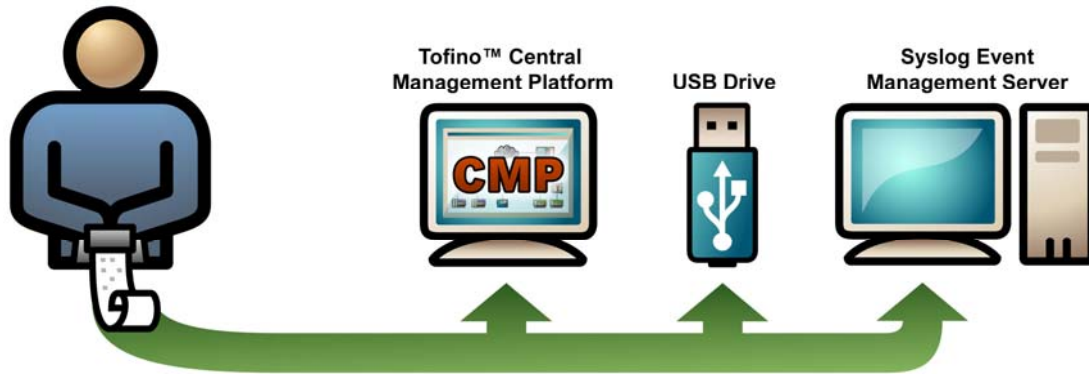


Tofino™ Event Logger LSM

Reliably logs security events and alarms

Data Sheet
MM-DS-LOG-100
Version 3-M

Tofino™ Event Logger LSM



Monitor and log security events and comply with ANSI/ISA-99 & NERC-CIP

Security standards demand that we monitor and log the security events and alarms that occur on industrial networks in order to better secure our plants.

The Tofino Event Logger Loadable Security Module (LSM) reliably records and protects security events and alarm information in SCADA and process environments. It is designed to be effective even when communication links are sporadic, providing unique triple protection of data: to remote IT syslog servers, to the Tofino Security Appliance for forwarding later when the connection is restored or offloaded to a USB key, and to the Tofino CMP (Central Management Platform) server.

The Tofino Event Logger LSM is deployable with or without a connection to a traditional IT syslog server or a Tofino CMP.

Reliably monitor and log your security events with the Tofino Event Logger LSM—an event logging system created for the industrial world.

Saves you money through:

- Increased industrial network reliability with triple logging of network events and alarms
- Easy data collection for standards compliance
- Reduced implementation, engineering and IT costs due to ease of deployment

Features:

- Provides triple redundancy by simultaneously recording security events to syslog servers, a Tofino CMP server, and local SA memory
- Protects event information even if communication links are interrupted
- Enables a Tofino SA to hold up to 20,000 security events and alarms in its memory
- Logs sent to a syslog server can be transported using UDP, TCP, or TLS protocols

Applications:

- Reliable event recording in SCADA systems that have sporadic communications
- Providing secure information from SCADA to traditional IT syslog servers
- NERC-CIP compliance: Monitoring (CIP 005), Ports & Services (CIP 007), and Security Status Monitoring (CIP 007)
- ISA-99 compliance when implemented as a part of the Tofino Industrial Security Solution

Tofino™ Event Logger LSM

Features and Specifications

Data Sheet

MM-DS-LOG-100

Version 3-M

| | |
|---|--|
| Triple protection event log generation | Enables a Tofino SA to log security and events alarms simultaneously: <ul style="list-style-type: none">▪ To a syslog server▪ Locally in the Tofino SA, for forwarding later when a connection is restored or for offloading to a USB storage device▪ To the Tofino CMP server |
| Event log back up | <ul style="list-style-type: none">▪ Continues to save logs even if syslog communications are interrupted▪ Enables a Tofino SA to save up to 20,000 security event logs locally |
| Transport protocols | Logs sent to a syslog server can be transported using UDP, TCP, or TLS |
| Encryption | Event logs sent to a syslog server can be encrypted (AES-128-CBC) for added security |
| Standards compliance | <ul style="list-style-type: none">▪ NERC-CIP compliance: Monitoring (CIP 005), Ports & Services (CIP 007), and Security Status Monitoring (CIP 007)▪ ISA-99 compliance: Helps create Zone-level Security™ when implemented as a part of the Tofino Industrial Security Solution |
| Configuration method | Simple, centralized configuration using the Tofino CMP |
| Operating modes | All standard <i>Tofino</i> modes supported: <ul style="list-style-type: none">▪ <i>Passive</i>: all traffic allowed, full reporting of new devices with SAM LSM▪ <i>Test</i>: all traffic allowed; alerts generated as per user rules▪ <i>Operational</i>: traffic filtered and alerts generated as per user rules |
| System requirements | <ul style="list-style-type: none">▪ Tofino Security Appliance▪ Recommended: USB storage device▪ Recommended: Tofino Central Management Platform |
| Ordering information | Part number: 9520-EL Name: Tofino Event Logger LSM Visit: www.mtl-inst.com/tofino for ordering info for all products. |

The Tofino™ Event Logger LSM is a component of the Tofino Industrial Security Solution:

Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control networks.



Loadable Security Modules

Firmware modules that customize the security features of *Tofino*.

- **Firewall**: Directs and controls industrial network traffic
- **Modbus TCP Enforcer**: Content inspection for Modbus
- **Secure Asset Management**: Tracks and identifies network devices
- **VPN**: Secures remote SCADA communication
- **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.



EUROPE (EMEA)
AMERICAS
ASIA PACIFIC
EMAIL

+44 (0) 1 582 723633
+1 888 9TOFINO
+65 6 487 7887
tofinosupport@mtl-inst.com

TOFINO™
tofinosecurity.com