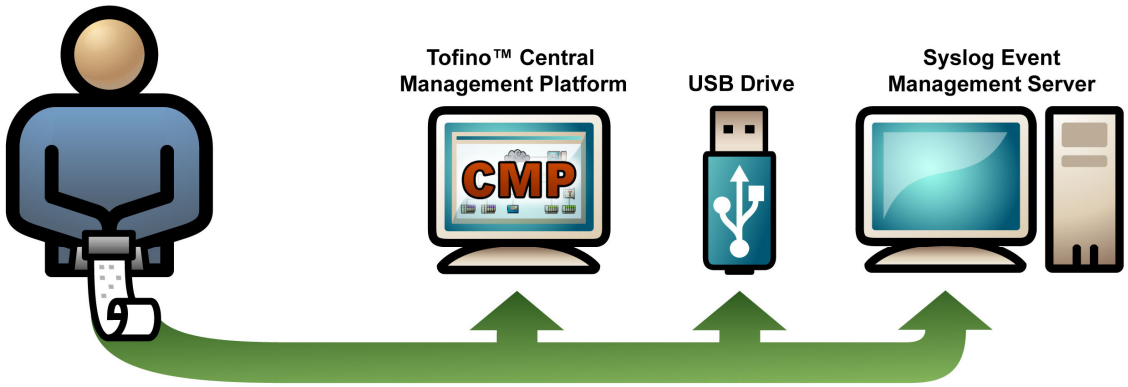
Tofino™ Event Logger LSM

Reliably logs security events and alarms

Data Sheet
DS-LOG-LSM
Version 5.0

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 facilities.

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 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

Unique capabilities:

- Provides triple redundancy by simultaneously recording to a syslog server, a CMP server and local Tofino 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

Typical 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

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

TOFINO®

Tofino™ Event Logger LSM

Features and Specifications

Data Sheet
DS-LOG-LSM
Version 5.0

Triple protection event log generation	Enables a Tofino SA to log security and events alarms simultaneously: ▪ To a remote 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	▪ Continues to save logs even if syslog communications are interrupted ▪ Enables a Tofino SA to save up to 20,000 security events 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	▪ 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 *Tofino* modes supported: ▪ *Passive*: all traffic allowed, full reporting of new devices with SAM LSM ▪ *Test*: all traffic allowed; alerts generated as per user rules ▪ *Operational*: traffic filtered and alerts generated as per user rules
System requirements	▪ Tofino Security Appliance ▪ Recommended: USB storage device ▪ Recommended: Tofino Central Management Platform
Ordering information	Part number: **LSM-LOG-100** Name: **Tofino™ Argon Event Logger LSM** For additional information, visit www.tofinosecurity.com/buy/tofino-argon

Tofino™ Event Logger LSM 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

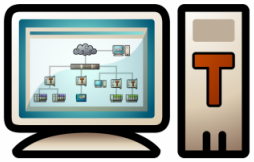
Loadable Security Modules

Firmware modules that customize the security features of each Tofino SA:

- **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 communication
- **Event Logger:** Reliably logs security events and alarms

Tofino CMP

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



Your authorized Tofino supplier:

TOFINO™
tofinosecurity.com