

# EdgeIPS™ Pro 工业网络集群式意向智能入侵防御 (IPS)

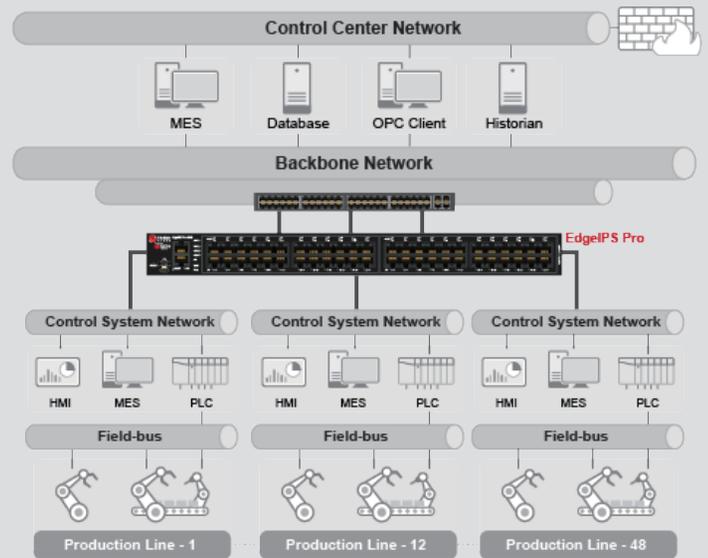
目录

## 工业级集群多点网络隔离、全透明式信息安全防护设备，保护关键工业设备确保生产线持续运作

在工业网络信息安全防护方法中，建立意向式网络隔离是一有效的防御基础，通过它可减少恶意攻击并且降低恶意攻击所造成的影响。一般来说，有两种有效的网络隔离方式：内部隔离 (Internal Segmentation) 与微隔离 (Micro-Segmentation)。严格来说微隔离是最有效的方式，但同时也需要考虑如何解决大规模网络部署与多点管理的问题。

EdgeIPS Pro 就是为了解决上述的问题而设计，除了提供机架式的解决方案部署外，搭配内置的深层工控网络协议解析功能，即使运用于复杂的工控网络内也让微隔离管理更加容易。EdgeIPS Pro 包含了 EdgeIPS 单点防护的所有功能并以此延伸至多点网络隔离防护的中央集群管理，此全透明式信息安全防护设备完全符合 IT-OT 集成的工作环境。

EdgeIPS Pro 在每个多点防护的网络端口全部支持第三代硬件旁路功能 (Hardware Bypass) 以确保生产线持续运作，此外 EdgeIPS Pro 除了提供高强度可视化的网络信息安全防护，还能将旧系统以及未能修补漏洞的重要设备纳入保护范围内。



## 产品功能特点

### 配置文件快速设置，轻松维护运行，高效信息安全管理

- 快速简易部署，无需修改现有网络架构。
- 方便不同管理要求，提供集中可视化管理系统 (OT Defense Console) 与单机管理功能。
- 符合 OT 环境硬件运作性能要求相关认证，支持标准机架安装尺寸，备用电源供给设计以及高可用性。

### 多点网络隔离功能针对不同要求及弹性部署而变化

- 针对不同要求所设计的弹性部署，通过中央管理接口迅速反应威胁确保信息安全保护持续运行。
- 保护旧系统以及未能修补漏洞的重要设备。
- 虚拟补丁 (Signature-Based) 为脆弱系统提供保护，阻断利用已知漏洞所发动的网络攻击。
- 配合工控 SOP 来对应信息安全事件。

### 呈现工控网络内部署的关键设备资产能见度

- 通过被动式网络查访来检测位于工控网络的资产设备。
- 寻找识别网络中隐藏的 OT 设备 (Shadow OT)。
- 净化过滤 OT 网络通讯。
- 无干扰纪录信息安全事件与网络监控日志功能设计。
- 内置日志查看查询功能。

### 高可用性设计容错多点网络隔离

- 容错转换采用主动检测与被动检测模式。
- 支持 24 组对称式与 48 组对称式网络接口以利多点网络隔离部署，每一组都支持硬件旁路功能，便利功能更新与系统维护时间内不影响生产线运作。
- 模块化可插拔网络扩充卡设计。

WWW.TXOne-networks.com

©2020 版权所有。TXOne Networks, Inc. 保留所有权利。Trend Micro 与 t 球形标志是趋势科技股份有限公司的商标或注册商标。所有其他公司和产品名称为各该公司的商标或注册商标。



## 主要功能

### ● 支持多点网络隔离的集成式防护

EdgelPS Pro 是针对 Purdue Model 之 L1 至 L3 网络架构所设计的信息安全解决方案，可以部署于重要设备前端或是在部署网络节点位置，在以不干扰工控网络做的前提下进行保护同时也可以全透明式检测位于其他部署于网络内的设备资产。

