Ticket types for Endpoint Security

Coro generates tickets for protected devices when it identifies the following security vulnerabilities:

- **Apple mobile file integrity disabled**
- **Development mode enabled**
- **Device password missing**
- **Firewall disabled**
- **Gatekeeper disabled**
- **Infected process**
- **Malware on endpoint**
- **System integrity protection disabled**
- **UAC notification missing**
- **Unencrypted endpoint drive**
- **VSS backup protection**
- **Non-genuine Windows Copy**
- **Forbidden Wi-Fi Connection**

Apple mobile file integrity disabled

Coro detected that Apple Mobile File Integrity (AMFI) is disabled on the device. AMFI helps ensure the integrity and security of executable code and system files on Apple devices. When AMFI is disabled, applications can be compromised with malicious code.

The following policy actions can be applied:

- **Review**: No auto-remediation is performed and a ticket is raised and classified as requiring review. The ticket remains open until either the Admin user closes it manually or the vulnerability is observed by the Coro endpoint agent as being resolved.
- **Enforce**: Auto-remediation is performed, recorded in a ticket, and the ticket is auto-closed.

Action	Outcomes
Close ticket	Close this ticket as considered remediated and take no further action.