IKARUS anti.virus
Safe Deployment Practices

Version: 1.0
Date: 18 03 2025

Content

Version history

2025-03-18, v1.0

IKARUS anti.virus: Safe Deployment Practices

IKARUS develops cybersecurity solutions that help businesses, critical infrastructure, and government organizations protect their data, systems, and devices from malware and cyberattacks.

- **Engine:** At the heart of all developments is the IKARUS Malware Scan Engine, providing cross-platform protection and reliable security even in offline environments. It is continuously enhanced to integrate new technologies and counter emerging attack techniques, with a strong focus on maximum performance and stability.
- **Content:** Virus databases contain detection data ranging from specific signatures to complex behavioral descriptions, enabling proactive malware detection. Known threats and exploits can be immediately identified and isolated during the initial scan, without the need for time-consuming analysis. To ensure the most up-to-date protection, new detection data is incorporated several times a day through frequent updates.
- **Application:** Users can configure their cybersecurity solutions and take targeted actions to assess, maintain, or restore security via software or a cloud interface. Regular updates ensure optimization, compatibility with new systems, bug fixes, and the integration of new features.

System Integration: Best Practices for Antivirus Provider

Through deep system integration, antivirus solutions are directly integrated into key operating system components and application processes. They monitor files, processes, and memory activity in real time to detect suspicious activity and block malicious files or threats before damage occurs.

Following Microsoft's best practices for security providers, IKARUS anti.virus uses an optimized, lightweight kernel driver that integrates security sensors and reliably enforces protection measures. Meanwhile, updates, parsing and configuration services, and operational management run in user-space mode, enabling faster and more targeted content updates while preventing system outages.

In addition, all updates undergo an intensive testing phase and a multi-stage rollout process to ensure effective, stable, and non-disruptive deployment to end users. The combination of rigorous quality assurance, phased rollout, and continuous optimization ensures a resilient and future-proof security architecture.

Extensive Testing Process

Before each release, the software undergoes a structured testing process that is continuously adjusted and optimized to reflect current operating conditions and integrate new features. To ensure compatibility, all supported and relevant systems are tested, including server and client operating systems, both on virtual machines (VMs) and physical hardware.

Because of the complex nature of the system landscape, load scenarios and edge cases play a critical role in ensuring that updates are stable and secure, even under heavy load and in unique system configurations.

The integrity and stability of new software releases is ensured through targeted testing, including:

- Auditing: Systematically review code and architecture for security risks and compliance requirements.
- Static Code Analysis: Automated analysis of source code to identify vulnerabilities, errors, or inefficient structures.
- Fuzzing: Testing the software with random or manipulated inputs to detect unexpected behavior, crashes, or security vulnerabilities.

These measures help identify and address potential vulnerabilities before deployment.

Staged Rollout

To minimize risks in the update process, the core components of the solutions—Engine, Content, and Application—are typically released and distributed separately. A defined **multi-stage rollout** process ensures a controlled deployment and enables early error detection.

If problems occur, the update in progress is immediately halted and a detailed investigation is initiated. The root cause is identified, and appropriate countermeasures are implemented before the update is safely resumed.

New **product features** are rolled out gradually to ensure smooth deployment and stable performance. A feature flagging mechanism is used to selectively enable functionality for specific user groups or environments.

This controlled release enables early collection and evaluation of customer feedback, allowing for improvements and adjustments as needed. As a result, new features can be delivered in a stable, optimized, and targeted manner based on demand.

Binary updates (Application and Engine) undergo an intensive internal testing phase before being gradually released to an Alpha test group, followed by a Beta test group. Feedback from these test groups, along with data from the monitoring system, is incorporated into the subsequent rollout process.

Before the update is rolled out globally, a **Canary Release** is conducted, where the new version is initially released to only 1–5% of users. This allows for stability validation in a real production environment with limited exposure.

If unexpected issues arise, the deployment can be paused or optimized. During this phase, ongoing feedback is analyzed to identify and address potential issues early, ensuring a stable final release for the entire user base.

