



**TÀI LIỆU MÔ TẢ SAFE DEPLOYMENT  
PRACTICES (SDP)**

**Sản phẩm:** SecurityBox Antivirus

**Đơn vị phát triển:** Công ty Cổ phần An toàn Thông tin MVS

## 1. Mục đích và phạm vi

Tài liệu này mô tả **Chương trình Triển khai Phần mềm An toàn** (Safe Software Deployment Program – SDP) của Công ty Cổ phần An toàn Thông tin MVS đối với sản phẩm **SecurityBox Antivirus**.

Mục tiêu của SDP:

- Đảm bảo mọi bản cập nhật (engine, driver, module bảo vệ, cơ sở dữ liệu nhận diện mã độc, thành phần quản lý trung tâm...) được triển khai **an toàn, có kiểm soát**, hạn chế tối đa rủi ro gây gián đoạn cho khách hàng.
- Giảm thiểu nguy cơ sự cố nghiêm trọng như: hệ điều hành không khởi động được, treo máy hàng loạt, mất kết nối mạng, xung đột với sản phẩm Microsoft hoặc phần mềm phổ biến khác.
- Thiết lập quy trình **giám sát, phát hiện sớm, thu hồi nhanh và cải tiến liên tục** dựa trên dữ liệu vận hành và phản hồi của khách hàng.
- Đáp ứng yêu cầu về **Safe Deployment Practices** trong chương trình Microsoft Virus Initiative (MVI), đồng thời phù hợp với các khuyến nghị của CISA/FBI/ACSC về triển khai phần mềm an toàn và NIST Secure Software Development Framework (SSDF).

Phạm vi bao gồm:

- Cập nhật **engine/chương trình chính** SecurityBox Antivirus trên Windows (endpoint, máy trạm, máy chủ).
- Cập nhật **cơ sở dữ liệu nhận diện mã độc**.
- Cập nhật **thành phần tích hợp** (agent thu thập log, console quản lý tập trung...).
- Cập nhật **cấu hình mặc định** được phân phối qua hệ thống cập nhật tự động.

## 2. Nguyên tắc chung và khung tham chiếu

Chương trình SDP của MVS được thiết kế theo các nguyên tắc:

### 1. Ưu tiên an toàn & lấy khách hàng làm trung tâm

Mọi quyết định triển khai được ưu tiên dựa trên **an toàn, ổn định và trải nghiệm khách hàng**, không chỉ dựa trên tốc độ phát hành.

### 2. Triển khai đa giai đoạn, có kiểm soát

Các bản cập nhật quan trọng được triển khai theo nhiều lớp: **Triển khai nội bộ** → **Triển khai thí điểm** → **Triển khai mở rộng có kiểm soát** → **Triển khai toàn bộ**, với ngưỡng dừng phát hành và thu hồi rõ ràng.

### 3. Đo lường & bằng chứng

Quyết định phát hành/thu hồi dựa trên **dữ liệu đo lường** (tỷ lệ crash, BSOD, CPU/RAM, tỷ lệ update lỗi, số lượng phản hồi lỗi, false positive...) thay vì cảm tính.

### 4. Phân tích sự cố và “suýt sự cố”

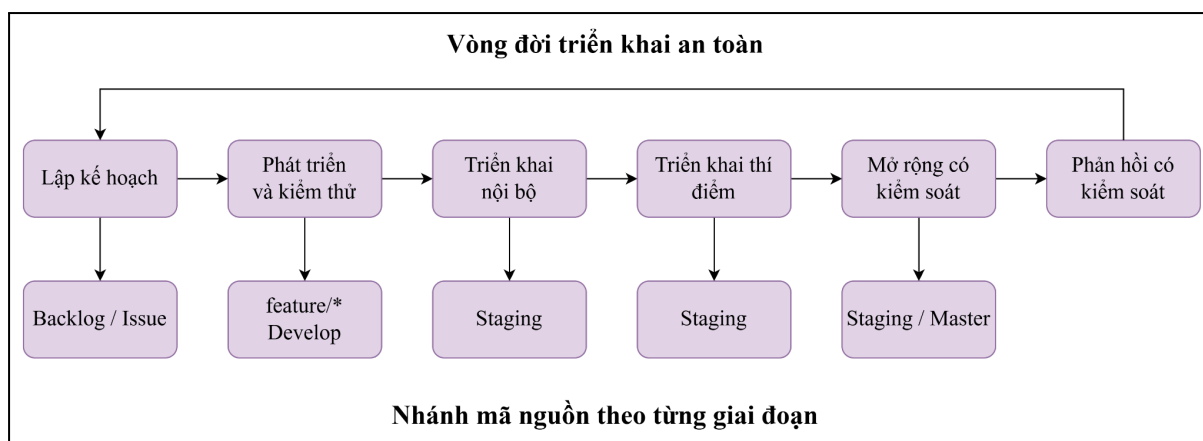
Mọi sự cố và các tình huống suýt trở thành sự cố (near-miss) đều được ghi nhận, phân tích và rút kinh nghiệm trên cơ sở *không đổ lỗi cá nhân* (blameless), nhằm mục tiêu cải thiện quy trình và chất lượng sản phẩm.

