# PROTECTING YOUR ASSETS WITH TPIL SECURE ENVIRONMENT

TPIL was founded to provide cyber security solutions that defy the current cyber security consensus. We established ourselves as experts in our field by successfully completing highly complex projects, based on our expertise and products, for Israel Ministry of Defense (MOD) customers. We seek to take our products and expertise one step further and breakthrough to larger markets.

Current cyber security solutions rely on the untrusted OS and its applications as their core of trust. They use the untrusted OS unreliable channels to pass and store sensitive information. However, this reliance does not hold water with over 50M lines of code, constant updates, and an extremely high vulnerabilities detection rate. TPIL does not rely on the untrusted OS. With TPIL, the user puts his trust in a much lighter and more secure environment that is completely isolated from the untrusted OS.

## TPIL Secure Environment

TPIL Secure Environment is deployed in a target machine (cloud or on-premise) during the early boot process and is served as the core of trust.

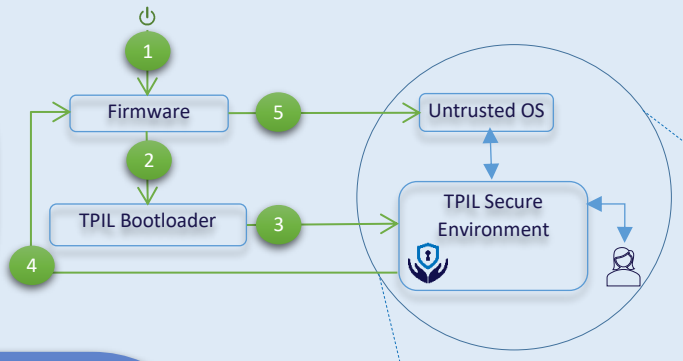
It completely controls the target HW and consequently the untrusted OS. Additionally, it provides OS inspection capabilities, isolated communication channel (for remote management), and secure storage. On top of TPIL Secure Environment, we implement various cyber security solutions through our Security Services. Security Services employed on top of TPIL Secure Environment are not affected by malware programs that exist on the untrusted OS and therefore can fulfill their security goals even when the OS is compromised.

### How Does It Work?

### TPIL Boot & Runtime Processes Diagrams

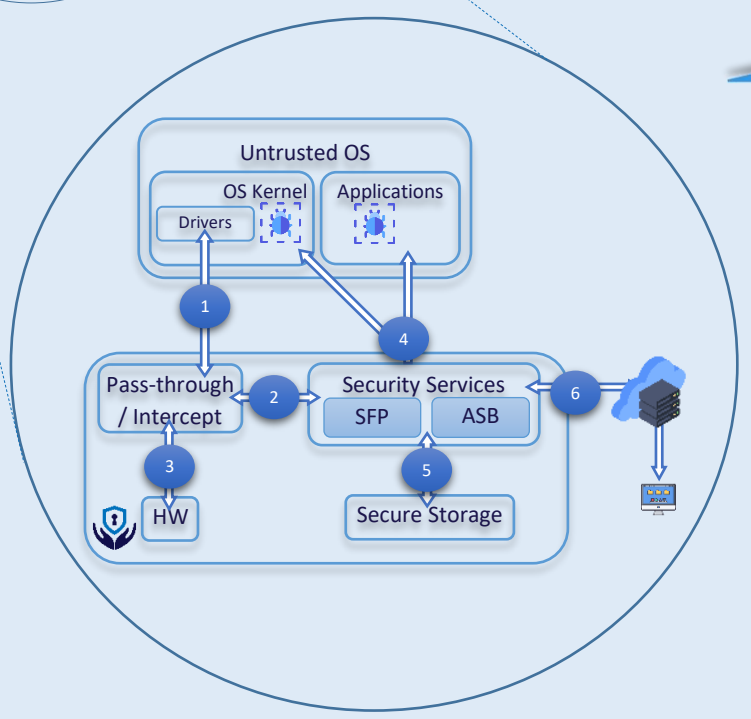
**Step-By-Step Boot Process:**

1. Machine powers-on to Firmware
2. Firmware loads TPIL Bootloader
3. TPIL Bootloader launches TPIL Secure Environment which now controls the machine
4. TPIL Secure Environment transfers control back to the firmware
5. Firmware loads the Untrusted OS which is under TPIL Secure Environment supervision




**Runtime Short-Explanation:**

1. HW Access by the OS is intercepted by TPIL Secure Environment
2. Relevant HW-events are passed to the security services employed in TPIL Secure Environment
3. Irrelevant HW-events are passed directly to HW
4. Employed Security Services inspect the OS kernel and applications
5. Employed Security Services uses an encrypted Secure Storage to store their data
6. An external user utilizes the TPIL Isolated communication channel to query/manage the employed Security Services




### TPIL Sensitive File Protection (SFP)

TPIL SFP protects your sensitive files from malware (e.g., ransomware-based) at the hardware level. TPIL SFP ensures that only legitimate processes can read sensitive data and that sensitive data is written untampered by legitimate processes.

### TPIL Application Sandboxing (ASB)

TPIL ASB protects an application at the hardware-level. TPIL ASB ensures that the application's code and data (both static and generated) are solely accessible to the sandboxed application.

TRULYPROTECT ISRAEL
PROTECT YOUR ASSETS

***Our Benefits***

- ✓ *Our solutions are not affected by the security state of the untrusted OS*
- ✓ *Our isolated communication channel is transparent to the untrusted OS and allows remote management of the protected targets*
- ✓ *Our secure storage allows storing persistent data in storage not accessible to the untrusted OS*
- ✓ *Our solutions support popular cloud providers including Amazon AWS, Google GCP, and Microsoft Azure*
- ✓ *Our isolated secure environment is very agile and can be easily extended to serve additional purposes with ease*
- ✓ *Our SFP solution effectively prevents high privileged ransomware-based malware*
- ✓ *Our ASB solution enhances the security level of your critical applications*

***Why Us***

- ✓ *We have more than 8 years of experience in computer security, virtualization, and trusted computing*
- ✓ *We've successfully completed highly complex for Israel MOD*
- ✓ *Among our customers are special, highly-qualified technological units*
- ✓ *We believe our infrastructure and capabilities are mature enough to breakthrough larger markets*

**CEO**

Dr. Roee Leon

Managing and Technologically Leading the Company for the Last Three Years