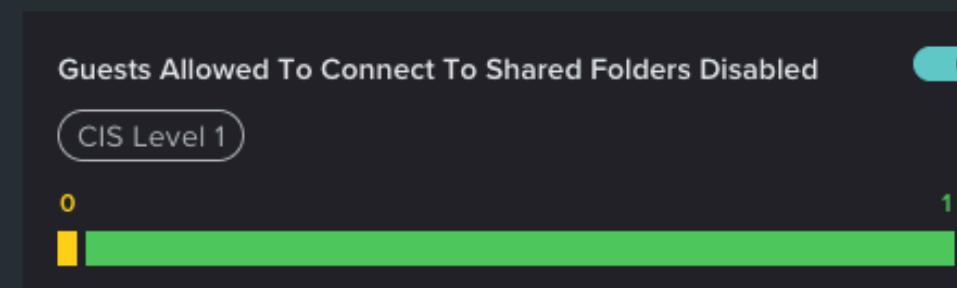
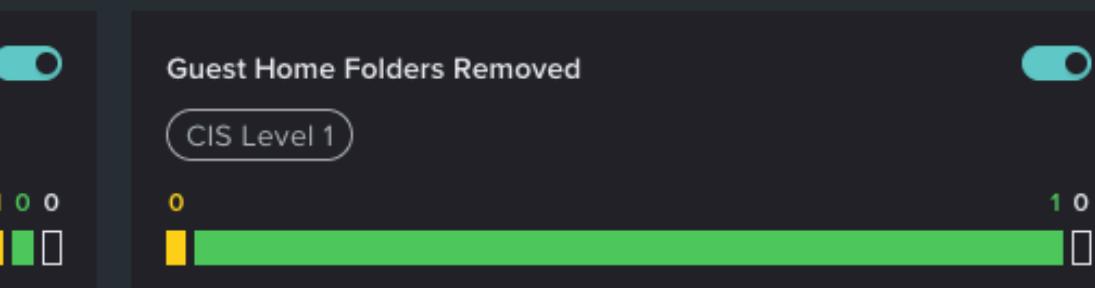
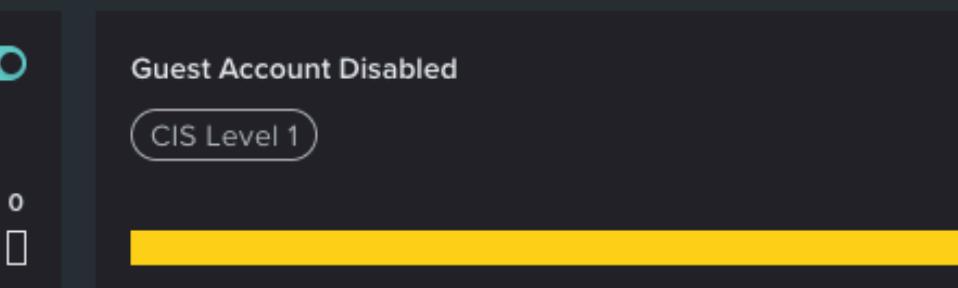
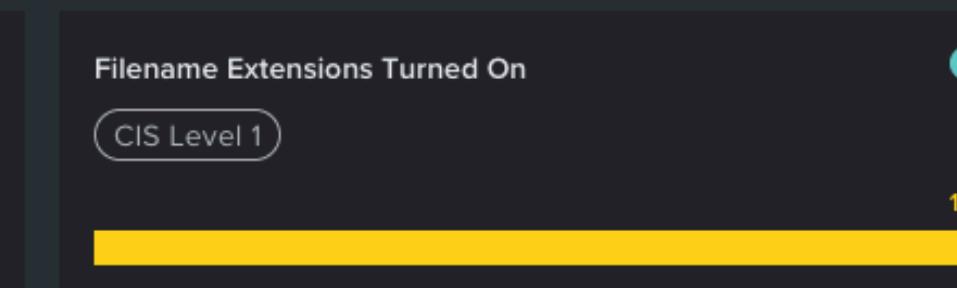
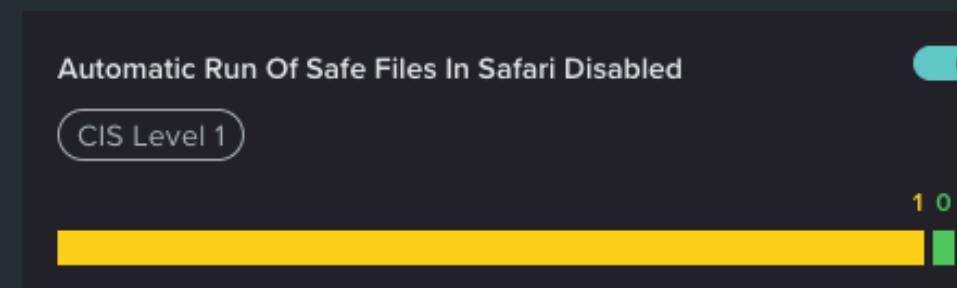
## Authorization



