Safe Deployment Practices

1. Rollback & Recovery Mechanism

All drivers in ForeNova's product suite are equipped with built-in fallback mechanisms. When a driver experiences three consecutive kernel-mode crash, it will automatically cease operation. After confirming the system anomaly is not caused by the product itself, the driver will resume normal operation after 100 hours. This mechanism significantly reduces large-scale system failures caused by internal product issues.

2. Extensive Testing

Our product has undergone comprehensive compatibility testing in our laboratory. The testing covers all Windows systems starting from Windows 7 SP1 and above, as well as mainstream Linux operating systems. In total, it supports 91 types of operating systems and has verified compatibility with over 1,900 software applications, including mainstream antivirus software, office software, and industry-specific software.

3. Monitoring and Metrics

We will collect our product’s quality data legally from customer, including os crash data, process crash data. If the product crash rate is abnormal, we will suspend the promotion of the product and contact customers to investigate the specific problem.

4. Transparent Communication

Customers can directly call the General Line: +49 8926 200 920 of

ForeNova to contact technical experts for quick processing, or email info@forenova.com to get support.

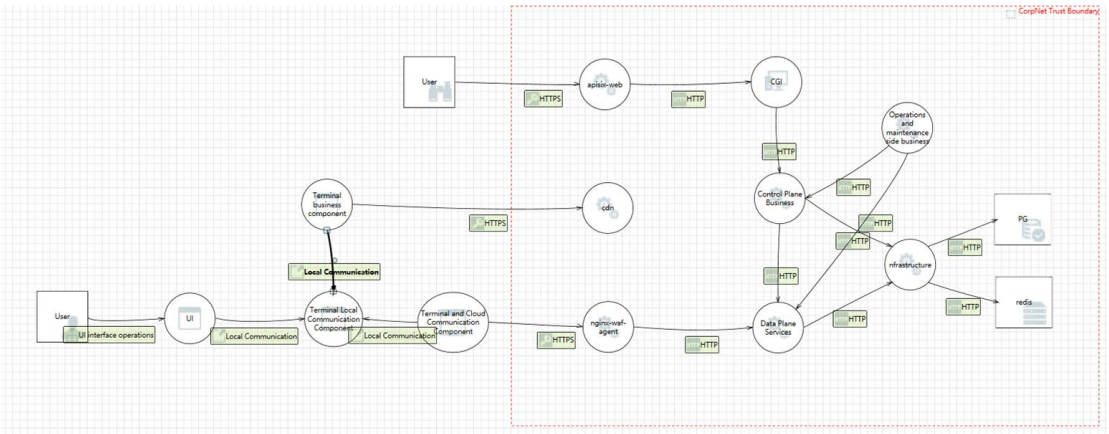
5. Staged Rollouts

Our product will not be released to individual customers, but exclusively to business customers. After launch, it will undergo a controlled trial phase with over 200 clients across more than 50,000 devices. Only after confirming no issues will we roll out the update to a broader group of willing customers.