### 5. Phù hợp chuẩn và hướng dẫn quốc tế

SDP được xây dựng tham chiếu:

- Tài liệu *Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers* của CISA, FBI, ACSC. [Internet Crime Complaint Center+1](#)
- NIST SP 800-218 – Secure Software Development Framework (SSDF). [NIST Computer Security Resource Center+1](#)

## 3. Mô hình vòng đời triển khai an toàn



*Hình 1: Mô hình vòng đời triển khai an toàn SecurityBox Antivirus*

Vòng đời triển khai an toàn SecurityBox Antivirus của MVS tổ chức theo 6 giai đoạn chính:

1. Lập kế hoạch (Planning)
2. Phát triển & kiểm thử (Development & Testing)
3. Triển khai nội bộ (Internal rollout / Dogfooding)
4. Triển khai thí điểm (Canary Deployment)
5. Mở rộng có kiểm soát (Controlled Rollout)
6. Phản hồi & cải tiến (Feedback & Continuous Improvement)

### 3.1. Giai đoạn lập kế hoạch (Planning)

Ở giai đoạn này, chúng tôi thực hiện:

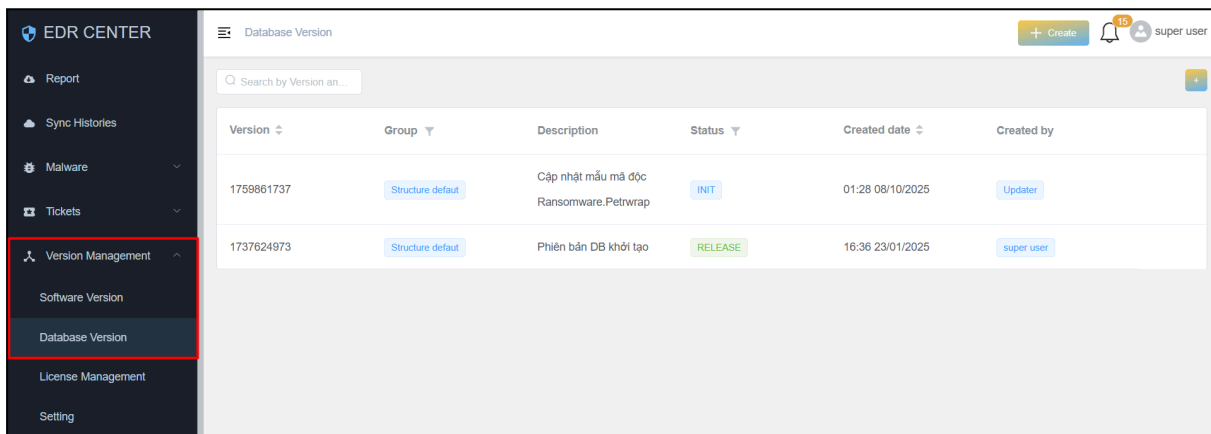
- **Phân loại bản cập nhật**
  - Cập nhật khẩn cấp (Critical Security Update) – ví dụ: vá lỗ hổng nghiêm trọng, khắc phục nhanh false positive trên file hệ thống.
  - Cập nhật bảo mật & chất lượng định kỳ (Regular Security & Quality Update).
  - Cập nhật engine/mô-đun lớn (Major Engine/Feature Release).

- Cập nhật cấu hình (Configuration-only Update).
- **Đánh giá rủi ro & kịch bản thất bại (pre-mortem)**
  - Phân tích các kịch bản xấu nhất: gây BSOD, không khởi động được Windows, mất mạng, xung đột driver, tăng CPU/RAM bất thường, false positive trên file/tiến trình hệ thống.
  - Xác định biện pháp giảm thiểu và kế hoạch thu hồi tương ứng cho từng kịch bản.
- **Xây dựng ma trận tương thích (Compatibility Matrix)**
  - Các phiên bản Windows được hỗ trợ: Windows 10/11 (bản Home/Pro/Enterprise), Windows Server (2016/2019/2022...)
  - Kiến trúc hệ thống: 32-bit/64-bit (nếu áp dụng), máy thật/máy ảo, môi trường VDI.
  - Tương thích với các sản phẩm Microsoft quan trọng (Windows Defender, Microsoft 365, các dịch vụ cloud của Microsoft) và một số phần mềm phổ biến khác (trình duyệt, Office, phần mềm kế toán, ERP...).
- **Chiến lược phát hành & tần suất**
  - Engine & driver: tần suất thấp hơn, được kiểm thử hồi quy (regression) sâu.
  - Database/signature: cập nhật nhiều lần trong ngày nhưng đi qua pipeline kiểm soát false positive riêng, có cơ chế thu hồi nhanh.
- **Kế hoạch thu hồi phiên bản & EOL**
  - Đảm bảo **mọi bản cập nhật đều có phiên bản tiền nhiệm ổn định** để thu hồi.
  - Xác định chính sách **End-of-Life (EOL)** cho các phiên bản engine cũ, lộ trình ép nâng cấp & thông báo tới khách hàng.

