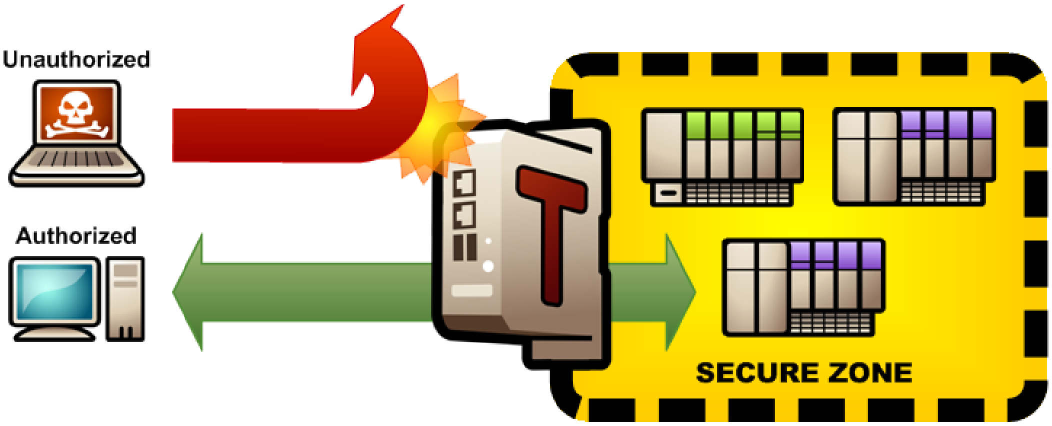
Tofino™ Argon Security Appliance

Creates Plug-n-Protect zones of security



Protect your control system against network problems and cyber threats

The electrical, environmental and operational requirements of SCADA and process control systems can make traditional IT-focused security solutions unsuitable for industrial networks. As a result, many critical systems operate with little protection against accidental or malicious cyber events. Entire plants have been shut down by an infected USB key or a mis-configured network device.

The Tofino Security Appliance (Tofino SA) is ideal for control professionals because it is a Plug-n-Protect™ product, designed to be installed in a live network with no pre-configuration, no network changes and no plant downtime. It provides a simple and cost-effective way to create zones of security – tailored protection for groups of PLCs, DCS, RTUs, IEDs and HMIs – as recommended by ANSI/ISA-99 and IEC Standards.

Tofino is designed with the environments, staff skills and needs of industry in mind. It protects better and is easier to install than IT firewalls and other security products.

Saves you money through:

- Improved system reliability and stability
- Reduced down time and production losses
- Lower maintenance costs
- Simplified regulatory and security standards compliance

Unique capabilities:

