FIELD SECURITY REPORT

CROWDSTRIKE FALCON GO: ONBOARDING & MANAGEMENT

RESEARCHED AND TESTED BY:
Nipun Juneja
Tanish Bhandari

JULY 2025

EXECUTIVE SUMMARY

The Field Security Report on CrowdStrike Falcon Endpoint Protection Go includes:

- Cyberease rating of onboarding experience of CrowdStrike Falcon Endpoint Protection Go.(the EPP solution designed for small and midsize businesses)
- Onboarding of agents tested on Windows Server 2025, 2022, 2012 R2, and Enterprise editions of Windows 7 SP1, 8.1, 10, and 11.
- Onboarding seamless for all systems except Windows 7 SP1 and 8.1, which are unsupported.
- Clear messaging and documentation provided for unsupported OSs, Windows 7 SP1 and 8.1.
- Deployment uses a single executable file, requiring no pre- or post-installation steps for supported systems.

Actionable Insights:

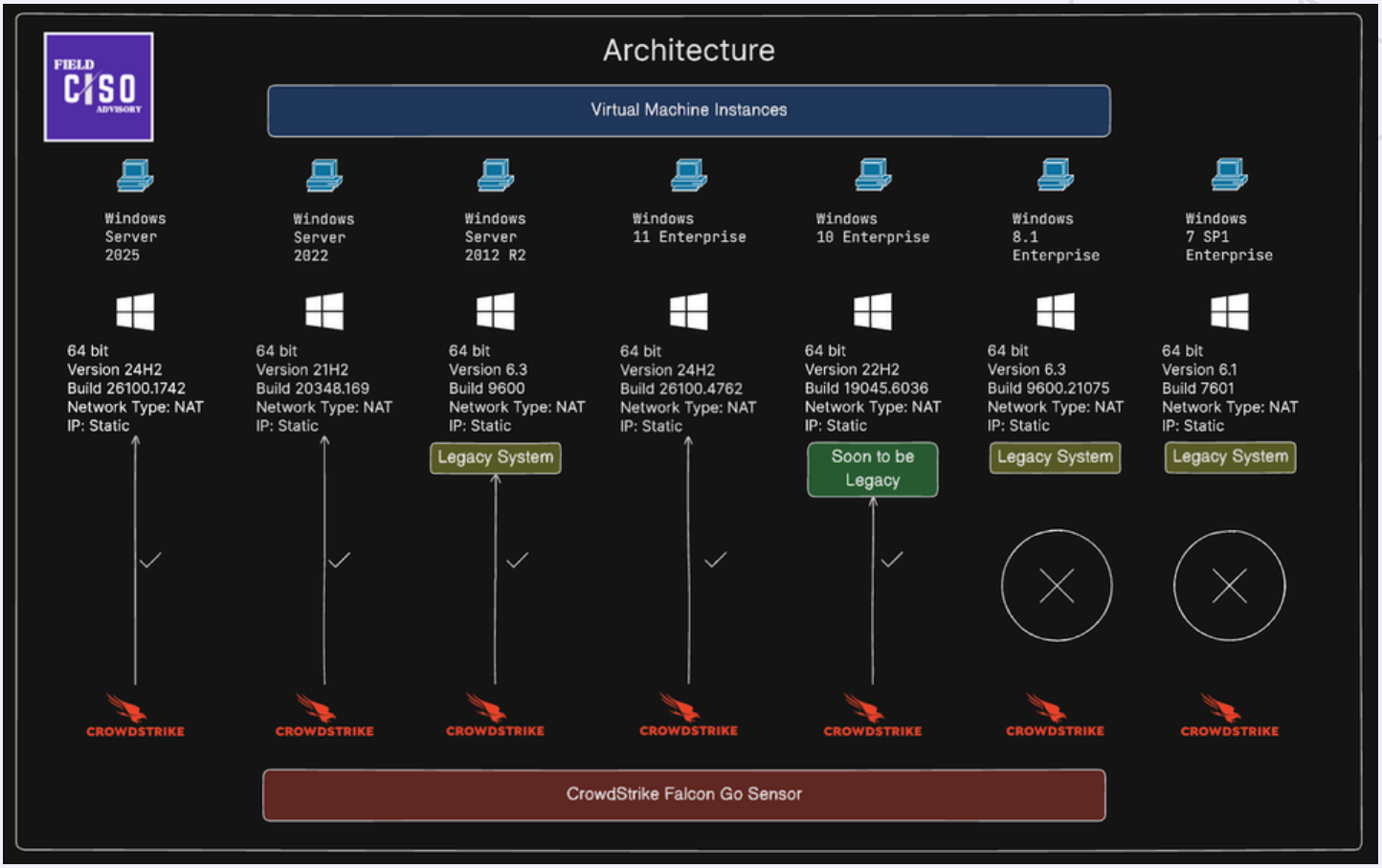
- Enterprises can deploy Falcon Go on modern Windows systems (Server 2025, 2022, 2012 R2, Windows 10, 11) with confidence in rapid, hassle-free onboarding.
- Organizations using Windows 7 SP1 and 8.1 must upgrade to a supported OS, at least Windows 10 or later to leverage Falcon Go.
- The single-executable model simplifies deployment, reducing IT workload and enabling quick scaling across enterprise environments.
- Clear documentation ensures transparency, aiding planning for legacy system upgrades.
- The global July 19th, 2024 incident underscored the critical importance of managing endpoint agent lifecycles and regular content updates to the agents.
- Our testing confirmed that Falcon Go provides the necessary policy controls to delay automatic agent upgrades, enabling enterprises to implement a phased agent upgrade rollout strategy and validate new sensor versions in a controlled environment before a fleet-wide deployment.