### 3.2. Giai đoạn phát triển & kiểm thử (Development & Testing)

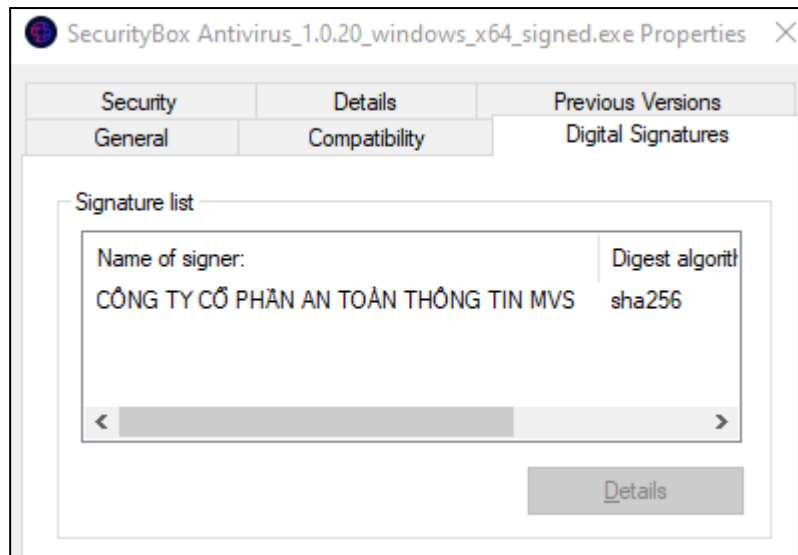
Ở giai đoạn này, chúng tôi tập trung vào:

- **Quy trình build an toàn**
  - Mã nguồn được quản lý trên hệ thống quản lý mã nguồn GitLab được triển khai nội bộ và có kiểm soát truy cập, log đầy đủ.
  - Mọi tính năng mới và hạng mục nâng cấp sau khi được đưa vào kế hoạch trong giai đoạn này đều được phát triển trên các nhánh tính năng (feature branches) và develop trong kho mã nguồn Git.
  - Build server tách biệt, có kiểm soát, chỉ chấp nhận code đã qua review.
  - Sản phẩm build (bản cài đặt, database) sẽ được checksum và ký số, sau đó lưu trữ nội bộ trên phần mềm quản lý tập trung EDR Center.
  - Hệ thống phần mềm quản lý tập trung EDR Center sẽ phân phối các phiên bản phần mềm, phiên bản database đến với các đơn vị phù hợp với các giai đoạn triển khai.



Version	Group	Description	Status	Created date	Created by
1759861737	Structure default	Cập nhật mẫu mã độc Ransomware.Petrwrap	INIT	01:28 08/10/2025	Updater
1737624973	Structure default	Phiên bản DB khởi tạo	RELEASE	16:36 23/01/2025	super user

Hình 2: Hệ thống quản lý các phiên bản phần mềm và phiên bản database



Hình 3: Bản cài đặt SecurityBox Antivirus đã được ký số

- **Kiểm thử chức năng & chất lượng**

- Unit test, integration test, regression test cho các module engine, driver, GUI, update service.
- Test tự động trên ma trận hệ điều hành và cấu hình máy khác nhau.
- Kiểm thử hiệu năng: CPU, RAM, I/O, thời gian khởi động, thời gian quét.

- **Kiểm thử bảo mật & tương thích hệ sinh thái Microsoft**

- Kiểm tra xung đột với Windows Defender và các tính năng bảo mật của Windows.
- Đảm bảo cập nhật không can thiệp bất thường vào cơ chế cập nhật Windows hoặc các thành phần lõi.
- Đảm bảo AV signature không đánh nhầm các file hệ thống Windows, file của các sản phẩm Microsoft phổ biến.

- **Kiểm thử database/signature & mô hình phát hiện**

- Chạy trên bộ mẫu:

- Tập dữ liệu clean (clean set) gồm hệ điều hành, phần mềm văn phòng, trình duyệt, phần mềm phổ biến.
  - Tập dữ liệu malware (malware set) gồm các mẫu mã độc chuẩn để kiểm tra chất lượng phát hiện.
- Đo lường: tỷ lệ phát hiện, tỷ lệ false positive, thời gian phát hiện, độ ổn định hệ thống khi áp dụng database mới.

### 3.3. Giai đoạn triển khai nội bộ (Internal rollout / Dogfooding)

Trước khi phát hành cho khách hàng, mọi bản cập nhật quan trọng đều được triển khai trong nội bộ:

- **Môi trường áp dụng**

- Hệ thống phòng LAB bao gồm máy trạm, laptop và server nội bộ của MVS với đa dạng các phiên bản HĐH Windows.
- Các máy tính, laptop nội bộ của developer thuộc MVS.
- Tại giai đoạn này, hệ thống EDR Center sẽ chỉ triển khai mặc định trong phạm vi phòng LAB và không cho phép triển khai tại các đơn vị khác.

