头豹 LeadLeo

# 2025中国工业防火墙行业洞察

## 安全升级，数字化转型的护航者

概览标签：工业防火墙、网络安全、工业协议安全

China Industrial Firewall Industry

中国インダストリアルファイアウォール産業



头豹研究院

# 研究目标

## 研究背景

本研究旨在系统性解构工业防火墙产业生态，通过深度解析其市场定位、产业链拓扑结构、技术演进轨迹及跨行业应用场景，揭示工业防火墙作为网络安全基础设施的战略价值，同步构建涵盖技术路线规划、产业链协同机制、场景化应用策略的三位一体实施框架，为产业界把握数字安全升级浪潮提供决策范式。

## 研究目标

- 分析工业防火墙的部署应用
- 分析工业防火墙跨行业应用场景与产业协同机制

## 本报告的关键问题

- 工业防火墙在网络安全产业生态中扮演何种核心角色？
- 工业防火墙在各行业中展现出哪些典型应用场景？

# 观点摘要

## 01 工业防火墙的痛点与驱动因素：

◆ 工业防火墙主要采用一次性买断和服务订阅两种商业模式，其中约70%的企业倾向于买断方式，而随着云服务发展，SaaS化订阅模式逐渐兴起，尤其适用于中小企业和数据敏感度较低的场景，占市场约25%

## 02 工业防火墙的行业应用：

◆ 工业防火墙已成为电力、石油化工等关键行业的核心安全防护设备，在应对勒索软件、APT攻击等网络威胁方面发挥重要作用，保障生产连续性与关键基础设施的稳定运行，正向更多行业加速渗透与应用

## 03 工业防火墙市场的竞争格局：

◆ 2024年，中国工业防火墙市场呈现明显梯队化竞争格局，启明星辰凭借技术积累和产品布局稳居领导者梯队，市场份额高达35.9%；威努特、天融信、奇安信位列挑战者梯队，具备各自差异化优势；六方云等厂商则处于追随者梯队，专注细分市场，形成多层次竞争态势

# 内容目录

# Chapter 1
# 工业防火墙行业市场综述

- 工业防火墙部署应用
- 工业防火墙发展历程

# 工业防火墙行业市场综述——部署应用

工控防火墙主要应用于工业控制系统的三个场景：一是层级间安全防护，防止IT层威胁渗透；二是同层级网络内不同控制域间的安全防护，限制攻击横向蔓延；三是现场控制层设备的安全防护