### ● OT 网络通讯深度智能学习运作

EdgelPS Pro 采用先进 TXOne One-Pass DPI (TXODI™) 工控网络分析引擎解析 L2 至 L7 的网络内容，更进一步提供了深度网络白名单管理功能。

### ● 多点高密度网络集群设计兼顾不同要求弹性部署

在兼顾信息安全防护与生产线运行的要求下，EdgelPS Pro 同时提供了监测模式与保护模式以方便不同的管理要求，并可支持至 24 对网络组别与 48 对网络组别。

### ● 检测网络中隐藏的 OT 设备 (Shadow OT) 以提高 IT 与 OT 融合环境的信息安全管理范围

EdgelPS Pro 方便在 IT 与 OT 融合的环境内兼顾不同的管理要求，另外也提供检测网络中隐藏的 OT 设备扩大信息安全防守范围。

### ● 特征式虚拟补丁

通过虚拟补丁，您的网络将拥有强大而实时更新的第一线防御来防范已知威胁。用户可精确掌控修补的流程，当发生信息安全事件时能为老旧系统提供额外的防护。

### ● 一流的威胁情报与数据分析

EdgelPS Pro 能利用最新的威胁信息来提供先进的未知威胁防护。以 Zero Day Initiative (ZDI) 漏洞悬赏计划的尖端研究为后盾，EdgelPS Pro 能针对尚未揭露的漏洞以及零时差威胁，为您的生产网络及系统提供独家防护。

### ● 广泛支持各种产业通讯协议

EdgelPS Pro 可支持的 OT 通讯协议包括 Modbus、Ethernet/IP、CIP、EDA 等等，因此 OT 和 IT 信息安全系统管理员能彼此配合，进而与现有的网络架构无缝集成。

### ● 通过方便的综合查看轻松集中管理

所有特征码更新与固件管理都能从中央控制台整批执行。系统管理员可通过 OT Defense Console (ODC™) 来管理已配置 EdgelPS Pro 的厂房，不仅能降低成本，更能大幅提升效率。

## EdgelPS™ Pro 规格



功能	EdgelPS Pro 1048	EdgelPS Pro 2096
支持的 IPS 流量检查吞吐量	10Gbps	20Gbps
平均延迟 (Latency)	< 200 microseconds	
并发联机数 (TCP)	2 Million	4 Million
支持的 ICS 通讯协议	Modbus / EtherNet IP / CIP / FINS / S7Comm / S7comm+ / TOYOPUC , 其它持续增加中	
政策规则	50,000 Rules	100,000 Rules
ICS 通讯协议配置文件	256 Profiles	256 profiles
机身规格	1U rack mount	2U rack mount
重量 (设备本体)	15.8kg (34.854 lb)	23.67kg (52.182 lb)
尺寸 (宽 x 深 x 高)	438mm x 750mm X 44mm (17.24 X 29.53 X 1.73 in)	438mm x 750mm X 88mm (17.24 X 29.53 X 3.46 in)
网络接口类型	10 / 100 / 1000 BASE-TX (RJ-45) x 48 ports	10 / 100 / 1000 BASE-TX (RJ-45) x 96 ports
故障安全机制 (Fail-Safe)	24 Segments Gen3 Hardware bypass	48 Segments Gen3 Hardware Bypass
USB 接口 / Serial Console	1x USB Interface (Type-A) / 1x USB Interface (Type-C) for serial console	
管理接口 (MGMT) / 镜向接口	1 x 10GE / 1GE RJ-45 (MGMT) / 1 x 10GE / 1GE RJ-45 (Mirror)	
高可用性 (HA) 端口	1 x 10 / 100 / 1GE RJ-45 for HA Port	1 x 10 / 100 / 1GE RJ-45 for HA Port
输入电压	90 ~ 264 VAC FULL RANGE	90 ~ 264 VAC FULL RANGE
操作温度	0 - 40°C (-40 - 167°F)	0 - 40°C (-40 - 167°F)
环境相对湿度	5 to 95% (non-condensing)	5 to 95% (non-condensing)
存储温度	-40 - 85°C (-40 - 185°F)	-40 - 85°C (-40 - 185°F)
震动	2 Gems @ UEC 60068-2-64, random wave, 5-500HZ, 1hr per axis (without any USB devices attached)	2 Gems @ UEC 60068-2-64, random wave, 5-500HZ, 1hr per axis (without any USB devices attached)
平均故障间隔时间 (MTBF)	500,000 hours based on 25°C	500,000 hours based on 25°C
安规认证	CE, UL, EN60950-1, IEC609-1, UL60950-1	CE, UL, EN60950-1, IEC60950-1, UL60950-1
电磁兼容性	VCCI, FCC	VCCI, FCC
绿色产品标志	Rohs, CRoHS, WEEE	Rohs, CRoHS, WEEE
中央管理系统	Supported OT Defense Console, ODC	Supported OT Defense Console, ODC