INTRODUCTION AND DEPLOYMENT INSIGHTS

CrowdStrike Falcon Endpoint Protection Go is a lightweight, cloud-native endpoint security solution designed for small and medium enterprises, for rapid deployment and ease of use. This report assesses the onboarding process across a range of Windows operating systems commonly used in enterprise environments. Our goal is to provide a clear, concise evaluation of deployment ease, highlighting system compatibility and any challenges encountered.

Please note that the findings are based on hands-on testing conducted by our Field Security Architects and this report is not sponsored by Crowdstrike

ARCHITECTURE



METHODOLOGY

1. Deployed Falcon Go on virtualized instances of:

- Windows Server 2025, 2022, 2012 R2.
- Windows 7 SP1, 8.1, 10, 11 (Enterprise editions).

2. Tested in controlled environment with standardized hardware:

- 4GB RAM, 4-core CPU, 60GB SSD.

3. Used the latest Falcon Go executable from CrowdStrike. (Version: 7.26.19809)

4. Evaluated based on:Installation simplicity.

- Installation simplicity.
- System compatibility.
- Error messaging.
- Additional configuration requirements.

5. Results quantified using CyberEase Rating system (1–5 stars).

.

ONBOARDING EXPERIENCE BY OPERATING SYSTEMS

The following table summarizes the onboarding experiences across tested operating systems with CyberEase Ratings assigned by FieldCISO Advisory (1–5 stars, 5 being the best, 1 being the worst):

Onboarding Experience Comparison

Operating System	Onboarding Method	Official Support	Notes/Challenges	CyberEase Rating
Windows Server 2025	Single Executable	Yes	Straightforward; completed in <5 min; seamless integration with management console.	★★★★★ (5/5)
Windows Server 2022	Single Executable	Yes	Straightforward; completed in <5 min; seamless integration with management console.	★★★★★ (5/5)
Windows Server 2012 R2	Single Executable	Yes	Straightforward; completed in <5 min; seamless integration with management console.	★★★★★ (5/5)
Windows 11 Enterprise	Single Executable	Yes	Efficient; completed in ~3 min; fully automated, no additional configurations.	★★★★★ (5/5)
Windows 10 Enterprise	Single Executable	Yes	Smooth; completed in ~3 min; no reboots or manual interventions required.	★★★★★ (5/5)
Windows 8.1 Enterprise	Single Executable	No	Unsupported; clear messaging; Windows Server 2012 R2 earliest supported version.	★☆☆☆☆ (1/5)
Windows 7 SP1 Enterprise	Single Executable	No	Unsupported; clear messaging; Windows Server 2012 R2 earliest supported version.	★☆☆☆☆ (1/5)

WINDOWS SERVER 2025, 2022, 2012 R2

- **Process:** Onboarding was straightforward using a single executable file. Installation completed in under 5 minutes per system. The agent integrated seamlessly with each server's management console.
- **Challenges:** No compatibility issues observed; no pre- or post-installation steps needed.
- **CyberEase Rating:** ★★★★★ (5/5) – Exceptional ease of onboarding with minimal complexity.

