Endpoint Security Report

Time Range	2025.07.06 - 2025.08.04
Scope	All endpoints
Generation Time	2025-08-04
Items	Endpoint Threats and Risks

Contents

1. Security Overview

Endpoint

Time Range

2025.07.06-2025.08.04

Uptime

106 day(s)

Total Endpoints

71

Targeted Endpoints

7

Intrusion Events

1163

Pending Viruses

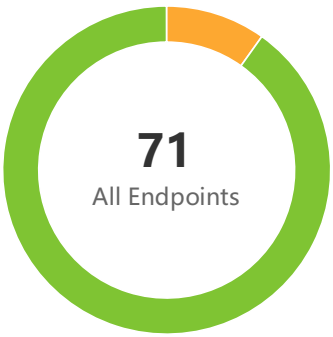
2

Fixed Viruses

2

Overview

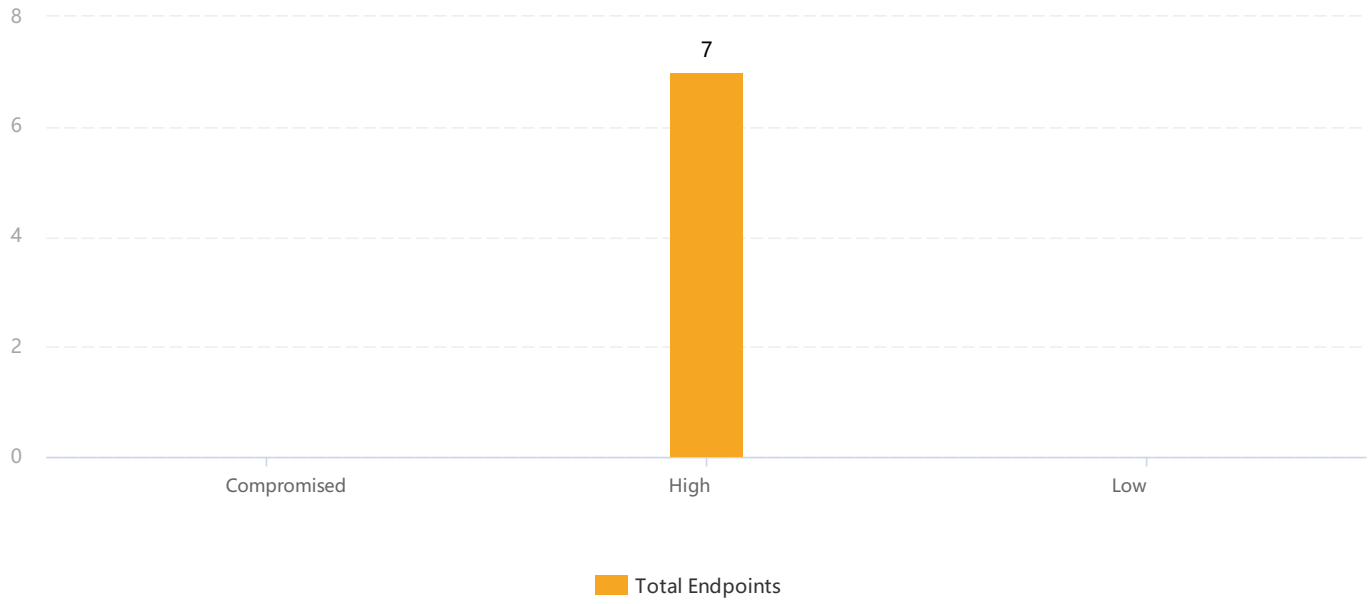
Targeted Endpoints: **7** pending, accounting for **9.86%** . Malware Events: **50.00%** fixed, Pending Malware Events: **2** pending; Intrusion Events: **0%** fixed, Pending: **1163** pending. Please log in to the Manager and go to Response page to fix target endpoints and security events.