The screenshot displays the configuration interface for SecurityBox Antivirus. It features a table for selecting operating systems and environments, and a sidebar with various settings.

Operating System	SB Private	SB-EDR	SecurityBox Antivirus
Windows 7/8/10/11 64-bit	Skip	Skip	2 files
Ubuntu Desktop 64-bit	Skip	Skip	Skip
Ubuntu Desktop 32-bit	Skip	Skip	Skip
Windows 7/8/10/11 32-bit	Skip	Skip	2 files

**TEST** (dropdown)

**Software Version:**  
1.0.20

**Description:**  
Release Note: Cập nhật giao diện thông báo

**Structure Database:**  
Structure default

**License:**

- 1link
- BTL 86
- DSS Company
- MVI Comparatives
- MVS
  - Phòng kỹ thuật
  - Phòng LAB
- Suntech

Hình 4: Phân phối thử nghiệm tại phòng LAB

- **Cơ chế thu thập dữ liệu**
  - Thông tin thu thập tự động về crash, log lỗi, BSOD, hiệu năng, thời gian khởi động, tỷ lệ cập nhật thành công.
  - Hệ thống phản hồi lỗi được khách hàng đang sử dụng phản ánh các kênh email [support@securitybox.vn](mailto:support@securitybox.vn) hoặc các nhóm chat hỗ trợ.
- **Tiêu chí vượt qua giai đoạn**
  - Không có sự cố nghiêm trọng (BSOD, không khởi động được, mất mạng hàng loạt).
  - Không có pattern crash hàng loạt trên cùng phiên bản.
  - Không ghi nhận false positive nghiêm trọng lên file hệ thống hoặc phần mềm nội bộ quan trọng.
  - Tỷ lệ cập nhật thành công đạt ngưỡng định sẵn.
  - Khi vượt qua các tiêu chí, mã nguồn sẽ được merge từ nhánh develop sang nhánh staging.

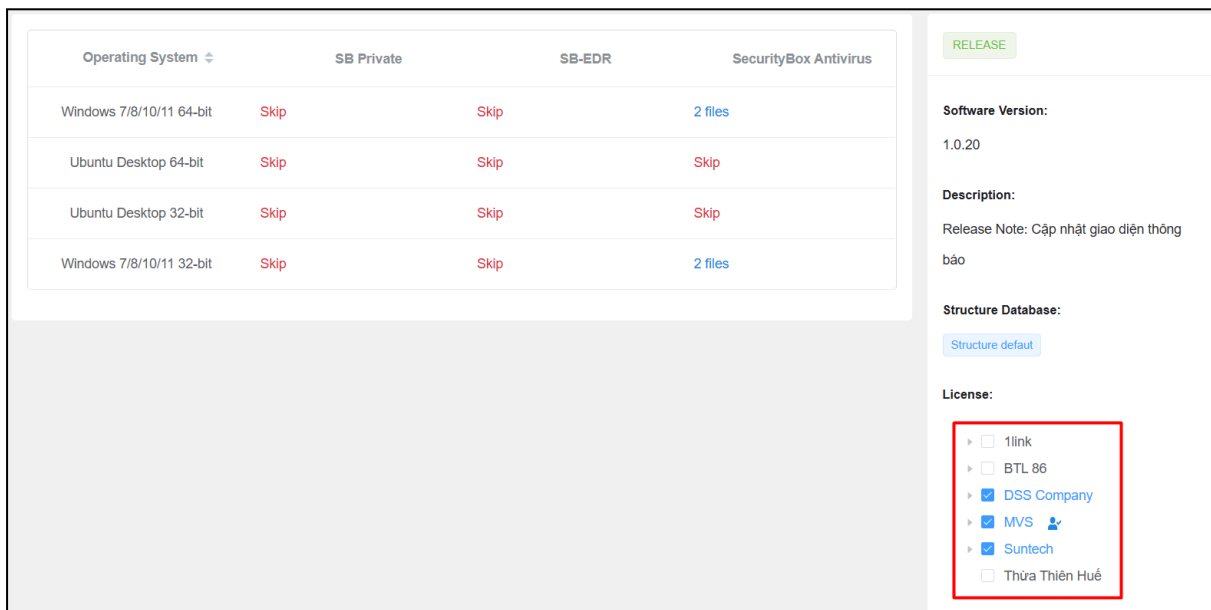
### 3.4. Giai đoạn triển khai thí điểm (Canary Deployment)

Giai đoạn triển khai thí điểm là giai đoạn triển khai cho một tỷ lệ nhỏ khách hàng để kiểm tra trong môi trường thực tế:

- **Lựa chọn nhóm thí điểm**
  - Một số khách hàng/doanh nghiệp đồng ý tham gia chương trình thử nghiệm bản beta.
  - Tỷ lệ triển khai ban đầu được giới hạn ở mức nhỏ (ví dụ khoảng 1–5% số lượng thiết bị đang hoạt động).

