SparkCognition™ DeepArmor™ Release Notes

v 1.47.1 - 01.2019

DeepArmor Release Notes

SparkCognition is pleased to announce DeepArmor Version 1.47.1.
This document lists the additions, enhancements and fixes included within this release.

Features

This version of DeepArmor includes the following new or enhanced features:

New Features

- New - Policy Based Alert Sensitivity
- New - User Interface and Notification Policy
- New - Auto-upload of Log files
- New - Alert Sensitivity Level device setting

Enhanced Features

- Handling of Quarantined Files
- File Restoration
- Client Debug Logging
- Windows In-Memory Monitoring

- PowerShell Detection
- Sorting
- Alert Details

Issues Addressed

- Macintosh - System scan is stuck on Gathering files for analysis and doesn't move forward.
- FP on RL known clean files
- Client: Uninstall Hardening
- Client: Verify Threat Counts are accurate (macOS/Windows)
- Execution Control doesn't work immediately when turned on
- Deprecation Warning on Alerts Index Page
- Automatic Threat action - Quarantine on Process Watcher (Execution Control) is not working.
- Root-cause and fix HTTP error log messages
- Device Details, Threats Tab: Cannot sort by descending
- Clean files are detected in offline mode and reported multiple times on the server after reconnect
- Alert activities widget - no alerts and time range within a day
- Device policy tool tip box is too small
- Padding and alignment issue for DA-3001 Widget - ATTACK VECTORS
- Padding and alignment issue for DA-3479
- Activities widget - each date should be at the center of the bar(s)
- Alert Activities - User should be able to click the highlighted area to go to the alerts page instead of clicking the bar
- Single File and Folder Scan (manual) should show "Network File Scanning is not supported"
- Hovering issues on Reporting column headers
- DeepArmor SDK Folder/File Scan Scannable Field Error
- Auto Assign Rules on Server Inside Device Groups Only Saves the Most Recent Rule
- Device tab -> Alerts section Action taken vs Action Required color coding should match Alert Index page
- [Device Details Page] Updating the meter chart in Device Security Profile widget
- Server - Inconsistency in timestamp format.
- UI Consistency on Quarantine Policy
- Background scan does not stop when client is unregistered
- Update Web Service URL button
- Server - Remote initiated scan on offline devices gets stuck at Canceling
- Audit log entries for Certificate whitelisting
- Date/Time Widget closes after changing one minute or hour
- Server - UI issues related to DA-3006 (agent version spread widget)
- CNs on Certificate Names not showing up on white list certificate page
- UI Issue - Content should stay in the box with scroll bar
- Client - Could not obtain Alert for ID 0
- datetime picker caches timestamp instead of last 24 hours, 7 days, 30 days.
- Datetimepicker time value needs to display local time zone
- Time stamp on audit logs details drop down is incorrect and inconsistent.
- Dashboard tab - Fix widget properties
- Server - Hide "Edit Notes" and "Delete" options from GlobalList for a manager
- Potential Double Alert Issue Associated with Online/Offline Mode
- Path Showing Up as Unknown on the Server
- Add permission button deletes all groups assigned if no changes are made in the edit menu
- mac client File Action menu sometimes shows a blank entry
- Server - Alert status being shown as "Action Required, Quarantine" if the alert is quarantined by the client
- Files with ps1 extensions need to be checked
- Remote initiated scan not canceling.
- remove TopRecentThreat from the code

- Error log - A 32 bit processes cannot access modules of a 64 bit process.
- 1.46.380 Registration during install is failing.
- Client is not registering after install.
- Client - "Deprecated Allow" is shows as Action Taken in alerts tab
- 1.47.408 Connection status does not change until the client GUI is restarted
- Device is losing assigned configuration (Group assigned)
- Log should state "Warn" rather than "Error" when connection to the server is unavailable.
- VPN and Offline Issues with Scans
- Can't open apps immediately on mac after turning on execution control
- Old ALLOWED alerts are conflicting with NONE
- Client not piping up alerts to the server (Mac)
- Client: Certificate Thumbprint wasn't being piped up if detected in offline mode
- Add Device Group, Multi-Select Filter to the Dashboard and Alerts Tabs
- Client: Exporting with a filename that contains a comma causes issues
- Story
- File actions - macOS Alerts tab implementation
- Windows Defender Security Center Integration - Register Function, Unregister Function, Update Status Function
- AMSI process kill and file quarantine capability
- Client: Auto-Upload of log files
- Server: Auto-upload of log files
- Complete URL analysis work
- Date/time picker consistent time format
- Dashboard refactoring
- Alerts Dashboard UI/UX
- Certificate Based Whitelisting GUI - Blacklist white list tab
- Add Policy Name for devices in Device Index (list) page.
- SDK: Certificate Whitelisting Support
- Research spike: policy-based alert sensitivity
- Implement incremental PowerShell model
- Identify and optimize queries for large number of devices
- New Alert Sensitivity Level device setting
- Allow for Sorting By Date Added and CN on Certificate Whitelist Page
- Alert Sensitivity Level policy backend/API
- Client: Optimize the macOS Process Execution
- SDK: Ensure parity with functionality between Client and SDK
- Management Console Alert Sensitivity Level
- Top Menu Bar - Changes to Make Wording Filter Results on the Alerts Page
- Client: Encryption of the config.json (Client and SDK)
- Minor UI Fix for Capitalization of Units
- Distinguish scanned file between Malicious and Abnormal
- Expand SDK to accept Malicious/Abnormal results from file scan
- Allow alerts take action status to automatically reflect on the alert detail page.
- login generates exception logs
- Agent API device policy endpoint rework
- Add Device Group, Multi-Select Filter to the Dashboard and Alerts Tabs
- Device Index:Add Search by User and IP
- Alert Details: Device Name link to Device Details
- File Reputation Business Logic and Data Collection Adjustment
- Blacklist/Whitelist Sorting
- Changing the Alert Options
- Alert Dashboard: Top Alerts Widget: Replace hash with most common file name
- Client: Enhanced Restore Functionality

- Alert Details (Event Details): Add "Cloud Service Connection", "Network Connection" and "Detection Method"
- Add devicegroups filter to all dashboard queries and alerts queries
- Research and Architecture on registration server
- Add Model, API for file upload for alert investigation
- DA server tuning
- Define registration DB table structure
- Remove FK dependency on user.id: Usermanagement
- Remove FK dependency on user.id: devices_device
- Remove FK dependency on user.id: Globallists
- Provide new format for how Scan completion message is displayed.
- Client: Add Current Status to the BaseWorker class
- Remove files scanned metric from the Metrics bar on Dashboard and Alerts pages
- Research spike: improved encryption for Client/SDK
- Improve PE Model Performance
- Update RL Download Script to use new API
- Client: Sync Implementation for Threat Actions
- Refactor SDK code to reflect ErrorInfo field more accurately
- Client: Add support for enum based logging
- Expose Method in SDK to allow the client to specify thresholds for various models
- Host qualified domain name showing up as IP address (host FQDN) on Mac
- Client: Not handling null responses on bulk_query gracefully
- Client: Updated ACL logic for Windows
- AMSI issue with quarantine
- Client: Filter out pyd files from being scanned
- Change alert Sensitivity text to be consistent with the req

---

Revision Table

Version	Date
v 1.40	02.23.2018
v 1.41	04.04.2018
v 1.42	05.23.2018
v 1.43	06.27.2018
v 1.44	07.27.2018
v 1.45	09.20.2018
v 1.45.1	10.05.2018
v 1.45.2	10.16.2018
v 1.46	11.26.2018
v 1.47.1	01.2019