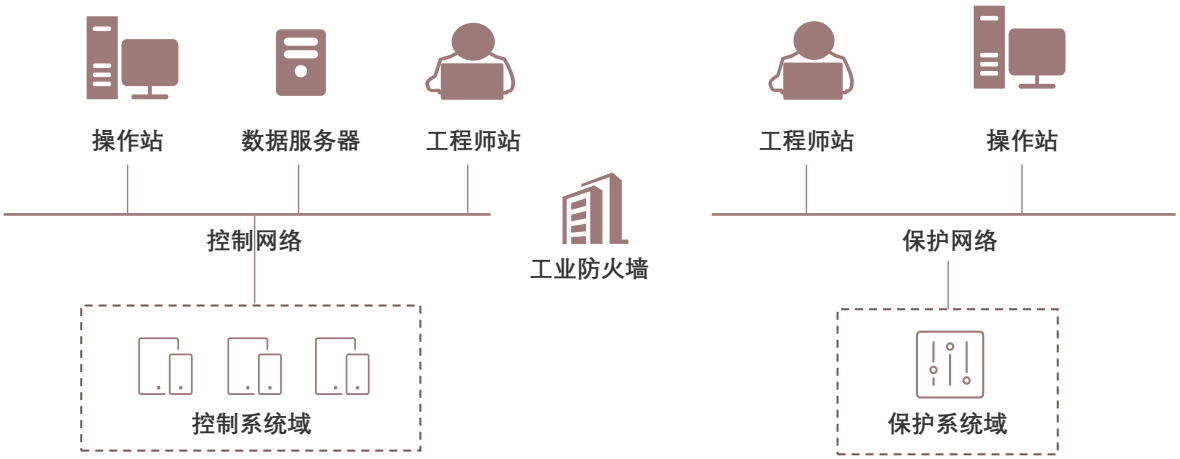
## 工业防火墙在工业控制系统的应用

➢ 工业防火墙在生产管理层网络与过程控制层网络之间的安全防护


■ 工业防火墙隔离管理层与控制层网络，防止外部威胁渗透控制系统，保护关键设备安全

生产管理层网络承担生产计划、调度等功能，常与办公网相连，面临较高外部攻击风险；过程控制层网络直接连接现场工业设备，负责实时监控生产过程。工业防火墙的部署可阻止生产管理层潜在威胁渗入过程控制层，保护关键生产控制设备与系统，同时防止过程控制层敏感信息被非法获取，保障生产连续稳定。

➢ 工业防火墙在区域间的安全防护




■ 工业防火墙隔离控制域间网络，防止风险扩散，并通过授权访问控制保障域间通信安全与独立性

大型工业控制系统中，同层级网络会按功能、区域或业务需求划分多个控制域，如化工企业不同车间或生产线。工业防火墙的部署可以隔离不同控制域网络流量，避免一个控制域的安全问题扩散至其他控制域。同时，还可以对不同控制域之间的通信进行访问控制，确保只有授权的通信才能通过，保障各控制域的独立性和安全性。

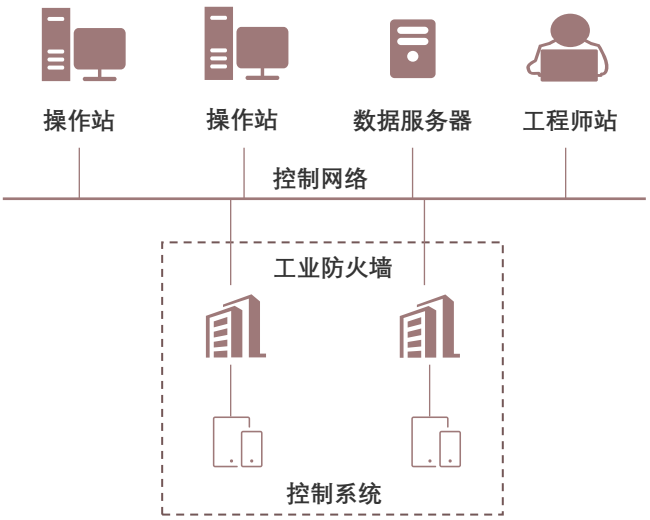
来源：专家访谈，头豹研究院

# （接上页——部署应用）

工业防火墙在工控系统中的三大应用场景呈现阶梯式分布：层级间防护（50%）构筑层级核心防线，同层级隔离（30%）实现横向威胁管控，设备级防护（20%）作为终端补充方案