- **Kiểm soát triển khai**

- Người vận hành được phân quyền quản lý triển khai bản cập nhật của hệ thống EDR Center sẽ chọn các đơn vị nằm trong phạm vi triển khai thí điểm.
- Có khả năng **tạm dừng triển khai** ngay lập tức cho các đơn vị thí điểm khi vượt ngưỡng rủi ro.



Hình 5: Vận hành việc triển khai thí điểm tại các đơn vị

- **Giám sát & ngưỡng dừng**

- Theo dõi real-time:
  - Tỷ lệ cập nhật thành công.
  - Crash, BSOD, lỗi hiệu năng.
  - Phản hồi của khách hàng/đối tác.

### 3.5. Giai đoạn mở rộng có kiểm soát (Controlled Rollout)

Sau khi triển khai thí điểm ổn định, bản cập nhật được mở rộng dần:

- **Tăng dần tỷ lệ triển khai**

- Ví dụ: 5% → 20% → 50% → 100% số lượng thiết bị tại các đơn vị, theo từng “vòng thử nghiệm”.
- Mỗi vòng thử nghiệm có thời gian quan sát nhất định (ví dụ 24–72 giờ) trước khi nâng lên vòng thử nghiệm kế tiếp.
- Sau khi đạt 100% số lượng thiết bị tại các đơn vị, mã nguồn sẽ được merge từ nhánh staging sang master và được các tag release với phiên bản tương ứng.

- **Phân tầng khách hàng**

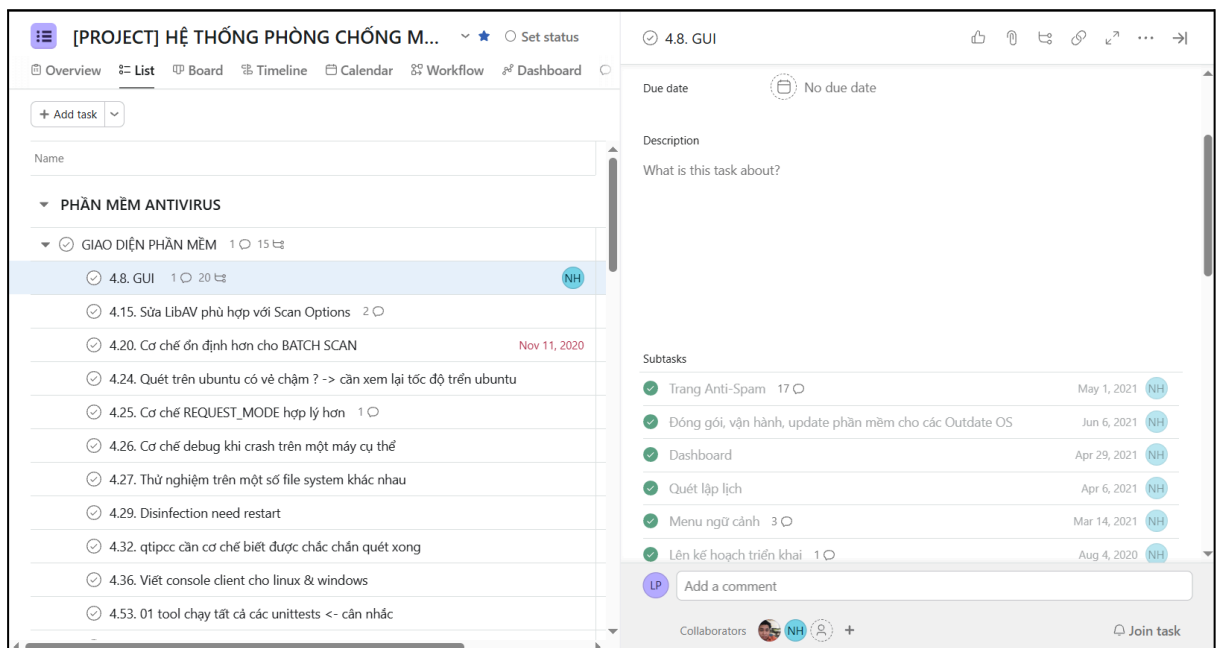
- Ưu tiên triển khai ở nhóm môi trường đơn giản, ít rủi ro trước; các môi trường nghiệp vụ trọng yếu được triển khai sau khi đã có đủ dữ liệu ổn định.
- Cho phép một số khách hàng doanh nghiệp **tuỳ chọn trì hoãn** nhận bản cập nhật lớn (engine major) trong một khung thời gian nhất định, nhưng không trì hoãn vô hạn để tránh rủi ro bảo mật.

### 3.6. Giai đoạn phản hồi & cải tiến (Feedback & Continuous Improvement)

Mỗi vòng triển khai đều cung cấp dữ liệu cho vòng sau:

- Ghi nhận và phân tích:
  - Lỗi phát hiện trong từng giai đoạn (dev, internal, canary, rollout).
  - Sự cố và tình huống suýt trở thành sự cố (suýt sự cố).
  - Phản hồi từ Microsoft (trong khuôn khổ MVI) và từ khách hàng.
- Cập nhật:
  - Quy tắc kiểm thử, ma trận tương thích.
  - Tiêu chí cho canary, rollout, rollback.