## Updates

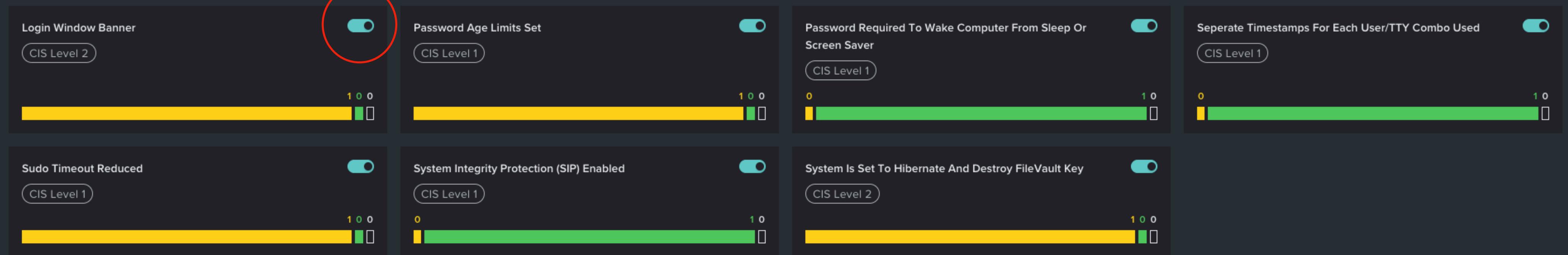
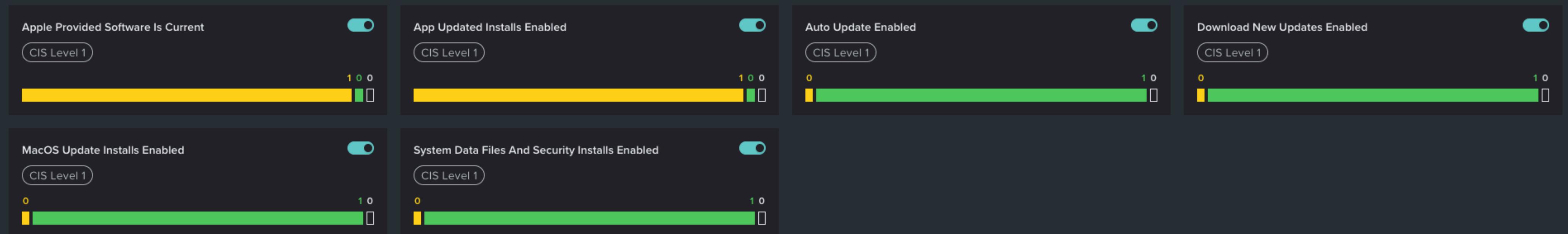
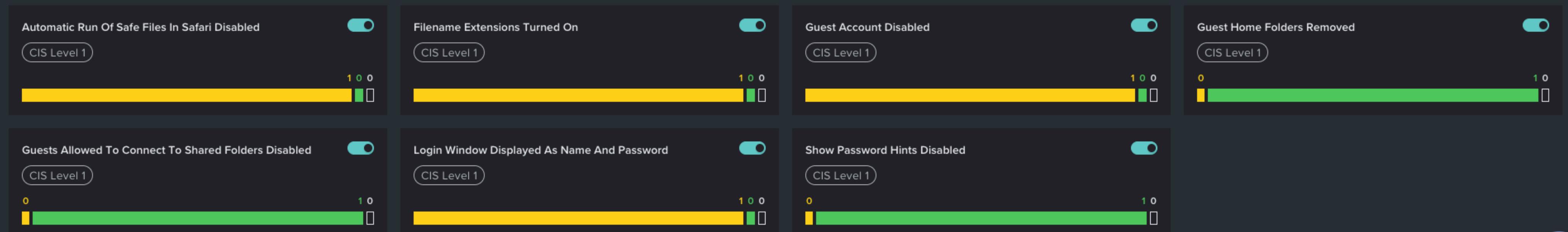