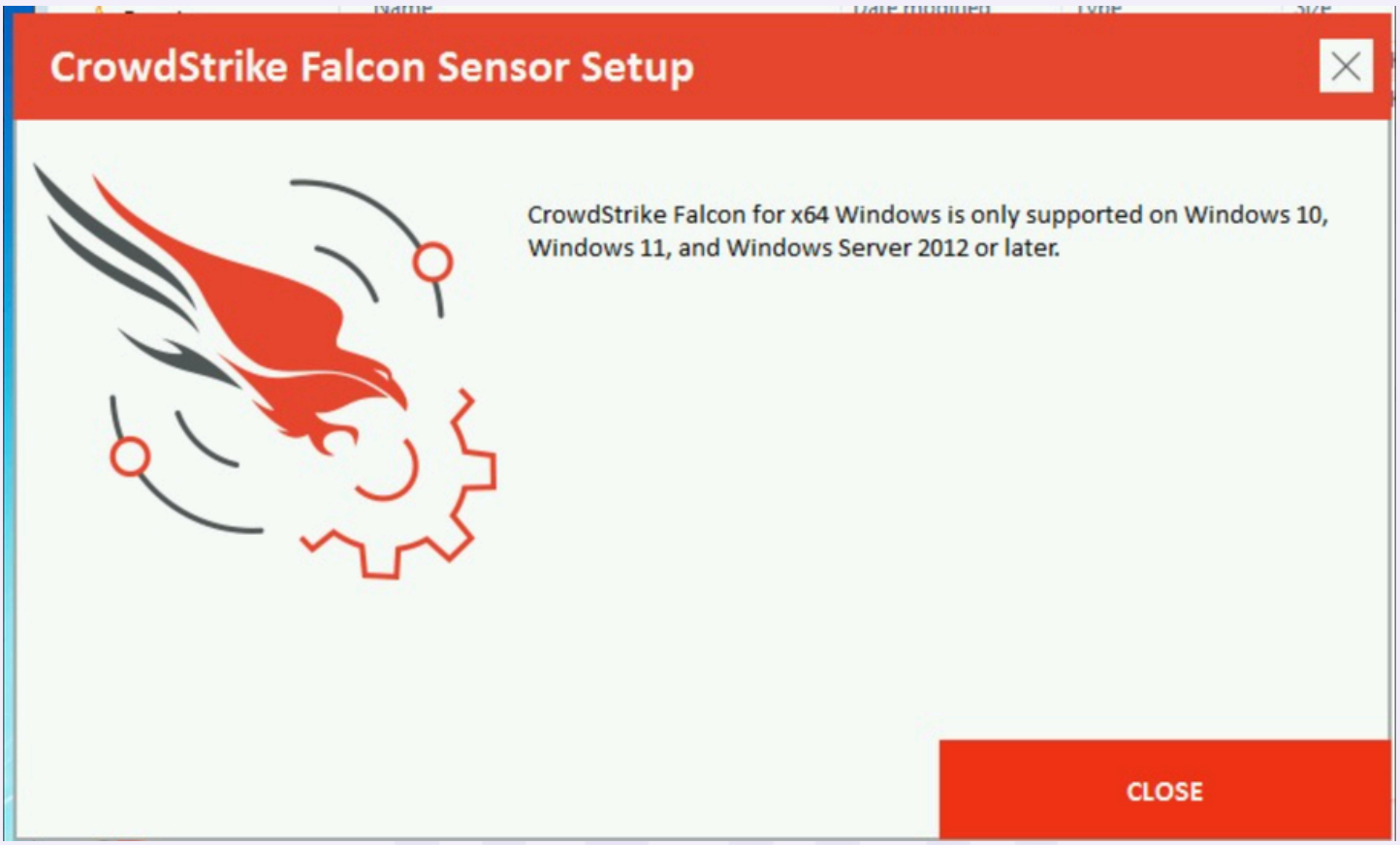
WINDOWS 11 ENTERPRISE

- **Process:** Deployment was efficient, with the executable installing the agent in approximately 3 minutes. The process was fully automated, and the agent initialized without additional configurations.
- **Challenges:** None; seamless and rapid deployment.
- **CyberEase Rating:** ★★★★★ (5/5) – Exceptional ease of onboarding with full automation.

WINDOWS 10 ENTERPRISE

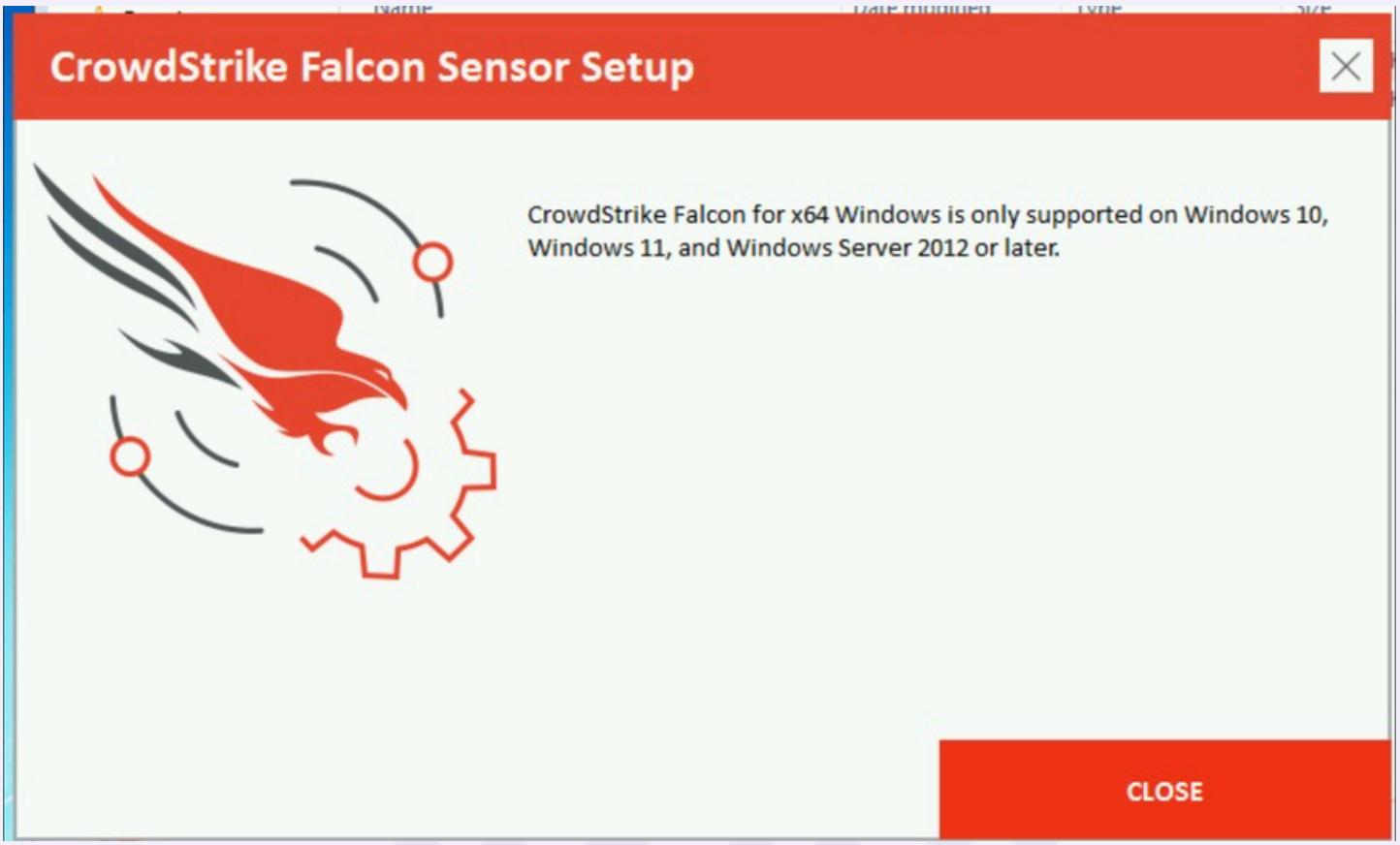
- **Process:** Onboarding was smooth, with the executable handling all tasks in approximately 3 minutes. No reboots or manual interventions were required.
- **Challenges:** None; consistent with Windows 11 experience.
- **CyberEase Rating:** ★★★★★ (5/5) – Exceptional ease of onboarding with no interruptions.

