

FIELD SECURITY REPORT

RESEARCHED AND TESTED BY:

Tanish Bhandari

SEPT 2025

EXECUTIVE SUMMARY

This report provides an in-depth evaluation of SentinelOne Singularity Control EDR onboarding across modern and legacy Windows operating systems. Testing focused on deployment simplicity, compatibility, and agent lifecycle management—critical factors in maintaining a resilient security posture amidst today’s dynamic threat landscape.

Key findings include:

- **Modern OS Seamlessness:** Windows Server 2025 (pre-release), 2022, 2019, Windows 10, and 11 onboard with near-zero friction using SentinelOne’s single-executable deployment model.
- **Legacy OS Considerations:** SentinelOne supports legacy systems Windows Server 2012 R2, Windows 7, and 8. However, they require additional updates and lack full feature parity (e.g., reduced behavioral AI and rollback capabilities).
- **Agent Lifecycle Control:** SentinelOne’s policy-driven upgrade model enables staged rollouts, mitigating risks highlighted by incidents such as the July 2024 CrowdStrike Falcon outage.
- **Purple AI Advantage:** Embedded Purple AI significantly accelerates threat hunting, root cause analysis, and response workflows, reducing mean time to detect (MTTD) and mean time to respond (MTTR) for security teams.
- **Operational Impact:** Minimal CPU and RAM overhead observed post-onboarding; performance spikes occur only primarily during initial scans which is an acceptable behaviour.

INTRODUCTION

Enterprises face increasingly sophisticated threat actors leveraging polymorphic malware, ransomware-as-a-service (RaaS), and identity-based attacks. In this environment, endpoint detection and response (EDR) platforms must balance rapid deployment with advanced threat detection and automated response.

SentinelOne Singularity Control EDR offers AI-driven endpoint protection and integrates with SentinelOne's extended detection and response (XDR) ecosystem, including Identity Threat Detection and Response (ITDR) and Purple AI-powered investigations.

This field report, prepared by [FieldCISO Advisory Services](#), evaluates onboarding experience across multiple Windows environments to help organizations plan secure, scalable deployments.

SCOPE AND METHODOLOGY

Tested Environments

Operating Systems

- Windows Server 2025 (preview), 2022, 2012 R2
- Windows 11, 10, 8, 7 (Enterprise editions)

Test Setup

- Virtualisation Platforms: Hyper-V and VirtualBox
- Hardware Baseline: 4-core CPU, 4GB RAM, 60GB SSD
- Agent Version Tested: 23.5.1.1234 (N-1 Version)

Evaluation Criteria

- Installation and onboarding simplicity
- Compatibility and error handling
- Resource consumption during and after install
- Upgrade and update policy controls
- Documentation clarity and support for legacy OS