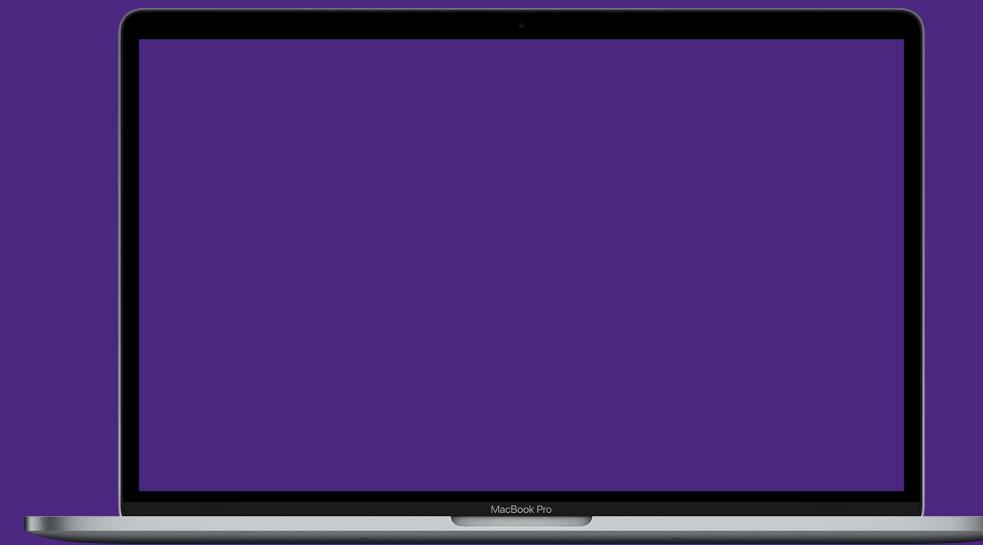
## Users



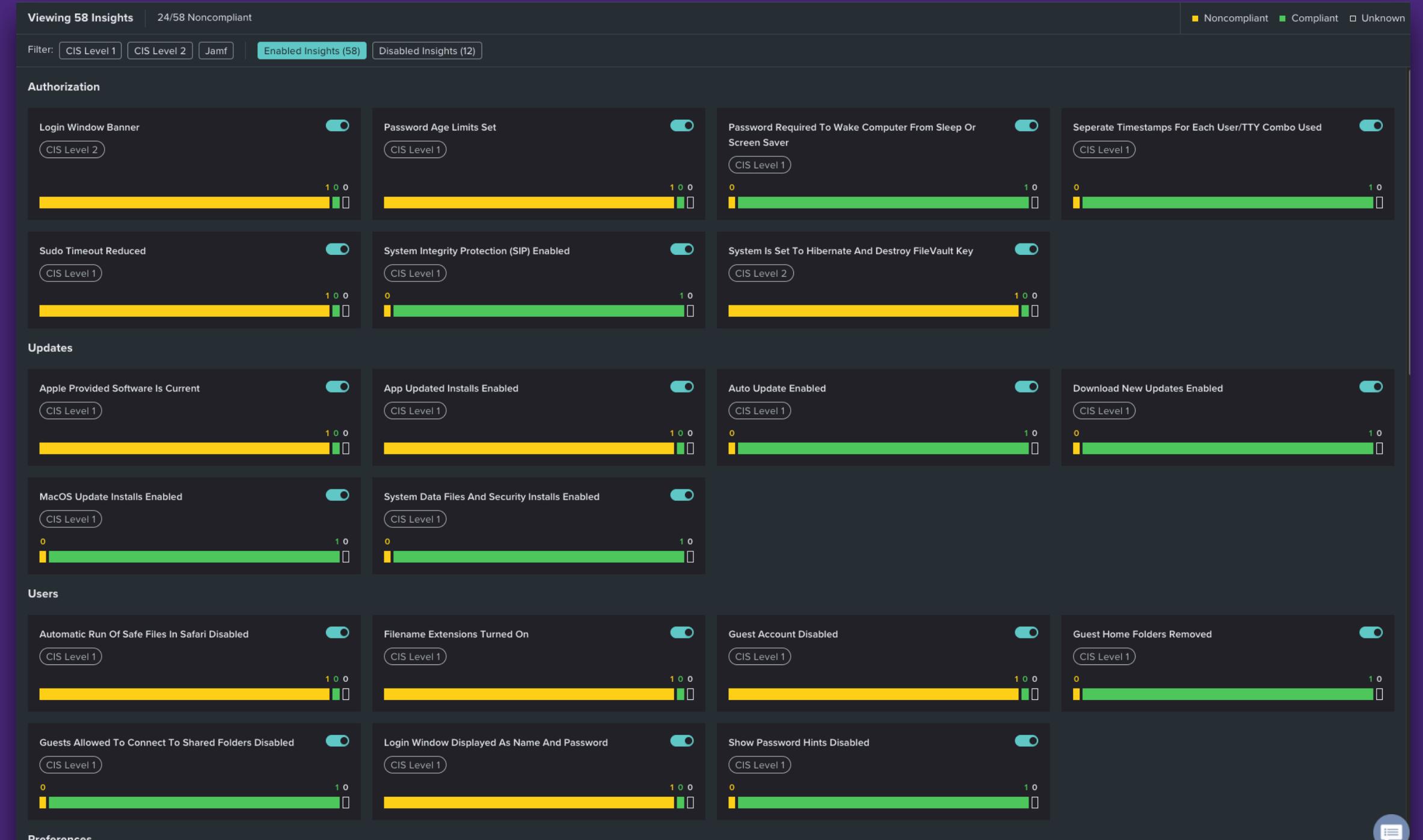
## Preferences



Filter: CIS Level 1 CIS Level 2 Jamf Enabled Insights (58) **Enabled Insights (58)** Disabled Insights (12)**Authorization****Updates****Users****Preferences**