WINDOWS 8.1 ENTERPRISE



- **Process:** **CrowdStrike Falcon Sensor Deployment Halted.** The CrowdStrike Falcon Sensor installer displayed a clear message: "CrowdStrike Falcon for x64 Windows is only supported on Windows 10, Windows 11, and Windows Server 2012 or later." This directly indicates that Windows 8.1 is not a supported platform for the sensor.
- **Challenges:** The fundamental obstacle is the hard block on installing the CrowdStrike Falcon Sensor on Windows 8.1. This means these devices cannot receive EPP from CrowdStrike, creating an unmitigated security risk. An urgent upgrade to a supported operating system is required to deploy the sensor and secure the endpoint.
- **CyberEase Rating:** ★☆☆☆☆ (1/5) – Incompatible OS prevents installation, leaving the endpoint unprotected; upgrade is mandatory.

WINDOWS 7 SP1 ENTERPRISE



- **Process:** Falcon Go is not supported. The installer provided clear, transparent messaging indicating Windows Server 2012 R2 as the earliest supported version.
- **Challenges:** Users advised to upgrade to a supported OS due to lack of support.
- **CyberEase Rating:** ★☆☆☆☆ (1/5) – Complete lack of support, preventing onboarding.

PERFORMANCE IMPACT DURING INSTALLATION

RAM Usage:

- Installation spike: 200-300 MB temporarily during the 3-5 minute deployment process
- Post-installation baseline: Stabilizes to 100-200 MB for normal operations
- System requirement: Minimum 4 GB total system RAM recommended for smooth onboarding

CPU Impact:

- During installation: 10-20% CPU utilization for the deployment duration
- Settling period: 20-30% CPU usage for 5-10 minutes post-installation during initial system scan and baseline establishment
- Ongoing operations: The Crowdstrike Falcon Sensor continuously monitors and logs real-time events with typical 2-5% CPU usage

Installation Characteristics:

- Network usage: 10-50 MB for initial policy download and agent registration
- Disk I/O: Moderate activity during agent deployment and initial configuration
- No reboot required: Installation completes without system restart on supported Windows versions

* These statistics are calculated as per the lab virtual machines

Operating System Coverage

Supported Operating Systems	Unsupported Operating Systems
Windows Server 2025	Windows XP & Windows Server 2003
Windows Server 2022	Windows Server 2003 R2
Windows Server 2012 R2	Windows Server 2008 & Windows Server 2008 R2
Windows 11 Enterprise	Windows Vista
Windows 10 Enterprise	Windows 7 SP1 & Windows 8.1 Enterprise

PROACTIVE CONTROLS AND AGENT MANAGEMENT IN THE WAKE OF THE CROWDSTRIKE INCIDENT

The CrowdStrike incident on July 19th served as a critical reminder of the complexities inherent in modern cybersecurity, particularly concerning the management of EPP solutions. While the incident itself was rooted in a content update, it profoundly underscored the necessity for organizations to possess granular control over not only the agent software deployed on their endpoints, but also the continuous stream of threat intelligence and operational content delivered to these vital systems. In light of such impactful events, a thorough understanding and judicious application of the controls available within EPP platforms like CrowdStrike Falcon Go become paramount for fortifying an organization's security posture and ensuring operational resilience.

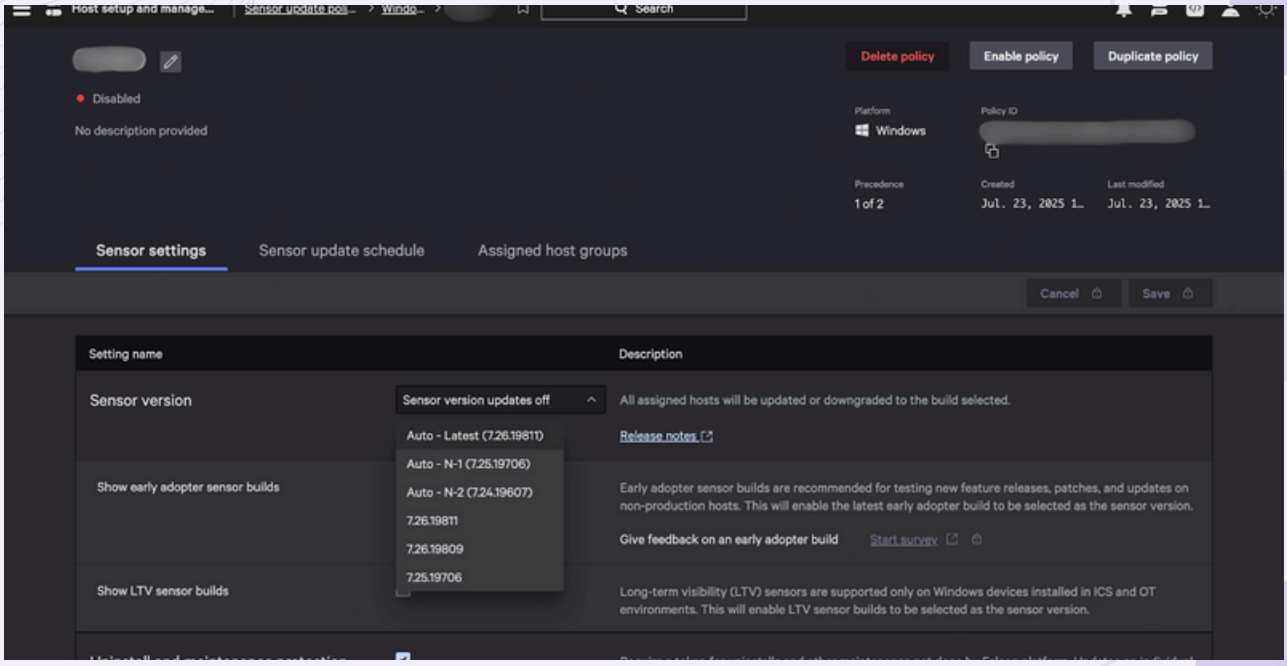
With this context in mind, our comprehensive review of CrowdStrike Falcon Go focused intently on its agent management capabilities. These are broadly, yet distinctly, categorized into two essential areas: Agent Upgradation and Agent Updation. These functionalities are designed to empower organizations with precise control over the lifecycle of their endpoint sensors, ensuring both robust security efficacy and minimal operational disruption.

