Under the hood of the Jamf Protect Agent

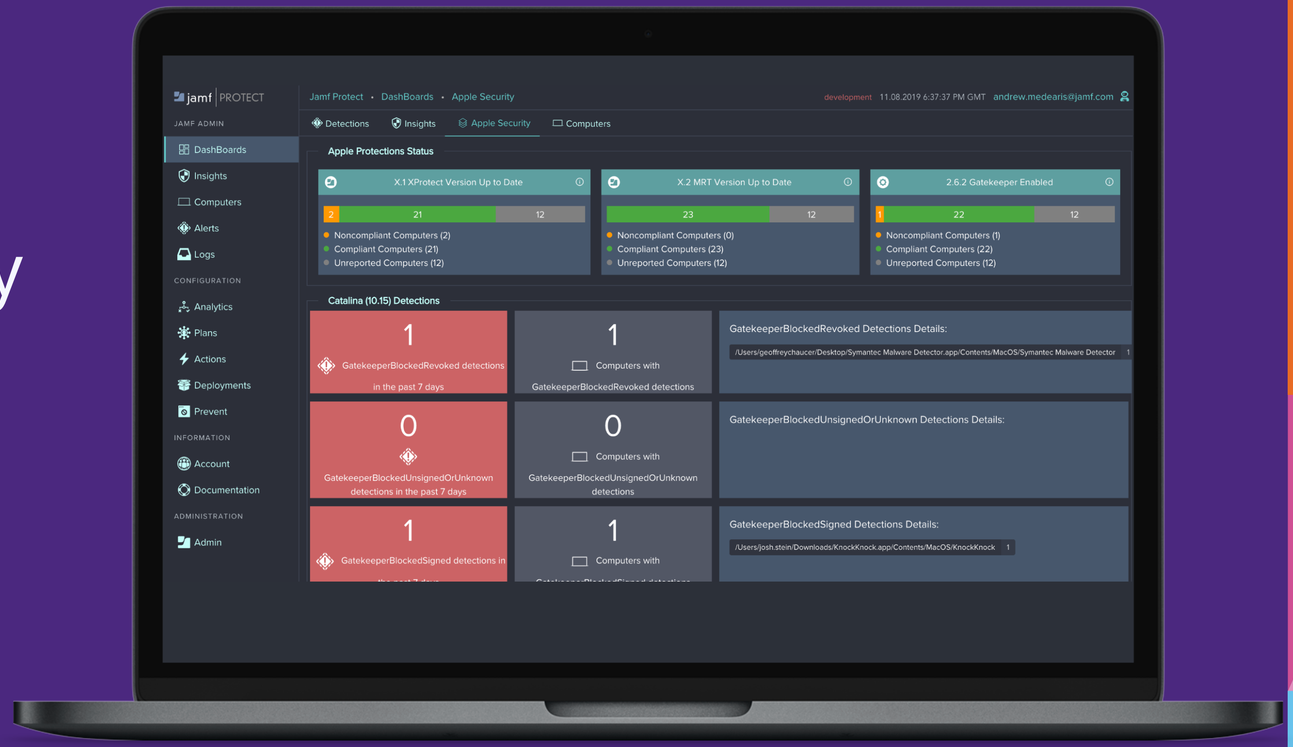
Matteo Bolognini

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

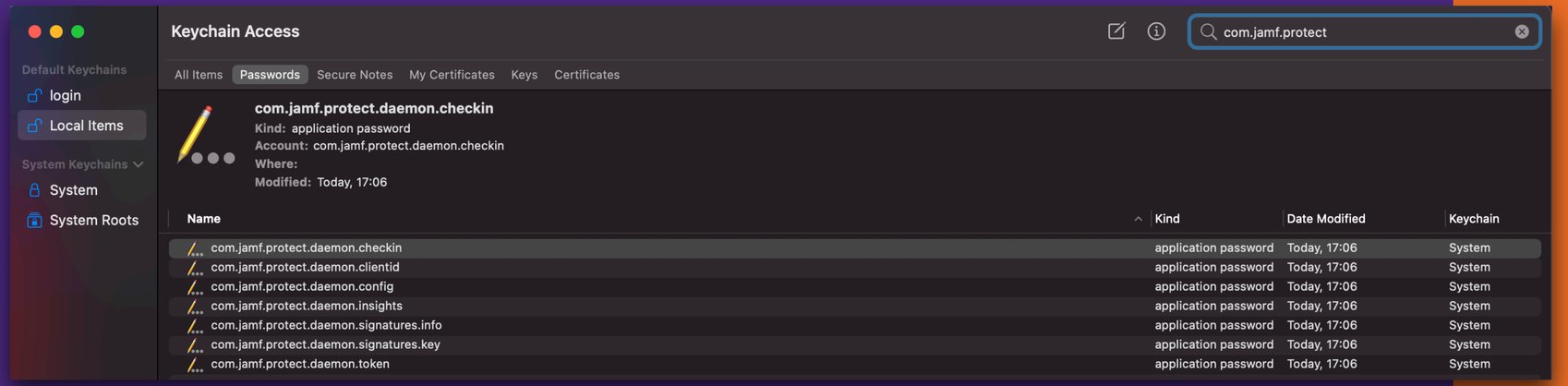
Monitor real-time event-driven activity

macOS 10.13 - 10.15 with System Extension

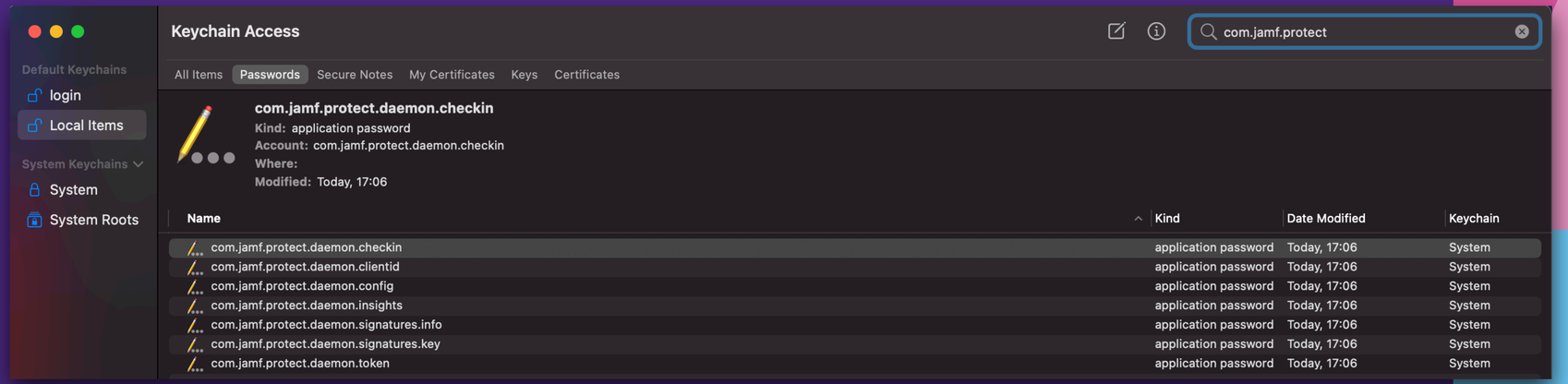
Jamf Protect Keychain Items

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

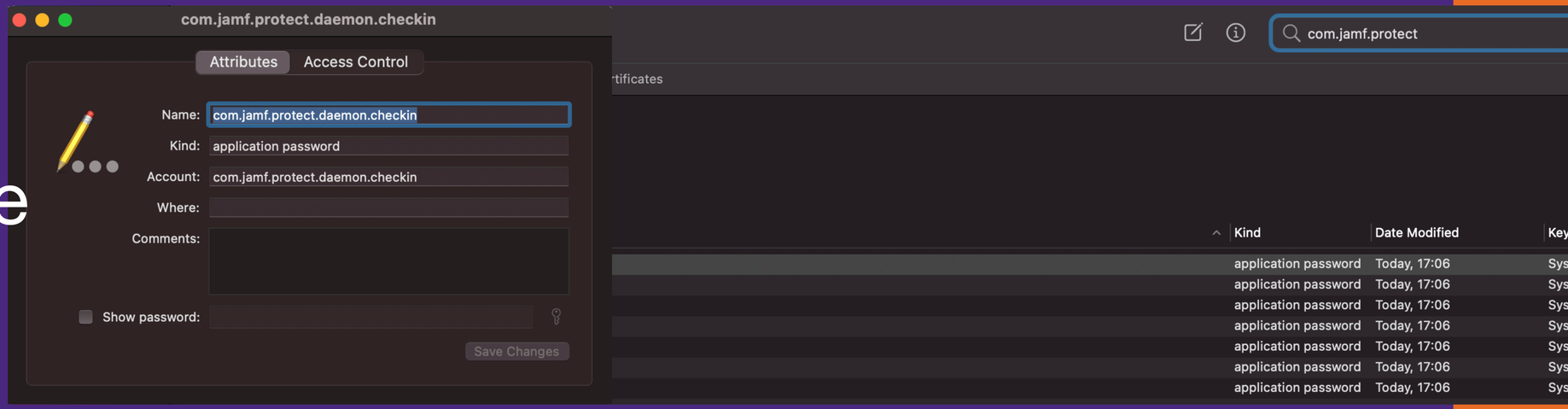
Last check-in time of the agent



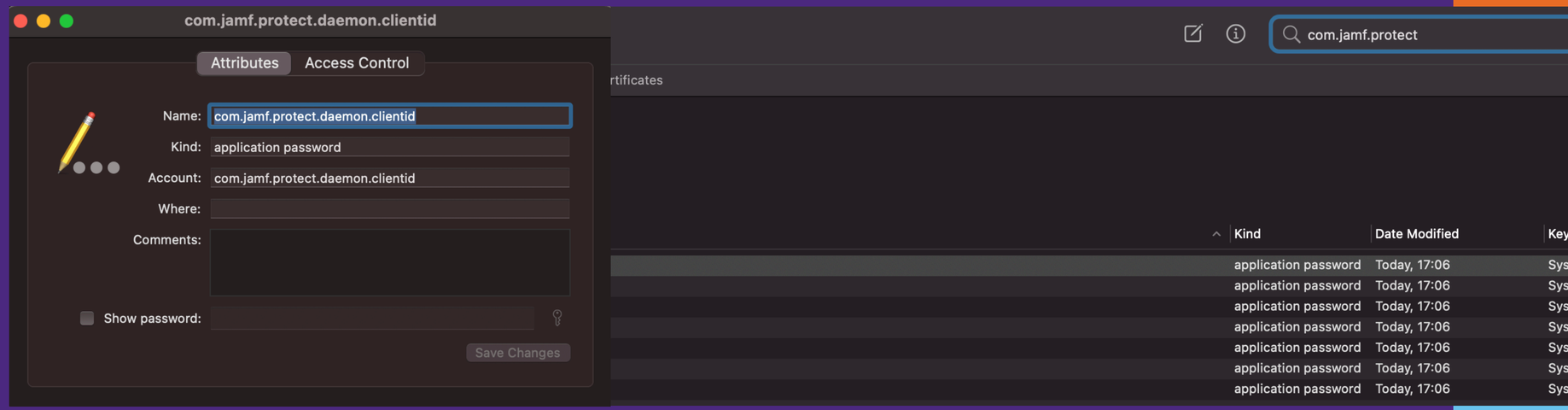
ClientID of the agent



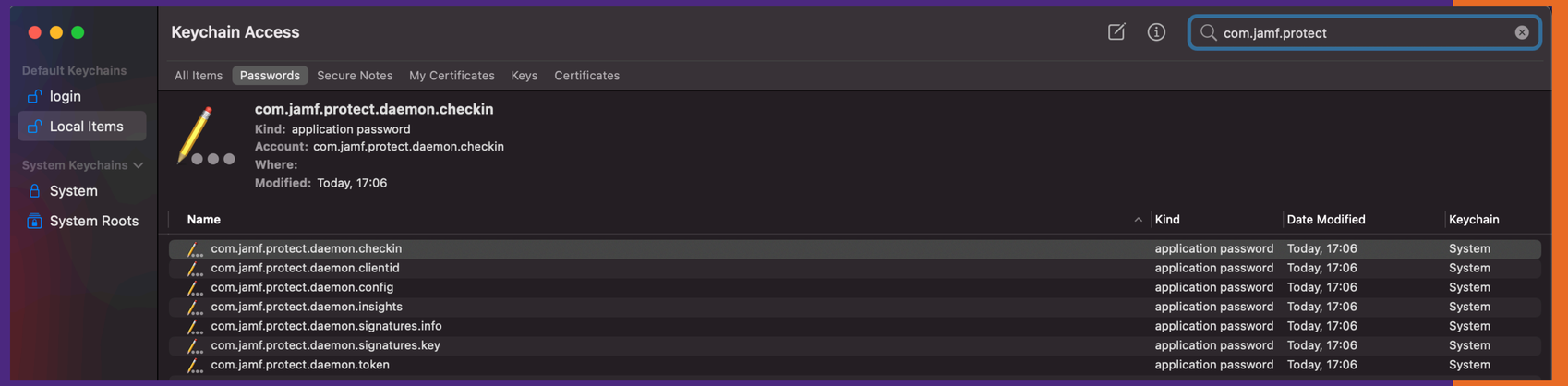
Last check-in time of the agent