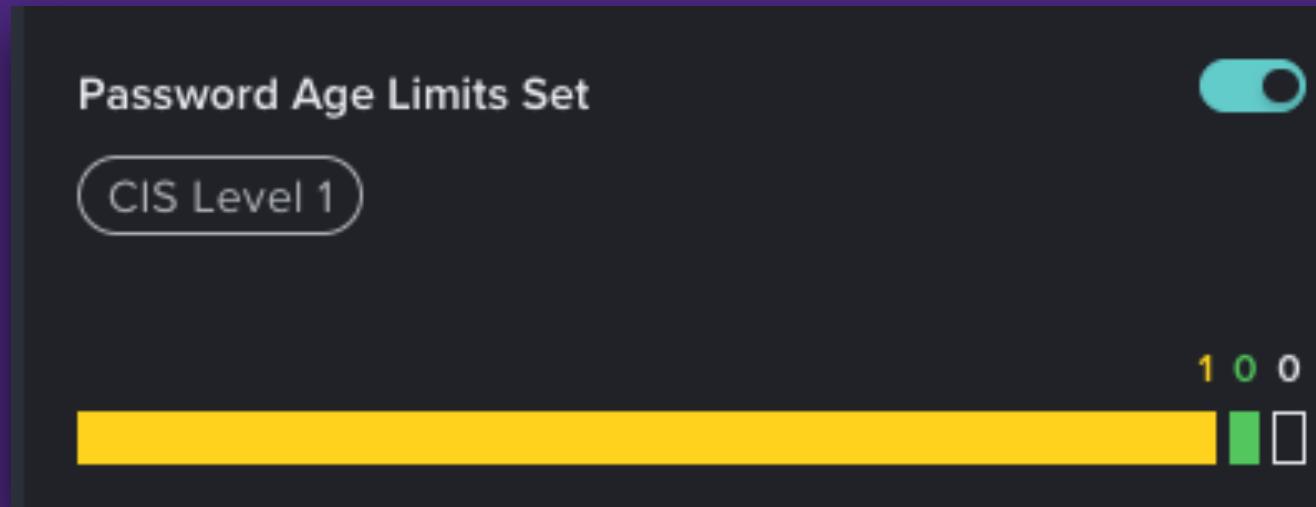


Default collection  
interval once per day



- Manually run: `protectctl checkin -insights`
- Enable or disable what you find important for device compliancy

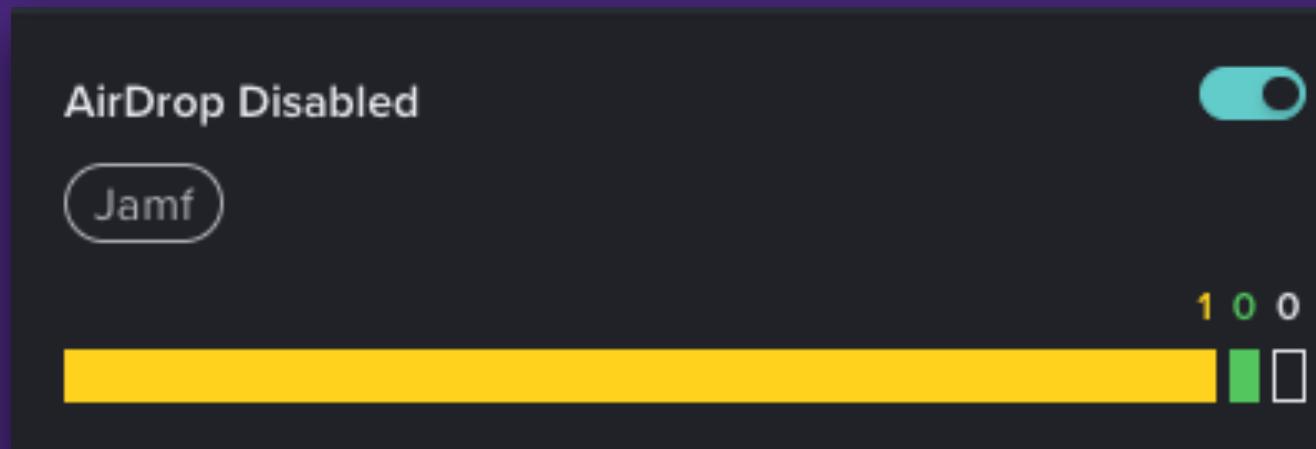
# CIS levels



- **The intent of the Level 1 profile benchmark is to lower the attack surface of your organization while keeping machines usable and not hindering business functionality.**



- **Level 2 profile is considered to be "defense in depth" and is intended for environments where security is paramount.**



- **Created by Jamf what might be important for you but is not part of CIS 1 or 2**

# Analytics

- Made and maintained by Jamf
- Different sensor types
- Understanding how this information is monitored