Targeted Endpoints	7	Pending	2	Pending	1163
Secure Endpoints	64	Fixed	2	Fixed	0

1.1 Endpoint Overview

Among the 7 targeted endpoints, **0** compromised. Compromised, high-risk, and low-risk endpoints are as follows:



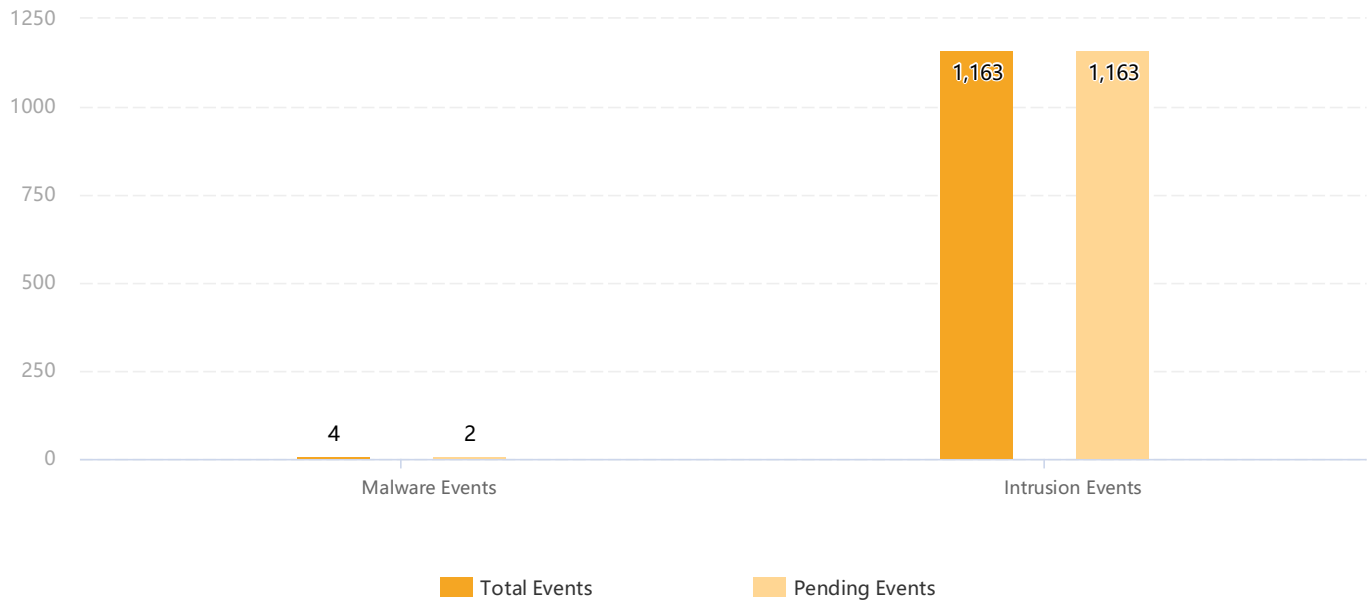
1.2 Threat Overview

During the period, **1167** event(s) occurred.

Malware events occurred **4** time(s), accounting for **0.34%** , **2** pending. It is recommended to fix them promptly via Defense > Malware Scan > Malware on Endpoint Secure.

Intrusion events occurred **1163** time(s), accounting for **99.66%** , **1163** pending. It is recommended to fix them promptly via Detection and Response > Security Events > Overview on Endpoint Secure.

The threat type distribution and fixing status are as follows:



2. Targeted Endpoint Analysis

Targeted Endpoints: 7 pending, among which 0 compromised, 7 highly insecure, and 0 insecure.

Details:

2.1 Compromised Endpoints

◆ **Top 10 Targeted Endpoints**

No data available

3. Security Event Analysis

During the period (2025.07.06-2025.08.04), 1167 security events were found.

Malware Events: 4, among which 0 high, 2 medium, 2 low, and 0 unknown.