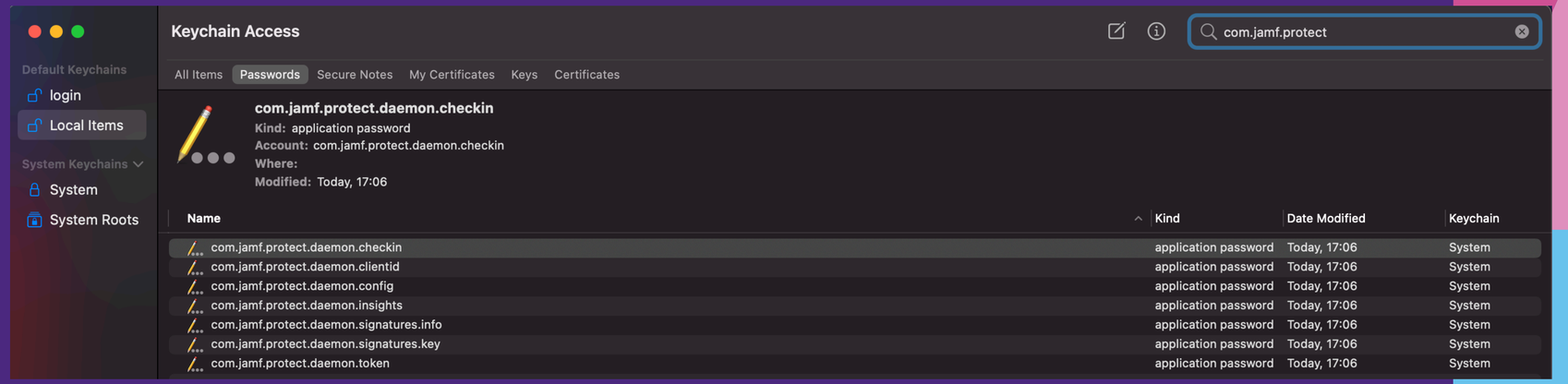
ClientID of the agent



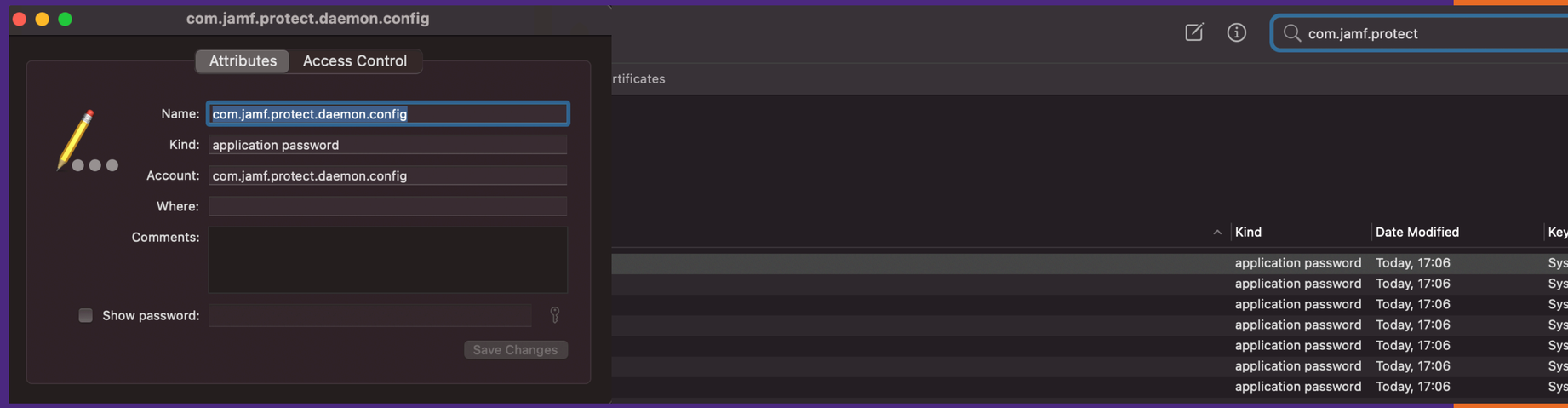
Configuration of the agent



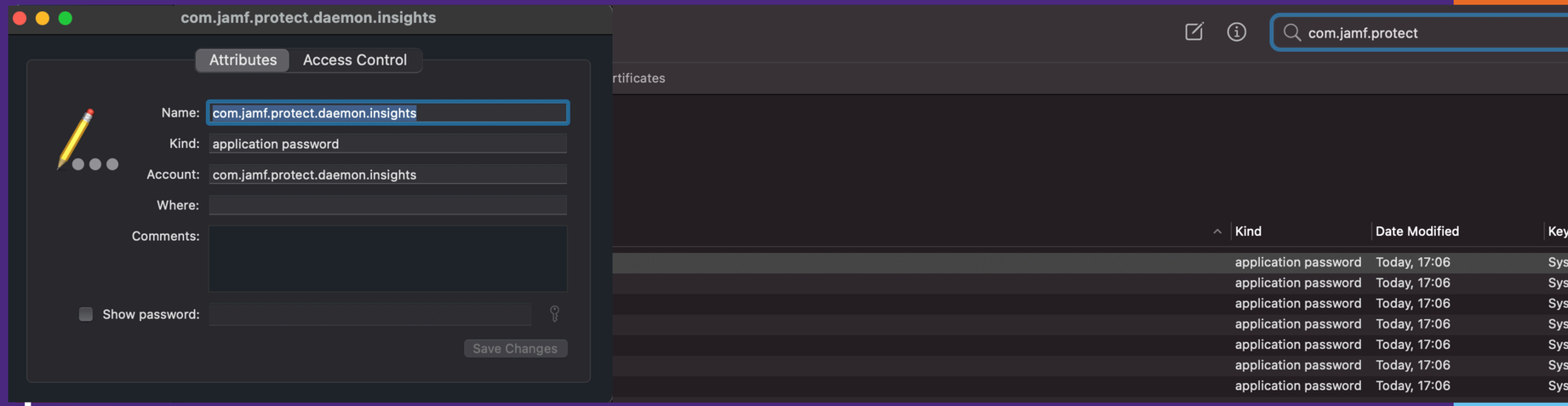
The last Insights time of the agent

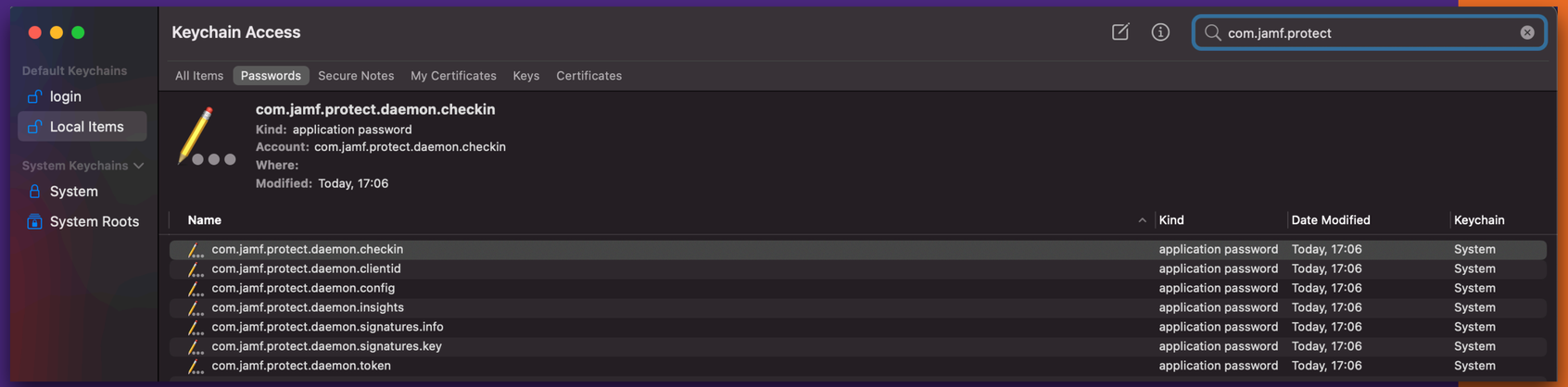


Configuration of the agent

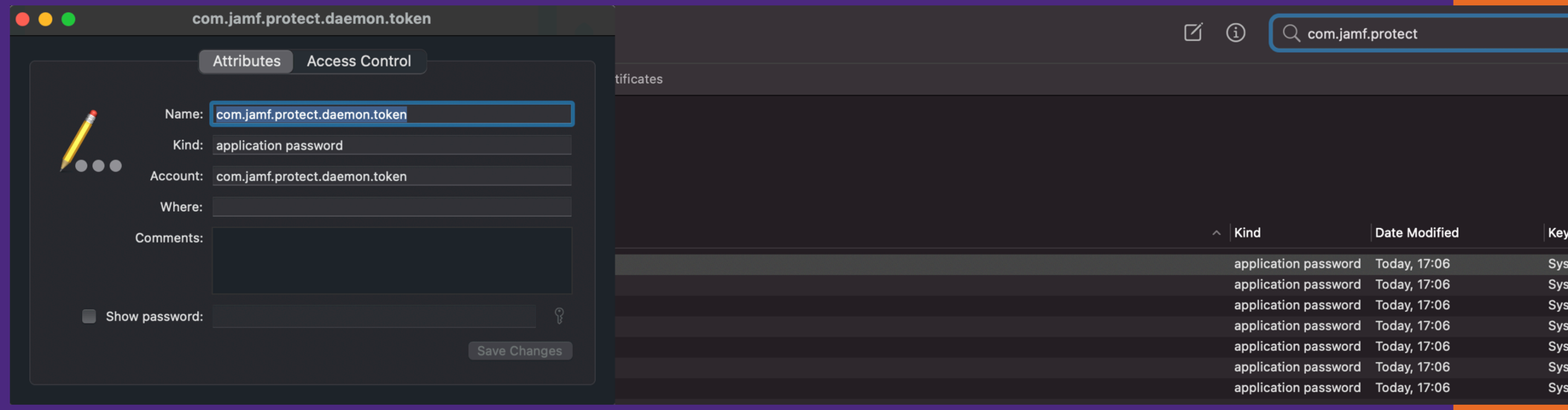


The last Insights time of the agent

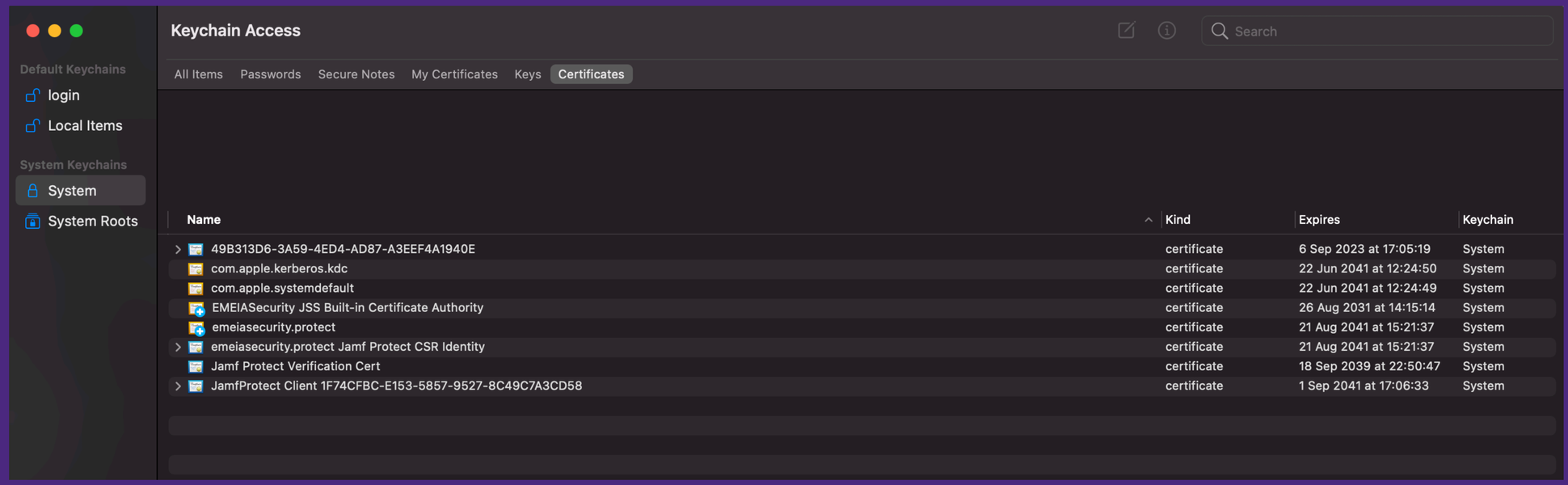




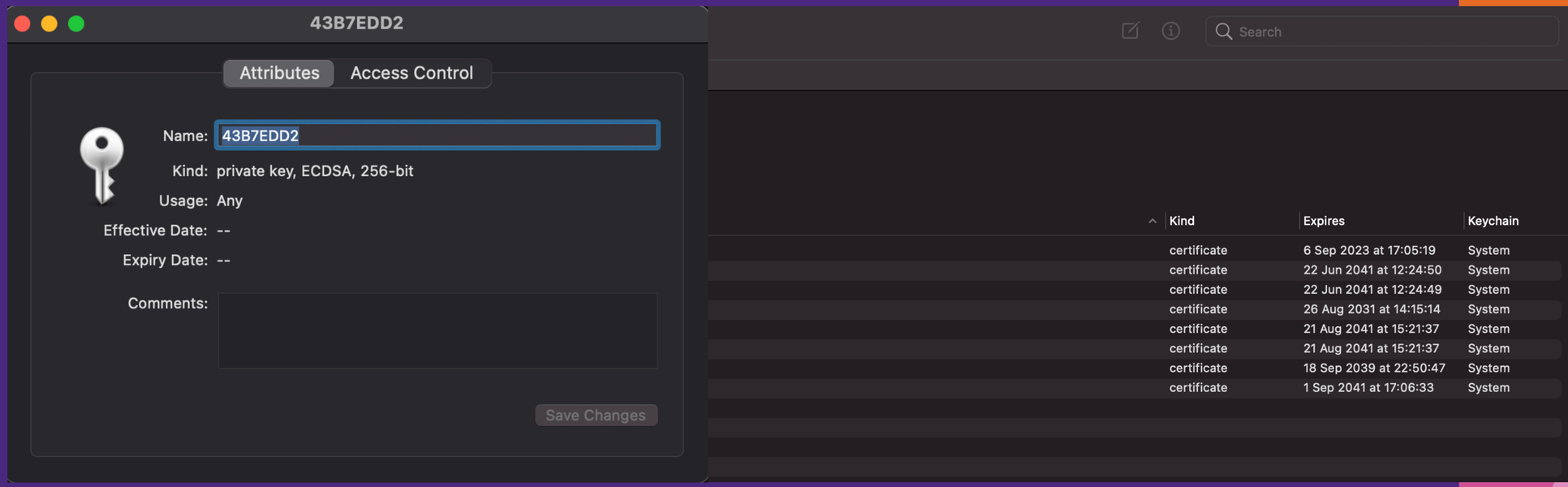
Bootstrap information for initial communication and configuration



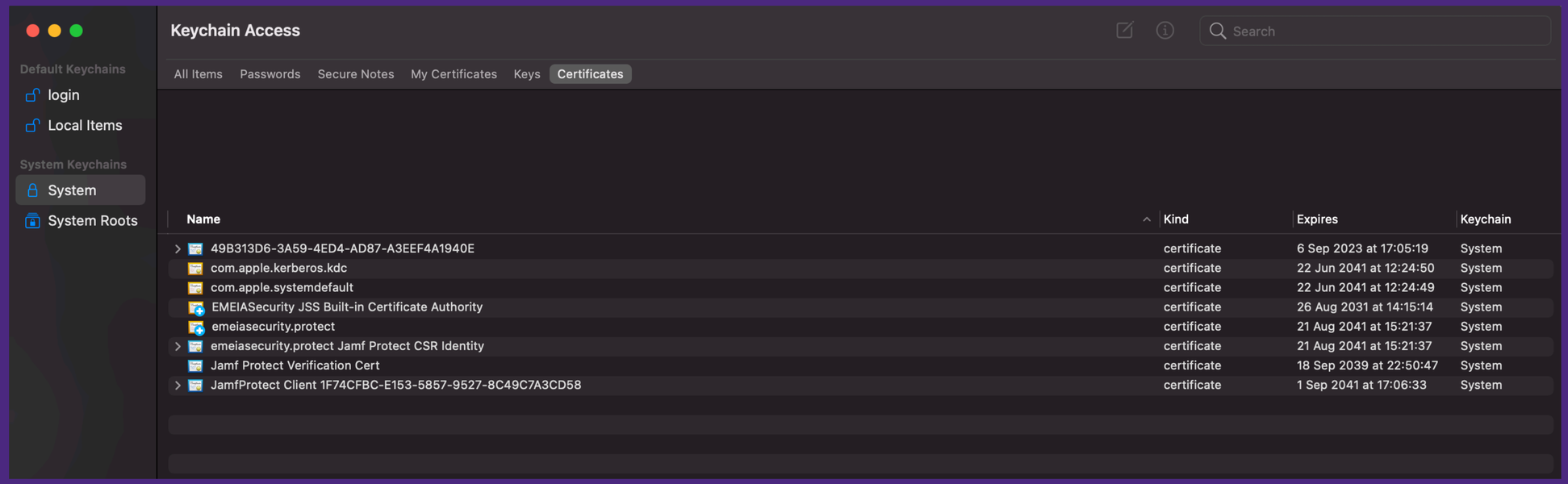
Bootstrap information for initial communication and configuration