Type	Owner	Modified	Name	Categories	Actions	Tags
File	✓	08/25/2021 9:02 PM GMT	AoboKeylogger	KnownMalware	Alert	Known Aobo_Keylogger
File	✓	08/25/2021 9:02 PM GMT	AppleJeusMalware	KnownMalware	Alert	Known AppleJeus
File	✓	08/25/2021 9:02 PM GMT	AppLoginItem	Persistence	Log	MITREattack Persistence LoginItems
File	✓	08/25/2021 9:02 PM GMT	BlazingKeylogger	KnownMalware	Alert	Known BlazingKeylogger
File	✓	08/25/2021 9:02 PM GMT	BucaMalware	KnownMalware	Alert	Known Buca
File	✓	08/25/2021 9:02 PM GMT	BundloreAdware	KnownMalware	Alert	Known Bundlore
File	✓	08/25/2021 9:02 PM GMT	CallMeMalware	KnownMalware	Alert	Known CallMe
File	✓	08/25/2021 9:02 PM GMT	CaretoMalware	KnownMalware	Alert	Known Careto
File	✓	08/25/2021 9:02 PM GMT	CodecmAdware	KnownMalware	Alert	Known Codecm
File	✓	08/25/2021 9:02 PM GMT	ConduitMalware	KnownMalware	Alert	Known Conduit
File	✓	08/25/2021 9:02 PM GMT	CronJob	Persistence	Log	MITREattack Persistence LocalJobScheduling
File	✓	08/25/2021 9:02 PM GMT	CustomURLHandlerCreation	Visibility	Log	Visibility
File	✓	08/25/2021 9:02 PM GMT	DevilRobberMalware	KnownMalware	Alert	Known DevilRobber
File	✓	08/25/2021 9:02 PM GMT	DisguisedExecutable	DefenseEvasion	Alert	MITREattack DefenseEvasion Masquerading Tuning
File	✓	08/25/2021 9:02 PM GMT	DNSModification	Visibility	Log	Visibility DNS
File	✓	08/25/2021 9:02 PM GMT	DocksterMalware	KnownMalware	Alert	Known Dockster
File	✓	08/25/2021 9:02 PM GMT	DSStoreDirCreate	DefenseEvasion	Alert	Masquerading DefenseEvasion MITREattack Tuning
File	✓	08/25/2021 9:02 PM GMT	DYLDInsert(App)	Persistence	Log	MITREattack Persistence
File	✓	08/25/2021 9:02 PM GMT	DYLDInsert(LaunchD)	Persistence	Log	MITREattack Persistence
File	✓	08/25/2021 9:02 PM GMT	EarthwormMalware	KnownMalware	Alert	KnownMalware EarthWorm
File	✓	08/25/2021 9:02 PM GMT	EleanorMalware	KnownMalware	Alert	Known Backdoor_MAC_Eleanor
File	✓	08/25/2021 9:02 PM GMT	EliteKeylogger	KnownMalware	Alert	Known EliteKeylogger
File	✓	08/25/2021 9:02 PM GMT	EmPyreMalware	KnownMalware	Alert	Known EmPyre_Agent
File	✓	08/25/2021 9:02 PM GMT	EventMonitor	Persistence	Log	MITREattack Persistence PlistModification
File	✓	08/25/2021 9:02 PM GMT	EvilOSXMalware	KnownMalware	Alert	Known
File	✓	08/25/2021 9:02 PM GMT	FileExtensionBeginsOrEndsWithSpace	Execution	Alert	MITREattack Execution SpaceAfterFilename Tuning
File	✓	08/25/2021 9:02 PM GMT	FlashDownloadNotSignedByAdobe	InitialAccess	Alert	MITREattack InitialAccess Tuning
File	✓	08/25/2021 9:02 PM GMT	GatekeeperBlockedRevoked	Gatekeeper	Alert	Gatekeeper
File	✓	08/25/2021 9:02 PM GMT	GatekeeperBlockedSigned	Gatekeeper	Log	Gatekeeper
File	✓	08/25/2021 9:02 PM GMT	GatekeeperBlockedUnsignedOrUnknown	Gatekeeper	Log	Gatekeeper

