Our Secure Supply Chain: Protecting Every Step

Supplier & Carrier Requirements

- Supply Chain Security and Information Security Policy
- Annual security checklist covering Procedural, Physical, Cyber, Personnel, and Training
- Mandatory AEO or CTPAT certification for carriers and 3PLs
- No sourcing from entities on the US Treasury SDN list

Manufacturing Integrity

- Full revision control of bill of materials and test processes
- Component traceability: Manufacturer, Part Number, Lot/Date Code, Serial Number
- Tamper-evident labels on all products

Counterfeit Detection & Avoidance

- Mandatory Counterfeit Electronic Part Detection and Avoidance System
  - Personnel training
  - Inspection/testing criteria
  - Traceability and AVL control
  - Reporting, quarantining, and suspect part identification
  - Flow-down to sub-tier suppliers
  - Awareness of counterfeiting trends

Product & Firmware Security

- Tamper-evident labeling on all products
- Only compiled binaries provided to suppliers (no source code)
- Secure Boot implemented on all high-end platforms since 2021 (e.g., 5420–8820)
- Encrypted/authenticated Linux kernel and bootloader using asymmetric keypairs

Global Supply Chain Resilience

- TAA-compliant manufacturing locations
- Multi-carrier transportation model to reduce risk
- Outsourced global service/RMA with location and system redundancy
- Best-in-class GTC processes to prevent unauthorized sales

©2026 EXTREME NETWORKS, INC. ALL RIGHTS RESERVED.