AGENT UPGRADATION

Agent upgradation pertains to the management of the Falcon sensor's software version. In Falcon Go, this process is controlled through flexible Sensor Update Policies within the cloud console, ensuring a balance between security and operational stability. Our review confirmed the platform's capability for us to set precise upgrade policies. Key options available include:

- **N-1 / N-2 Policies:** The ability to configure agents to automatically remain one or two full versions behind the latest release.
- **Fixed Version (No Upgradation):** The option to lock agents to a specific, fixed version, which is ideal for critical systems where changes must be strictly controlled.
- **Specific Older Agent Versions:** The flexibility to choose from a list of available prior sensor versions if a specific build is required for compatibility or testing purposes.

Crucially, all agent version upgrades are managed seamlessly through the console and do not require a system restart, minimizing operational disruption.

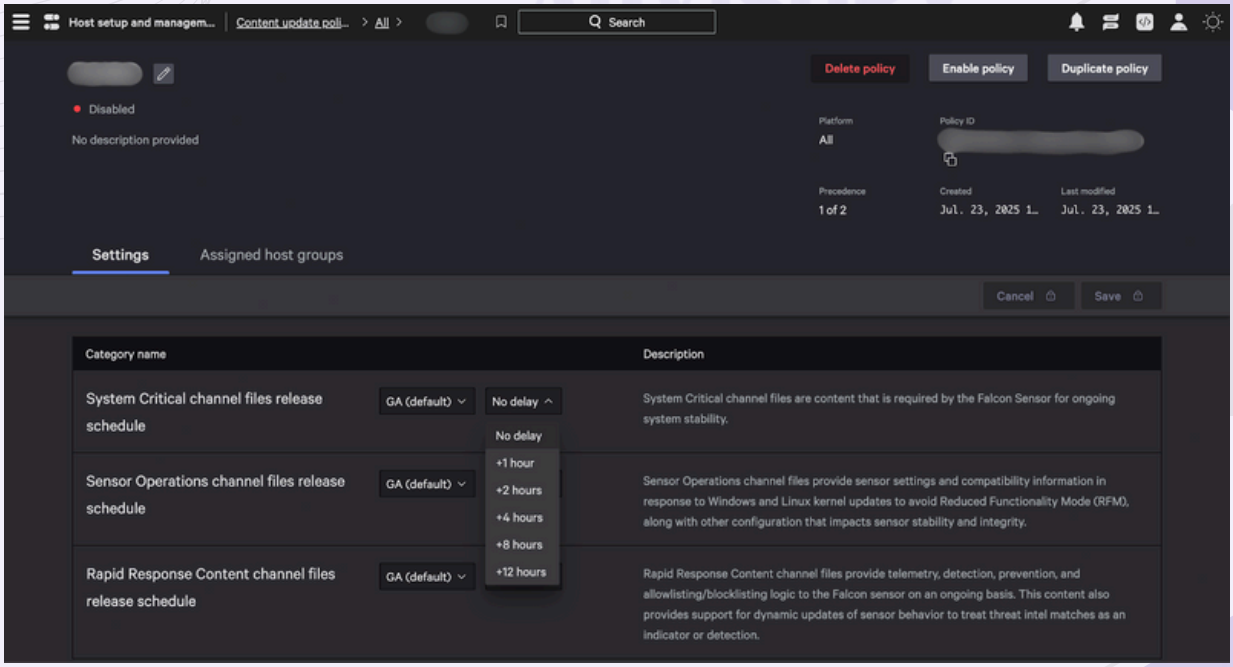


• AGENT UPDATION

Agent updation refers to the updating of threat intelligence and operational content—such as detection logic, configuration settings, and stability files—rather than the agent software itself. Our hands-on review confirms that Falcon Go provides a dedicated Content Update Policy system. This feature offers granular control over the rollout of various types of agent content, allowing for a phased deployment to ensure stability for critical systems. Through these policies, a delayed release schedule can be set for different content channels, including:

- **System Critical channel: For files essential to ongoing sensor stability.**
- **Sensor Operations channel: For sensor settings and compatibility information.**
- **Rapid Response Content channel: For telemetry, detection, prevention, and blocklisting logic.**

For each channel, an administrator can configure a specific delay (e.g., +1 hour, +4 hours, +12 hours). This capability is crucial for environments that demand maximum stability, providing a mechanism to validate new content on a pilot group before a fleet-wide release.



CONCLUSIONS

- Falcon Go offers streamlined onboarding for supported systems:
  - Windows Server 2025, 2022, 2012 R2.
  - Windows 10, 11 Enterprise editions.

- Single-executable deployment model eliminates complexity.

- Attractive for organisations seeking efficient endpoint protection.

- Clear communication for unsupported Windows 7 SP1 and 8.1 ensures transparency.

- Recommended for enterprises prioritizing rapid deployment and compatibility.

- Organizations using Windows 7 SP1 and 8.1 should upgrade to a supported OS.