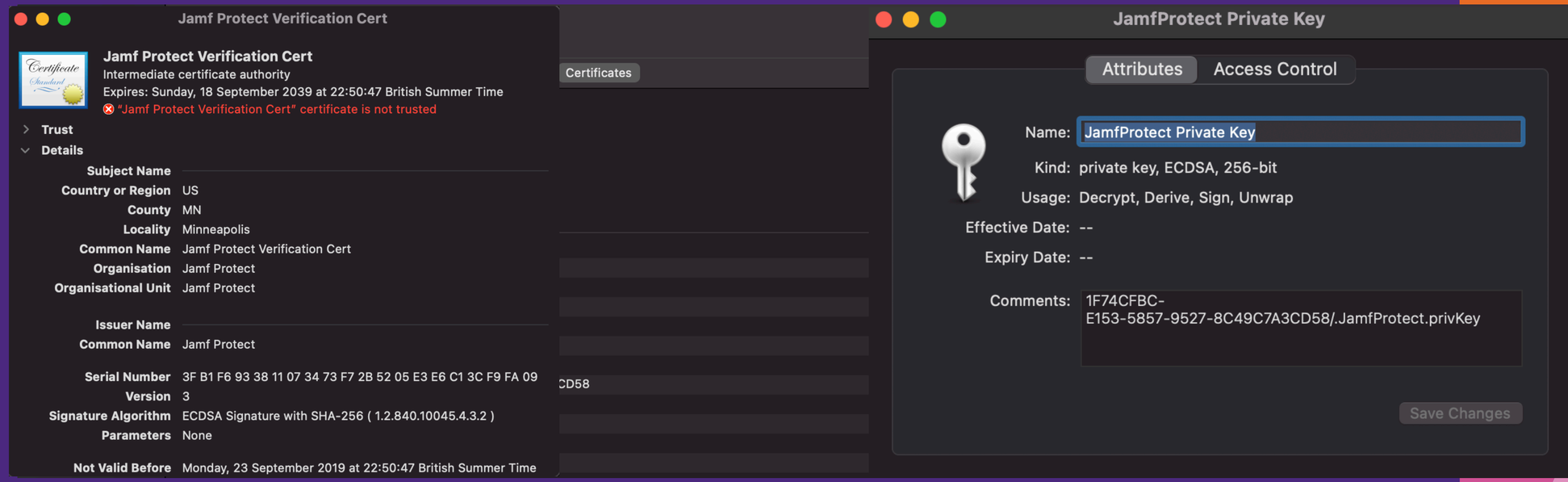
Jamf Protect Public Key



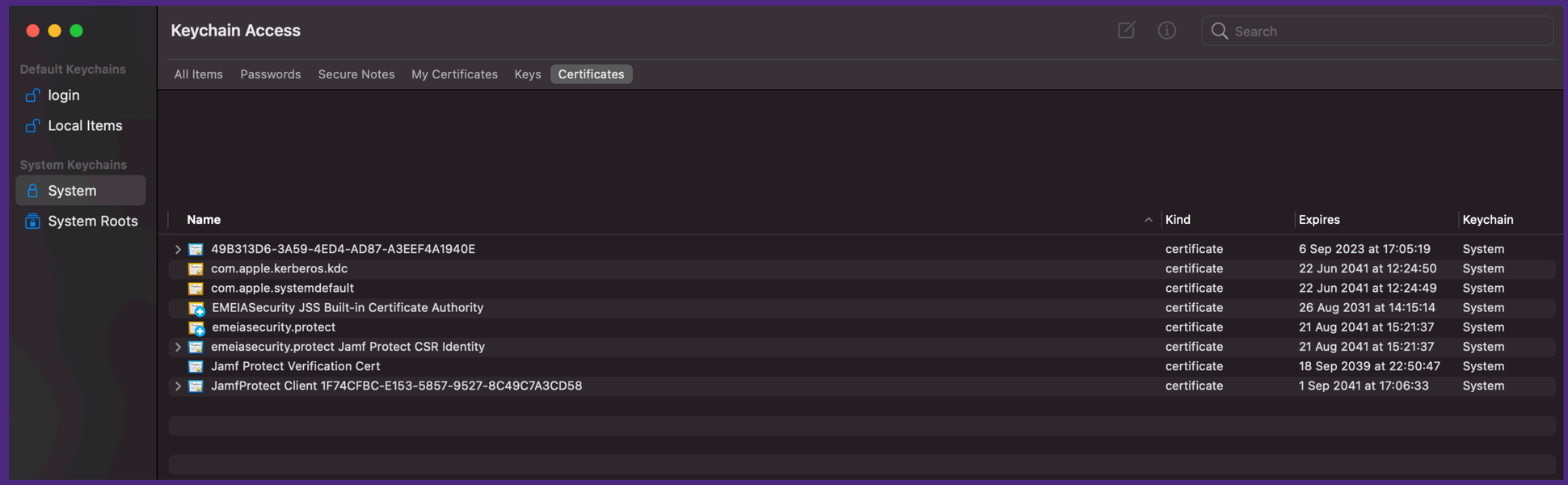
Jamf Protect Public Key



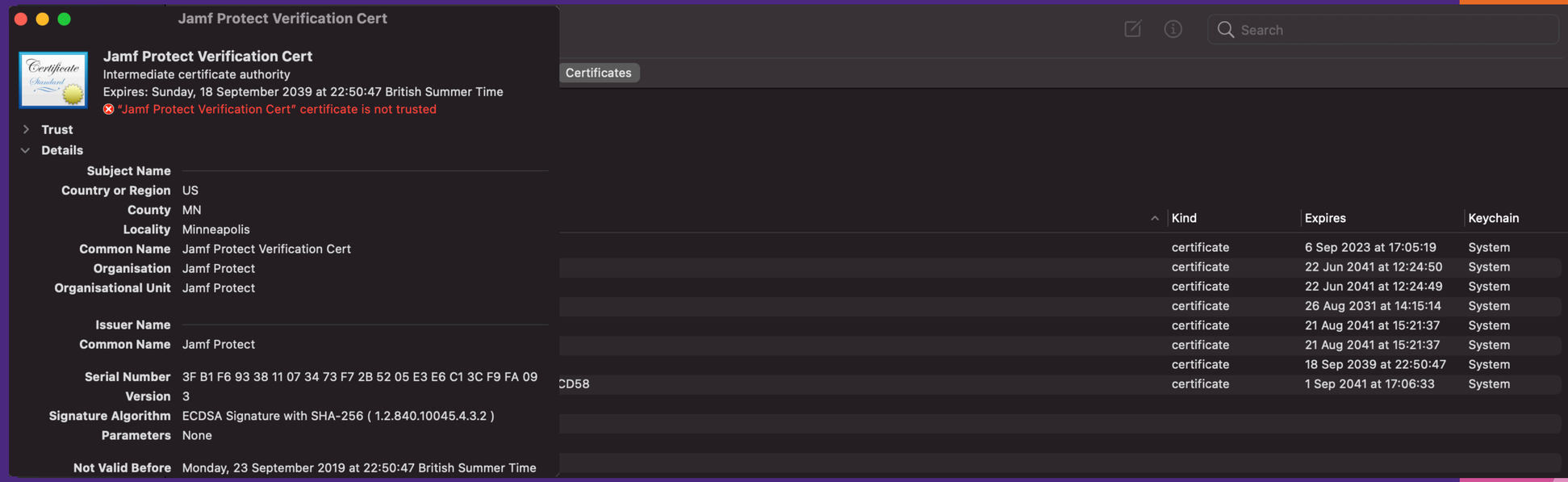
JamfProtect client certificate (JamfProtect Client <UUID>) Jamf Protect Private Key