## 工业防火墙在工业控制系统的应用

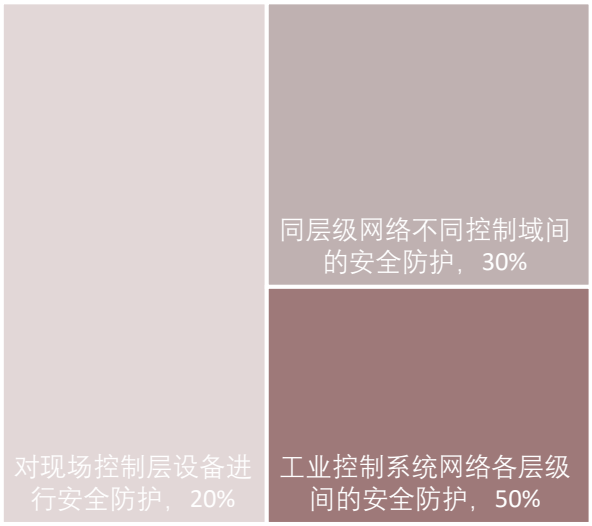
➢ 工业防火墙在现场控制层设备的安全防护




■ **工业防火墙可保护现场控制层设备免受网络攻击，但因引入延迟，不适用于对通信实时性要求高的场景**

现场控制层设备是工业控制系统的底层基础，直接与生产过程交互，其安全性至关重要，如PLC（可编程逻辑控制器）、RTU（远程终端单元）和DCS（分布式控制系统）均直接参与生产过程的控制与监测。工业防火墙可部署在此层级关键节点（如PLC、传感器与执行器）前端，通过深度包检测与访问控制，过滤异常或恶意网络流量，有效防范针对设备的网络攻击与非法控制指令，如阻止对PLC程序的远程篡改，避免由此引发的生产故障或安全事故。然而，由于防火墙的流量解析与策略执行可能引入延迟，该部署方式不适用于对通信实时性要求较高的控制场景。

➢ 工业防火墙的不同应用比例，2024年




■ **工业防火墙应用呈层级优先、精细演进、终端补充的差异化格局**

工业防火墙在工业控制系统中的三大典型应用场景呈现出明显的差异化分布，其中层级间防护占比高达50%，依旧构成工业防火墙的“基本盘”，表明企业普遍重视隔离管理层与控制层等不同网络层级，以防止IT侧威胁下沉至OT核心系统，满足等保2.0等标准对分区隔离的强制要求。其次，同层级隔离占比达30%，体现出工业网络安全从“粗放式分区”逐步迈向“精细化管控”，通过划分安全域，限制横向攻击的传播路径，适配多产线、多系统并行运行的复杂工况。相比之下，设备级防护仅占20%，说明直接防护如PLC、传感器等终端设备的方式受限于实时性和成本等因素，更多依赖轻量级方案作为补充。

来源：头豹研究院

# 中国工业防火墙行业综述——发展历程

工业防火墙发展历经技术迭代：1989年静态包过滤起步，2000年代实现国产化突破，2010年代完成标准化建设，2020年代形成集威胁检测、协议解析于一体的智能防护体系

## 防火墙与工业防火墙的发展历程

**1989年**

### 第一代防火墙

采用静态包过滤技术，依赖路由器功能，按预设规则检查数据包，遵循最小特权原则进行访问控制。

### 第二代防火墙

通过TCP连接中继网络，客户端与服务器不直接连接，无法识别应用协议，需客户端提供连接信息。

### 第三代防火墙

基于代理结构，通过应用层代理服务实现内外系统隔离，增强对应用流量的控制能力。

### 第四代防火墙

采用动态包过滤技术，根据实时连接状态与预设逻辑动态生成规则，提升数据流控制的灵活性。

**1998年**

### 第五代防火墙

引入自适应代理技术，提升代理处理效率与智能化水平，拓展传统代理防火墙的能力边界。

**2004年**

### 第六代防火墙

统一威胁管理（UTM）概念提出，集成防火墙、防病毒、入侵检测等功能于一体，提升整体防御力。

**2008年**

### 下一代防火墙

具备应用感知、内容识别与智能防护功能，集成IPS与安全情报，提升企业级网络安全可视化与管控力。

## 工业防火墙的发展历程

**1990年代**

### 防火墙早期发展阶段

1996年，中国推出了第一套自主知识产权的NGFW2.0，标志着中国防火墙技术的起步。随后，1998年，基于包过滤技术的防火墙系统开始出现，2000年，应用代理技术的NGFW3000系列面世，这些早期产品主要面向IT环境，尚未涉及工业控制领域。

**2000年代中后期**

### 工业防火墙的兴起

随着工业4.0和智能制造的推进，工业控制网络的开放性和复杂性增加，对网络安全提出了更高要求。2005年，中国第一套采用自主研发ASIC芯片的“猎豹”系列防火墙问世，标志着国产防火墙在性能和功能上达到国际一流水平。

**2010年代**

### 工业防火墙的标准化

2010年代，随着国家对工业信息安全的重视，工业防火墙的标准工作逐步推进。2013年全国信息安全标准化技术委员会批准《信息安全技术—工业控制系统专用防火墙技术要求》的制定工作。