- Flexible policies allow organizations to maintain N-1/N-2 automatic updates, fix versions for critical systems, or deploy specific older builds, ensuring stability with minimal disruption.

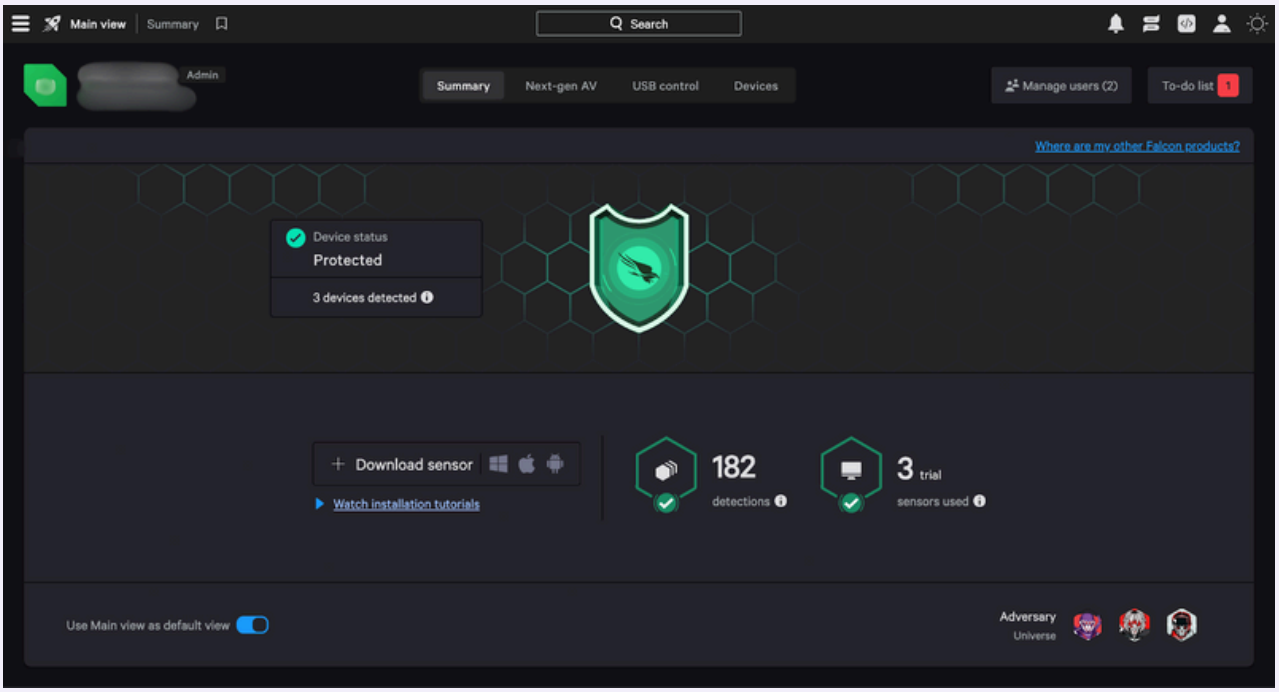
- Dedicated policies enable phased deployment of threat intelligence and operational content, allowing for validation on pilot groups before fleet-wide release. This significantly enhances operational resilience against unforeseen update issues.

