esper

EMM Cybersecurity Checklist

Cloud Platform Security

□ 1.1 Ease-of-Use

□ 1.2 Secure Cloud Gateway

□ 1.3 MDM User Access Permissions

□ 1.4 Data Integrity

□ 1.5 Easily-Accessible Info on Devices, Policies & more

□ 1.6 Intelligent Event Feeds

Device Hardware Security

□ 2.1 Support Current & Future Fleet Device Types

□ 2.2 Support Current & Future Device Use Cases

□ 2.3 Offer Interoperability with Your Devices

□ 2.4 Simplify Device Updates

□ 2.5 Offer Validated Hardware

Network Security

□ 3.1 Limiting Wi-Fi Connectivity to Trusted Networks

□ 3.2 Detecting Wi-Fi Network Changes

□ 3.3 Locking Mobile Devices if They Leave the Network

□ 3.4 Wiping Lost or Stolen Mobile Devices

□ 3.5 Blocking User Access to Wi-Fi / Data Settings

□ 3.6 Detecting Unusual Data Usage Patterns

App Security

□ 4.1 Install and Uninstall Apps

□ 4.2 Manage App Versions

□ 4.3 Update Apps

□ 4.4 Support Single or Multi-App Kiosk Mode

□ 4.5 Monitor App Behavior

□ 4.6 Offer Restricted Access to Google Play or Play for Work

□ 4.7 Limit Users to Downloading Authorized Apps Only

Alerts & Remediation

□ 5.1 Custom Alerts

□ 5.2 Intelligent Notifications

□ 5.3 Automated Security Alert Responses

□ 5.4 Geofencing

□ 5.5 Device Lock Down

□ 5.6 Remote View & Control

□ 5.7 Remote Debugging & Wipe

□ 5.8 Device Tracking

□ 5.9 Offline Device Actions

User Experience

□ 6.1 Load Kiosk Mode Apps When Powered On

□ 6.2 Restrict Calls & SMS Messages

□ 6.3 Block Settings Access

□ 6.4 Hide Notifications

□ 6.5 Hide Status Bar

□ 6.6 Restrict Camera & Screenshots

□ 6.7 Block Local App Installs

□ 6.8 Block Browser Access

□ 6.9 Block Google Voice Assistant

Website: www.esper.io | Contact us: andi@esper.io