Safe Deployment Practices (SDP) Document

For TrustOne Endpoint Antivirus Product Virus Pattern Release

1. Introduction

To ensure end-user security and system stability, our company strictly follows Microsoft-recommended Safe Deployment Practices (SDP) in the virus pattern release process for TrustOne endpoint antivirus products. This document describes our virus database update strategy, verification mechanisms, rollback plans, and exception response procedures, with special integration of a comprehensive false positive prevention system. Through multiple mechanisms including technical protection, ecological cooperation, and emergency response, we achieve a balance between security and accuracy in virus pattern releases. This process also complies with internal release specification P594, includes pre-production (pre-opr) verification, and supports rollback capabilities for both management console and endpoint agents.

2. Tenets of Safe Deployment Practices

2.1 Roll out changes progressively

We implement a multi-stage virus pattern update mechanism to ensure updates undergo sufficient verification before wide deployment:

- **Internal Testing Phase**: All virus database updates must be verified in internal testing environments, including static analysis, dynamic sandbox testing, and performance testing. In particular, automated verification is conducted on the full white sample library (2 billion+) through the false positive prevention server cluster to ensure detection by core engine multiple protection mechanisms (see section 2.5 for details).
- **Pre-production (pre-opr) Verification**: According to internal release process P594 requirements, virus patterns must undergo real-scenario verification in the pre-production environment (pre-opr) before official release, covering 10% of endpoint nodes in the production environment, with focus on monitoring false positive rates and system resource usage.
- **Canary Release**: Initially released to a small number of internal endpoints and controlled external test customers (<5%). Special monitoring items are set (e.g., false positive rate, memory usage, CPU peaks).
- **Progressive Expansion**: If the Canary phase is stable without anomalies, gradually release to more endpoints (25%, 50%, 100%). Each phase maintains an observation window (e.g., 2 hours ~ 1 day) to ensure no issues before proceeding to the next phase.

2.2 Treat every change to production equally

All virus database updates, whether major virus rules or minor fixes, follow the complete release process uniformly. Before updates, they must include:

- Automated test results (including false positive prevention system verification report)
- Signature verification (digital signature)
- **Internal release process P594 compliance checklist**

2.3 Automate validation and rollback

- **Automated Verification**: CI/CD pipelines trigger automated testing, including virus identification accuracy and false positive rate regression testing. **The false positive prevention server cluster implements full/incremental verification switching through hot and cold systems**: Full releases use Hive/Spark analysis engines to complete billion-level white sample coverage verification, while incremental releases achieve 2-hour rapid verification through popular sample libraries.
- **Automatic Rollback Mechanism**: If false positives, performance degradation, or other issues occur during the Canary phase, automatic rollback will be triggered immediately. All endpoints retain the previous version of the virus database to ensure 100% rollback capability.
- **Dual-direction Manual Rollback Capability**:
  - **TrustOne Management Console**: Supports administrators to trigger one-click virus pattern rollback for all or specified ranges of endpoints, with rollback instructions pushed to endpoint agents through encrypted channels.
  - **Endpoint Agent Local Rollback**: Endpoints have a built-in virus pattern version management module, allowing users to manually select rollback to the previous version through the Agent interface, with rollback process independent of network connectivity.

2.4 Integrated False Positive Prevention

2.4.1 Ecological Cooperation and White Sample Library Construction

- Establish long-term cooperation with system vendors to **synchronize operating system distribution updates weekly**, automatically collect and analyze white samples to ensure zero false positives for key files of domestic systems.
- Build a white sample library covering 500+ operating systems (Windows/Linux/UOS, etc.) and 100+ intelligence sources, storing over 60 million popular white samples, with false positive rate controlled below 0.01%.

2.4.2 Core Engine Triple Protection Mechanism

- **System Critical File Protection**: Ensure zero false positives for system files through critical path filtering, whitelisting of 100,000+ critical files, and real file type filtering.

- **Operating System API Double-check**: Call system APIs such as SFC (System File Checker) to reconfirm file legitimacy and prevent misjudgment of critical files.
- **Trusted Signature Publisher Verification**: Built-in whitelist of over 2000 trusted digital signature publishers (Good Company List), confirming legitimacy by parsing PE file signatures.

3. Risk Control and Rollback Strategy

All virus database versions have unique version numbers, signatures, and release time records. Every update supports one-click rollback on either the endpoint or server side. Automatic rollback is triggered when false positive rate exceeds 0.01% or system resource usage peaks exceed thresholds, with simultaneous emergency cloud virus pattern fixes pushed through the false positive prevention platform.

- **Rollback Trigger Conditions**:
  - Automatic Trigger: False positive rate > 0.01%, CPU usage > 80% for 5 minutes, memory usage > 500MB
  - Manual Trigger: Initiated through management console or endpoint agent
- **Rollback Data Assurance**: Endpoints locally cache the latest 3 versions of virus database files to ensure rollback capability to historical versions even in offline environments.