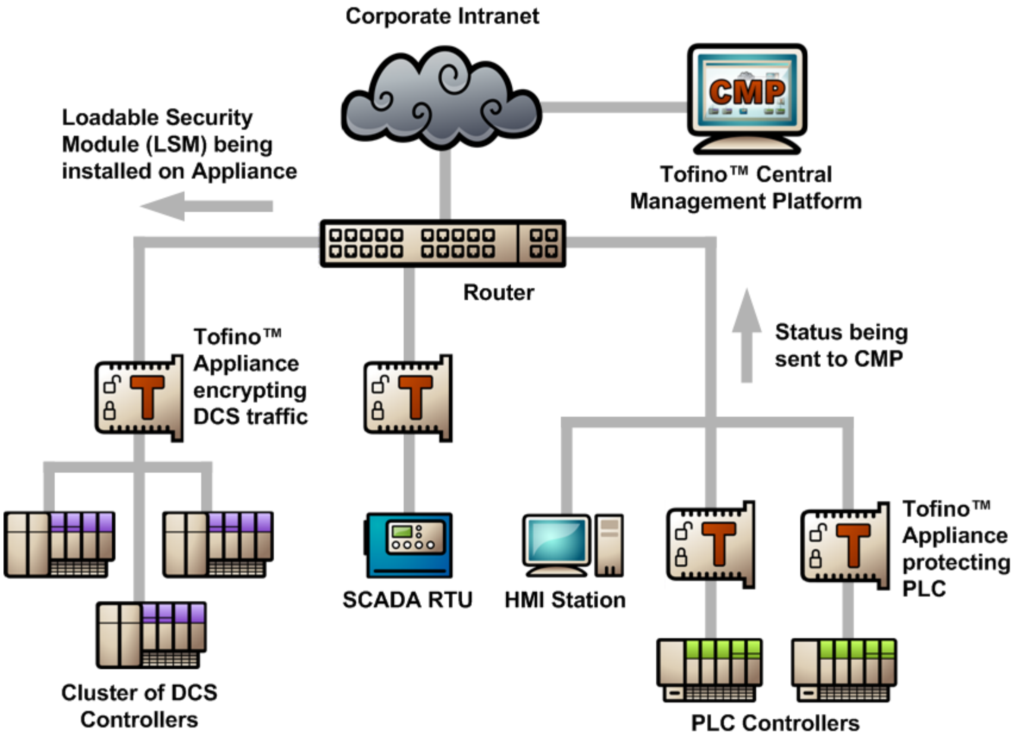
- Plug-n-Protect™ installation requires no pre-configuration, no network changes and no disruption to the control system
- Simple configuration over the network using the Tofino Central Management Platform (CMP) software
- Unique 'Test' mode allows firewall and VPN testing with no risk to your operation
- Compatible with all DCS, PLC, SCADA, networking and software products
- Rugged hardware design for years of reliable service

Typical applications:

- Secure networks with security zones as per NERC, ANSI/ISA-99 and IEC standards
- Protect connections to partner networks and wireless networks
- Improve SCADA and process control network reliability and performance

FROST & SULLIVAN
2010 World Customer Value Enhancement Award
tofinosecurity.com/awards

TOFINO®


Corporate Intranet
Loadable Security Module (LSM) being installed on Appliance
CMP
Tofino™ Central Management Platform
Router
Tofino™ Appliance encrypting DCS traffic
Status being sent to CMP
SCADA RTU
HMI Station
Tofino™ Appliance protecting PLC
Cluster of DCS Controllers
PLC Controllers

Protect vulnerable controllers	The PLCs, DCS, IEDs and RTUs in control networks are optimized for real-time I/O performance, not for robust networking connections. Even normal network traffic, like broadcast and multicast messages, can overload some devices and cause them to crash. *Tofino* makes it easy for the control technician to define rules that specify which network devices are allowed to communicate, and what protocols they may use. Any network traffic that does not fit the rules is automatically blocked by the Tofino SA and reported as a security alert.
Improve network segmentation	Many control systems have evolved from simple, stand-alone systems to complex interconnected networks. These networks are typically unprotected with no isolation between different sub-systems, so if a problem occurs in one area, it can quickly spread throughout the network. The Tofino SA is the ideal solution for segmenting a control network into security zones. It is installed into an existing system with no changes to the network, forming 'conduits' of communications between the zones. The control engineer defines rules that specify which network devices are allowed to communicate and what protocols they may use.
Guard against accidental and malicious intrusion	Even if your control network doesn’t connect to the Internet, you’re still at risk. Studies show that the vast majority of cyber security incidents originate from a variety of secondary points of entry into the network, including the enterprise network, maintenance connections, third-party networks (such as partner companies and contractors) and even transient sources, such as laptops and USB keys. A security risk assessment, combined with *Tofino*'s Zone Level Security strategy, identifies potential threat sources and entry points and isolates those points. If an attack does originate from a secondary entry point, the potential damage is easily contained within the zone in which the attack originated.
Installation	Plug-n-Protect installation to an operating control network with no pre-configuration, no network changes, no disruption to network traffic and no downtime