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

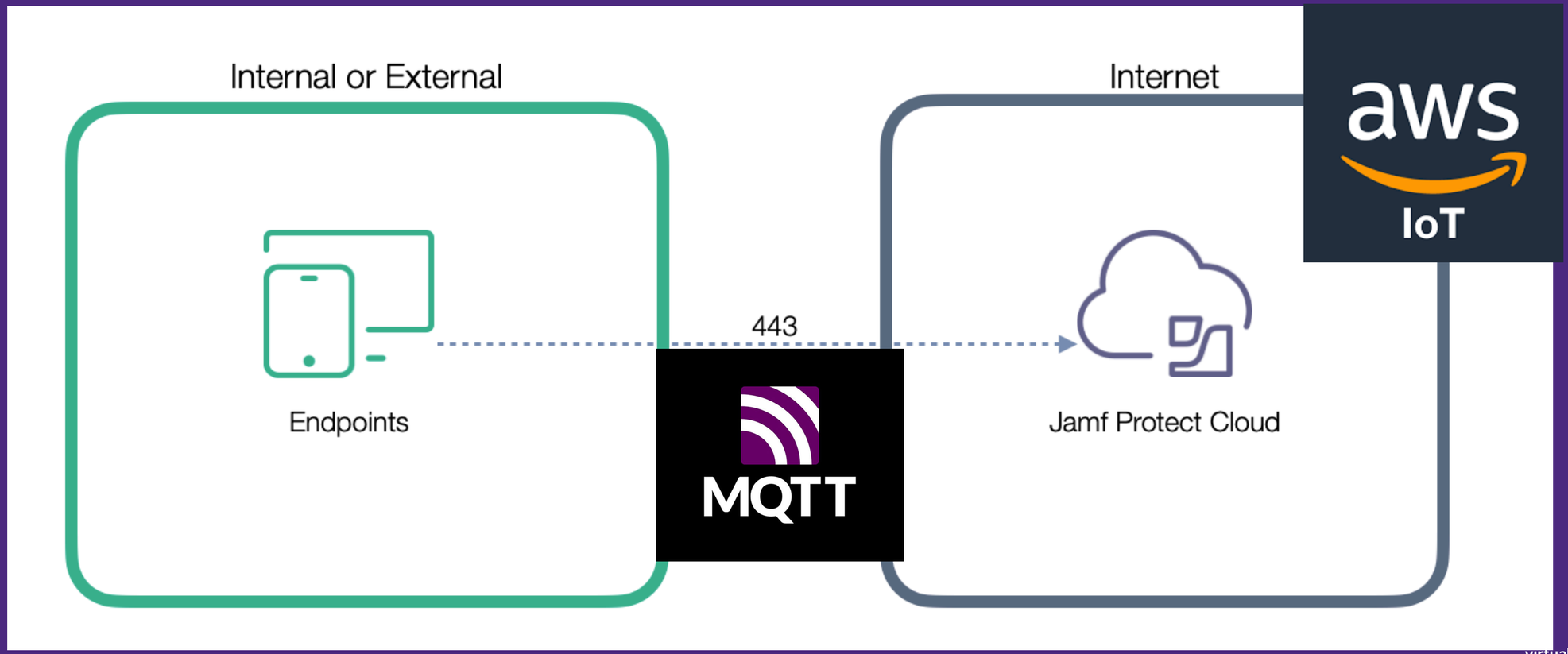
Authentication

Network protocols

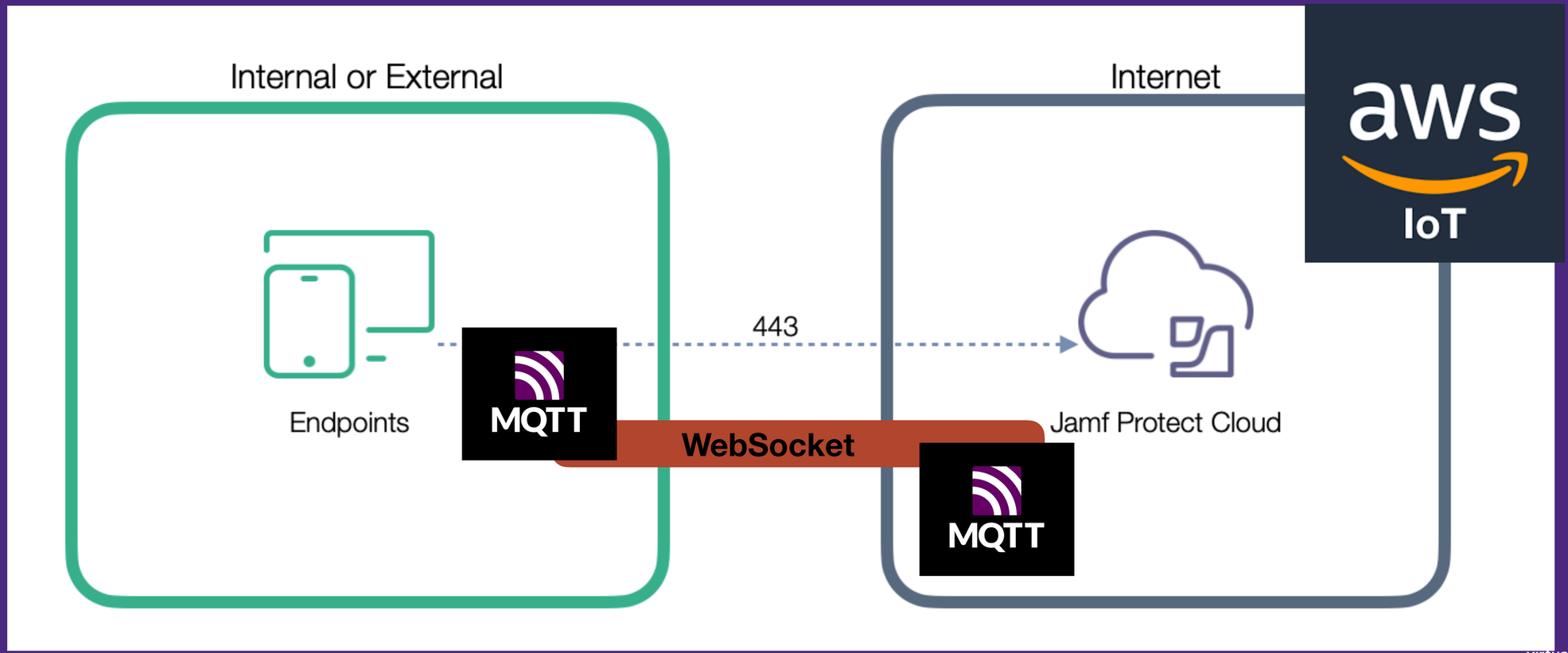
MQTT

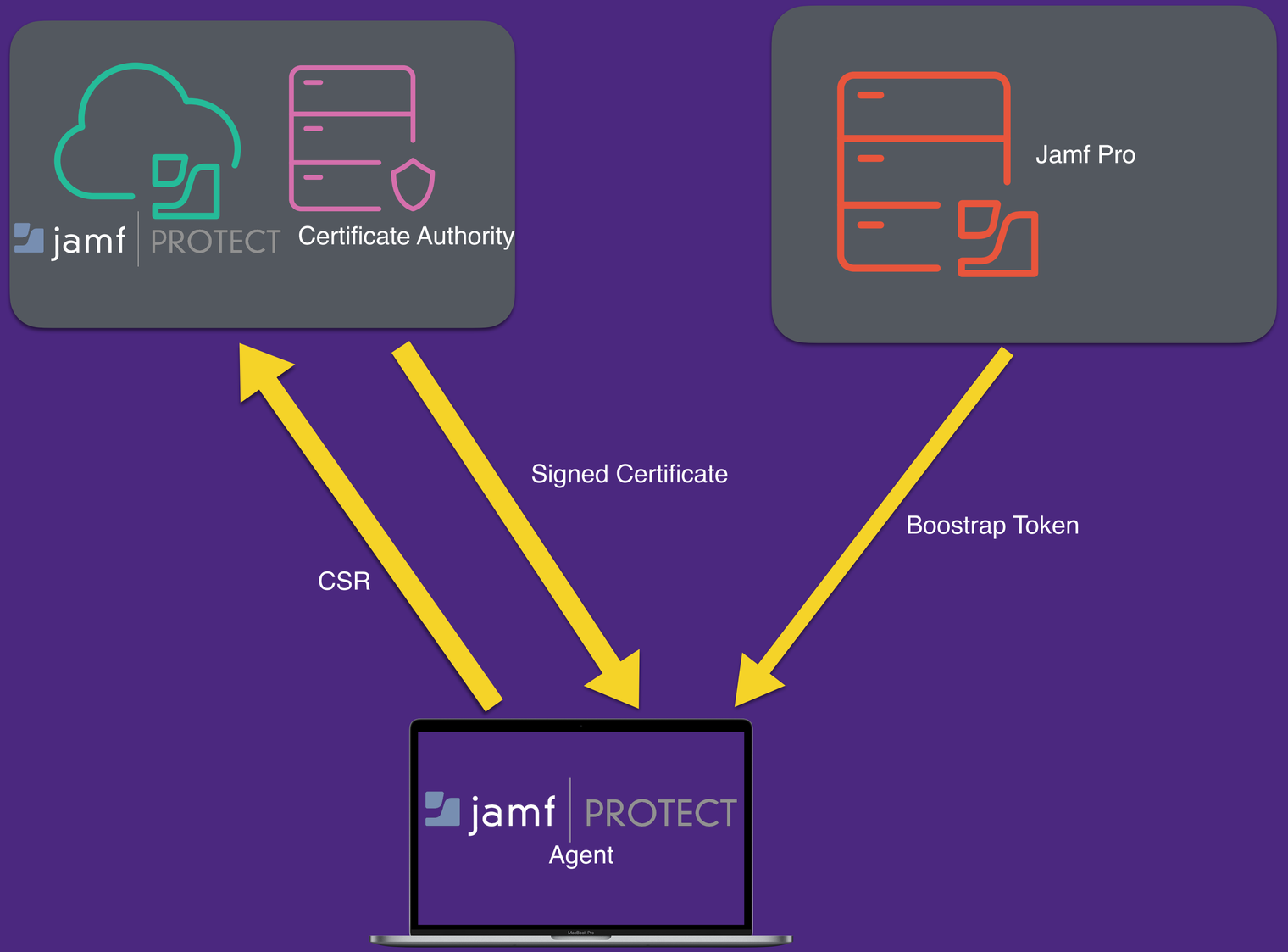
WebSocket

Network Communications

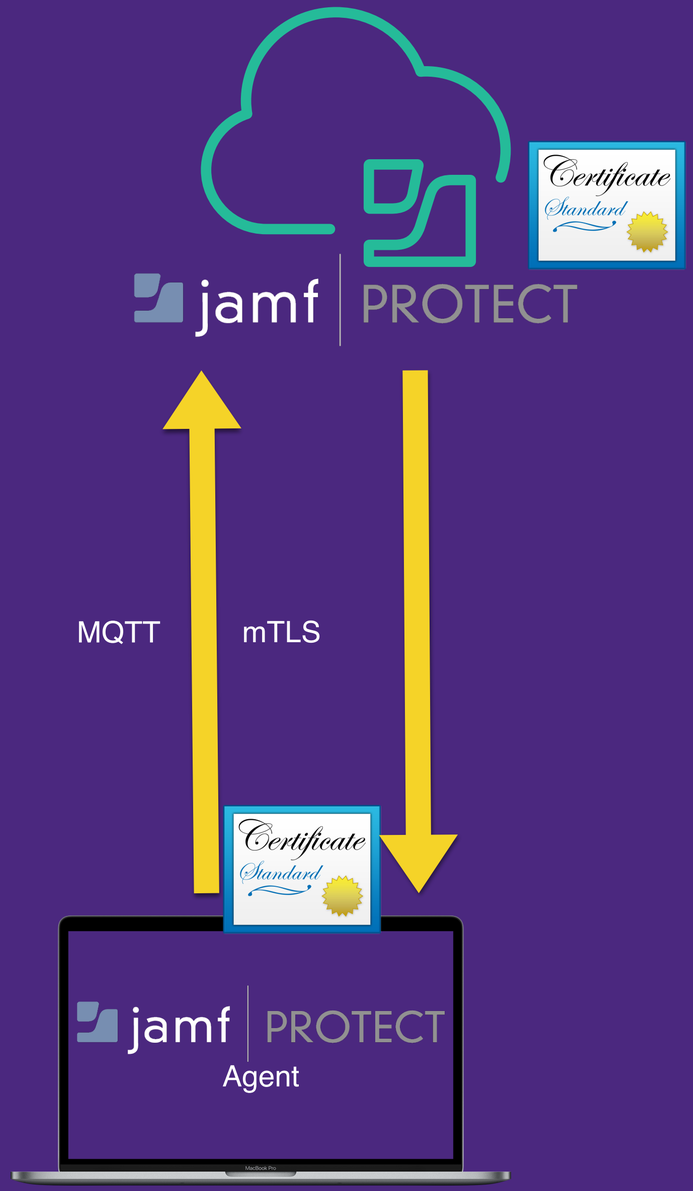


Network Communications

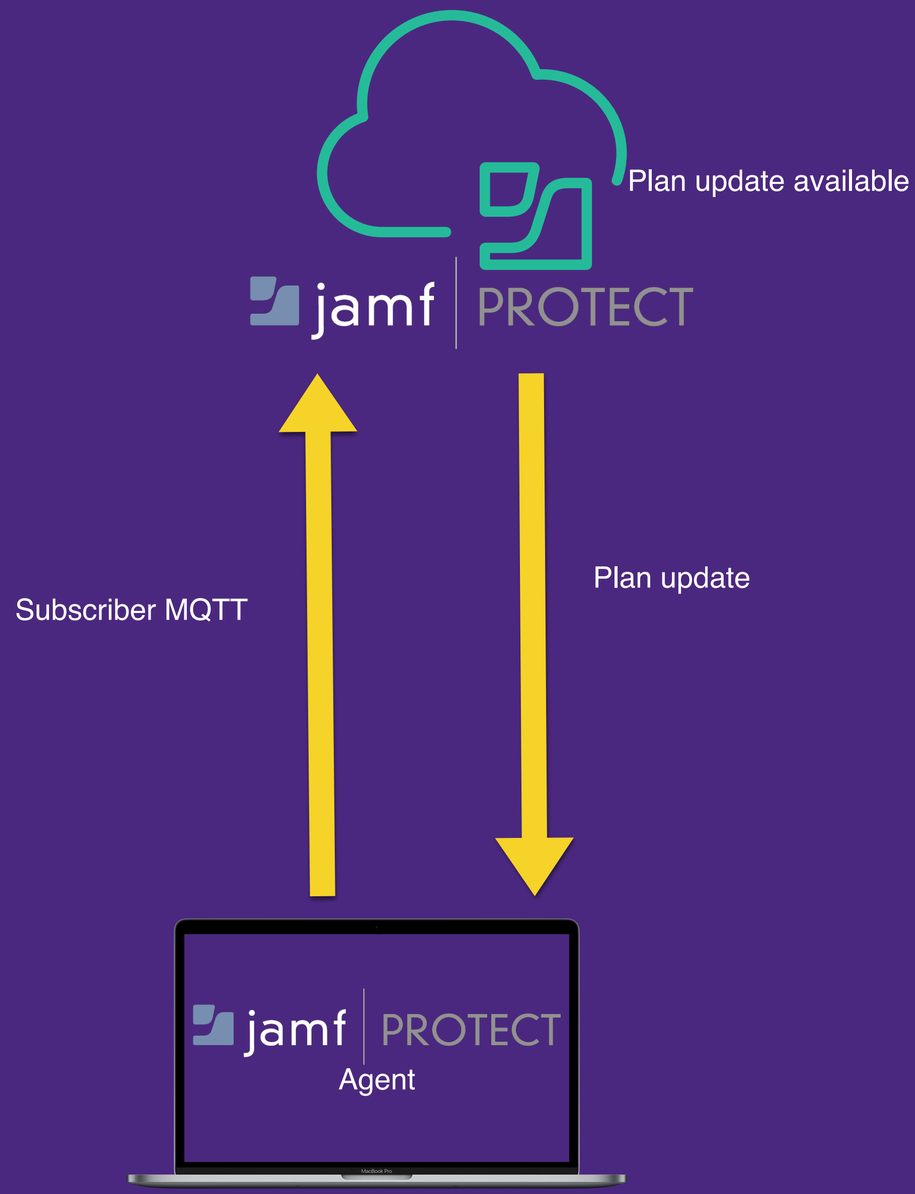




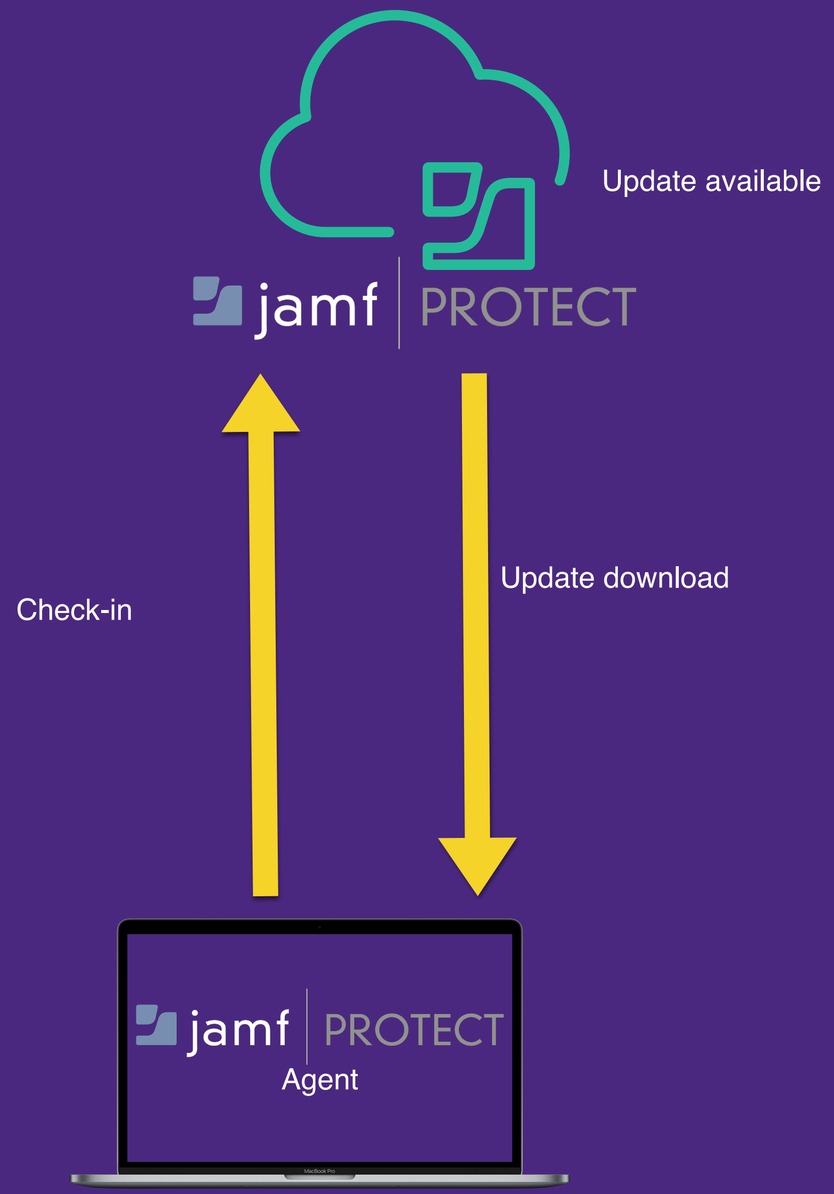
Authentication



Plan update



Agent update

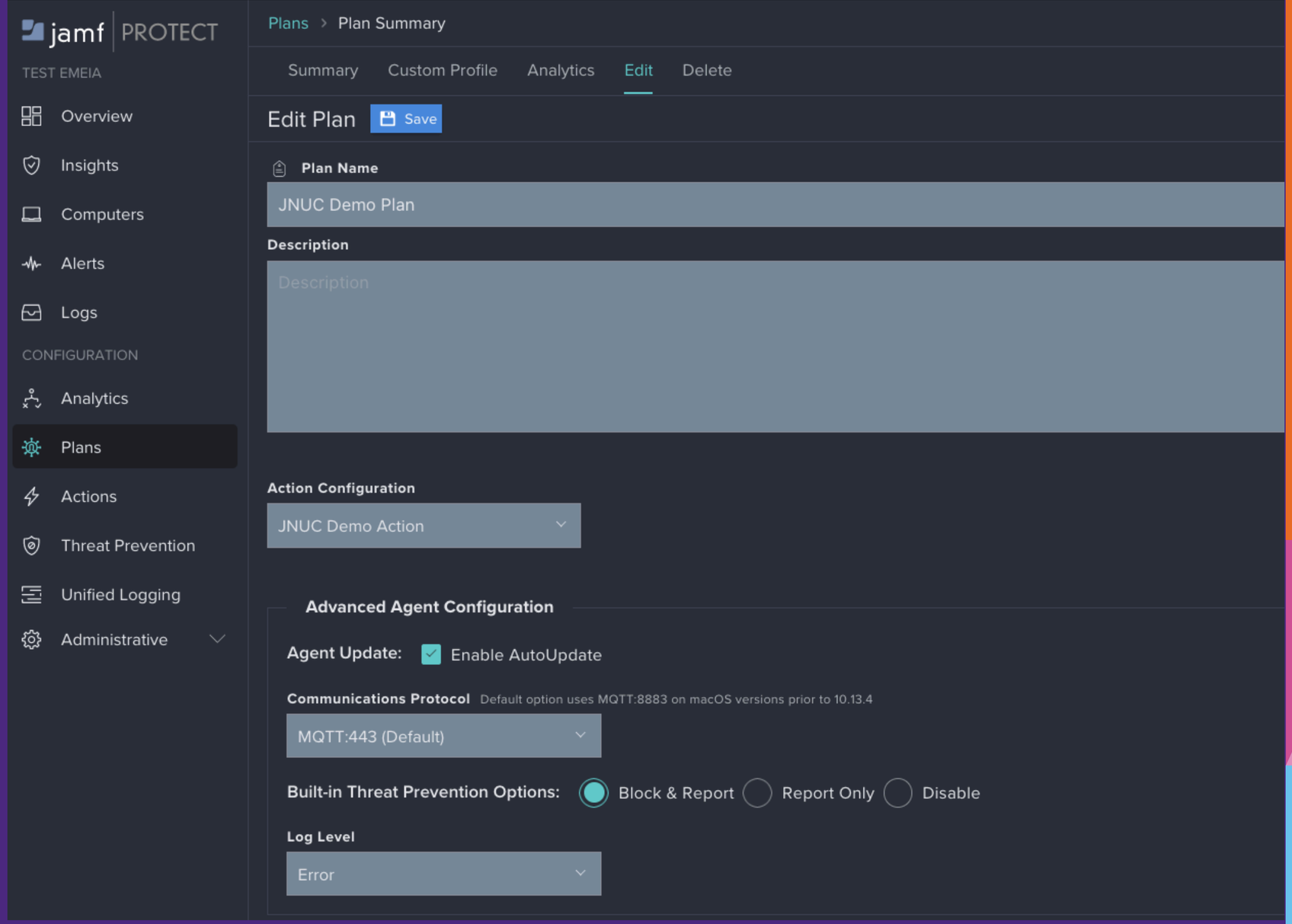


Jamf Protect Plans