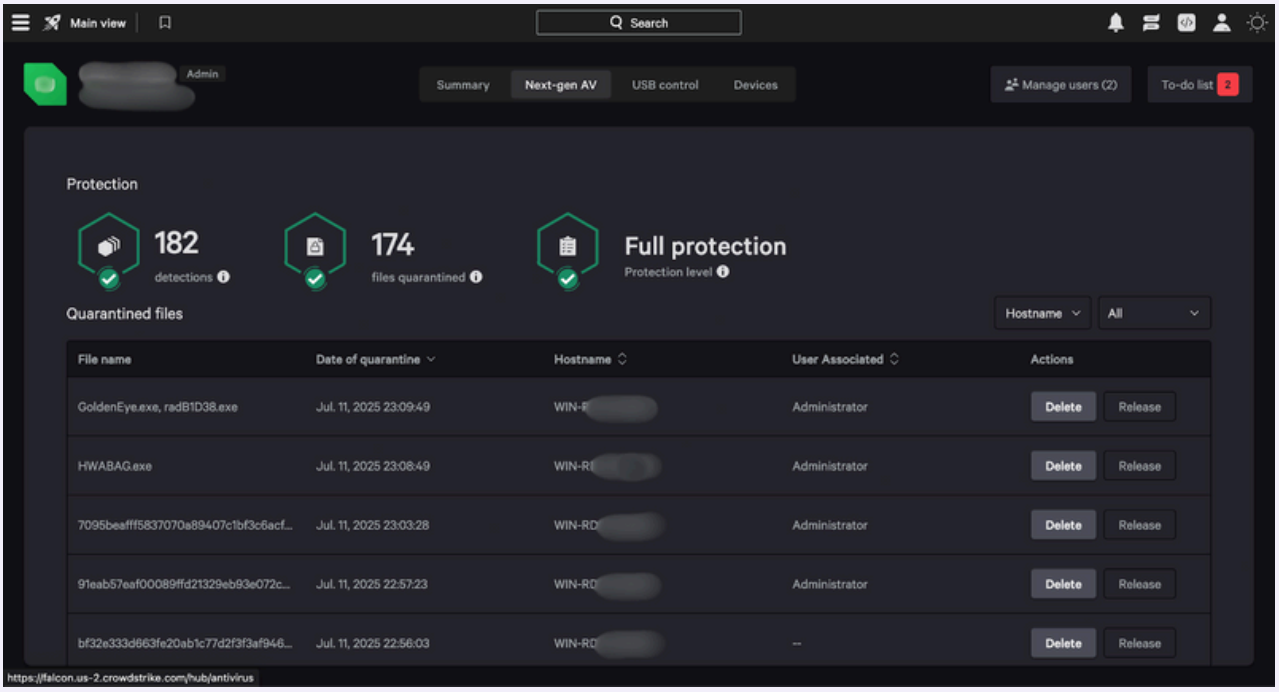
APPENDIX

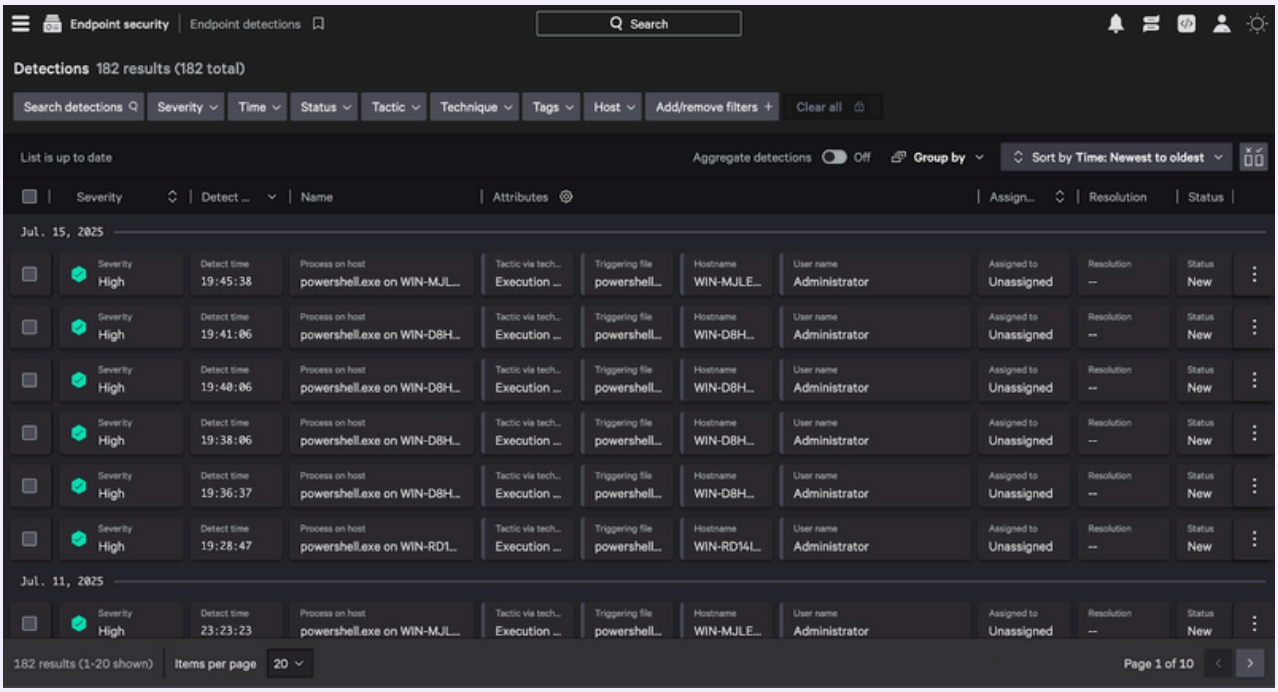
HOW DO WE CALCULATE CYBEREASE RATINGS?

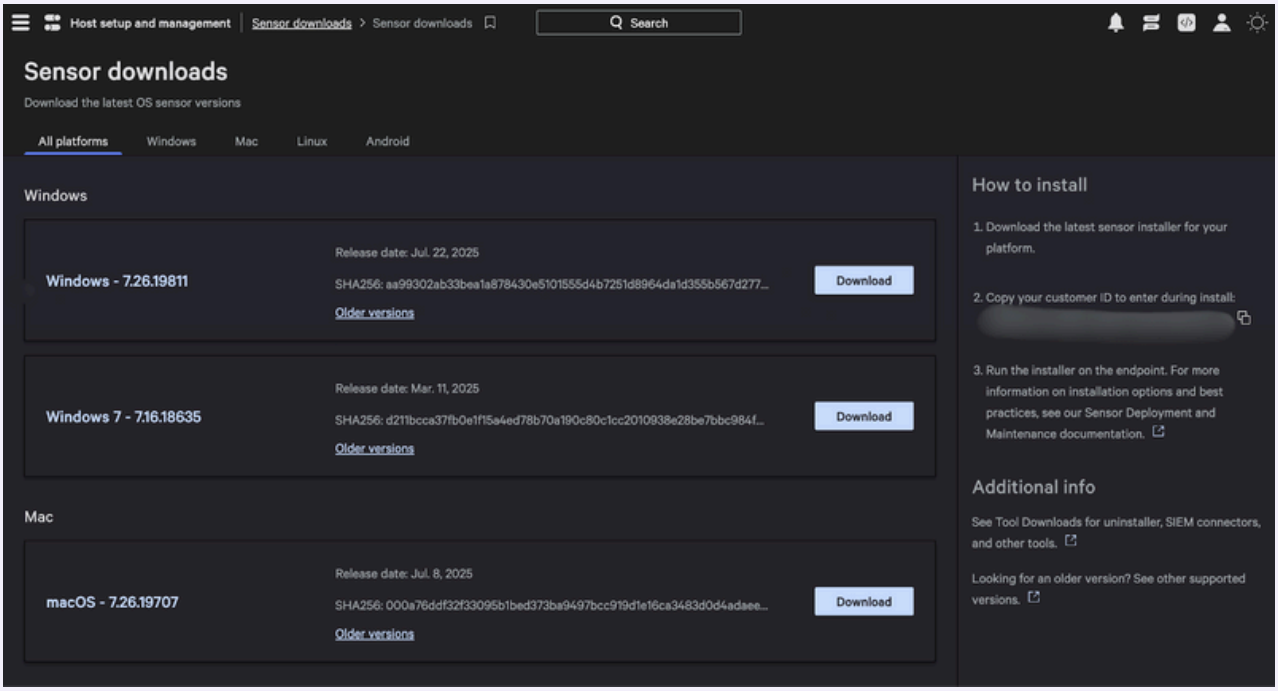
EEach star represents a distinct criterion for evaluating the onboarding experience of endpoint security solutions:

