



Security Fabric

Secure Networks Have Four Things in Common



Security Intelligence Processing

Security awareness and threat intelligence boosts the performance of security tools.

- SSL decryption of traffic for improved distribution
- Data masking of sensitive data for improved compliance performance
- Threat intelligence blocks traffic from known bad IP addresses and regions where you do not do business



ATIP and ThreatARMOR™



Vision ONE

Context-Aware Data Processing

Identify the application, source location, and device type of each packet to decide which security tools need it, which do not, and which already have a duplicate of it.

- Enhanced Netflow awareness for improved intelligence
- Application intelligence and authentication
- Data conditioning like deduplication, timestamping, and burst protection

Security Resilience

Programmable bypass switches recognize and reroute traffic around outages.

- Industry's fastest heartbeat ensuring your tools are always available
- Serial tool-chaining or parallel paths for high availability
- Multiple failover options (active/active) (active/standby)



iBypass VHD



FlexTaps

Data Access Anywhere

Taps physical and virtual data anywhere, not just where a network switch exists.

- Ixia offers fiber, copper and virtual taps
- Get 100% access to physical and virtual traffic
- Higher reliability in heavy traffic conditions

What about SPAN ports

SPAN ports fall short as they drop packets, modify packet characteristics, and are deprioritized when network switches get busy.

Enterprise Security Solutions

Ixia Security Fabric integrates four layers for stronger enterprise protection. Connect inline or out-of-band tools with confidence.



And many more