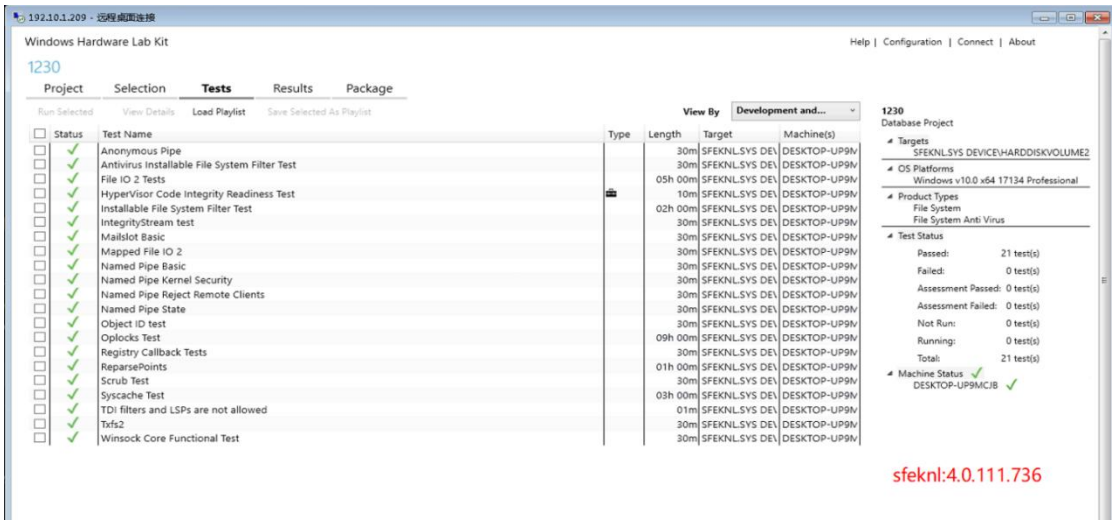
6. Security product testing

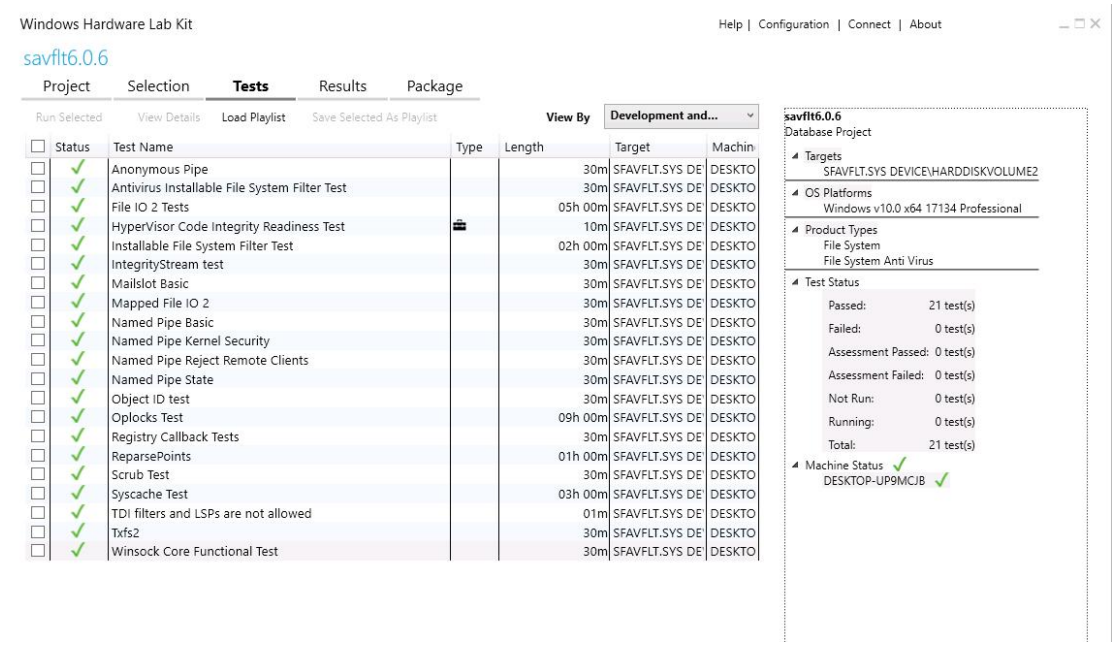
The product development process of ForeNova will follow the complete internal security development process, covering the minimum expected testing practices for security product.

(1) During the product design phase, we will maintain a threat model of the module in product.