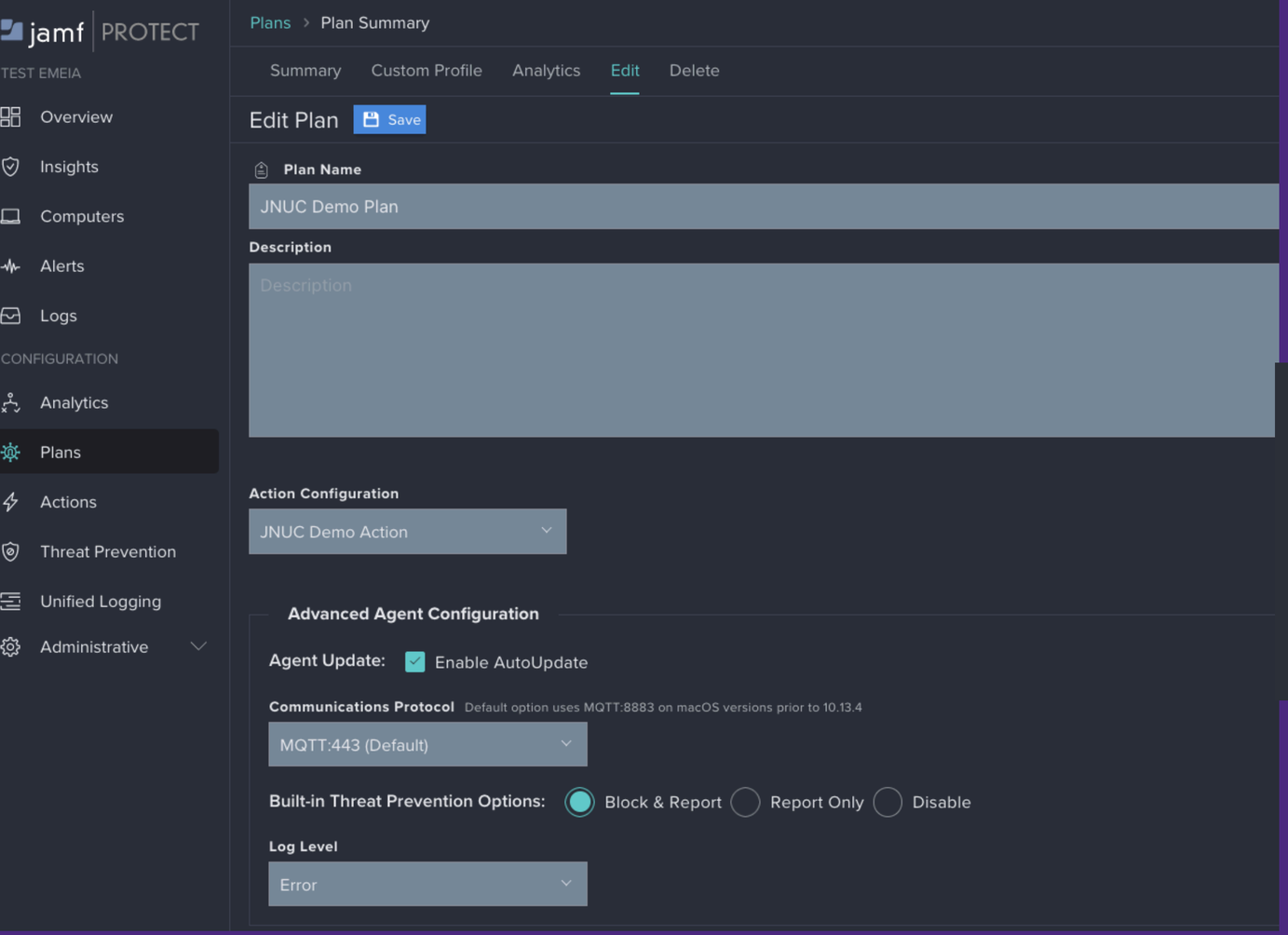
Configuration Profiles

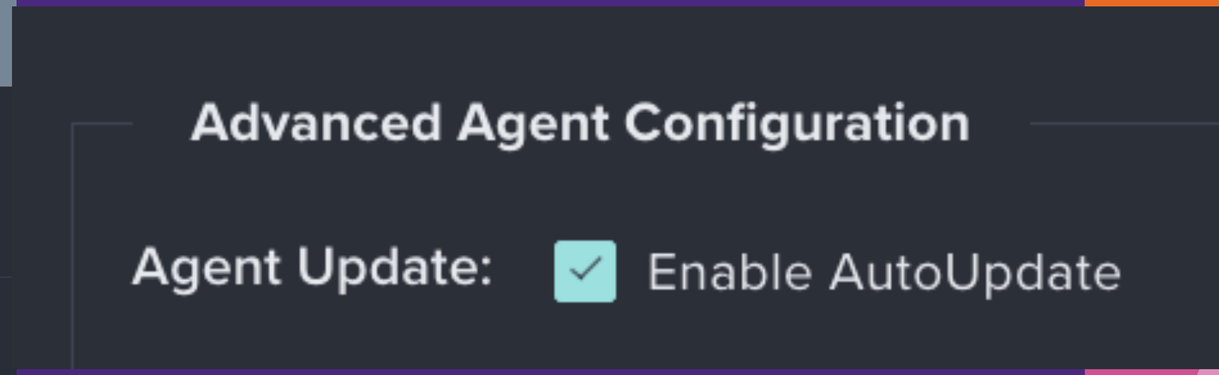
Set of Analytics paired with Actions

Agent Auto-Update



virtual JNUC 2021

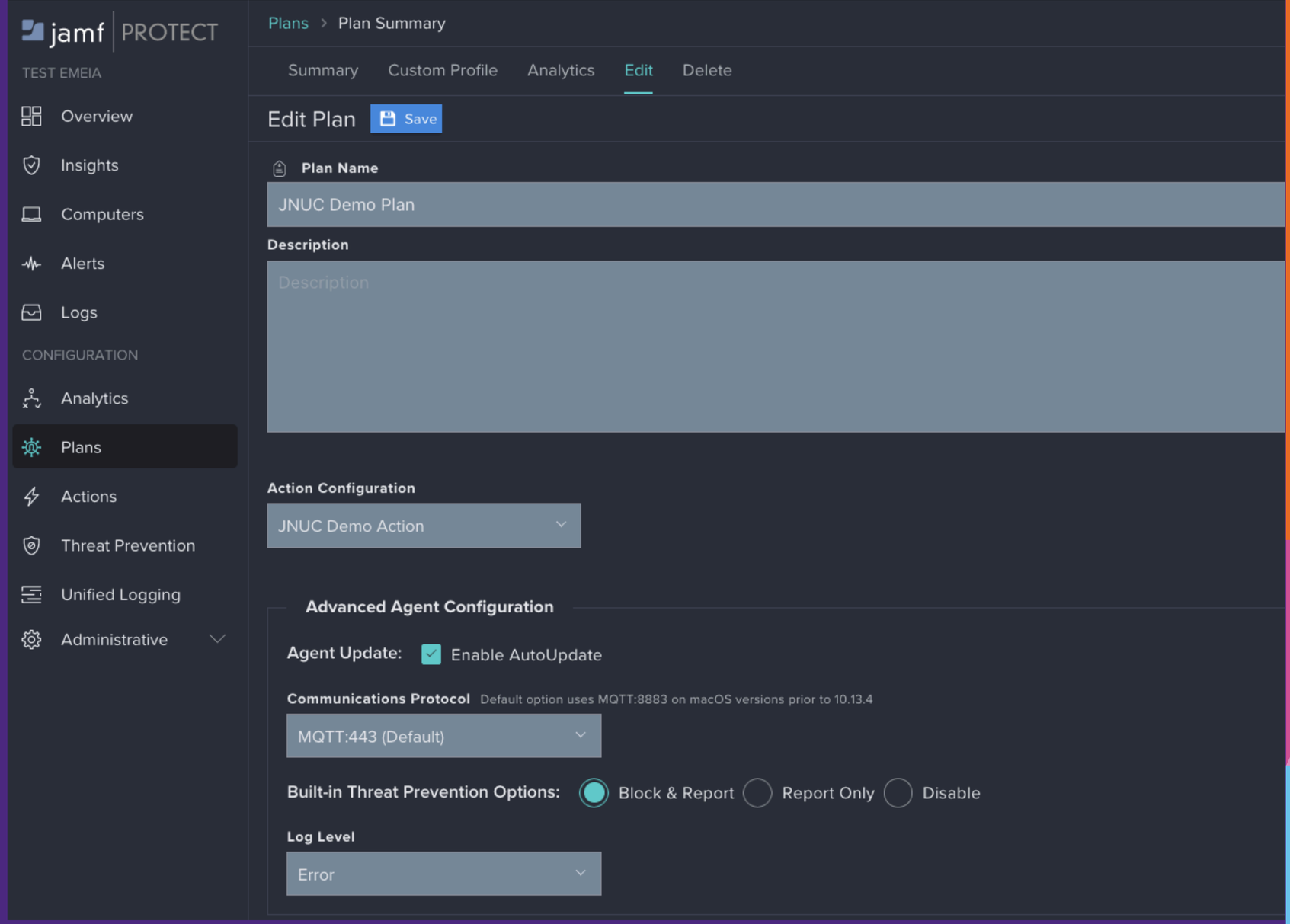


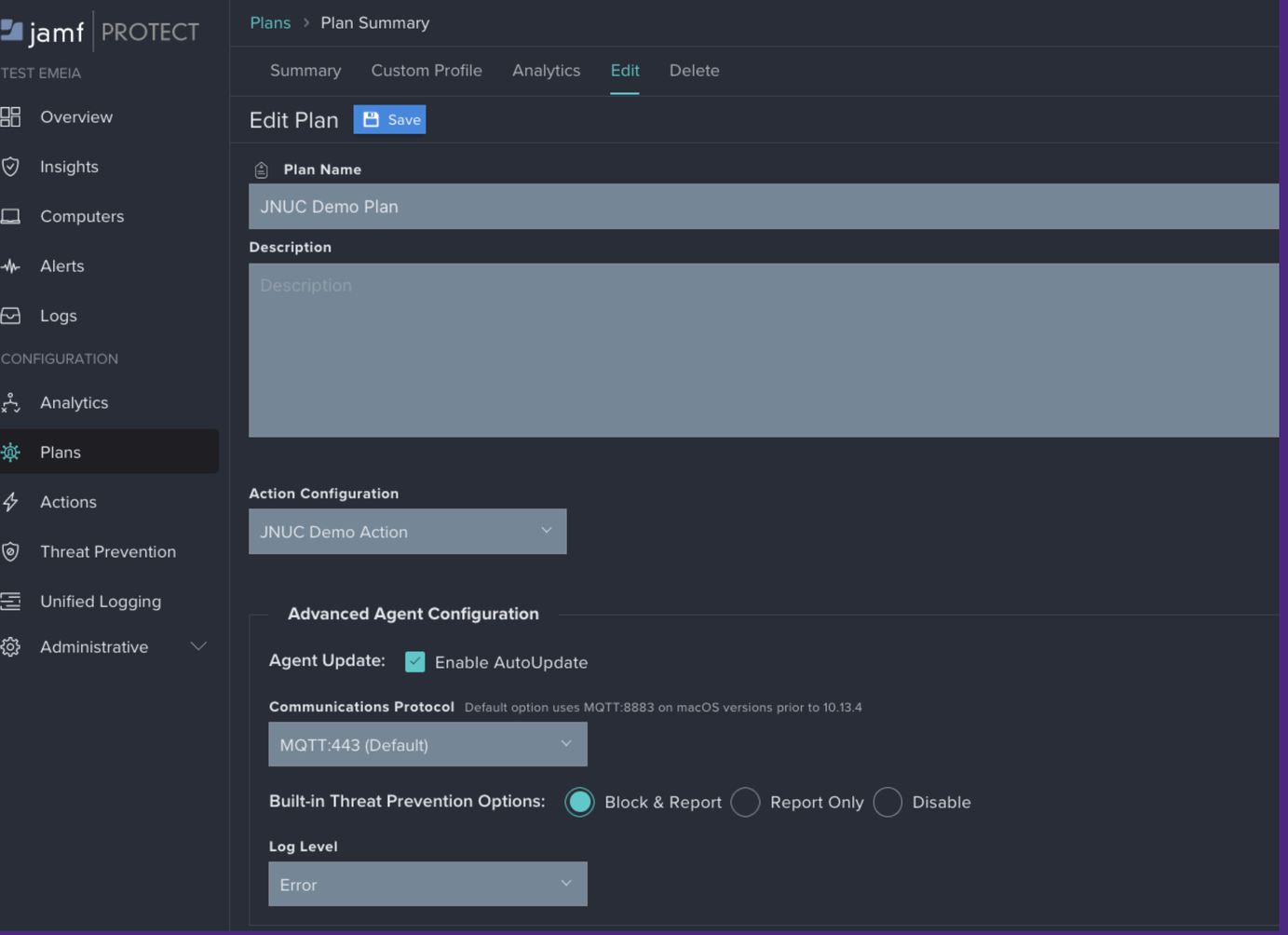


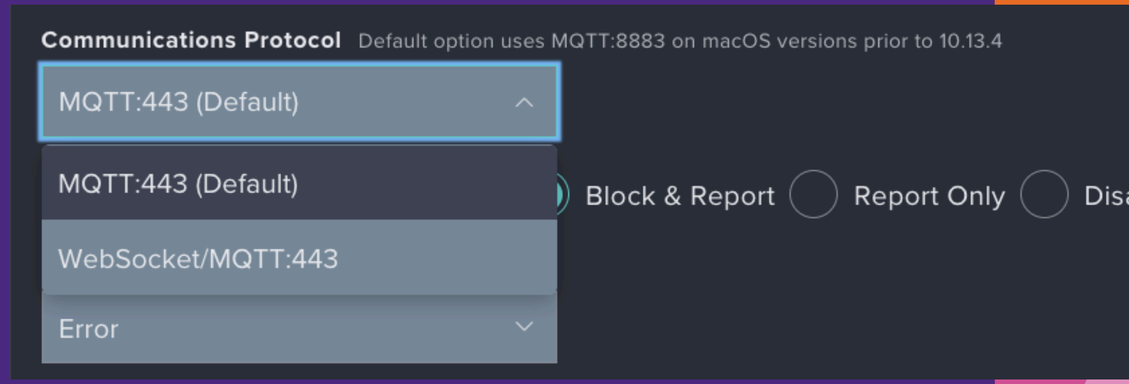
Agent Auto-Update

virtual JNUC 2021

Agent protocol



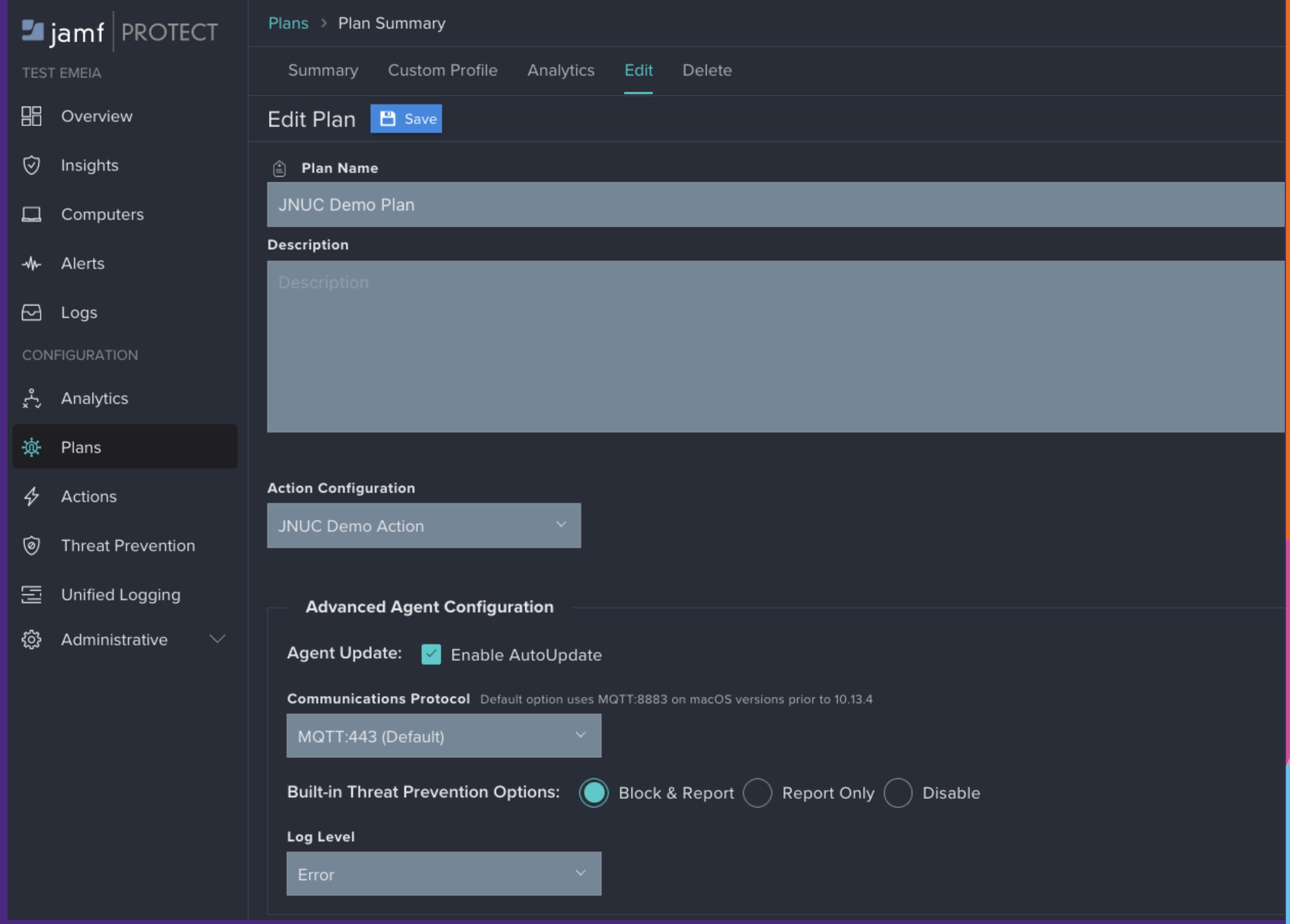




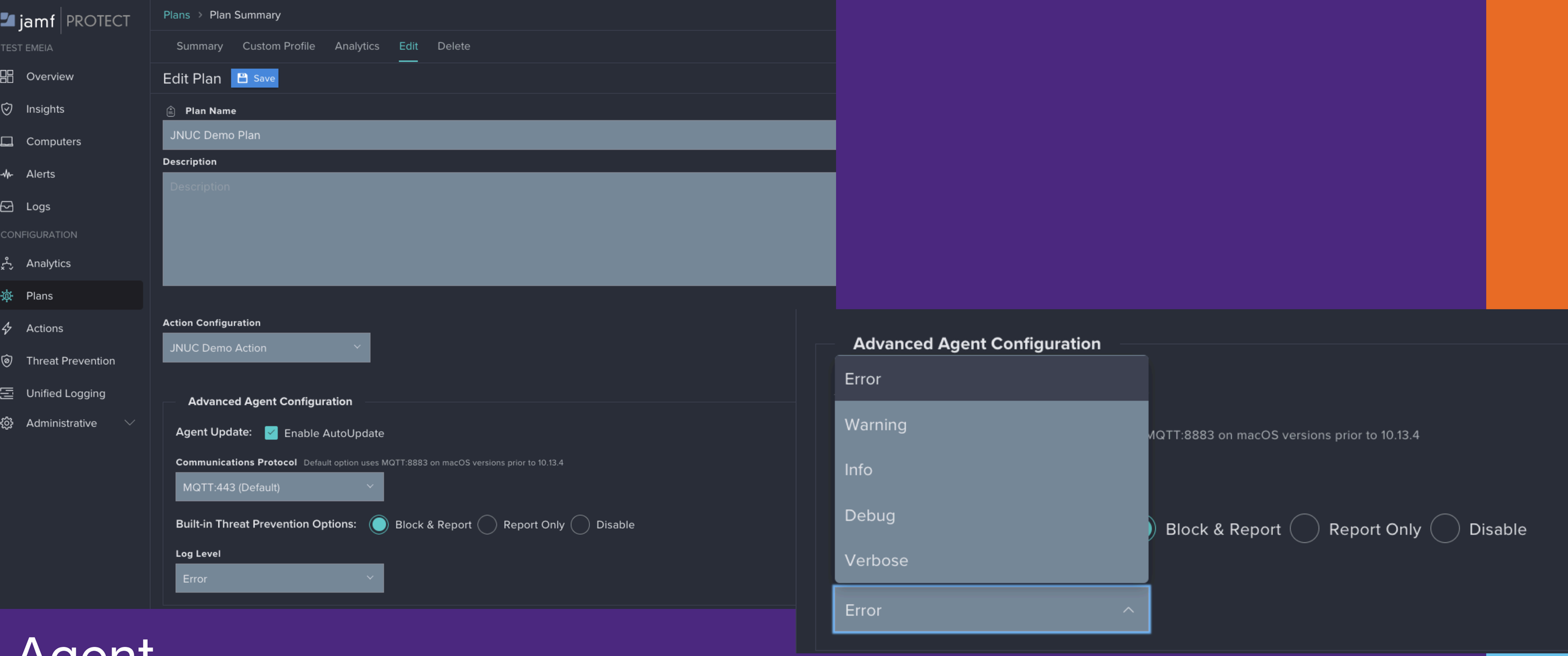
Agent protocol

virtual JNUC 2021

Agent
Log Verbosity



