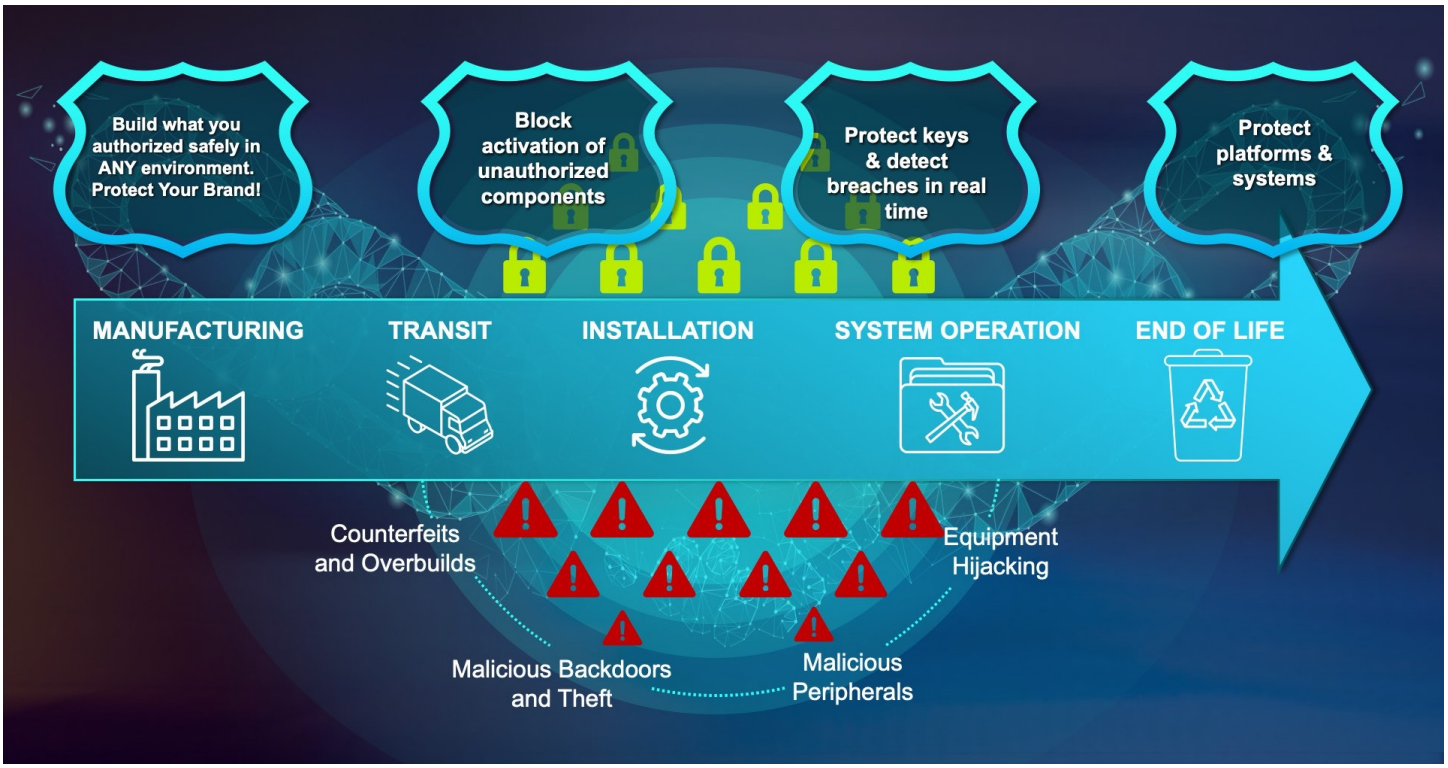
Lattice SupplyGuard™

Supply Chain Protection Service

LATTICE SupplyGuard



Robust End-to-End protection throughout today's supply chains, using standard Transportation, Factories, and Equipment

Ensuring end-to-end security throughout today's highly distributed and efficient supply chains is a daunting task: This system of common carriers, multiple suppliers and external, often offshore assembly houses provides many entry points for malicious actors to attack customer systems with malware, or to build cloned or overbuilt systems.

Lattice SupplyGuard™ provides an efficient end-to-end supply chain security solution for manufacturing which works with existing distribution, transportation, and manufacturing systems. No specialized or added equipment or processes is necessary.

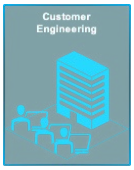
Lattice SupplyGuard provides powerful resiliency against tampering, trojans, overbuilding, and cloning throughout today's distributed and international supply chains.

SupplyGuard protection begins during FPGA production at Lattice. This protection is transferred to the customer's encrypted configuration bitstream, within the FPGA, when the FPGA is programmed at the customer manufacturing site. The result is a powerful end-to-end platform security.

End-to-End Security Service for Systems Based on a Platform Root of Trust

SupplyGuard-protected MachXO3D FGPAs are factory-locked

These FPGAs are locked using protected crytographic credentials known only to the end customer. These FPGAs can only be programmed with the customer's encrypted configuration bitstream containing those credentials.



SupplyGuard provides Customers with encryption credentials through a High Security Module (HSM). Customers use these credentials to cryptographically protect their FPGA's configuration bitstream.

This encrypted configuration bitstream can only be programmed onto SupplyGuard-protected FPGAs manufactured specifically for the customer.

During factory assembly, control is passed from the factory-locked state to the customer-locked state inside of the XO3D itself, using standard bulk programming tools. **No HSM required at the contract manufacturer.** Integrity remains protected at all times.

The customer's cryptographically-protected configuration bitstream can implement Lattice's Sentry Solutions Stack. This protection extends security to the rest of the firmware in the platform.

September 2022
I0274 Rev 2