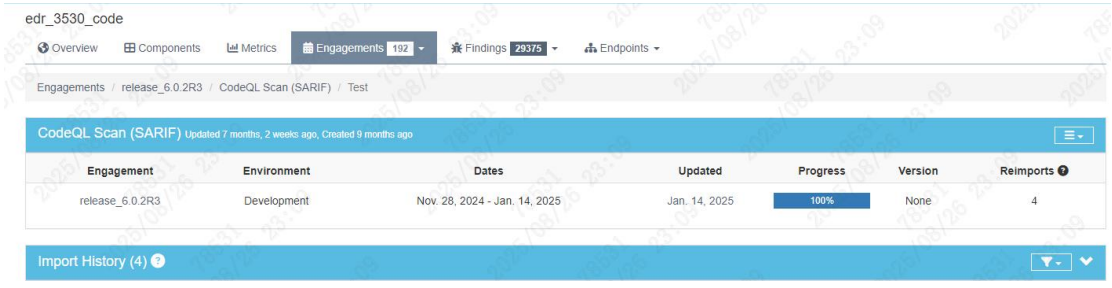


(2) Verifer testing



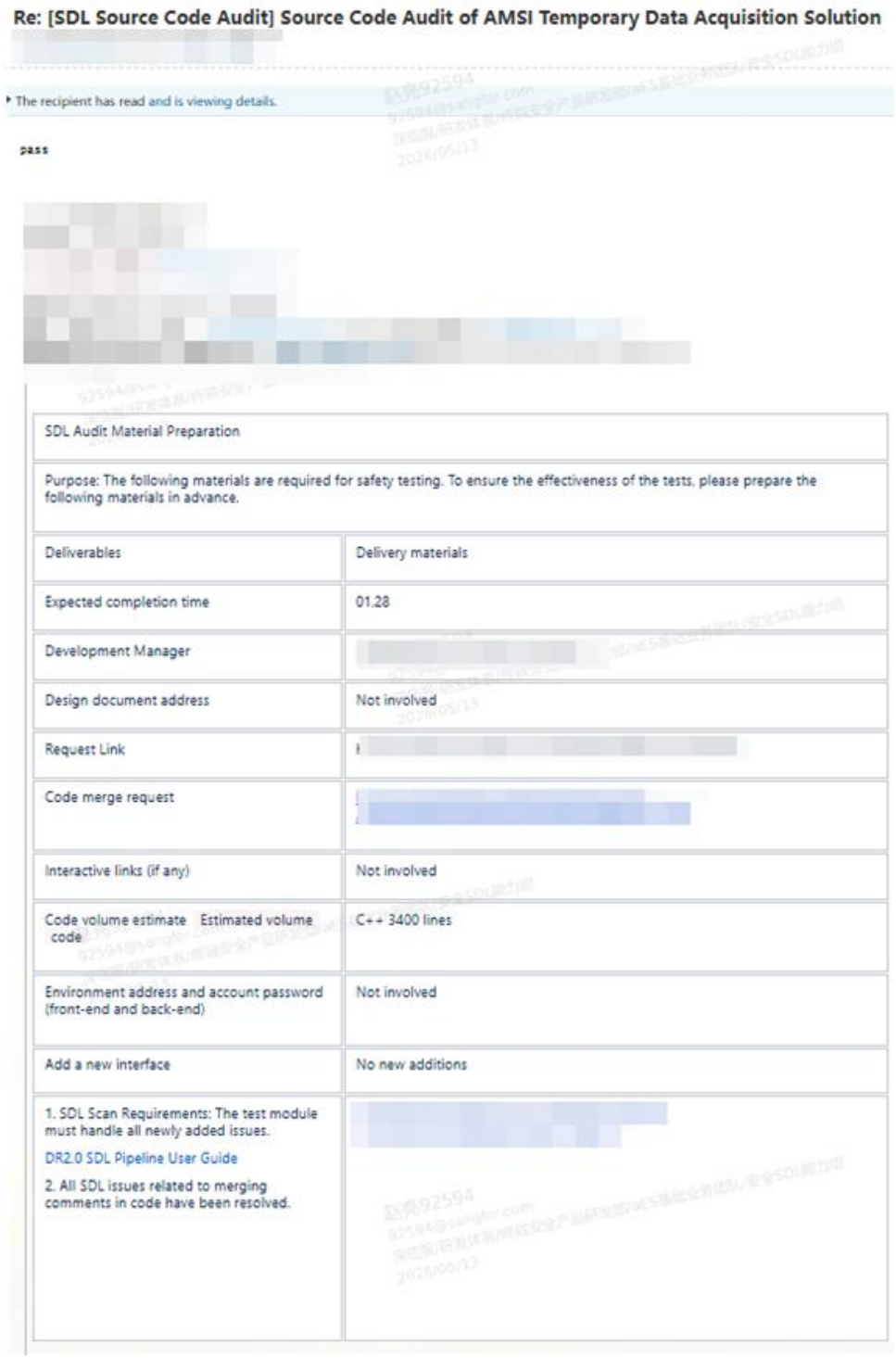


(3)CodeQL



(4) Compile driver with InitAll

We reviewed all our code before release product by our own SDL team, and all the bugs has been fixed before release.



Re: [SDL Source Code Audit] Source Code Audit of AMSI Temporary Data Acquisition Solution

The recipient has read and is viewing details.

pass

SDL Audit Material Preparation	
Purpose: The following materials are required for safety testing. To ensure the effectiveness of the tests, please prepare the following materials in advance.	
Deliverables	Delivery materials
Expected completion time	01.28
Development Manager	
Design document address	Not involved
Request Link	
Code merge request	
Interactive links (if any)	Not involved
Code volume estimate Estimated volume code	C++ 3400 lines
Environment address and account password (front-end and back-end)	Not involved
Add a new interface	No new additions
1. SDL Scan Requirements: The test module must handle all newly added issues. DR2.0 SDL Pipeline User Guide 2. All SDL issues related to merging comments in code have been resolved.	

(5) KASAN

KASAN has not been implemented in our drivers, and will be implemented in the latest new product(will be released at the end of 2026).

(6) Validate signatures

We validated all the signatures.