**2015年**

### 工业防火墙的规范化

2015年，公安部联合深信服科技等厂商发布了第二代防火墙标准，标志着国内下一代防火墙产品有了指导标准。2019年，公安部第三研究所发布了《信息安全技术 工业控制系统专用防火墙技术要求》（征求意见稿），进一步完善了工业防火墙的标准体系。

**2020年代**

### 工业防火墙高速发展

2020年代，工业防火墙在工业4.0和智能制造的推动下，市场需求持续增长。2024年，启明星辰集团连续六年稳居中国工业防火墙市场第一，技术革新与国产化适配助力工业网络安全新时代。

来源：专家访谈，头豹研究院

# Chapter 2
# 中国工业防火墙产业链洞察

- 产业链中游-部署方式
- 产业链下游-行业应用

# 中国工业防火墙产业链中游分析——部署方式

工业防火墙部署以本地为主（60%），兼顾云部署（40%）；商业模式上，一次性买断（70%）仍占主流，服务订阅（25%）随云发展逐渐兴起，满足中小型企业灵活需求

## 工业防火墙部署方式



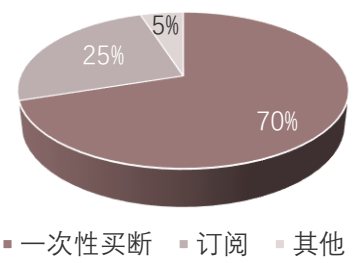
### 部署特点

- 数据保留在企业内部，减少了通过公共网络传输带来的风险
- 更高的定制化能力，可以根据企业的具体需求调整配置
- 初始投资较高，包括硬件购买、安装及维护成本

### 部署特点

- 降低了初期资本支出，采用按需付费模式，灵活性强
- 快速部署，易于扩展，可以迅速适应业务增长的需求
- 可能存在一定的安全隐患，因为数据需要通过互联网进行传输和存储

## ➢ 工业防火墙商业模式分析




■ **工业防火墙商业模式主要分为两种：一次性买断和服务订阅**

一次性买断是工业防火墙最常见的商业模式，企业一次性购买包括软硬件及授权在内的全套服务，获得永久使用权，只需进行后续如特征库更新等维护工作，约70%的企业倾向于这种模式。随着云服务的发展，技术外包和服务订阅（SaaS化）也成为一种趋势。供应商提供基于云的工业防火墙服务，用户通过租赁或订阅方式使用这些服务，这种方式特别适合数据敏感度不高、规模较小的企业，占据市场总量的25%左右。

来源：专家访谈、头豹研究院

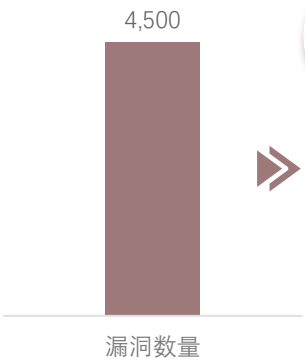
# 中国工业防火墙产业链下游分析——行业应用

工业防火墙在电力、石油石化等行业应用广泛，成为核心安全设备；精细化工、轨道交通、冶金、制药行业逐步加强防护；装备制造业智能制造增多但安全投入有限；纺织/轻工行业多以物理隔离为主