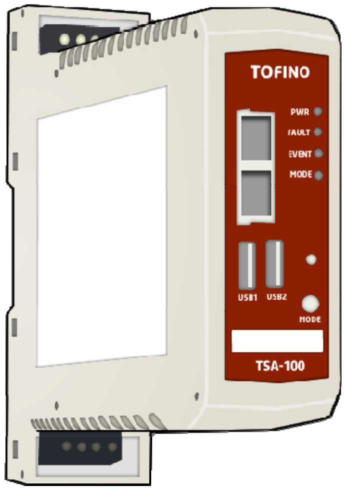
Configuration method	▪ *Network*: Tofino Central Management Platform (CMP) uses secure communications to configure Tofino SAs ▪ *Manual*: Encrypted configuration files may be saved on a USB storage device and loaded into the Tofino SA via a secure USB port
Operating modes	▪ *Passive*: all traffic allowed, no alerting ▪ *Test*: all traffic allowed; alerts generated as per user rules ▪ *Operational*: traffic filtered and alerts generated as per user rules
Mode changes	Operating mode is controlled remotely from the Tofino CMP
Security alerts	All alerts are reported to the Tofino CMP via 'heartbeat' messages or via optional syslog reporting
Diagnostics	Diagnostics may be captured by the Tofino CMP, or locally via USB storage device
Status indicators and controls	▪ Status indicators: 'Power', 'Fault', 'Mode' ▪ Traffic indicators: link status, speed and activity for each Ethernet port ▪ Pushbutton loads configuration from encrypted files or saves diagnostics to USB storage device
System requirements	▪ Tofino Central Management Platform (CMP) ▪ Loadable Security Modules (LSM) to implement the desired security features

	Tofino Argon 100	**Tofino Argon 220**
Interfaces	Two 10/100 Base T Ethernet twisted-pair interfaces (TX/TX)*	Two 10/100 Base T Ethernet fiber (MM) or twisted-pair (TX) interfaces in 4 variants (TX/TX, TX/MM, MM/TX, MM/MM)*
Power	▪ 9-32VDC; 24VDC nominal ▪ 170mA typical, 350mA max. at 24VDC ▪ Dual redundant power inputs; 24-12AWG screw cage terminals ▪ Dual power-fail indicator digital inputs	▪ 2-48VDC or 24 VAC (Rated); 60VDC Max ▪ Power consumption: 6.9W at 24VDC ▪ Dual redundant power inputs; 24-12AWG screw cage terminals ▪ Device/Interface fault relay output
Environmental	▪ Operating temperature: -40°C to +70°C ▪ Storage temperature: -40°C to +85°C ▪ Relative humidity: 10%-90% (non-condensing)	▪ Operating temperature: 0°C to +60°C ▪ Storage temperature: -40°C to +70°C ▪ Relative humidity: 10%-95% (non-condensing)
Certifications	▪ Class I, Div 2 hazardous environments ▪ CE mark (EMC compatibility) ▪ MUSIC 2008-1 security certification (Foundation) ▪ Certified Modbus compliant by Modbus-IDA	▪ Safety of industrial control equipment cUL 508 ▪ Germanischer Lloyd (pending) ▪ MUSIC 2009-1 security certification (Foundation) ▪ Certified Modbus compliant by Modbus-IDA
Vibration and shock	▪ IEC 60068-2-6: 1g @ 20-500Hz ▪ IEC 60068-2-27: 30g for 11ms shock ▪ EN 61326: EMC Annex A ▪ EN 61010-1	▪ IEC 60068-2-6: 1g @ 20-500Hz ▪ IEC 60068-2-27: 30g for 11ms shock
Mechanical	▪ Protection Class: IP20 ▪ Mounting: 35mm DIN rail ▪ Dimensions (mm): 42W x 146H x 138D ▪ Weight: 290g	▪ Protection Class: IP20 ▪ Mounting: 35mm DIN rail ▪ Dimensions (mm): 60W x 145H x 123D ▪ Weight: 615g
EMI radiation and immunity	▪ EN 55022 Class A ▪ EN 61000-4-2, EN 61000-4-3	▪ EN 55022 Class A ▪ EN 61000-4-2, EN 61000-4-3, EN 61000-4-4