- Tài liệu kỹ thuật và playbook triển khai/sự cố.
- Cải tiến:
  - Toàn bộ các lỗi phát hiện hoặc các phản hồi khách hàng sẽ được tổng hợp lại, tạo ticket, giao việc cho từng bộ phận chịu trách nhiệm và được quản lý trên Asana.
  - Đối với các lỗi gây các sự cố nghiêm trọng được phát hiện sau quá trình triển khai mở rộng sẽ kích hoạt quá trình hotfix với vòng đời tương tự.



Hình 6: Một vài ticket được triển khai trong quá trình phát triển

#### 4. Quản lý rủi ro triển khai & tình huống suýt trở thành sự cố

MVS xây dựng **đăng ký rủi ro triển khai** (deployment risk register) cho sản phẩm SecurityBox Antivirus, trong đó:

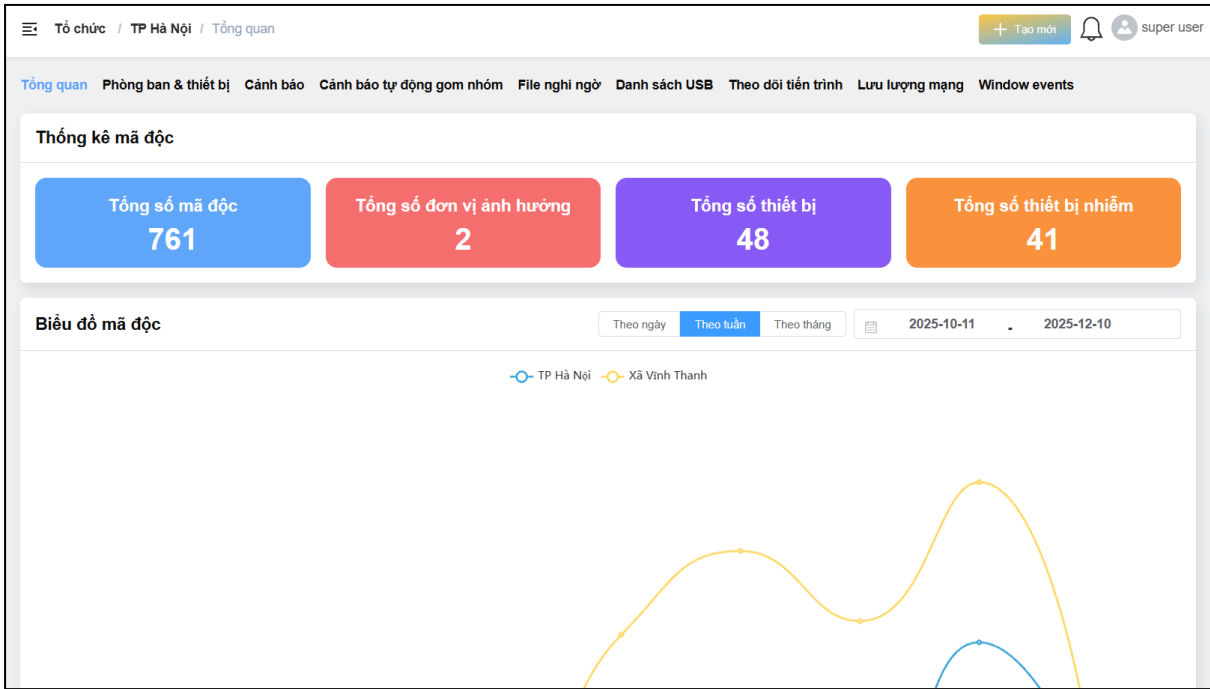
- Mỗi loại rủi ro (ví dụ: BSOD, xung đột driver, false positive trên file hệ thống, lỗi hiệu năng nghiêm trọng, chặn dịch vụ Windows Update...) được mô tả: nguyên nhân, khả năng, tác động, biện pháp giảm thiểu.

- Khi xuất hiện tình huống “suýt trở thành sự cố” (near-miss) (ví dụ: phát hiện lỗi nghiêm trọng ở giai đoạn thí điểm, chưa kịp ảnh hưởng diện rộng), sự kiện vẫn được ghi nhận như một sự cố nội bộ, và được phân tích nguyên nhân gốc (RCA) và hành động khắc phục cụ thể.