Intrusion Events: 1163, including 0 WebShell backdoor intrusions, 0 brute-force attacks, and 1163 other events.

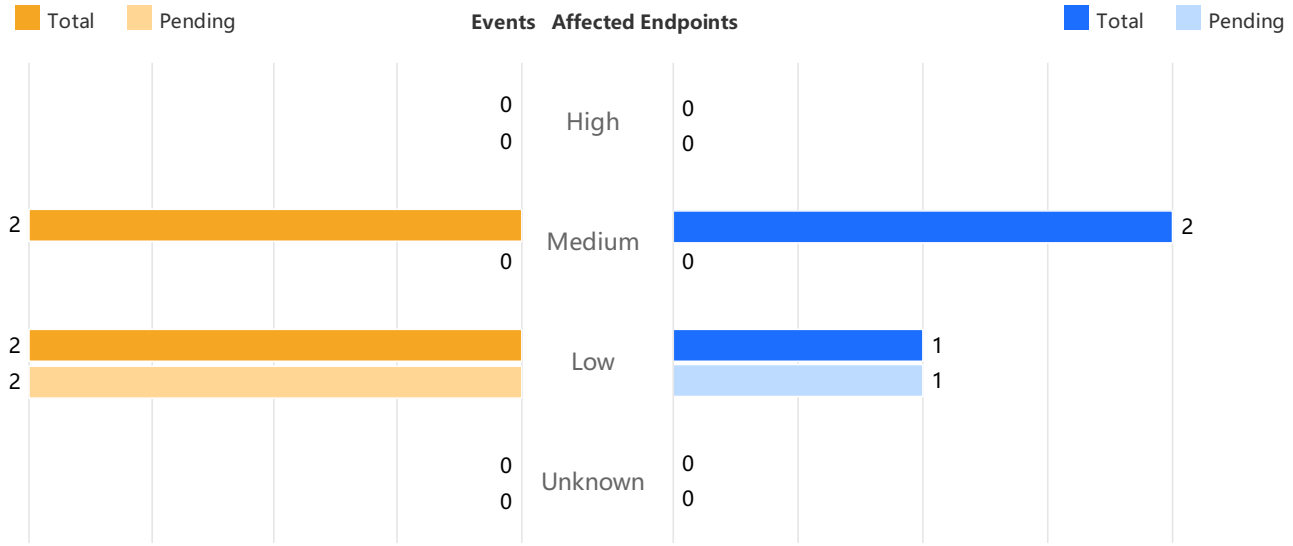
Security event details:

3.1 Malware

◆ Malware Intrusions and Fixes

Endpoint Secure has detected 4 malware intrusions and 3 endpoints are infected.

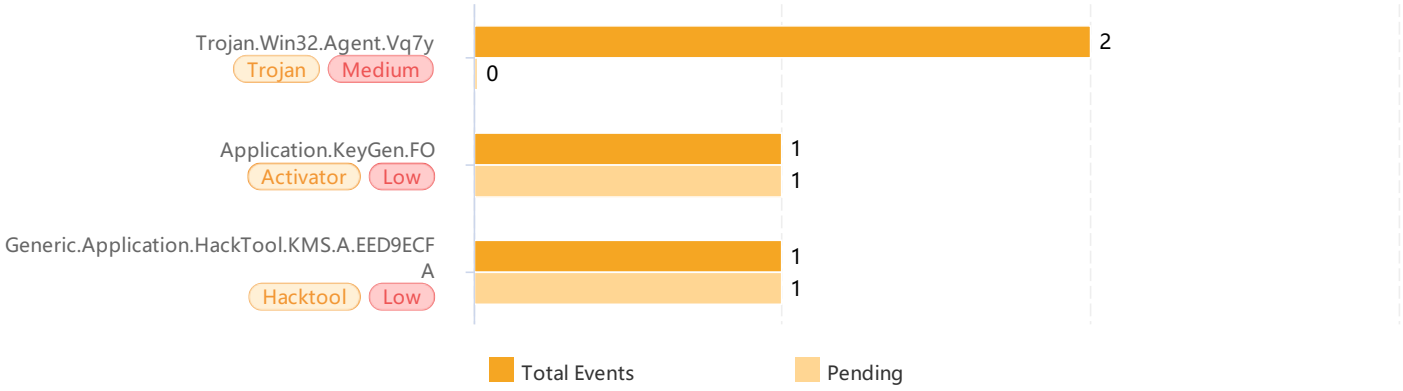
Among all the malware intrusions, **0** high-severity **(0%)** , **2** medium-severity **(50.00%)** , **2** low-severity **(50.00%)** , and 1000 unknown **0** unknown virus intrusion(s) **(0%)** , **0** pending high-severity malware intrusions and **0** pending endpoints involved. Intrusion and fix details are as follows:



◆ Top 5 Malware Detected

Trojan- **Trojan.Win32.Agent.Vq7y** occurred **2** times and infected **2** endpoint(s), making it the top malware intrusion. Top 5 are as follows:

Endpoint Security Report



3.2 WebShell Backdoors

◆ WebShell Backdoor Intrusions and Fixes

Endpoint Secure has detected 0 Webshell backdoor intrusions during the period.
0 high-severity WebShell backdoor intrusions **（0%）**, **0** medium-severity WebShell backdoor intrusions **（0%）**, and **0** low-severity WebShell backdoor intrusions **（0%）**. , threat(s) are pending **0** threats are pending, and **0** pending endpoints involved in WebShell backdoor intrusions. Intrusion and fix details are as follows:

No data available

◆ Top 5 WebShell Backdoor Intrusions

WebShell-(None) occurred **0** times and infected **0** endpoints, making it the top WebShell backdoor intrusion. Top 5 are as follows:

No data available

3.3 Brute-Force Attacks

◆ **Brute-Force Attacks and Fixes**

During this period, Endpoint Secure has detected 0 brute-force attack.
Among them, **0** RDP brute-force attack(s) **(0%)** , and 0 SMB brute-force attack(s) **(0%)** , **0** MSSQL brute-force attack(s) **(0%)** , and **0** SSH brute-force attack(s) **(0%)** , **0** brute-force attacks are pending and **0** endpoint(s) involved. Brute-force attack and fix details are as follows:

No data available

◆ **Top 10 brute-force attackers**

The most active brute-force attacker is **(None)** , attacked **0** internal endpoint(s). Top 10 active attackers are as follows:

No data available

The top target endpoint **(None)** , has been attacked **0** time(s). Top 10 target endpoints are as follows:

No data available

4. Appendix

◆ How To Assess Risks

Endpoint Secure assesses endpoint security based on risk rating and threat severity on endpoints. Risk rating indicates the possibility of an endpoint to be compromised, including compromised, highly insecure, and insecure. The higher the risk rating, the higher the possibility endpoints are to be compromised.

Threat severity indicates the impact level of a security event, including high, medium, and low. The higher the threat severity, the severer the impacts.

◆ Security Planning Recommendations

1) Update anti-virus database and engine to the latest version to ensure virus detection capability.

2) Configure appropriate security policies to protect your endpoints.

3) Use Endpoint Secure to quarantine infected files or even isolate infected endpoints if infection is severe in order to prevent virus spread.

4) Perform a compliance check on the Risk Assessment page to detect and fix endpoints that do not meet security requirements.

5) If you encounter any problem, visit Sangfor official website (https://www.sangfor.com/en) to get online help or call Sangfor security team at +60 12711 7129 (7511).

◆ Learn More

To read more security information, vulnerabilities, attack techniques, threat intelligence, etc., visit Sangfor Security Center Wiki site (http://sec.sangfor.com/events/lst.html) or follow Sangfor on WeChat.