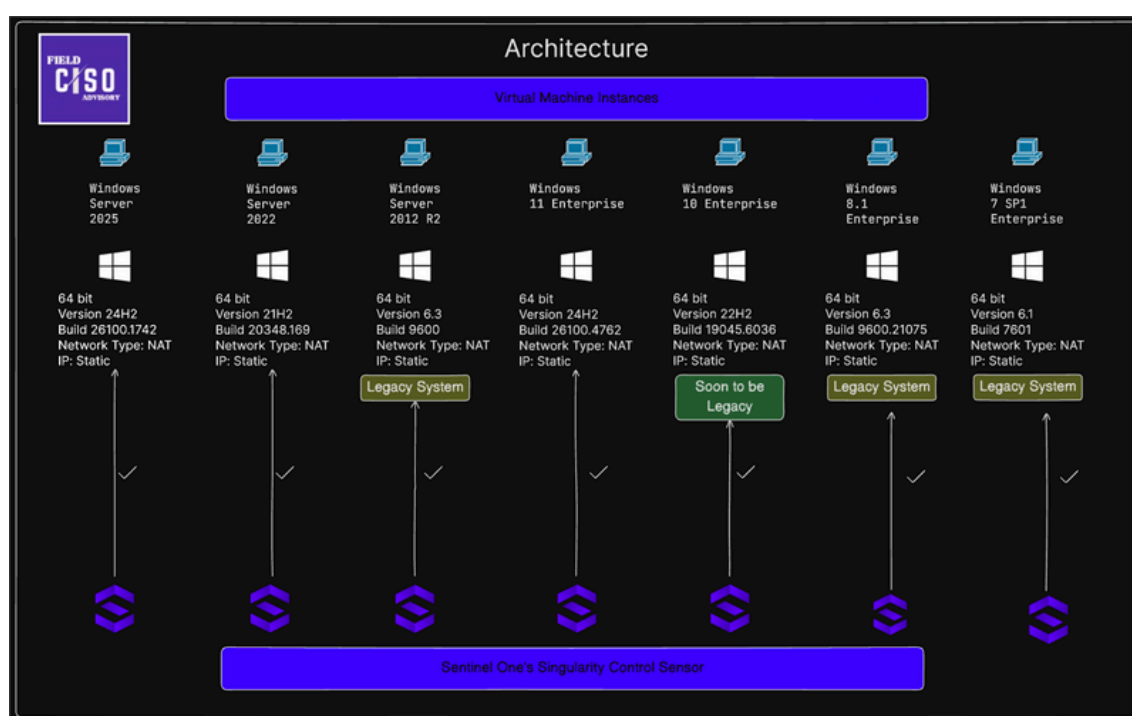
Rating System

CyberEase Rating (1–5 stars): Measures ease of deployment (1 = failed onboarding, 5 = seamless out-of-the-box).

ARCHITECTURE

SentinelOne's cloud-native architecture integrates lightweight agents with a centralized management console. Agents leverage AI-driven analytics and behavioral storyline correlation to detect and respond to threats autonomously, even offline.

Purple AI, built into the Singularity platform, simplifies every stage of the deployment journey. From the moment organizations begin onboarding, Purple AI delivers contextual guidance, step-by-step troubleshooting, and instant access to relevant support documentation. Instead of searching through manuals, administrators can ask natural-language questions and receive precise, actionable responses. By turning onboarding into a conversational experience, Purple AI accelerates rollouts, minimizes deployment friction, and ensures security teams realize value from Singularity faster.



→ can you help me onboard windows 11

- ◆ To onboard Windows 11 with SentinelOne, you need to ensure that you are using a compatible version of the SentinelOne Agent. Here are the steps to follow:

Step 1: Check SentinelOne Agent Version

1. Ensure that you have SentinelOne Agent version **21.5.2** or higher. This version fully supports Windows 11.
2. If you have an older version, you must upgrade the Agent before proceeding with the Windows 11 installation.

Step 2: Upgrade the SentinelOne Agent (if necessary)

If your current version is lower than 21.5.2, follow these steps to upgrade:

1. Download the latest version of the SentinelOne Agent from the SentinelOne Management Console.
2. Run the installer on the endpoint where you want to upgrade the Agent.
3. Follow the prompts to complete the installation.

Step 3: Prepare for Windows 11 Installation

1. **Prevent Automatic Upgrades:** To ensure a smooth transition, prevent Microsoft updates to Windows 11 on your production endpoints until you can upgrade to a supported SentinelOne Windows Agent version (21.5.2+).
2. **Backup Important Data:** Always back up important data before performing an OS upgrade.

Step 4: Upgrade to Windows 11

1. Once the SentinelOne Agent is confirmed to be version 21.5.2 or higher, you can proceed with the Windows 11 upgrade.
2. You can upgrade through Windows Update or by using the Windows 11 installation media.

Important Notes

- If you attempt to upgrade to Windows 11 with a SentinelOne Agent version lower than 21.5.2, you will receive an "upgrade blocked" message from Microsoft.
- After upgrading to Windows 11, ensure that the Agent is functioning correctly. You may need to reboot the endpoint after the upgrade.

Step 5: Verify Agent Functionality

1. After the upgrade, check the status of the SentinelOne Agent:
 - Open a command prompt and run:

```
sentinelctl.exe status
```

2. Ensure that the Agent is reporting correctly and that there are no errors.

If you encounter any issues during the onboarding process, please contact SentinelOne support for further assistance.