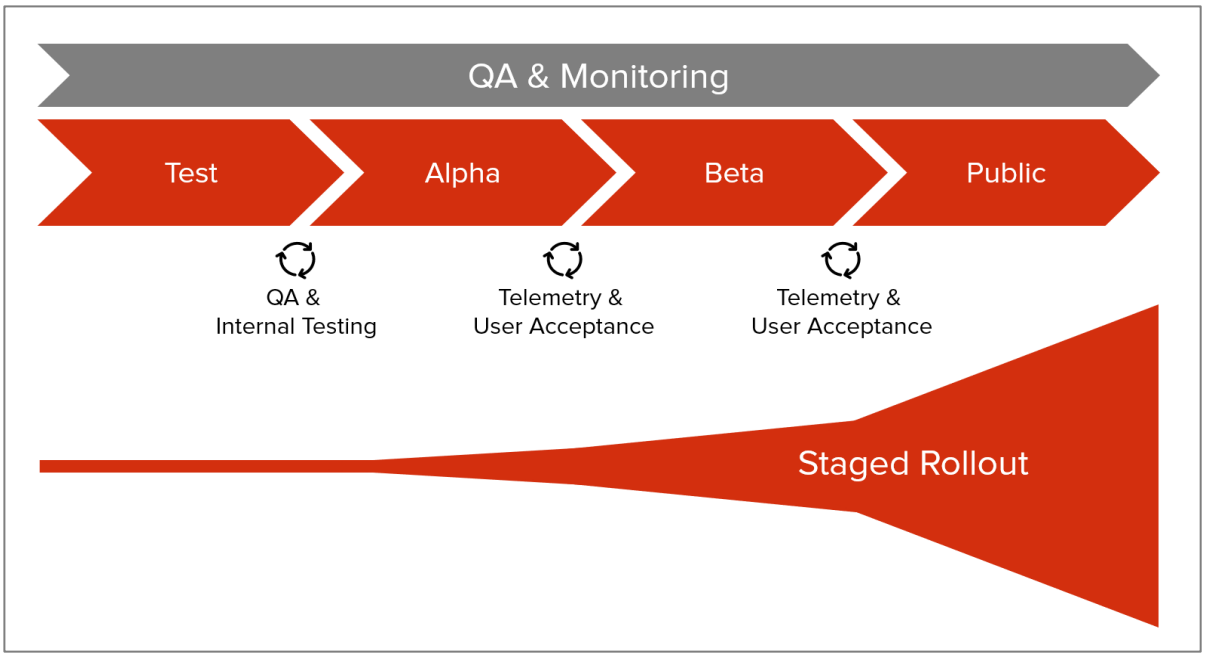

Fig. 1: Rollout Process for Binary Releases

Content updates, including virus database updates, are also distributed through a staged rollout process. After an extensive internal testing phase, deployment occurs gradually—first to internal deployments, then to managed services, and finally to on-premises solutions.

Continuous feedback loops are used to identify and resolve potential problems early to ensure stable and reliable update distribution.

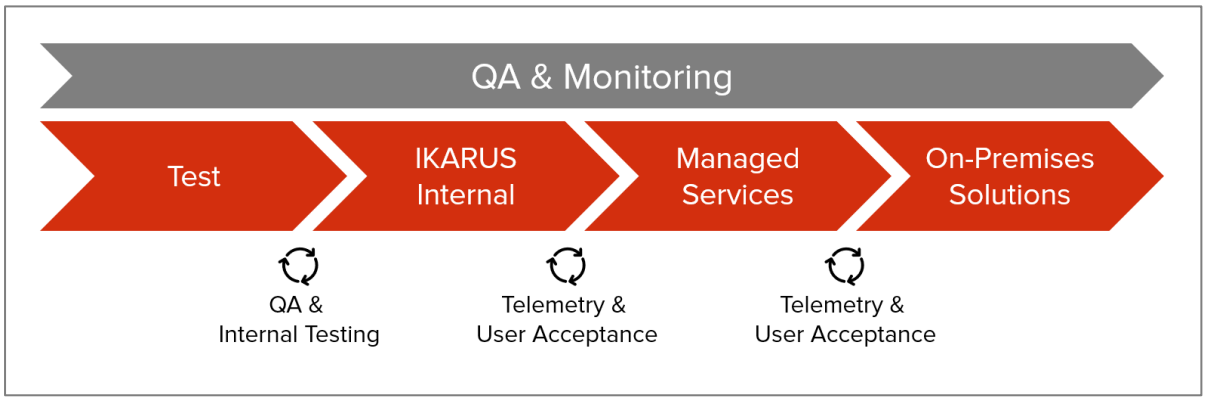

Fig. 2: Rollout Process for Content Updates

Monitoring and Optimizations

A central monitoring system monitors both ongoing operations and the deployment of new software versions and components at all stages. Defined processes ensure a smooth transition between rollout phases, allowing optimization opportunities to be identified early and exploited effectively.

An integrated anomaly detection system identifies unusual patterns that may indicate potential issues and automatically triggers countermeasures or investigative processes. Additionally, telemetry data is used to detect unexpected effects or deviations in real-time, allowing for rapid adjustments.

Continuous system metrics monitoring helps identify optimization opportunities, enabling targeted improvements to process and performance.

Recovery Strategies

Before making changes to software components, Windows snapshots are automatically created to quickly and automatically restore a previous system state. This allows users to recover from unexpected problems and prevents unintended shutdowns or system failures. In addition, new virus databases are checked for integrity before they are loaded, eliminating the possibility of corrupt or damaged updates.

Additionally, disaster recovery processes are implemented to initiate structured restoration procedures in the event of serious disruptions or system failures, ensuring a rapid recovery of full operations.

A rollforward strategy ensures that problematic updates can be reverted to a stable state without requiring a full rollback. Potential errors are addressed through targeted corrective updates—without downtime or manual intervention. In case of severe startup issues, Windows can automatically revert to the last known working configuration using the "Restore Previous System Configuration" function.

An Incident Response Team is available for a rapid response to security critical incidents. It analyzes threats in real time, implements immediate countermeasures, and secures affected systems. Fast remediation strategies enable the prompt resolution of vulnerabilities, ensuring system integrity and uninterrupted operations.

The effectiveness of rollback, rollforward, and recovery processes is regularly tested through failure simulations and stress tests. Based on the test results, processes, systems, and response strategies are continuously optimized to ensure fast and reliable recovery in critical situations.

The current and previous software versions are always available for download on the IKARUS website, allowing users to seamlessly revert to a previous version if needed.

Communication & Support

Relevant information about the current software version, releases, service status, and known issues is published on the IKARUS Website. Additionally, users and partners are informed about product updates via technical newsletters and, if necessary, through service providers.

For questions, feedback, feature requests, bug reports, and support, the IKARUS technical support team is available by phone and email.

Direct support from the manufacturer provides users and partners with direct access to in-depth technical and product knowledge, rapid problem resolution, and customized support for their specific system environment and usage. Complex issues can also be escalated directly to development teams for efficient resolution.

Resources:

- IKARUS Status Overview: www.ikarussecurity.com/status
- Support Information: https://www.ikarussecurity.com/support/
- Technical Newsletter: https://www.ikarussecurity.com/support/ikarus-info-mailings/
- IKARUS Contact data: https://www.ikarussecurity.com/kontakt/