ASRock Industrial

AI Safeguard

ASRock Industrial Safeguard

Key Features

- Real-Time Device Identification
- Honeypot Sandbox Isolation
- Trusted Access Control
- AI-powered Threat Analysis
- Data Integrity and System Resilience
- Centralized Security Integration

Product Overview

AiSafeguard is an intelligent device isolation solution designed to strengthen endpoint security and operational reliability. Leveraging advanced Honeypot Sandbox technology, it automatically detects, classifies, and isolates external devices in real time, allowing trusted peripherals to access host resources securely while containing untrusted devices within an isolated sandbox for behavioral analysis. By integrating a behavioral threat intelligence engine with AI-powered analytics, AiSafeguard provides continuous risk assessment, minimizes system vulnerabilities, and ensures secure operations in industrial and enterprise environments.

Product Features

Adaptive Isolation Architecture

Built on modular isolation layers that dynamically separate trusted and untrusted environments, ensuring zero interference between user operations and threat analysis.

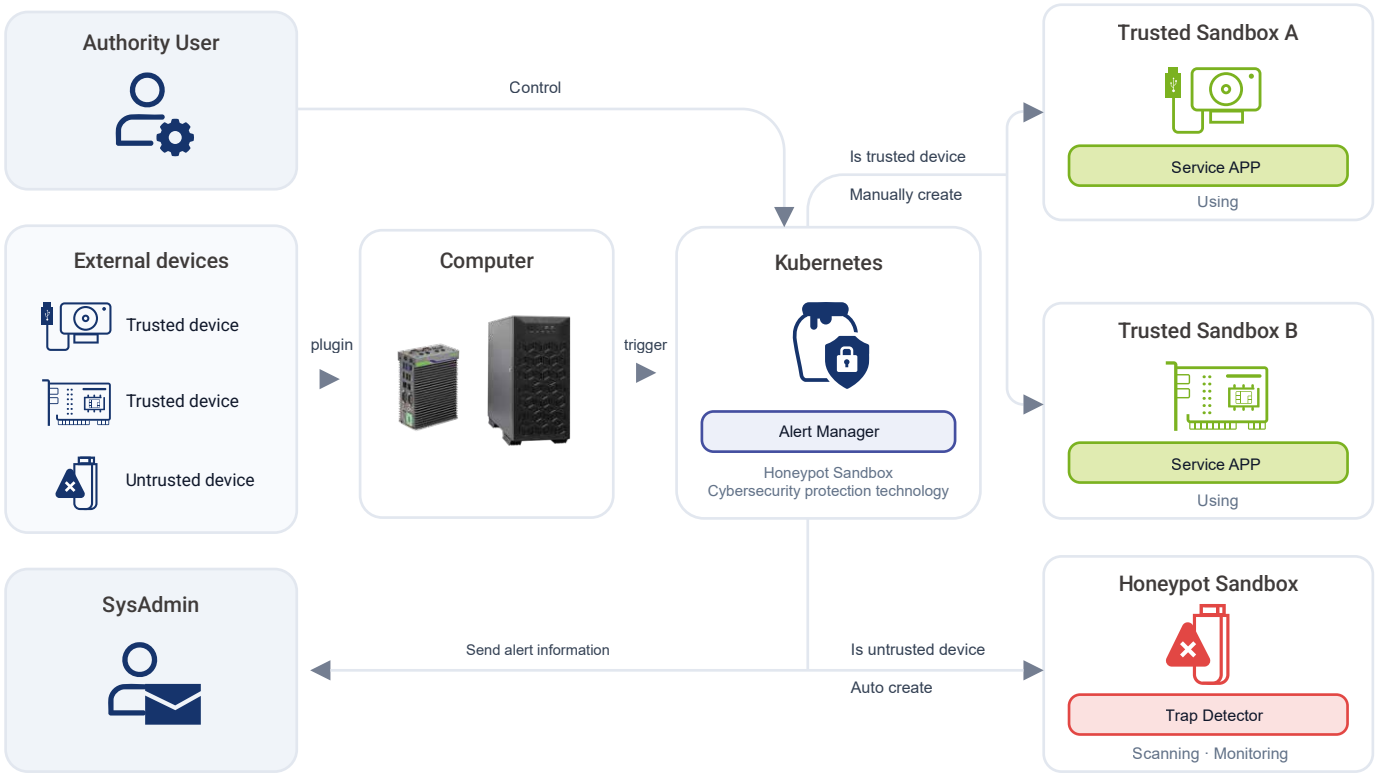
AI-Powered Threat Analysis

Utilizes standardized AI APIs to transform system data into actionable security insights. The engine identifies configuration gaps and potential risks, providing automated recommendations to harden zero trust postures and mitigate vulnerabilities.

Unified Management and Policy Control

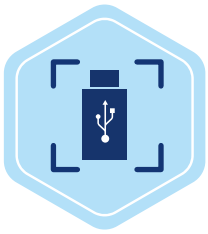
Offers centralized configuration, policy enforcement, and audit management through integration with SIEM (Security Information and Event Management) / SOC (Security Operation Center) platforms, enabling enterprise-grade scalability and compliance.

How it works



AiSafeguard Device Onboarding Workflow

AiSafeguard automates external device detection and isolation through a policy-driven workflow that safeguards host systems from unauthorized access and malicious activity.



1. Device Detection

When an external device connected, AiSafeguard automatically triggers a detection event and reports it to the central control module for validation.

2. Security Assessment & Classification

The **Alert Manager**, serving as the Honeypot Sandbox security core, evaluates device trust attributes including certificates, identifiers, and historical records, and classifies the device as Trusted or Untrusted based on predefined security policies. The classification results are reported to the **Authority User** or **SysAdmin** and synchronized with the central management console.

3. Trusted Device Handling

Once verified, the **Authority User** or automated process determines whether to establish an execution environment.
The system then creates a corresponding **Trusted Sandbox** and authorizes the device to interact with the **Service APP**, ensuring smooth operation and data integrity within a secure environment.

4. Untrusted Device Handling

Devices identified as untrusted are automatically redirected to the **Honeypot Sandbox** for behavioral analysis and real-time threat monitoring. The **Trap Detector** is automatically activated to perform continuous scanning and monitoring, preventing potential intrusion or data compromise.

5. Reporting & Feedback

The **Alert Manager** continuously records all device actions and anomalies, generating detailed reports for the **SysAdmin** to review, analyze, and respond to incidents promptly.

6. Control & Policy Optimization

The **Authority User** refines trust policies and sandbox parameters based on security event insights.

System Requirements

Specifications	Description
CPU	Intel® Core™ / Xeon® processor
OS	Linux (Ubuntu 22.04 LTS or compatible)
Memory	16 GB RAM minimum
Storage	4 GB available disk space