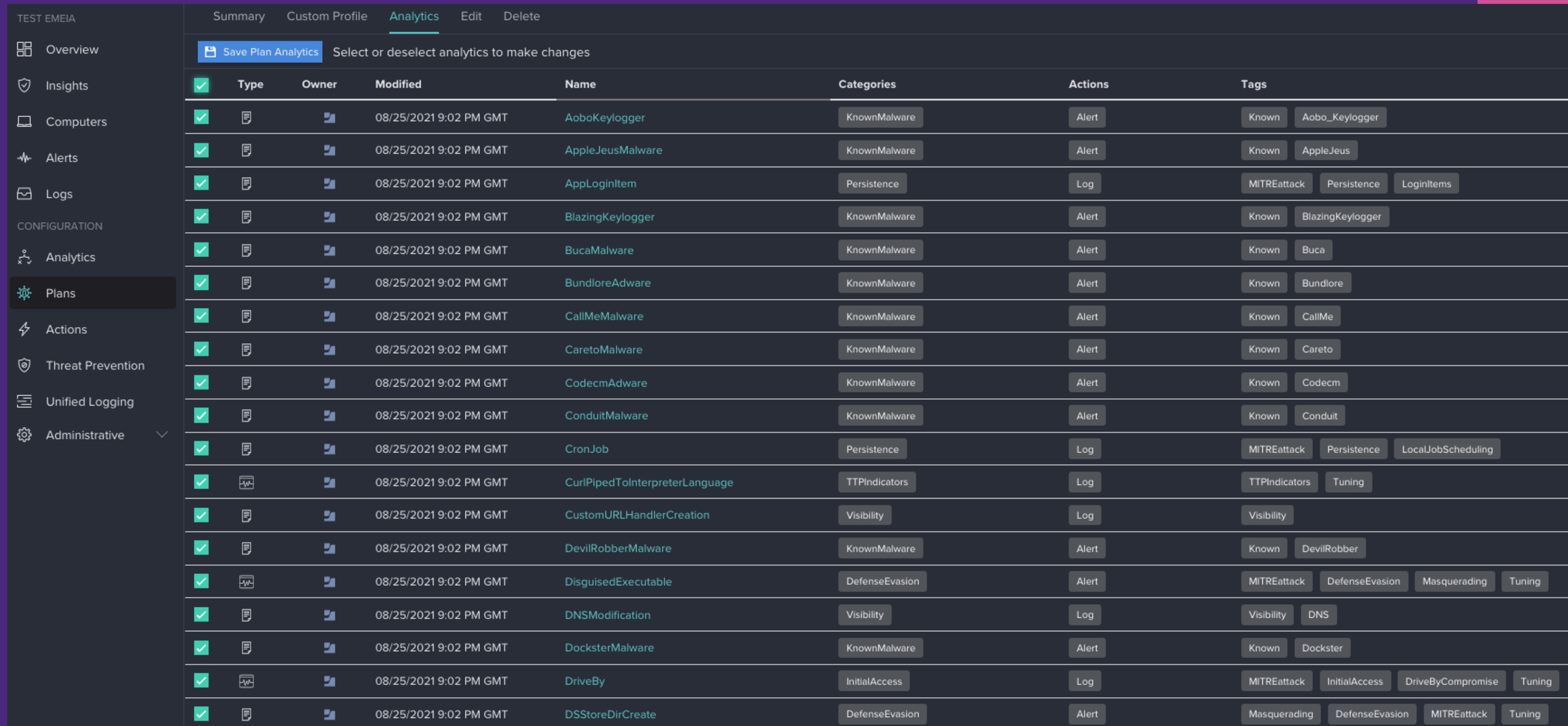
virtual JNUC 2021



Agent Log Verbosity

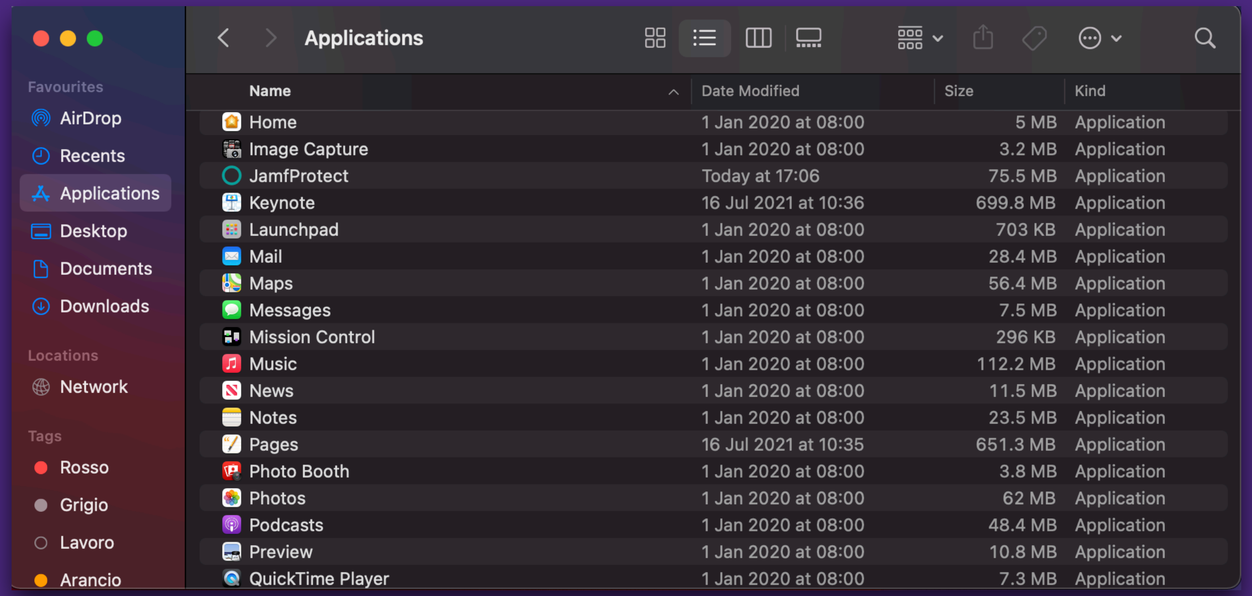
virtual JNUC 2021

Analytics


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

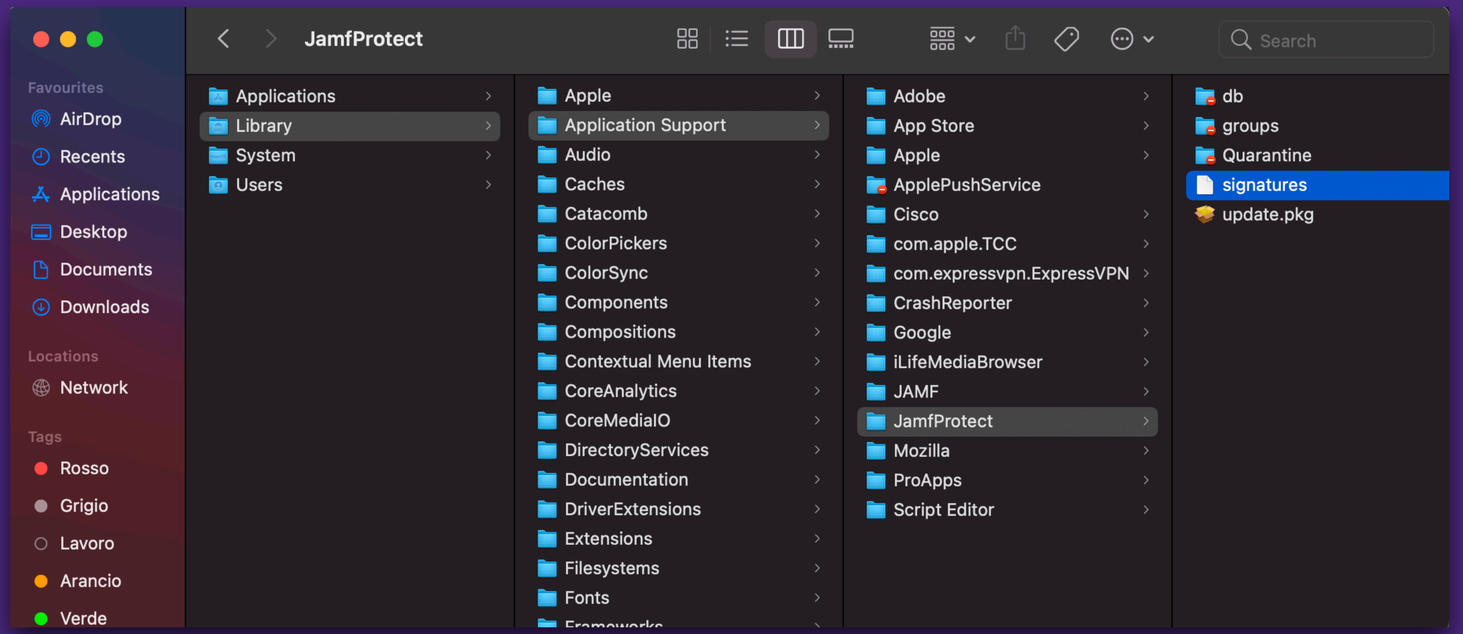
Components

LaunchDaemon vs System Extension



App bundle: /Applications/JamfProtect.app/

App bundle: /Applications/JamfProtect.app/

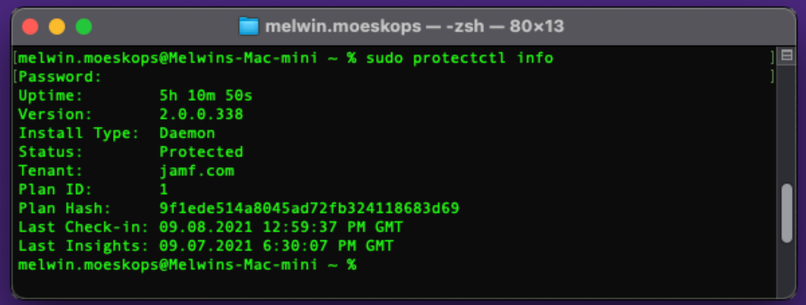


/Library/Application\ Support/JamfProtect/

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:



Agent Detection

- What is Agent Detection

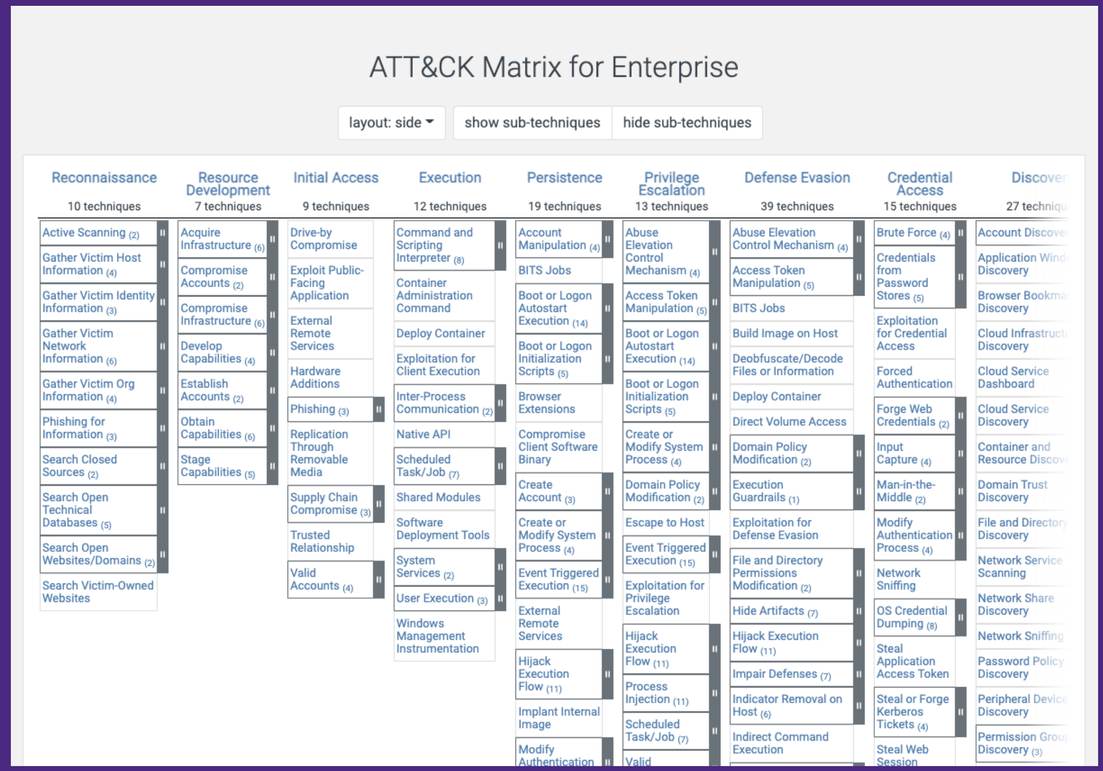
Signature detection

- What is signature detection

Behaviour detection

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

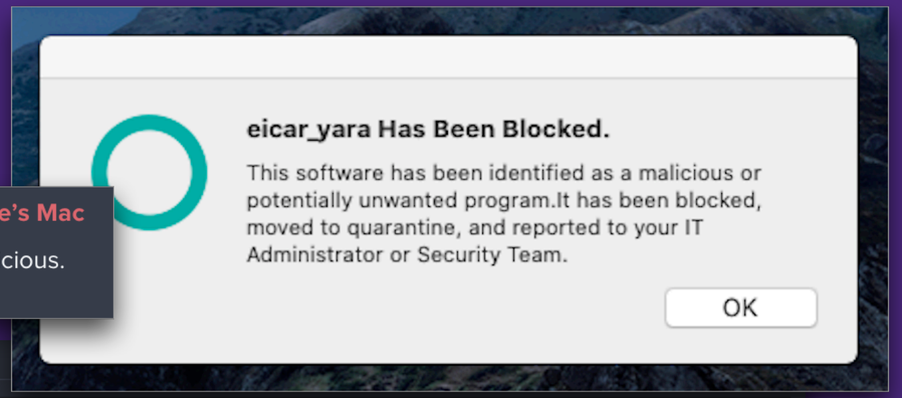
https://attack.mitre.org/

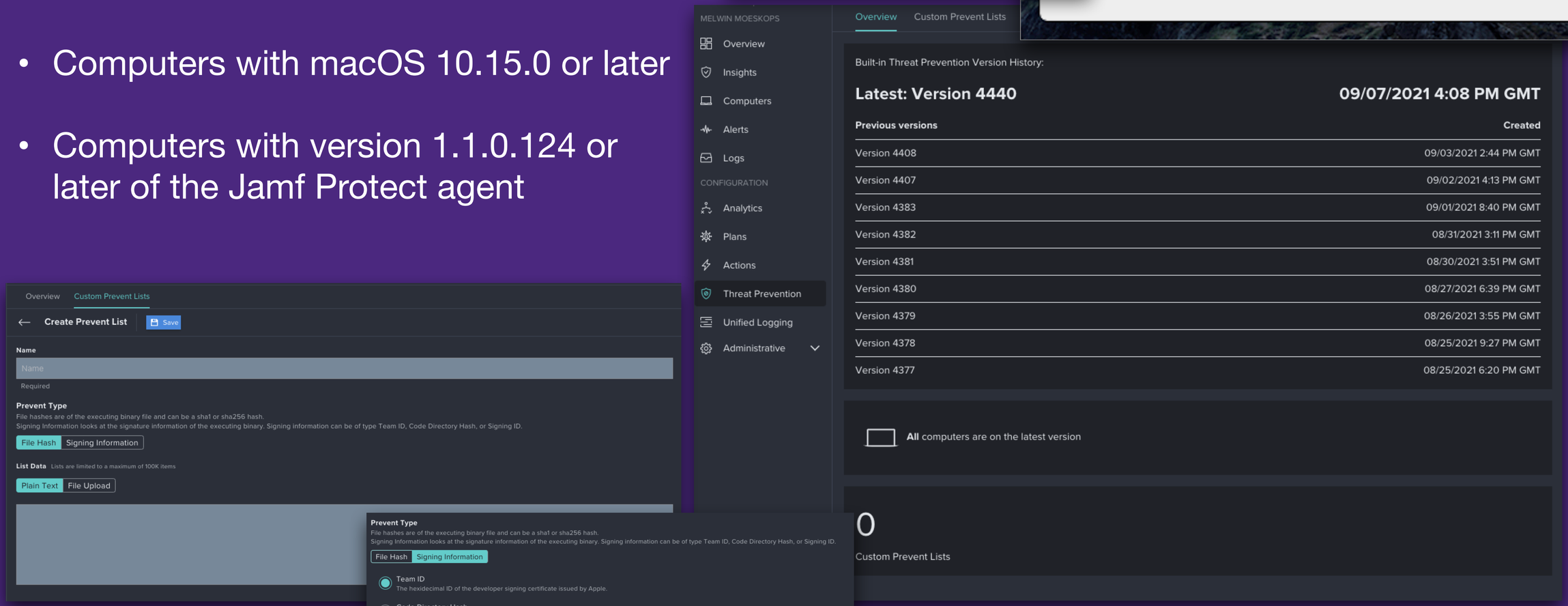


virtual JNUC 2021

Threat prevention

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

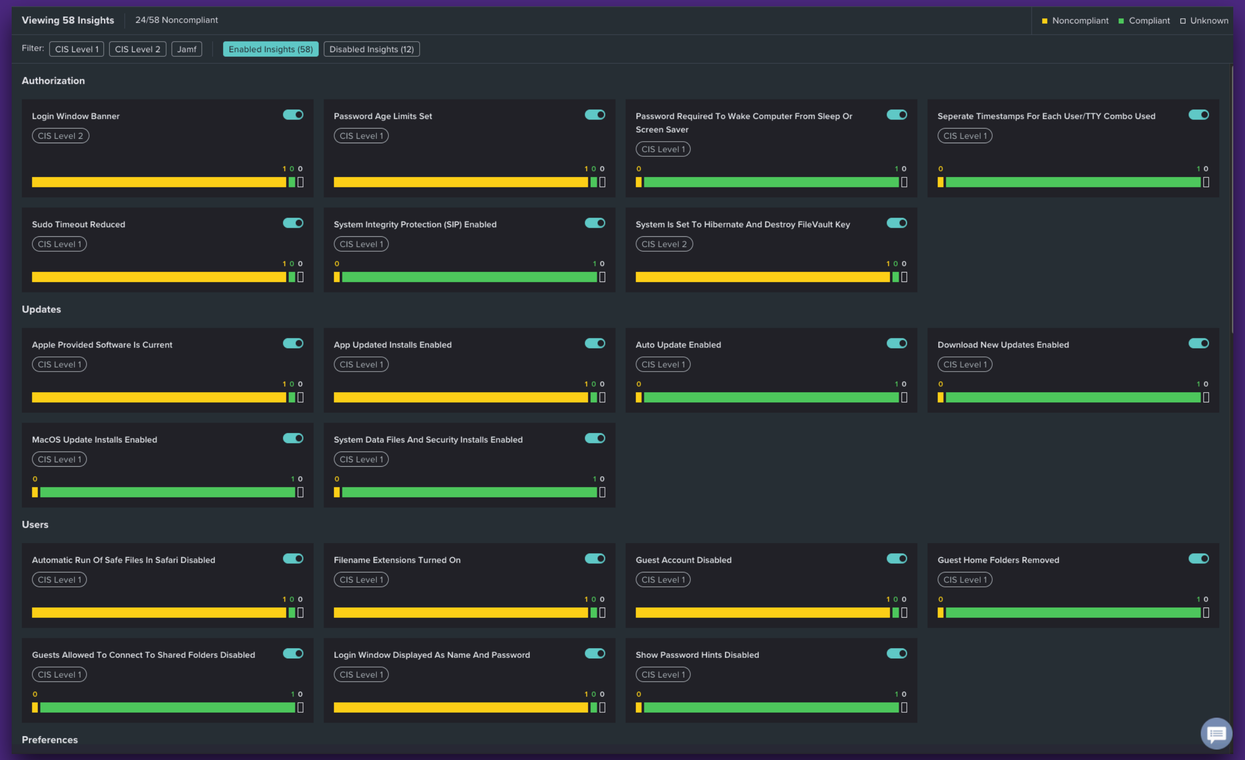


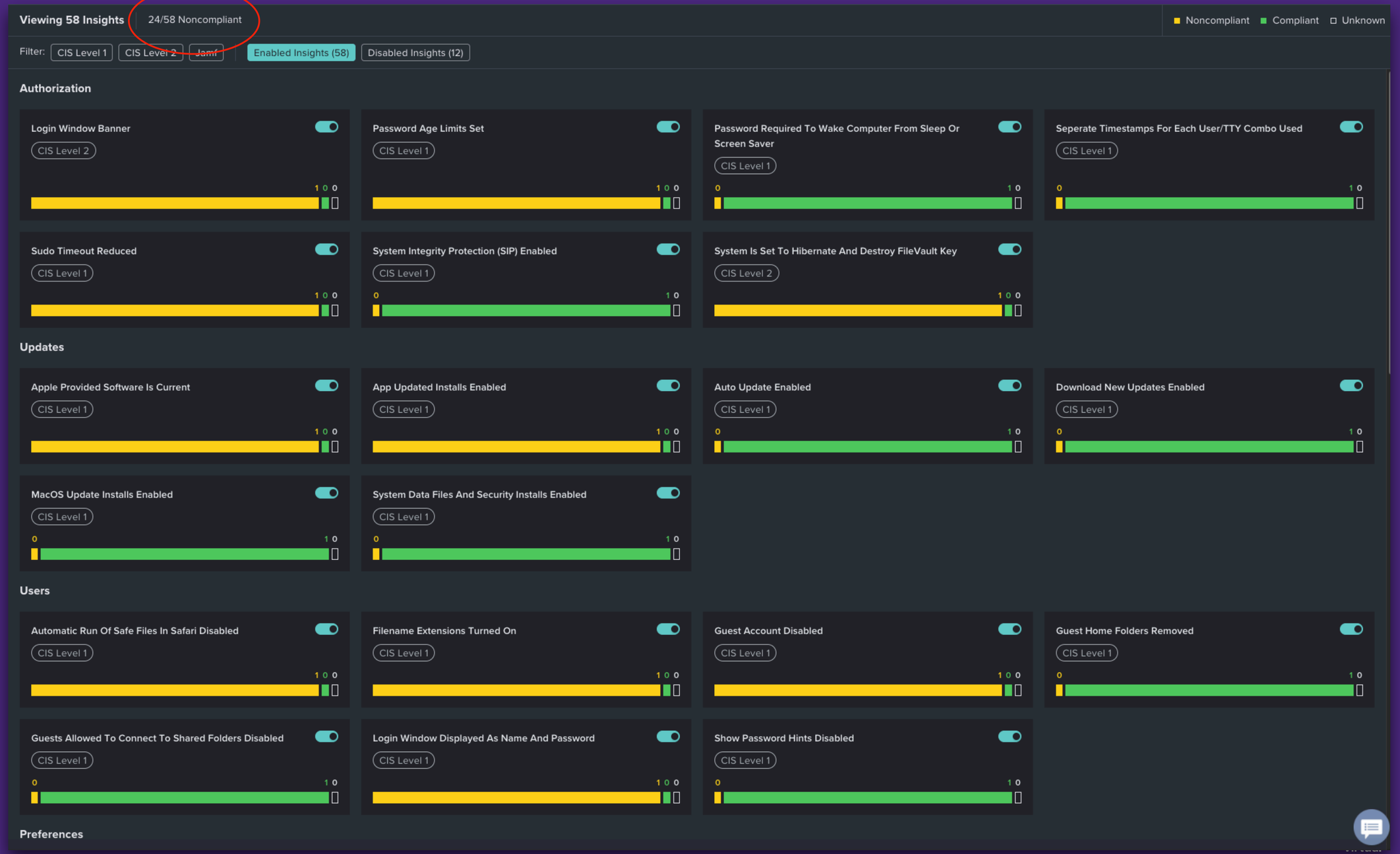


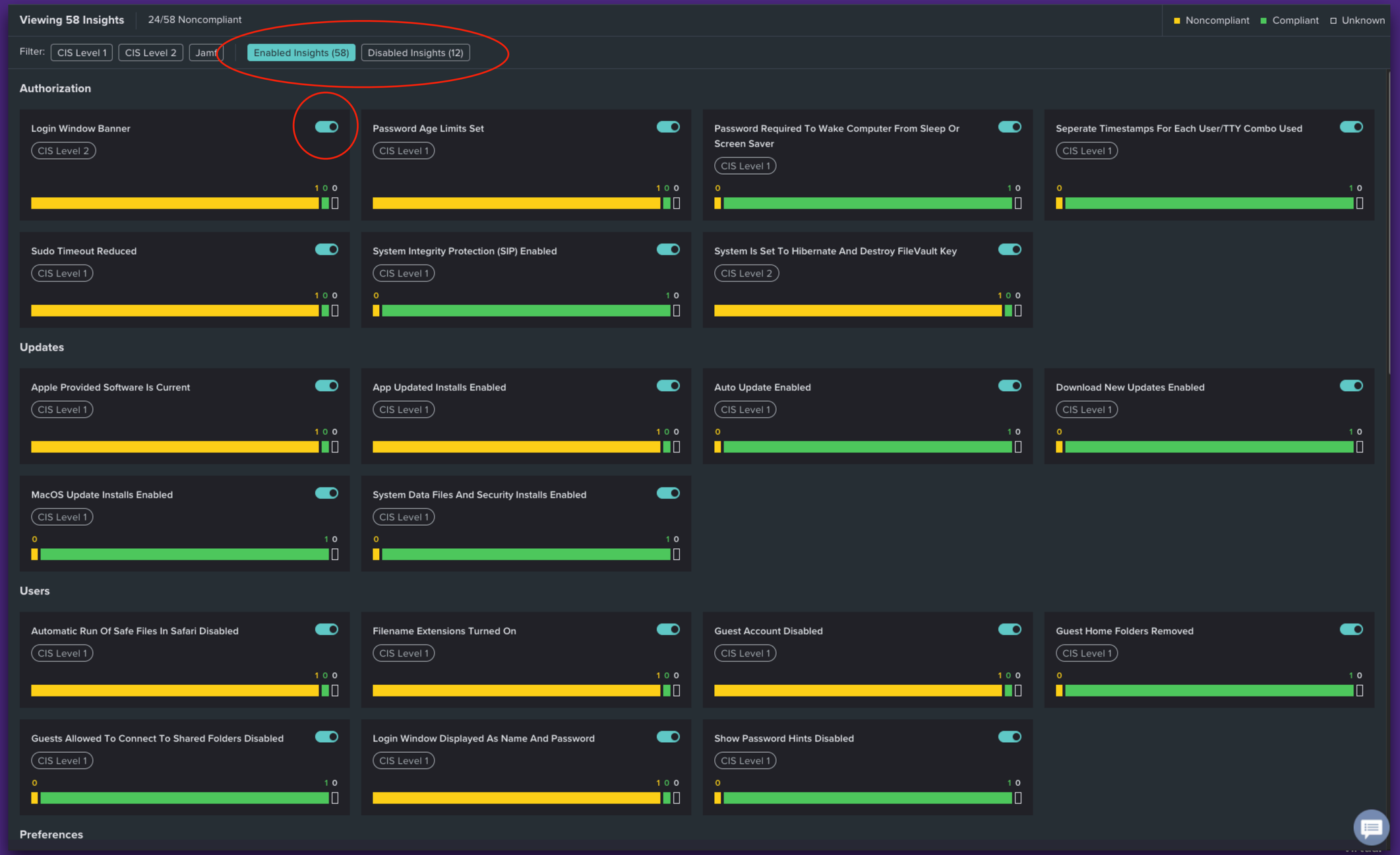
Insights & Analytics

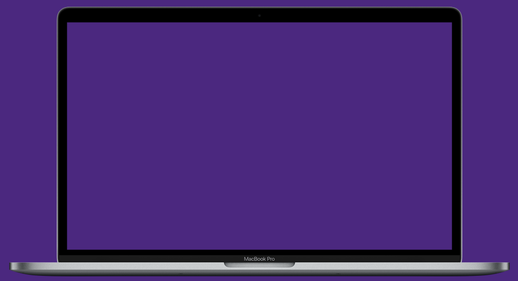
Insights