- [SentinelOne Help - Windows 11 Support](#) 
- [SentinelOne Help - Windows 11 22H2 Upgrades](#) 

👍 🗨 ⌚ ● Question 1 out of 20

Ask Purple AI...



Purple AI can make mistakes. Consider checking important information.

24



Singularity™
Operations Center

Global /

Cloud Native SecurityMarketplaceHelp

Search for a page

Search

Dashboards

Purple AI

TRiage

Alerts

Exposures

DISCOVER

Event Search

Inventory

Graph Explorer

Activities

AUTOMATE

RemoteOps

CONFIGURE

Detections

Agent Management

Reports

Policy & Settings

New Notebook

Filter notebooks

Shared Notebooks

Created: Aug 6, 2025 20:51

Add description...

Actions

Show me all lateral movement attempts in the last 24 hours*

✓

| filter(event.type == "Behavioral Indicators" AND indicator.description contains:anycase("Lateral Movement"))
| columns event.time, event.id, event.type, site.id, site.name, agent.uuid, src.process.storyline.id, src.process.user, src.process.uid,
src.process.cmdline, src.process.image.path, indicator.category, indicator.name, indicator.description, indicator.metadata
| sort - event.time
| limit 1000

4 results found from Aug 5, 2025 20:51:28 to Aug 6, 2025 20:51:28

Open PowerQuery

Table

Event Time	Event ID	Event type	Site ID
Aug 6 2025 09:58:42		Behavioral Indi...	225675088854

Ask Purple AI...

Purple AI can make mistakes. Consider checking important information.

FIELD CISO ADVISORY

FIELD SECURITY REPORT 2025

7

Onboarding Experience by Operating System

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

FIELD CISO ADVISORY On boarding experience comparison				
Operating System	Onboarding Method	Official Support	Remarks	CyberEase Rating
Windows Server 2025	Single Executable	☒ Yes ▾	Seamless; completed in <5 min; effortless integration with management console.	★ ★ ★ ★ ★ (5/5)
Windows Server 2022	Single Executable	☒ Yes ▾	Seamless; completed in <5 min; effortless integration with management console.	★ ★ ★ ★ ★ (5/5)
Windows Server 2012 R2	Single Executable	☒ Yes ▾	Required 4 manual Windows updates as indicated by SentinelOne installer error messages; completed in <10 min with smooth integration.	★ ★ ★ ★ ☆ (4/5)
Windows 11 Enterprise	Single Executable	☒ Yes ▾	Seamless; completed in <3 min; fully automated, no additional configuration needed.	★ ★ ★ ★ ★ (5/5)
Windows 10 Enterprise	Single Executable	☒ Yes ▾	Seamless; completed in <3 min; fully automated, no additional configuration needed.	★ ★ ★ ★ ★ (5/5)
Windows 7 Enterprise	Single Executable	☒ Yes ▾	Required 4 manual Windows updates as indicated by SentinelOne installer error messages; completed in <10 min with smooth integration.	★ ★ ★ ★ ☆ (4/5)
Windows 8 Enterprise	Single Executable	☒ Yes ▾	Required 4 manual Windows updates as indicated by SentinelOne installer error messages; completed in <10 min with smooth integration.	★ ★ ★ ★ ☆ (4/5)

PERFORMANCE IMPACT ANALYSIS

CPU and RAM Usage

- During Install: 8–15% CPU, 150–250 MB RAM spike for ~5 min
- Post-Onboarding Initial Scan: 10–20% CPU for 10–15 min
- Steady State: 1–4% CPU, 80–150 MB RAM

Note: Observations reflect virtualized lab conditions; physical deployments may show lower baseline impact.

Disk and Network I/O

- 10–40 MB network transfer during policy registration
- Light disk I/O for driver and policy configuration
- No reboot required in most cases; may be prompted for driver-level changes on older OS

Proactive Controls and Agent Management in the Wake of the CrowdStrike Incident

The CrowdStrike incident on July 19th highlighted the complexities of managing endpoint protection platforms (EPP) in modern cybersecurity, particularly the need for granular control over agent software and the continuous stream of threat intelligence updates. This event emphasized the importance of robust controls within EPP solutions like SentinelOne Singularity Control EDR to strengthen security posture and ensure operational resilience. With this in mind, our detailed review of SentinelOne Singularity Control EDR focused on its agent management capabilities, categorized into Agent Upgradation and Agent Updation, designed to provide precise lifecycle management with minimal disruption.

Agent Lifecycle and Update Management

The screenshot shows a 'Create Auto Upgrade Policy' window with a dark theme. On the left is a vertical sidebar with four steps: 'Policy Details' (selected with a blue circle), 'Policy Settings', 'Impacted Endpoints', and 'Summary'. The main area is titled 'Policy Details' and contains the following fields:

- OS Type:** A dropdown menu currently showing 'Windows' with the Windows logo.
- Name:** A text input field containing 'Smart-Updates'.
- Description (Optional):** A larger text input field with the placeholder text 'Enter description...'.

At the bottom left of the window is a 'Cancel' button, and at the bottom right is a 'Next' button.

Global / [Progress Bar]

Create Auto Upgrade Policy

✓ Policy Details

● Policy Settings

○ Impacted Endpoints

○ Summary

Policy Settings

Version

Select Version

Maximum number of retries if upgrade fails

5

Update Schedule

☐ Effective Immediately ☒ Maintenance Window

Cancel

Back

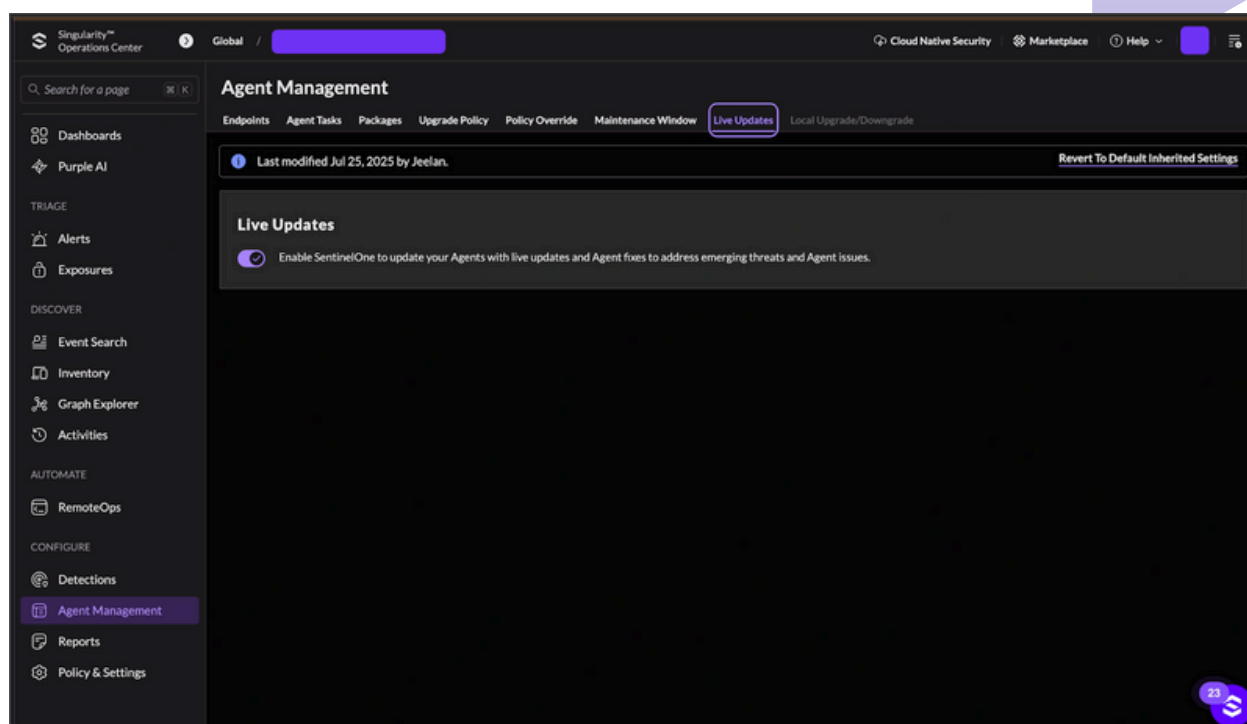
Next

Agent upgradation

Agent upgradation focuses on overseeing the software version of the Singularity agent, with SentinelOne providing a thoughtfully designed strategy through adaptable upgrade policies accessible via the cloud console to ensure a balance of security and system stability. Key features include:

- **Smart Policies:** Agents are automatically (after first being declared by the admin) set to adopt the latest update for testing in a controlled environment, with n-1 deployed in production and n-2 maintained as a fallback for added reliability.
- **Fixed Version (No Upgradation):** Capability to pin agents to a specific version, perfect for critical systems where stringent change management is essential.
- **Specific Older Agent Versions:** Option to choose from an extensive range of prior sensor versions to meet compatibility or testing requirements.
- Administrators can define precise upgrade policies, targeting users based on operating system, groups, or profiles, with the flexibility to apply policies immediately or schedule them within a maintenance window—a designated low-impact period to minimize operational disruption.
- All upgrades are executed smoothly through the console, eliminating the need for system restarts and reducing overall impact on operations.

Agent Updation



Threat Intelligence Updates

- Distinct from version upgrades; deliver new IOCs, heuristics, and behavioral models
- Can be toggled or delayed for validation before enterprise-wide deployment

This granular control directly mitigates risks exemplified by the **CrowdStrike Falcon July 2024 outage**, where uncontrolled content updates triggered global BSOD events.

CONCLUSIONS

SentinelOne Singularity Control EDR demonstrates exceptional onboarding efficiency across modern Windows environments, significantly reducing IT overhead and accelerating time-to-protection. Its single-executable deployment and intelligent policy management streamline rollout even in large-scale enterprises.

Key advantages observed:

- Seamless deployment on Windows 10/11 and Server 2022+
- Robust lifecycle controls preventing uncontrolled upgrades
- Purple AI-driven threat hunting and response drastically improves SOC productivity
- Legacy OS support provides baseline protection but lacks advanced rollback and AI features

Recommendations:

- Prioritize modern OS adoption to fully leverage SentinelOne's advanced capabilities
- Use staged upgrade policies and fixed-version pinning for mission-critical workloads
- Leverage Purple AI for continuous threat hunting and executive-level reporting
- Plan phased decommissioning of Windows 7/8 to mitigate legacy threat exposure

APPENDIX

How We Calculate CyberEase Ratings

CyberEase Ratings measure the ease and reliability of onboarding SentinelOne agents across different operating systems. Ratings consider installation effort, compatibility, and post-onboarding functionality, including threat detection and visibility in the management console.

- **1 Star – Failed Onboarding Despite Claimed Support**

- The operating system is documented as supported, but onboarding fails despite applying all required updates and following SentinelOne guidance. Even with vendor support intervention, the agent cannot be deployed or fails to register in the console.

- **2 Stars – Onboarding with Significant Effort**

- Onboarding succeeds and the endpoint appears in the management console, but the process requires extensive troubleshooting (e.g., undocumented patches, driver signing issues) or multiple manual steps beyond standard deployment procedures.

- **3 Stars – Onboarding with Additional Configuration for Threat Visibility**

- Installation succeeds, but additional manual configuration (e.g., enabling detection policies, applying kernel-level updates, or modifying endpoint security settings) is required to achieve full threat detection and response capabilities.

- **4 Stars – Onboarding with Minor Documented Updates**

- Onboarding is successful and the endpoint registers in the console, but requires minor, well-documented updates or patches (e.g., Windows KB updates) that can be applied quickly without major operational disruption.

- **5 Stars – Seamless Out-of-the-Box Onboarding**

- is **fully automated and effortless**; the endpoint appears in the Onboarding console with complete functionality and no manual pre- or post-installation steps required. Full threat detection and response capabilities are available immediately.



STRATEGIC FORSIGHT, HUMAN WISDOM

Contact Us:

for further information contact:
tanish@fieldciso.com or

visit us at **fieldciso.com**

PEER REVIEWED BY:

Prateek Bhajanka ,Devesh Taneja and Tanaa Chauhan

©FIELD CISO ADVISORY 2025