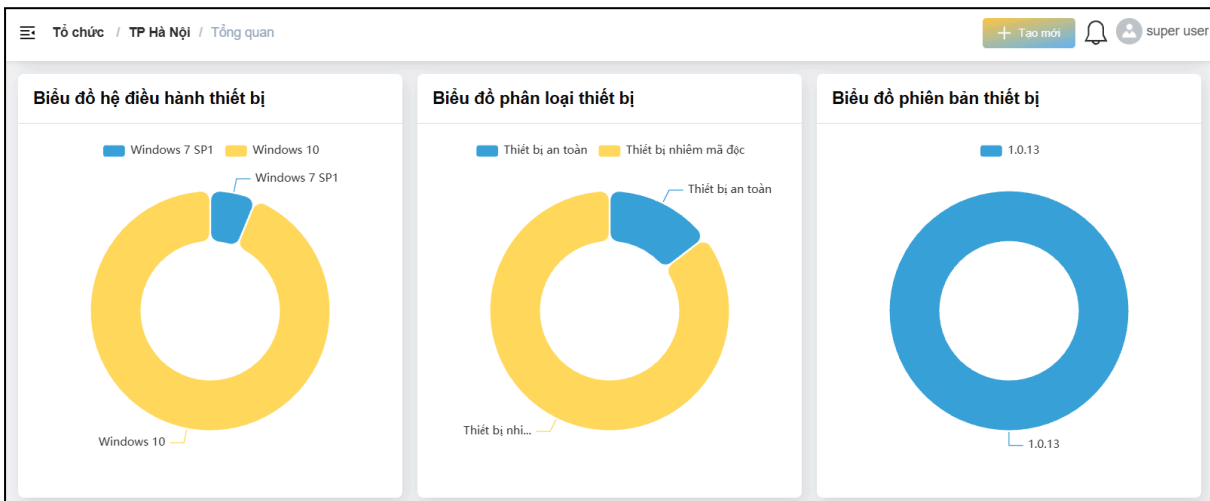
## 5. Giám sát, đo lường và cảnh báo trong quá trình triển khai

Để hỗ trợ việc triển khai an toàn, hệ thống SecurityBox Antivirus triển khai:

- **Thu thập dữ liệu giám sát vận hành (telemetry)** một cách tự động khi được khách hàng cho phép:
  - Tỷ lệ cập nhật thành công/thất bại theo phiên bản.
  - Thông tin về crash, BSOD, event log liên quan đến service/driver của SecurityBox Antivirus.
  - Chỉ số hiệu năng: CPU, RAM, I/O bất thường sau khi cập nhật.
- **Hệ thống quan trắc và cảnh báo**
  - Dashboard nội bộ hiển thị các chỉ số theo phiên bản, kênh cập nhật, khu vực.
  - Cảnh báo tự động khi vượt ngưỡng:
    - Crash rate tăng bất thường sau khi phát hành bản mới.
    - Lượng ticket/phản ánh từ khách hàng tăng đột biến.
    - Tỷ lệ cập nhật thất bại cao trên một phiên bản cụ thể.
- **Liên kết với quy trình ứng phó sự cố**
  - Khi vượt ngưỡng, hệ thống tự động hoặc người trực có thể **kích hoạt playbook sự cố**, dừng triển khai, hoặc thu hồi phiên bản theo chính sách.



Hình 7: Dashboard thống kê cho từng đơn vị



Hình 8: Dashboard thống kê cho từng đơn vị

## 6. Kế hoạch ứng phó sự cố và thu hồi phiên bản

MVS xây dựng và duy trì bộ quy trình chuẩn (playbook) cho việc triển khai và ứng phó sự cố đối với SecurityBox Antivirus, trong đó bao gồm việc phân loại mức độ sự cố như sau:

- **Phân loại mức độ sự cố**

- Mức 1: Ảnh hưởng trong phạm vi hẹp, có thể khắc phục bằng biện pháp tạm thời/giải pháp thay thế đơn giản, không gây tác động rộng.
- Mức 2: Ảnh hưởng đáng kể tới một nhóm khách hàng, cần phát hành bản sửa lỗi hoặc thu hồi phiên bản (rollback) trong thời gian ngắn.
- Mức 3: Ảnh hưởng trên diện rộng, có nguy cơ tác động đến tính sẵn sàng của hệ thống, cần thực hiện thu hồi phiên bản khẩn cấp và phối hợp chặt chẽ với các đối tác liên quan (bao gồm Microsoft).

- **Quy trình xử lý**

- Phát hiện và xác nhận sự cố (triage).
- Tạm dừng phát hành trên các đơn vị bị ảnh hưởng.
- Ra quyết định: thu hồi bản cập nhật (engine/database) hoặc phát hành hotfix.
- Thông báo tới khách hàng, đối tác, và khi cần thiết là Microsoft (trong phạm vi MVI).
- Theo dõi sau sự cố, xác minh hiệu quả của rollback/hotfix.
- Thực hiện post-incident review, cập nhật quy trình SDP.

- **Thu hồi kỹ thuật**

- Client SecurityBox Antivirus có khả năng **quay lại phiên bản engine hoặc database ổn định trước đó**, một cách tự động khi phát hiện lỗi trong quá trình cập nhật.
- Hệ thống cập nhật có khả năng ưu tiên phân phối bản “rollback update” tới toàn bộ thiết bị bị ảnh hưởng.