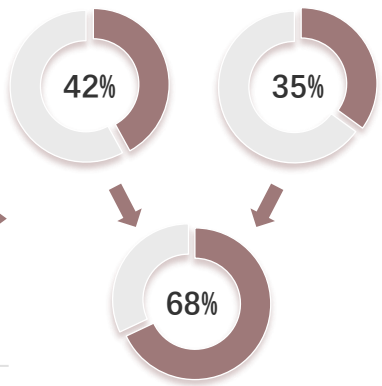
## 工业防火墙在行业的应用

| 排序 | 行业名称 | 应用特点与说明 | 应用渗透率 |
|---|---|---|---|
| 1 | 电力行业 | 国家电网、南方电网等推行“安全防护三道防线”，防火墙为核心设备 | |
| 2 | 石油石化 | 对DCS、SCADA系统安全要求高，且为重点监管行业 | |
| 3 | 精细化工行业 | 以精细化工和大型装置为主，数据隔离与安全通信需求强烈 | |
| 4 | 轨道交通/铁路运输 | 城市轨道系统通信SCADA与综合监控系统需安全隔离 | |
| 5 | 冶金行业 | 炼钢炼铁控制系统逐步信息化，防护逐年加强 | |
| 6 | 制药行业 | 与FDA/GMP合规相关，越来越重视数据完整性和系统安全 | |
| 7 | 污水/环保行业 | 自动化程度较高，数据采集系统需安全加固 | |
| 8 | 装备制造业 | 智能制造场景增多，但整体安全投入有限 | |
| 9 | 纺织/轻工行业 | 自动化程度较低，防火墙应用滞后，多以物理隔离为主 | |

- **电力行业中遭受的网络威胁（以漏洞为例）**
- **能源行业的漏洞数量（个），2023年**




**能源行业漏洞中，高危漏洞和ICS漏洞占比**




**威胁电力设施的ICS高危漏洞占比**

- **工业防火墙是保障电力工控系统安全、防止恶意攻击的关键防线**

2023年全球能源行业披露漏洞达4,500个，其中42%为高危漏洞，工控系统（ICS）漏洞占比高达35%。值得一提的是，这些ICS高危漏洞中有68%直接威胁电力设施安全。电力行业作为关键基础设施的核心组成部分，其工控系统一旦遭受攻击，可能导致大面积停电、设备损坏甚至安全事故，造成严重的经济损失和社会影响。而工业防火墙作为工控网络安全的第一道防线，能够有效隔离网络威胁，从而阻断针对电力系统的恶意攻击。

来源：头豹研究院

# （接上页——行业应用）

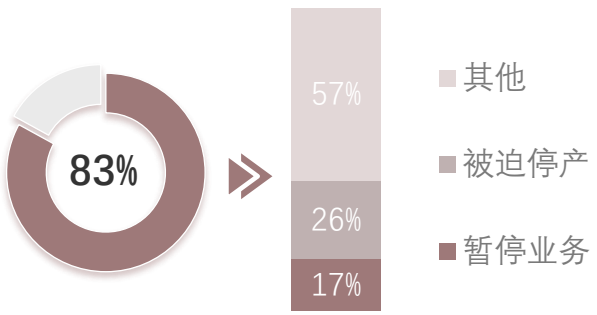
工业防火墙作为关键防护措施，在电力、石油化工、制造业及交通等行业中发挥核心作用，有效应对勒索攻击、APT威胁等网络安全风险，保障生产安全、系统连续性与关键基础设施稳定运行

## 工业防火墙在各行业应用的必要性分析

### ■ 石油化工网络风险高，工业防火墙是保障生产安全的关键防护措施

2024年，石油化工遭受的网络攻击占比仅次电力行业（24%），比例为19%。由于石油化工生产系统具有工艺流程复杂、设备互联度高、实时性要求严格等特点，一旦遭受网络攻击可能导致生产中断、设备故障甚至安全事故，造成重大经济损失和环境污染。而工业防火墙能够有效构建石油化工工控系统的安全边界，通过协议深度解析、访问精准控制和安全域隔离等技术手段，防范勒索软件、APT攻击等网络威胁。

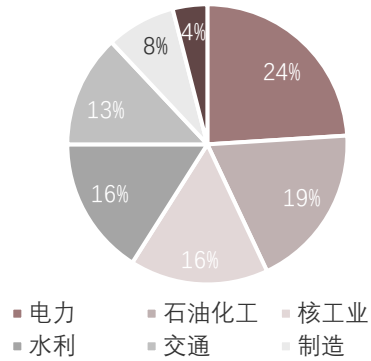
➢ **制造业中遭受的网络威胁，2024年**




### ■ 交通行业网络风险加剧，工业防火墙部署尤为关键

2024年，全球交通行业遭受勒索攻击同比增长33%。交通行业与数字技术的紧密结合，为网络攻击带来了新的漏洞。随着自动驾驶、智能交通系统（ITS）、云平台调度、车联网（V2X）等技术的快速应用，交通基础设施愈发依赖数字系统。一方面，这些技术提升了运输效率与用户体验；另一方面，也使整个行业面临更复杂的网络安全风险。在此背景下，工业防火墙的部署与应用变得尤为关键。工业防火墙可用于保护轨道交通信号系统、机场调度中心、智能收费系统等核心设施，防止攻击者通过边缘设备或通信链路入侵生产网络，从而维护交通系统的连续性与安全性。

