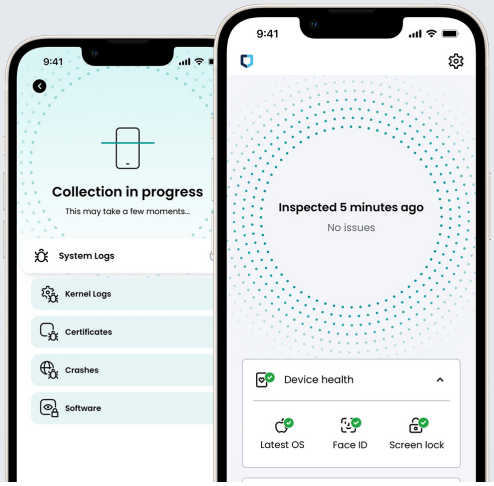
Jamf Executive Threat Protection Technical Guide

Achieving Jamf Trusted Access for high-risk individuals would not be complete without detailed forensic capabilities on mobile devices. Jamf Executive Threat Protection takes a privacy-centric approach to obtaining a deep analysis of mobile threat activities. This provides InfoSec and SecOps teams the visibility needed to identify 0-day attacks.



How does Jamf Executive Threat Protection do this?

Risk and Compromise Detection

Jamf Executive Threat Protection has a mobile app installed on endpoints that has privileges to detect if and when a device was attacked, how the attack occurred, and what was the impact. A deep inspection is offered via the Threat Protect Connector app which is installed on macOS or Windows devices and enables users to connect their mobile device via physical cable to complete scans. Threat detection abilities apply to corporately-owned and BYOD iOS, iPadOS, and Android devices.

Pre and Post Travel Inspections

By integrating Jamf Executive Threat Protection into your analysis workflows, end users or admins can perform device checks on mobile devices before and after traveling to determine risk and perform remediation prior to connecting the device back to the corporate network.

Digital Forensics and Incident Response (DFIR) Analysis

The Jamf Executive Threat Protection advanced digital forensics investigation capabilities provide your SOC team with automated analyst reports, unique sophisticated analysis engine that can detect malicious activity and 0-days based on anomalies, known and unknown threat intelligence. Our solution provides automated analysis to complete the heavy lifting for SOCs, potentially saving months of manual investigation work per device. Due to its deep analysis functionality, the tool is suitable for IT admins, InfoSec as well as internal research teams.

Jamf Executive Threat Protection

Methods for deployment

Client side

Threat Protect Connector app installed on workstation, while Threat Protect mobile app and widget (Mobile app includes the building of Jamf Executive Threat Protection VPN on iOS/iPadOS devices.)

The Threat Protect Connector app is installed on a workstation, either macOS or Windows computer, to complete activations of Threat Protect mobile app or to complete cabled inspections of mobile endpoints.

The Threat Protect mobile app can be deployed to iOS, iPadOS and Android devices either through MDM (recommended) or manually from Apple's App Store or Google Play Store. Activation will require physical connection to the Jamf Executive Threat Connector app on a host computer. Widget should be installed on mobile device through manual process. The process is shown during the activation of the Threat Protect app.

Server side

Cloud, on-premises and air-gapped hosting of server components.

Jamf Executive Threat Protection cloud hosting option is the recommended solution for all organizations.

The benefits of cloud

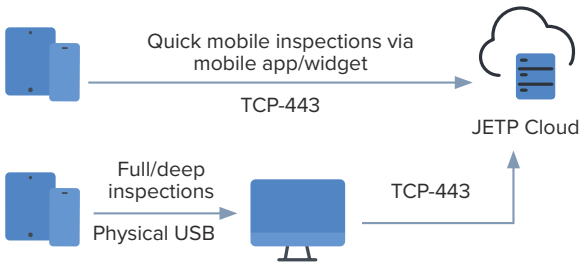
1. Active, real-time updates to threat rule engine
2. Real-time updates to UI
3. Active scanning, file gathering, end-user notification and remediation options on endpoints-- using the Threat Protect mobile app

Jamf Executive Threat Protection can be hosted either on-premises or in air-gapped networks. These environments will require manual updating of the easily deployable server software via customer. Jamf Professional Services is available for initial server setup upon request.

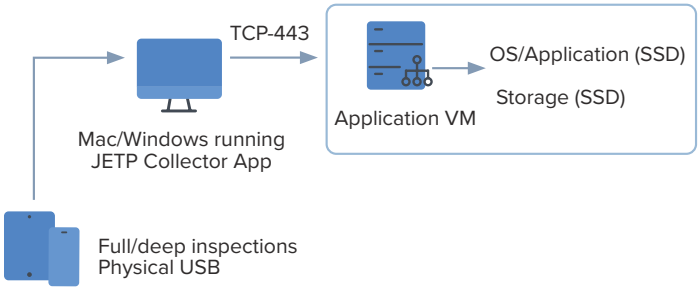
Additional considerations of on-premises or air-gapped installations are:

1. All endpoint data gathered is kept within customer's environments (still without end-user PII)
2. Upgrades are controlled by the customer
3. Use of Threat Protect mobile app unavailable
4. Jamf Threat Labs security research not actively applied, as updates to the threat rule engine will not be active or live

Cloud Deployment Architecture



On-premises Deployment Architecture



Server/Hardware Requirements can be sent by your Jamf Account team

Threat intelligence capabilities

Jamf Executive Threat Protection identifies attacks on mobile devices by analyzing:

- Operating system (OS) logs
- Faults, errors
- Kernel logs
- Diagnostic files
- Processes and other operating system-level data
- Files and filepaths
- Crashlogs
- IPS files
- Installed applications
- WiFi Manager logs
- App Store logs
- Stackshots/Spindumps

What do we do with that data?

Jamf Executive Threat Protection uses a combination of unique Indicators of Compromise* (IOC) and behavioral detection techniques. These techniques help identify 0-day, 0-click, or 1-click attacks, Persistence mechanisms, and Commercial/nation-state malware or espionage processes.

It is privacy friendly and does **not** collect the following:

- Photos/videos
- Emails
- Text messages (including iMessage)
- Call data
- Passwords
- Data in applications or files
- Browser history
- Contacts

*The Indicators of Compromise within Jamf Executive Threat Protection are property of Jamf and owned by **Jamf Threat Labs.**

Digital forensics investigations

Jamf Executive Threat Protection also supports digital forensics investigations with tools to assist malware researchers.

Threat and Process Explorers	Rules Engine	Threat Intelligence
Enables deep searching of threats with a query engine capable of searching based upon many attributes while gathering results from all Jamf Executive Threat Protection enabled endpoints in your organization	Allows customers to tag, allow list, or block list different types of indicators of attacks (IOA) as well as Indicators of Compromise (IOC). Complex rules can be built based upon many attributes including YARA, bundle identifiers, and process names.	Used to map known exploits and vulnerabilities to events and devices.

Gain extended visibility into your mobile fleet with sophisticated analysis and curated insights from Jamf Threat Labs researchers. **Get started today.**