## 7. Quản lý cấu hình, kênh cập nhật và tương thích Microsoft

- **Quản lý kênh cập nhật**
  - Internal Channel – dành cho nhân viên MVS.
  - Canary/Beta Channel – nhóm khách hàng/đối tác tham gia chương trình thử nghiệm.
  - Stable Channel – khách hàng thông thường.
- **Chính sách cập nhật trên Windows**
  - Tôn trọng chính sách Windows về khởi động lại (reboot). SecurityBox Antivirus không tự động khởi động lại hệ thống nếu không thực sự cần thiết.
  - Không thay đổi hoặc can thiệp trái phép vào cơ chế cập nhật của hệ điều hành Windows.
  - Đảm bảo SecurityBox Antivirus không gây cản trở hoạt động bình thường của Microsoft Defender và các giải pháp bảo mật khác của Microsoft.
- **Quản lý cấu hình**
  - Cấu hình mặc định được thiết kế an toàn, tránh gây gián đoạn bất ngờ cho người dùng cuối.
  - Các thay đổi cấu hình lớn được đưa qua pipeline giống như cập nhật chức năng (có internal, canary, rollout, giám sát...).

## 8. An toàn chuỗi cung ứng phần mềm và hạ tầng triển khai

Để đảm bảo cập nhật SecurityBox Antivirus không bị can thiệp hoặc giả mạo:

- **Ký số & xác thực**
  - Mọi bản dựng (installer, engine, driver, module, signature...) đều được **ký số bằng chứng thư code signing** (EV code signing) của MVS do hãng SSL cấp.

- Client chỉ chấp nhận cập nhật nếu chữ ký số hợp lệ và được phát hành từ kho chứng thư tin cậy.

- **Bảo vệ hạ tầng build & update**

- Hệ thống build và máy chủ phân phối cập nhật được tách vùng mạng, áp dụng MFA, logging và nguyên tắc đặc quyền tối thiểu.
- Kiểm soát truy cập chặt chẽ đối với tài khoản có khả năng đẩy (publish) bản cập nhật mới.
- Lưu log đầy đủ các sự kiện build, sign, publish để phục vụ điều tra khi cần thiết.

- **Kiểm soát nguồn phụ thuộc**

- Thiết lập và duy trì danh mục thành phần phần mềm (Software Bill of Materials) cho các thành phần chính.
- Đánh giá rủi ro đối với thư viện bên thứ ba, cập nhật kịp thời các bản vá bảo mật quan trọng.

## 9. Giao tiếp và hỗ trợ khách hàng trong quá trình triển khai

MVS cam kết:

- **Thông báo trước khi cập nhật lớn**

- Với các bản cập nhật engine hoặc thay đổi lớn, MVS sẽ cung cấp thông tin trước: phạm vi thay đổi, tác động tiềm năng, yêu cầu hệ thống, thời gian dự kiến.

- **Công bố ghi chú phát hành (Release Notes)**

- Mỗi bản phát hành đều có release notes mô tả các thay đổi chính, lỗi được sửa, điểm cần lưu ý.

- **Kênh hỗ trợ sự cố khẩn cấp**

- Kênh liên hệ hỗ trợ (email, hotline, portal) dành riêng cho sự cố liên quan tới cập nhật, để khách hàng có thể báo cáo nhanh và nhận hướng dẫn xử lý, thu hồi.

- **Minh bạch sau sự cố**

- Khi xảy ra sự cố có ảnh hưởng đáng kể, MVS sẽ thông tin tới khách hàng/đối tác và, khi cần, Microsoft, bao gồm: mô tả sự cố, phạm vi ảnh hưởng, biện pháp khắc phục, và các bước cải tiến quy trình.

## 10. Cơ chế quản trị và rà soát chương trình SDP

- **Trách nhiệm quản trị**

- **Chủ sở hữu SDP:** một bộ phận/bộ phận kết hợp (ví dụ: Bộ phận Phát triển Sản phẩm & Bộ phận Đảm bảo Chất lượng/An toàn Thông tin) chịu trách nhiệm duy trì, cập nhật và giám sát việc tuân thủ SDP.
- **Ban lãnh đạo:** xem xét định kỳ các chỉ số chất lượng triển khai và báo cáo sự cố/tình huống suýt trở thành sự cố.

- **Rà soát định kỳ**

- SDP được rà soát tối thiểu **mỗi năm một lần**, hoặc sau mỗi sự cố nghiêm trọng, hoặc khi có thay đổi lớn trong kiến trúc sản phẩm/hạ tầng triển khai.
- Việc rà soát cũng tham chiếu cập nhật mới từ CISA, NIST và các yêu cầu của chương trình MVI (nếu có điều chỉnh).

- **Đào tạo & nâng cao nhận thức**

- Nhân sự tham gia vào quá trình xây dựng, kiểm thử, phát hành và vận hành SecurityBox Antivirus đều được đào tạo về triển khai an toàn, thiết kế bảo mật ngay từ đầu và quy trình xử lý sự cố.
- MVS khuyến khích xây dựng văn hóa báo cáo lỗi và các tình huống suýt trở thành sự cố (near-miss) trên cơ sở không quy trách nhiệm cá nhân.