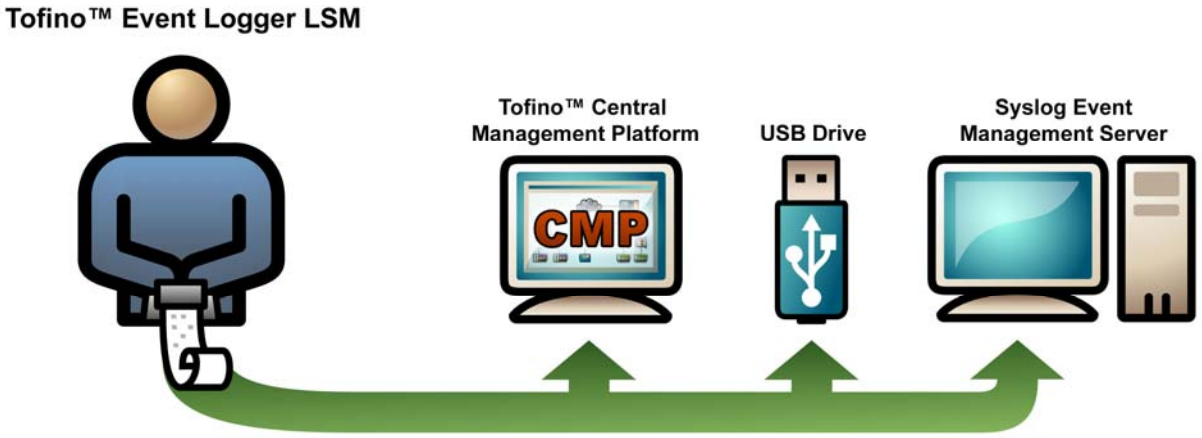
Tofino™ Event Logger LSM

可靠的安全事件日志和警报



遵从 ANSI/ISA-99 & NERC-CIP 监控和记录安全事件

为了更好地保护我们的设备，安全标准要求我们能够监测和记录发生在工业网络上安全事件和报警。

Tofino 的事件记录可装载模件（Tofino Event Logger Loadable Security Module）可以在 SCADA 及过程控制环境下真实可靠地记录并保护安全事件和报警信息，即使是不定时的通讯连接它仍然是有效的。它具有独特的三重数据保护功能：传输到远 程 IT syslog 服务器；当故障连接恢复后或一个 USB 密钥被卸载时传输到 TSA 上；传输到 CMP 服务器。

不管是否连接到 IT 系统日志服务器或 CMP 上，事件记录可装载模块都是可以轻易进行部署设置的。

Tofino 事件记录可装载模块对您的安全事件提供了可靠的监控功能和记录 功能，它是 一个专为工业控制网络设计的日志记录系统。

节约成本措施：

- 凭借三重网络安全事件和报警记录功能增强网络可靠性
- 为各种标准的执行提供了便捷的数据采集
- 通过简化设备部署达到降低项目实施、工程设计及 IT 产品成本的目的。

特有功能：

- 同时在系统日志服务器、CMP、和本地 TSA 存储器上记录事件信息，达到三重冗余的效果。
- 即使网络通信中断仍然可以保护事件信息。
- 一台 TSA 的存储器可以支持多达 20000 条安全事件和报警的存储。
- 可以通过 UDP、TCP 或 TLS 等协议将安全日志传输到系统日志服务器。

典型应用:

- 为不定时通讯的 SCADA 系统提供可靠的事件记录。
- 提供从 SCADA 系统到传统 IT 系统日志服务器之间传输的路径。
- 遵从 NERC-CIP（北美电力可靠性委员会关键基础设施保护）解决方案: 监控 (CIP 005), 端口与服务 (CIP 007), 安全状态监控 (CIP 007)
- Tofino 工业安全解决方案的实施遵从 ISA-99 标准

TOFINO®

Tofino™ Event Logger LSM

特点及规格

三重保护事件日志生成	允许TSA同时记录安全事件和报警： ▪ 记录到远程 syslog 服务器 ▪ 当通讯故障或 USB 存储设备卸载后在 TSA 本身进行事件记录，当通讯故障解决或插入 USB 存储设备后事件记录自动转储 ▪ 记录到 Tofino CMP 服务器
事件日志备份	▪ 即使 syslog 通讯中断仍然能保存系统日志记录 ▪ 一台 TSA 的存储器可以支持多达 20000 条安全事件和报警的本地存储
传输协议	可以使用 UDP，TCP 或 TLS 等传输协议将日志发送到 syslog 服务器
记录加密	为增强安全性，事件日志发送到系统日志服务器时可以进行加密（AES – 128-CBC ）
遵从标准	▪ 遵从 NERC-CIP 解决方案: 监控(CIP 005), 端口及服务 (CIP 007), 安全状态监视 (CIP 007) ▪ 遵从 ISA-99 标准: 当 Tofino 安全解决方案实施时可以建立网络区域分层安全模式
配置方式	使用 CMP 可以既简单又集中地进行配置
操作模式	支持所有标准 Tofino 模式： ▪ 被动模式：允许所有的通讯，全面提供新设备 SAM LSM 模块的报告 ▪ 测试模式：允许所有的通讯，为每个用户安全规则生成报警信息 ▪ 操作模式：过滤通讯内容，为每个用户安全规则生成报警信息
系统要求	▪ Tofino 安全设备 ▪ 推荐：USB 存储设备 ▪ 推荐：Tofino 中央管理平台（CMP）
订购信息	产品型号: **LSM-LOG-100** 名称: **Tofino™ Argon Event Logger LSM** 更多内容请访问 www.tofinosecurity.com/buy/tofino-argon

Tofino™ Event Logger LSM 是 Tofino 工业安全解决方案的重要组成部分之一:

Tofino 安全设备（TSA）

Tofino Security Appliance

通过硬件平台为控制和 SCADA 网络安全建立了即插即用安全保护区域。

可装载安全模块（LSM）

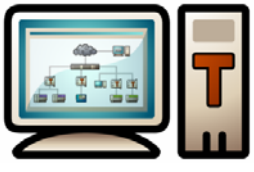
Loadable Security Modules

为 TSA 专门定制的各种可装载安全模件：

- **防火墙**：指导并控制工业网络信息流通
- **Modbus 与 OPC 应用:**深层次的 Modbus 及 OPC 的通讯检测和连接管理
- **安全资产管理:** 追踪并识别网络设备
- **VPN:** 安全的虚拟网络远程通讯
- **事件记录:** 可靠的安全事件和报警信息记录

Tofino CMP

通过一台工作站或服务器对所有 Tofino 安全设备（TSA）进行集中组态、管理并进行报警记录的软件系统



TOFINO™
tofinosecurity.com