- **1 Star: Failed Onboarding Despite Claimed Support** – The operating system is documented as supported, but onboarding fails despite applying all recommended updates and configurations, even with support intervention.
- **2 Stars: Onboarding with Significant Effort** – Onboarding succeeds, and the device appears in the console, but requires extensive effort, multiple installation steps, debugging, and support interaction for undocumented updates or information.
- **3 Stars: Onboarding with Additional Configuration for Detection** – Onboarding is achieved by running a setup process, but further manual changes (e.g., installing antivirus software) are required to enable malware detection functionality.
- **4 Stars: Onboarding with Minor Documented Updates** – Onboarding is successful and the device appears in the console, but requires installation of a few minor, easily available, and well-documented updates or configurations.
- **5 Stars: Seamless Out-of-the-Box Onboarding** – Onboarding is effortless, completed out-of-the-box with no prerequisites or post-installation configurations, and the device appears instantly in the console with full functionality.


Main view
Summary
Search
Admin
Summary
Next-gen AV
USB control
Devices
Manage users (2)
To-do list 1
Where are my other Falcon products?
Device status
Protected
3 devices detected
Download sensor
Watch installation tutorials
182
detections
3 trial
sensors used
Use Main view as default view
Adversary
Universe


Main view
Search
Admin
Summary
Next-gen AV
USB control
Devices
Manage users (2)
To-do list 2
Protection
182
detections
174
files quarantined
Full protection
Protection level
Quarantined files
Hostname
All
File name
Date of quarantine
Hostname
User Associated
Actions
GoldenEye.exe, radB1D38.exe
Jul. 11, 2025 23:09:49
Administrator
Delete
Release
HWABAG.exe
Jul. 11, 2025 23:08:49
Administrator
Delete
Release
7095beafff5837070a89407c1bf3c6acf...
Jul. 11, 2025 23:03:28
Administrator
Delete
Release
91eab57eaf00089ffd21329eb93e072c...
Jul. 11, 2025 22:57:23
Administrator
Delete
Release
bf32e333d663fe20ab1c77d2f3f3af946...
Jul. 11, 2025 22:56:03
Delete
Release
https://falcon.us-2.crowdstrike.com/hub/antivirus


Endpoint security
Endpoint detections
Search
Detections 182 results (182 total)
Search detections
Severity
Time
Status
Tactic
Technique
Tags
Host
Add/remove filters
Clear all
List is up to date
Aggregate detections
Off
Group by
Sort by Time: Newest to oldest
Severity
Detect ...
Name
Attributes
Assign...
Resolution
Status
Jul. 15, 2025
High
19:45:38
powershell.exe on WIN-MJL...
Execution ...
powershell...
WIN-MJLE...
Administrator
Unassigned
New
High
19:41:06
powershell.exe on WIN-D8H...
Execution ...
powershell...
WIN-D8H...
Administrator
Unassigned
New
High
19:40:06
powershell.exe on WIN-D8H...
Execution ...
powershell...
WIN-D8H...
Administrator
Unassigned
New
High
19:38:06
powershell.exe on WIN-D8H...
Execution ...
powershell...
WIN-D8H...
Administrator
Unassigned
New
High
19:36:37
powershell.exe on WIN-D8H...
Execution ...
powershell...
WIN-D8H...
Administrator
Unassigned
New
High
19:28:47
powershell.exe on WIN-RD1...
Execution ...
powershell...
WIN-RD14L...
Administrator
Unassigned
New
Jul. 11, 2025
High
23:23:23
powershell.exe on WIN-MJL...
Execution ...
powershell...
WIN-MJLE...
Administrator
Unassigned
New
182 results (1-20 shown)
Items per page
20
Page 1 of 10


Host setup and management
Sensor downloads
Sensor downloads
Search
Sensor downloads
Download the latest OS sensor versions
All platforms
Windows
Mac
Linux
Android
Windows
Windows - 7.26.19811
Release date: Jul. 22, 2025
SHA256: aa99302ab33bea1a878430e5101555d4b7251d8964da1d355b567d277...
Download
Older versions
Windows 7 - 7.16.18635
Release date: Mar. 11, 2025
SHA256: d211bcca37fb0e1f15a4ed78b70a190c80c1cc2010938e28be7bbc984f...
Download
Older versions
Mac
macOS - 7.26.19707
Release date: Jul. 8, 2025
SHA256: 000a76ddf32f33095b1bed373ba9497bcc919d1e16ca3483d0d4adaee...
Download
Older versions
How to install
1. Download the latest sensor installer for your platform.
2. Copy your customer ID to enter during install:
3. Run the installer on the endpoint. For more information on installation options and best practices, see our Sensor Deployment and Maintenance documentation.
Additional info
See Tool Downloads for uninstaller, SIEM connectors, and other tools.
Looking for an older version? See other supported versions.

STRATEGIC FORSIGHT, HUMAN WISDOM

Contact Us:

for further information contact:
tanish@fieldciso.com or
visit us at **fieldciso.com**

PEER REVIEWED BY:

Prateek Bhajanka and Devesh Taneja

DESIGNED BY:

Tanaa Chauhan