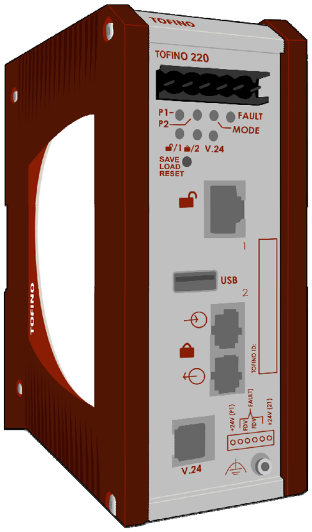
*For VPN deployment the upper or "untrusted" interface of the Tofino Argon Security Appliance must be used as the encrypted (i.e. external-facing) connection to the network. For all other applications, using this port as the external-facing connection is optional, but highly recommended to simplify rule configuration.

Tofino Argon 100 Model

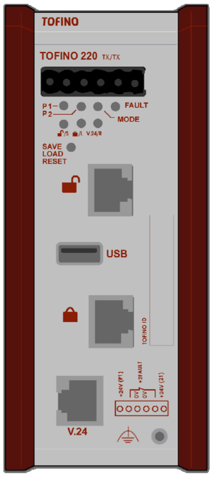
Tofino Argon 220 Models



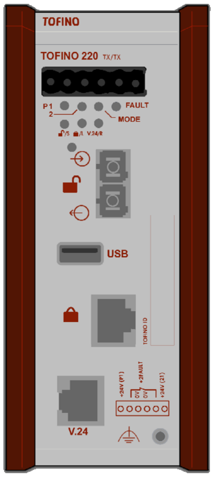
FA-TSA-100-TX/TX



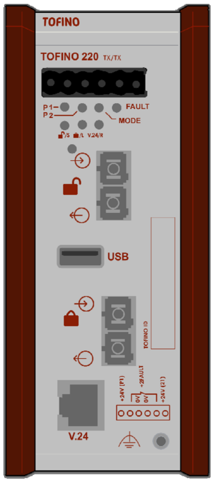
FA-TSA-220-TX/MM



FA-TSA-220-TX/TX



FA-TSA-220-MM/TX



FA-TSA-220-MM/MM

Part # FA-TSA-100-TX/TX	Name: **Tofino™ Argon 100 Security Appliance** (Untrusted Interface = Twisted Pair / Trusted Interface = Twisted Pair)
Part # FA-TSA-220-TX/MM	Name: **Tofino™ Argon 220 Security Appliance** (Untrusted Interface = Twisted Pair / Trusted Interface = Multimode Fiber)
Part # FA-TSA-220-TX/TX	Name: **Tofino™ Argon 220 Security Appliance** (Untrusted Interface = Twisted Pair / Trusted Interface = Twisted Pair)
Part # FA-TSA-220-MM/TX	Name: **Tofino™ Argon 220 Security Appliance** (Untrusted Interface = Multimode Fiber / Trusted Interface = Twisted Pair)
Part # FA-TSA-220-MM/MM	Name: **Tofino™ Argon 220 Security Appliance** (Untrusted Interface = Multimode Fiber / Trusted Interface = Multimode Fiber)
Ordering information	For additional information, visit www.tofinosecurity.com/buy/tofino-argon

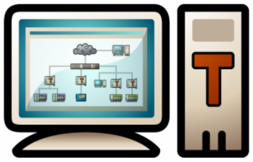
The Tofino™ Argon Security Appliance is a component of the Tofino Security Solution:

Tofino Security Appliance
Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks

Loadable Security Modules
Firmware modules that customize the security features of Tofino:

- **Firewall:** Directs and controls industrial network traffic
- **Modbus and OPC Enforcers:** Content inspection and connection management for Modbus and OPC
- **Secure Asset Management:** Tracks and identifies network devices
- **VPN:** Secures remote communications
- **Event Logger:** Reliably logs security events and alarms

Central Management Platform
Software that provides coordinated security management of all Tofino Security Appliances from one workstation or server



Your authorized Tofino supplier: