HarfangLab

# HARFANGLAB
# SAFE DEPLOYMENT PRACTICES

**Ref :** Safe Deployment Practices
**Date :** 8th of April, 2026
**Version :** 1.2

# I – INTRODUCTION

HarfangLab provides endpoint security solutions to businesses and public organisations. These solutions are comprised of an agent software that is compatible with Windows, Linux and macOS and a cloud or on-premises manager instance to which each agent is connected and configured.

Deployments of both the manager instance and the agent are distinct, and each follow their own staged rollout onto HarfangLab's cloud and on-premises customers.

Agents are provided with threat intelligence data which is also updated through a custom staged mechanism.

# II – TESTING

HarfangLab solutions are tested extensively on all supported environments (Windows, Linux and macOS) including all supported Windows versions (from Windows 7 to the latest Windows 11 version for workstations and from Windows 2008 R2 to the latest Windows 2025 version for servers).

Multiple times per day, HarfangLab provisions virtual testing environments for each supported operating system and runs a series of unit, integration and end-to-end tests to ensure that HarfangLab solutions (following list not exhaustive):

- Correctly run on the target OS and version.
- Can connect to its manager instance, upgrade and rollback to previous versions.
- Can correctly detect and remediate malware.
- Has a limited, manageable and measurable impact on the host's performance.
- Does not cause any system crashes or instability.

The same series of tests, in addition to extensive manual testing by HarfangLab's QA team, is applied to each new version of the solutions before starting deployment in the phases described in chapter III.

## III – MANAGER UPDATE PHASES

HarfangLab solutions features the following stages of deployment:

1. Pre-release: a new release of the solutions is built and tested internally:
   a. Phase a: all features of the solutions are automatically end-to-end tested on all OS versions supported by the solutions, then a manual testing suite is applied.
   b. Phase b: the new version of the solutions is deployed in testing and lab environments featuring real-user interaction.

2. Initial version release: if the pre-release testing stage is a success, the new version is deployed on a small portion of devices covered by the solutions in waves, to customers that explicitly accepted the level of risk. Activity on updated hosts is tightly monitored through HarfangLab's alerting & monitoring software so that updates featuring critical or high severity bugs are quickly stopped during rollout.

3. Main update rollout: wave by wave (by order of criticity), customers are updated with the new version of the solutions. The same monitoring mechanism is applied, and HarfangLab can stop the update at any moment.

4. On-premise update rollout: once the update has been deployed on all cloud customers for 1-month time, the release is ready to be shipped to on-premises customers.

## IV – AGENT UPDATE

Once the manager has been updated, customers are eligible to update their agent to the latest version. HarfangLab solutions features agent update strategies through its manager configuration.

Customers can choose the speed of the update rollout, which group of agents should be updated first, and the update channel the host should follow (latest or stable).

Should updates fail:

- HarfangLab includes a circuit breaker mechanism that automatically monitors newly updated agents and can, if a certain threshold of agents fails to update, block any further updates.
- HarfangLab installer can stop the update mechanism and rollback to a previous stable version.

It is important to note that the final customer has full control over its agent update strategy and can choose not to update, partially or fully update its entire IT. HarfangLab provides a fully featured and safe configuration mechanism for update strategies allowing manager administrators to align their update strategies with their own organization's internal policies.

Since HarfangLab is a **B2B-only security solution** and not a publicly available consumer software, the solution does not cover personal computers and therefore will not update automatically on personal computers. Enterprise update strategies are controlled in conjunction with the customer and HarfangLab to ensure a smooth, safe and controlled update process.

## V – THREAT INTELLIGENCE UPDATE

HarfangLab's threat intelligence data is updated daily via the manager the instance, which is centrally connected to HarfangLab's update servers. The threat intelligence is updated in the following stages:

1. The threat intelligence update is unit tested in HarfangLab's testing framework and manually tested by a detection engineer to ensure that the detection logic update correctly detects the targeted threat and does not impact existing detection logic.
2. A detection logic update is first sent silently (without direct impact to the customer) to a non-critical wave of customers. Alerting is put in place to monitor the rule's impact of agents of updated customers.
3. The silent detection logic update is rolled out more broadly. Same monitoring applies.
4. If the rule did not generate system crashes, instability and did not cause detection issues (false positives), the update is then made public.

Should a threat intelligence update cause instabilities inducing boot loops on a single host, the agent can locally put itself in a "minimal mode" to disable features that can cause system instabilities and therefore make the system recoverable.

HarfangLab features a very transparent threat intelligence interface allowing customers to have full control over the contents and blocking or detection behavior of each detection rule. This implies that customers can disable or reconfigure HarfangLab's detection rules and can therefore choose to ignore HarfangLab's threat intelligence updates.

## VI – **MONITORING**

HarfangLab closely monitors current cloud and on-premises (for customers that allow it) instances as well as rollouts of new updates.

HarfangLab is able to closely monitor:

- OS stability through RAM and CPU consumption of hosts and automatic internal logging mechanisms.
- Stability of cloud and on-premises instances.
- Possible HarfangLab-caused system crashes and instabilities through automatic minidump collection.
- False positives or detection instabilities caused by threat intelligence updates.

All these indicators are linked to alerts that can be handled by HarfangLab's Devops team to either stop rollout or trigger an incident should they need investigating.

## VII – **COMMUNICATION**

Since HarfangLab is a **B2B-only security solution** and not a publicly available customer software, we do not provide a publicly accessible communication page detailing any instabilities or future updates in HarfangLab's infrastructure or deployments.

Customers are individually notified of future deployments through both an email to the main customer contact and through a notification in the manager console.

Feedback is obtained through our internal support ticketing system that customers all have access to.

harfanglab.io

HarfangLab