# Summary

- **Analytic Description**
- **Analytics Filter**
- **Analytic Actions**
  - Alert/Log
    - SIEM Solution or Jamf Protect
  - Smart Computer Groups
  - Cache
    - Stays on the device and is located in the Console app

Type	Owner	Modified	Name	Categories	Actions	Tags
File	✓	08/25/2021 9:02 PM GMT	AoboKeylogger	KnownMalware	Alert	Known Aobo_Keylogger
File	✓	08/25/2021 9:02 PM GMT	AppleJesusMalware	KnownMalware	Alert	Known AppleJesus
File	✓	08/25/2021 9:02 PM GMT	AppLoginItem	Persistence	Log	MITREattack Persistence LoginItems
File	✓	08/25/2021 9:02 PM GMT	BlazingKeylogger	KnownMalware	Alert	Known BlazingKeylogger
File	✓	08/25/2021 9:02 PM GMT	BucaMalware	KnownMalware	Alert	Known Buca
File	✓	08/25/2021 9:02 PM GMT	BundloreAdware	KnownMalware	Alert	Known Bundlore
File	✓	08/25/2021 9:02 PM GMT	CallMeMalware	KnownMalware	Alert	Known CallMe
File	✓	08/25/2021 9:02 PM GMT	CaretoMalware	KnownMalware	Alert	Known Careto
File	✓	08/25/2021 9:02 PM GMT	CodecmAdware	KnownMalware	Alert	Known CodecM
File	✓	08/25/2021 9:02 PM GMT	ConduitMalware	KnownMalware	Alert	Known Conduit
File	✓	08/25/2021 9:02 PM GMT	CronJob	Persistence	Log	MITREattack Persistence LocalJobScheduling
File	✓	08/25/2021 9:02 PM GMT	CustomURLHandlerCreation	Visibility	Log	Visibility
File	✓	08/25/2021 9:02 PM GMT	DevilRobberMalware	KnownMalware	Alert	Known DevilRobber
File	✓	08/25/2021 9:02 PM GMT	DisguisedExecutable	DefenseEvasion	Alert	MITREattack DefenseEvasion Masquerading Tuning
File	✓	08/25/2021 9:02 PM GMT	DNSModification	Visibility	Log	Visibility DNS
File	✓	08/25/2021 9:02 PM GMT	DocksterMalware	KnownMalware	Alert	Known Dockster
File	✓	08/25/2021 9:02 PM GMT	DSStoreDirCreate	DefenseEvasion	Alert	Masquerading DefenseEvasion MITREattack Tuning
File	✓	08/25/2021 9:02 PM GMT	DYLDInsert(App)	Persistence	Log	MITREattack Persistence
File	✓	08/25/2021 9:02 PM GMT	DYLDInsert(LaunchD)	Persistence	Log	MITREattack Persistence
File	✓	08/25/2021 9:02 PM GMT	EarthwormMalware	KnownMalware	Alert	KnownMalware EarthWorm
File	✓	08/25/2021 9:02 PM GMT	EleanorMalware	KnownMalware	Alert	Known Backdoor_MAC_Eleanor
File	✓	08/25/2021 9:02 PM GMT	EliteKeylogger	KnownMalware	Alert	Known EliteKeylogger
File	✓	08/25/2021 9:02 PM GMT	EmPyreMalware	KnownMalware	Alert	Known EmPyre_Agent
File	✓	08/25/2021 9:02 PM GMT	EventMonitor	Persistence	Log	MITREattack Persistence PlistModification
File	✓	08/25/2021 9:02 PM GMT	EvilOSXMalware	KnownMalware	Alert	Known
File	✓	08/25/2021 9:02 PM GMT	getExtensionBeginsOrEndsWithSpace	Execution	Alert	MITREattack Execution SpaceAfterFilename Tuning
File	✓	08/25/2021 9:02 PM GMT	FlashDownloadNotSignedByAdobe	InitialAccess	Alert	MITREattack InitialAccess Tuning
File	✓	08/25/2021 9:02 PM GMT	GatekeeperBlockedRevoked	Gatekeeper	Alert	Gatekeeper
File	✓	08/25/2021 9:02 PM GMT	GatekeeperBlockedSigned	Gatekeeper	Log	Gatekeeper
File	✓	08/25/2021 9:02 PM GMT	GatekeeperBlockedUnsignedOrUnknown	Gatekeeper	Log	Gatekeeper

