Palitronica

ANVIL

Anvil SV–1 Product Overview

ANVIL SV-1

SEMICONDUCTOR INTEGRITY CHECKPOINT

1. **Verifies the hardware integrity of SoC and expansion card products post-manufacture.**
2. **Deploys end-of-line at the foundry for SoCs and at the contract manufacturer for expansion cards.**
3. **Detects hardware integrity attacks and modifications introduced during sourcing and manufacture.**

SV-1 ENABLES YOU TO

- Protect your products from hardware supply chain threats
- Drive stronger customer trust
- Enforce supplier accountability
- Shield your brand from supply-chain-enabled hardware attacks

SV-1 PROTECTS YOU FROM

- ✓ Hardware Implants
- ✓ Component Swapping
- ✓ Semiconductor Trojans
- ✓ Hardware Modifications
- ✓ Dormant Trojans
- ✓ Counterfeit Components

BEYOND PROVENANCE

Provenance is no longer sufficient. Hardware assurance is quickly emerging as a requirement from governments and cloud providers — with responsibility placed on semiconductor companies. With Anvil SV-1, you can efficiently and effectively meet these emerging requirements.

MITIGATE FABLESS RISK

Outsourced fabrication has driven fear amongst governments and cloud providers due to the potential for subversion. Anvil SV-1 allows you to benefit from outsourced fabrication while providing the assurance your customers require.

HARDWARE ASSURANCE THAT WORKS

Traditional hardware assurance practices are resource-intensive, unscalable, and require supplier participation. Anvil SV-1 enables you to provide efficient hardware assurance at scale and independent of your suppliers.

Anvil SV-1 recently demonstrated 100% accuracy in successfully detecting 120 compromised SoCs from a set of 220 units.

PALITRONICA

ANVIL RTS CASE STUDY

DEPLOYING ANVIL

1. BASELINE YOUR PRODUCT

Create a baseline for the SoC/expansion card SKU, enabling Anvil SV-1 to accurately verify the product against its known, “secure” baseline.

2. VERIFY PRODUCT END-OF-LINE

Anvil SV-1 verifies the SoC/expansion card end-of-line at the foundry (SoCs) or contract manufacturer (expansion cards) using the secure baseline.

3. SECURE PRODUCT DELIVERED

Your customer receives their secure SoC/expansion card alongside a digital certificate of hardware integrity.

UNIFIED VERIFICATION

Anvil SV-1 utilizes an in-situ test protocol, enabling whole-device verification in a single step — whether verifying an SoC or an expansion card.

ANVIL FEATURES

- ✓ **SUPPLIER AGNOSTIC**
  Supplier participation not required
- ✓ **UNPOWERED**
  Device is unpowered during verification
- ✓ **BLACKBOX COMPLIANT**
  No proprietary device information required
- ✓ **NON-DESTRUCTIVE**
  Verification does not alter the device
- ✓ **RAPID CYCLE TIME**
  Verification completed in seconds

CORE TECHNOLOGY

Anvil SV-1 employs proprietary, leading-edge side-channel analysis technology to verify device integrity against a known, secure baseline. When a device is modified, Anvil detects a discepency from the device’s baseline and alerts the operator.

HOW ANVIL WORKS

Anvil SV-1 verifies device integrity by connecting to the device’s ports. A button is pressed on Anvil SV-1, intiating the 5-15 second verification process. The operator is alerted following the process whether the device has been altered.