- 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.

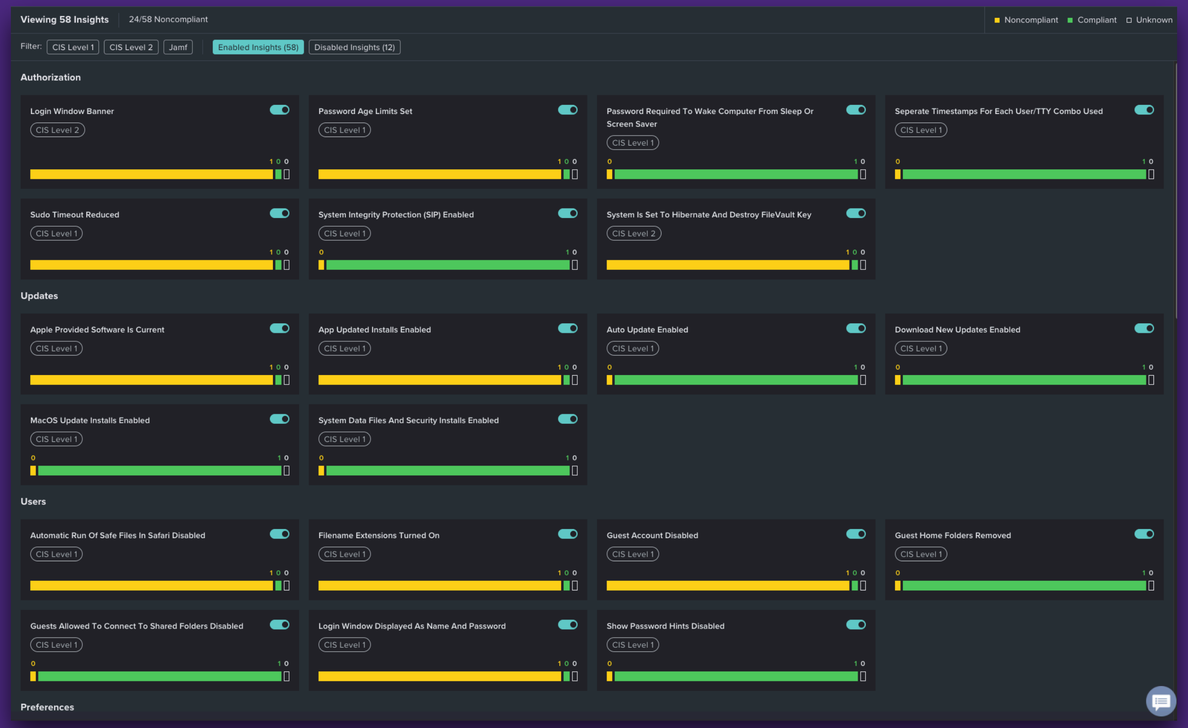






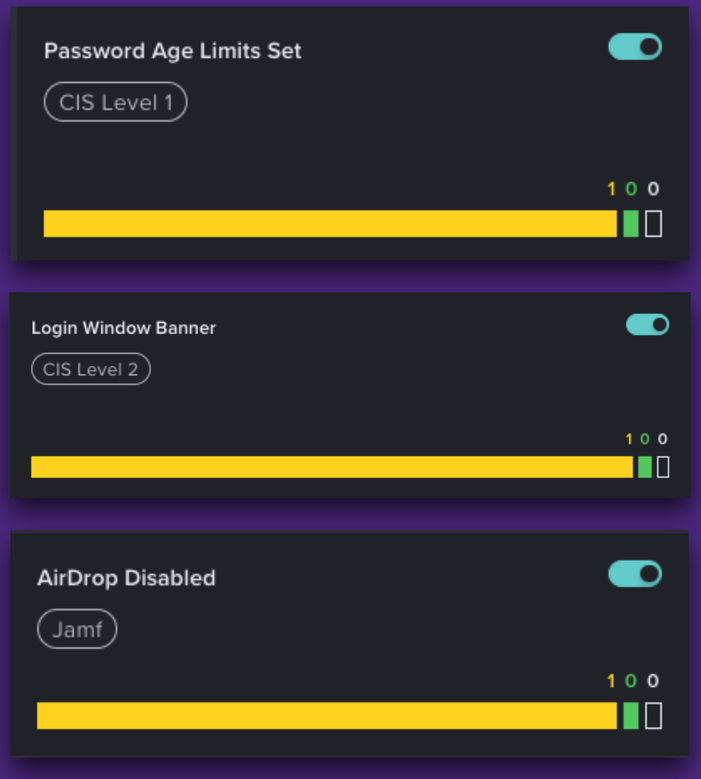


Default collection interval once per day



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

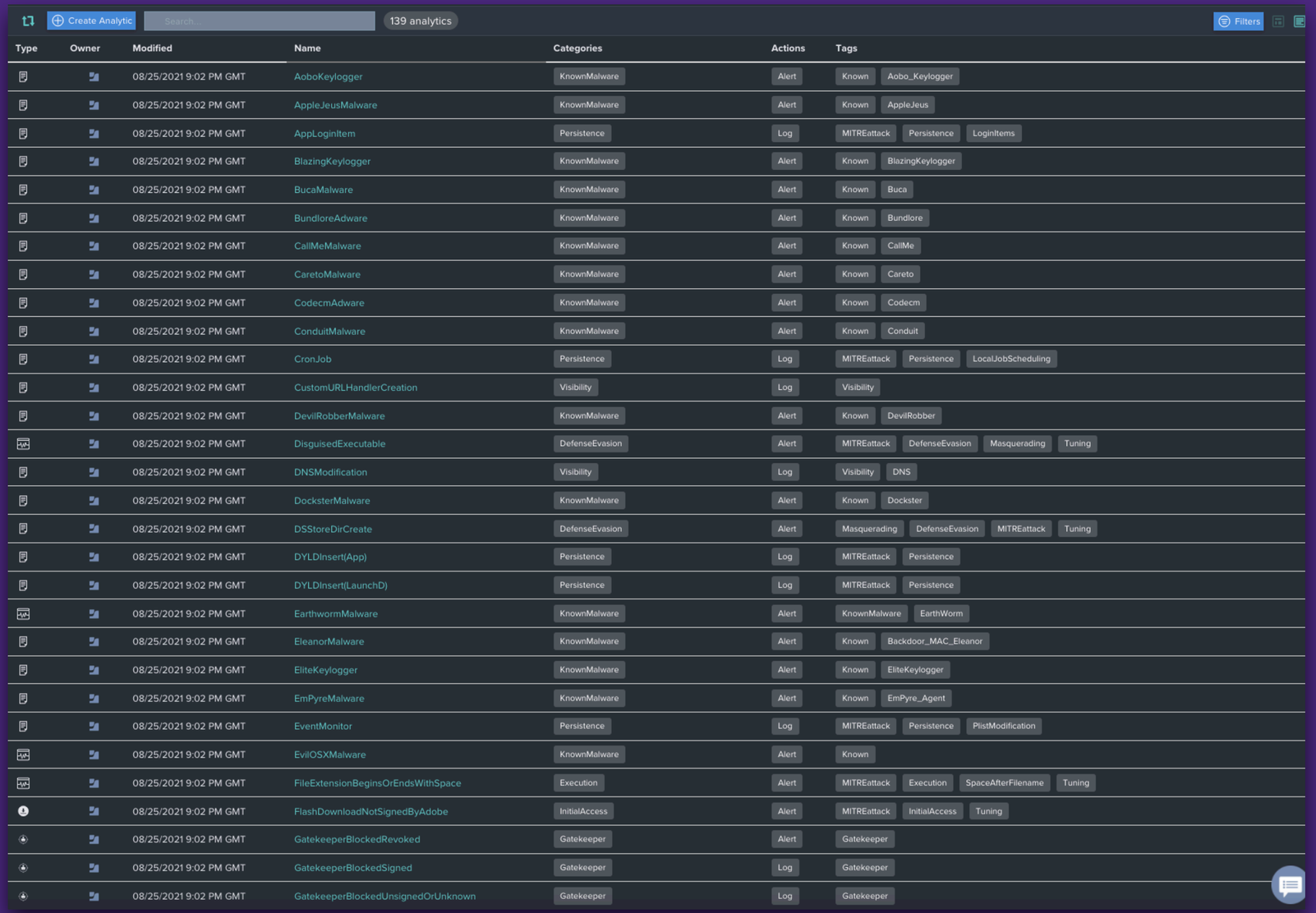
CIS levels



- 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

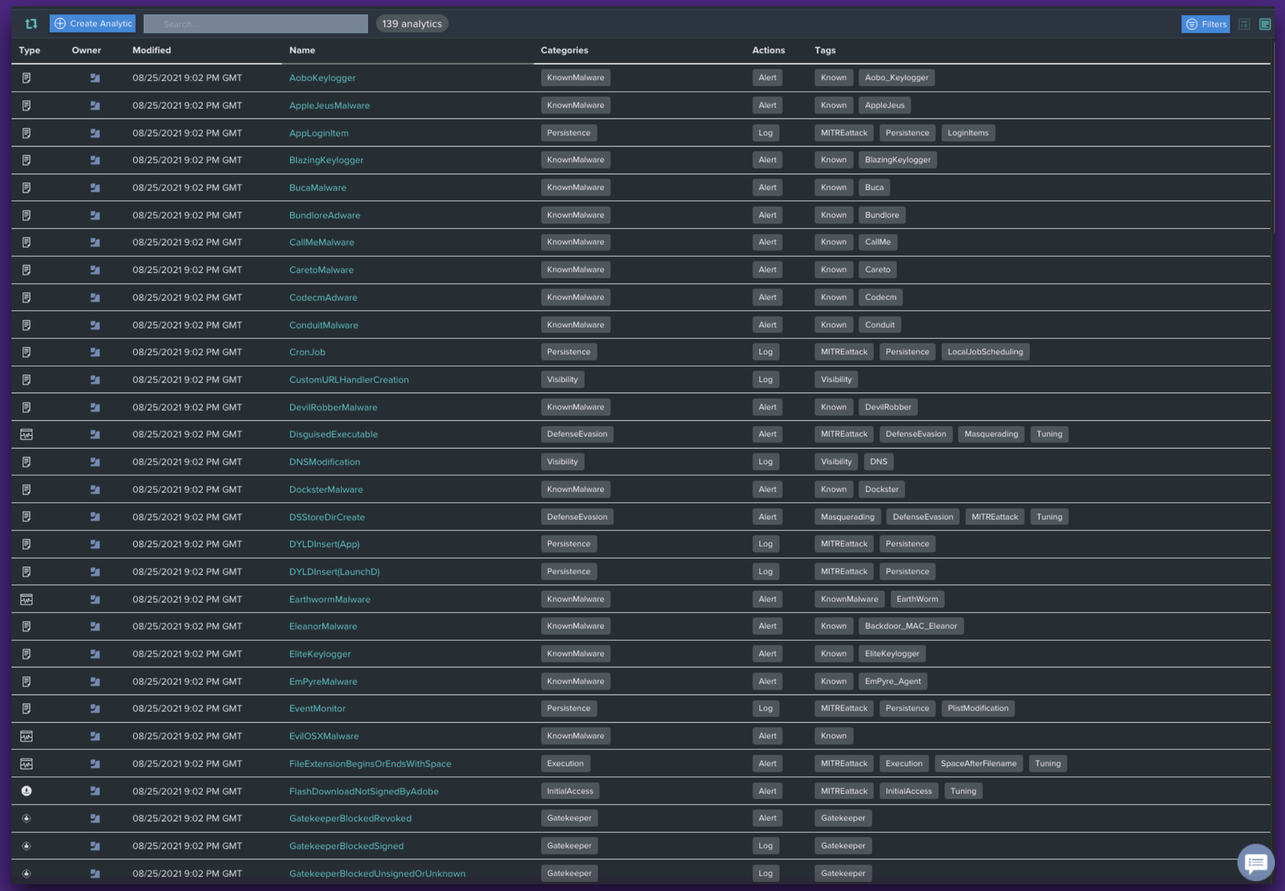
- Made and maintained by Jamf
- Different sensor types
- Understanding how this information is monitored



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

Sensor Types

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