# Sensor Types

Type	Owner	Modified	Name
File		08/25/2021 9:02 PM GMT	AoboKeylogger
File		08/25/2021 9:02 PM GMT	AppleJesusMalware
File		08/25/2021 9:02 PM GMT	AppLoginItem
File		08/25/2021 9:02 PM GMT	BlazingKeylogger
File		08/25/2021 9:02 PM GMT	BucaMalware
File		08/25/2021 9:02 PM GMT	BundloreAdware
File		08/25/2021 9:02 PM GMT	CallMeMalware
File		08/25/2021 9:02 PM GMT	CaretoMalware
File		08/25/2021 9:02 PM GMT	CodecmAdware
File		08/25/2021 9:02 PM GMT	ConduitMalware
File		08/25/2021 9:02 PM GMT	CronJob
File		08/25/2021 9:02 PM GMT	CustomURLHandlerCreation
File		08/25/2021 9:02 PM GMT	DevilRobberMalware
File		08/25/2021 9:02 PM GMT	DisguisedExecutable
File		08/25/2021 9:02 PM GMT	DNSModification
File		08/25/2021 9:02 PM GMT	DocksterMalware
File		08/25/2021 9:02 PM GMT	DSStoreDirCreate
File		08/25/2021 9:02 PM GMT	DYLDInsert(App)
File		08/25/2021 9:02 PM GMT	DYLDInsert(LaunchD)
File		08/25/2021 9:02 PM GMT	EarthwormMalware
File		08/25/2021 9:02 PM GMT	EleanorMalware
File		08/25/2021 9:02 PM GMT	EliteKeylogger
File		08/25/2021 9:02 PM GMT	EmPyreMalware
File		08/25/2021 9:02 PM GMT	EventMonitor
File		08/25/2021 9:02 PM GMT	EvilOSXMalware
File		08/25/2021 9:02 PM GMT	FileExtensionBeginsOrEndsWithSpace
File		08/25/2021 9:02 PM GMT	FlashDownloadNotSignedByAdobe
File		08/25/2021 9:02 PM GMT	GatekeeperBlockedRevoked
File		08/25/2021 9:02 PM GMT	GatekeeperBlockedSigned
File		08/25/2021 9:02 PM GMT	GatekeeperBlockedUnsignedOrUnknown

-  • **Screenshot Events (GPScreenshotEvent)**

— Monitors a user's screenshot activity on computers, the path of the resulting screenshot, and the file metadata associated with the screenshot.

-  • **Download Events (GPDownloadEvents)**

— Monitors files downloaded from the internet.

-  • **USB Events (GPUSBEEvent)**

— Monitors USB devices inserted into computers.



- **Malware Removal Tool (MRT) Events**
  - Monitors actions and logs from MRT, Apple's built-in application responsible for removing targeted files from macOS.



- **Gatekeeper Events**—  
Monitors actions and logs from Gatekeeper, Apple's built-in feature for enforcing code signing and verifying downloaded apps before opening them.



- **Keylog Register Events**
  - Monitors for new "event tap" registrations via the Core Graphics framework on macOS. Core Graphic event taps are often used by certain types of keylogging and accessibility software.



- **Synthetic Click Events (GPSyntheticClickEvent)**
  - Monitors programmatic mouse clicks used to dismiss notifications, approve actions, or interact with user prompts.



- **Process Events (GPProcessEvent)**
  - Monitors processes that are launched or terminated on computers.



- **File Events (GPFSEvent)**
  - Monitors files that are written, edited, or deleted from computers or mounted volumes.

# Thank you for listening!