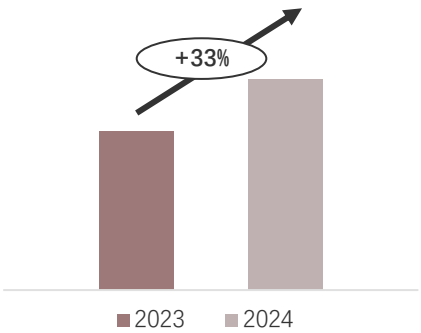
➢ **石油化工行业中遭受的网络攻击情况**




### ■ 制造业勒索软件攻击频发，工业防火墙部署对保障其网络安全至关重要

2024年，超过83%的制造业单位遭遇勒索软件攻击，其中26%的攻击导致系统离线和业务中断，17%企业被迫暂时停业。面对严峻的威胁，68%的受害企业选择支付赎金，且其中66%多次支付。目前制造业已成为网络攻击的高发领域，网络安全防护形势尤为紧迫。在此背景下，工业防火墙作为核心防护手段，其部署对保障制造业网络安全、有效抵御勒索软件攻击具有重要意义。

➢ **全球交通行业遭受勒索攻击增长率**




来源：头豹研究院

# Chapter 3
# 中国工业防火墙行业竞争分析

- 竞争格局
- 领导者分析——启明星辰

# 中国工业防火墙行业竞争分析——竞争格局

2024年中国工业防火墙市场竞争格局分明，启明星辰以35.9%的市场份额及技术优势位居领导者梯队，威努特、天融信、奇安信等厂商为挑战者梯队，六方云、中电安科等厂商为追随者梯队

## 工业防火墙竞争格局



**威努特、天融信、奇安信等厂商属于挑战者梯队。**威努特以“白环境”解决方案为核心，自主研发工业防火墙、工控安全监测与审计系统等产品，在交通、电力等领域建立差异化优势。天融信工控防火墙采用“白+黑”组合方式制定安全防护策略，从访问控制、业务行为、业务数据等层面解决安全威胁。奇安信工业防火墙采用四重白名单深度防御和一体化引擎机制，以满足工业安全的深度安全要求与低时延需求。

**六方云、中电安科、浙江中控等厂商位于追随者梯队。**这些企业大多专注于工业互联网安全，在工业防火墙等细分领域具备差异化优势。如六方云工业防火墙采用先进安全技术，具备自主可控安全操作系统、细粒度工控操作指令等优势。

来源：专家访谈，头豹研究院

# 中国工业防火墙行业竞争分析——领导者分析（启明星辰）

启明星辰工业防火墙具备协议自定义过滤、专业威胁防护、兼容多种工业协议等优势，提供边界防护和深度检测能力，确保设备可靠性和用户体验优化，提升协议审计与安全告警水平

## 启明星辰工业防火墙技术优势

**协议自定义过滤**
- ✓ 支持函数、运算符等方式，对非加密协议进行精准、深入的内容级检测

**专业威胁防护能力**
- ✓ 内置工业IPS与攻击事件库，支持自定义规则，高效应对工业入侵

**未预置协议灵活适配**
- ✓ 提供编程语言与多种函数，支持协议数据格式的自定义检测

**工业协议细粒度检测**
- ✓ 提供编程语言与多种函数，支持协议数据格式的自定义检测

**兼容多种工业协议**
- ✓ 预置百种协议，深度支持OPC、Modbus、S7、EIP、DNP3、IEC104等

**部署灵活无干扰**
- ✓ 兼容多种部署方式，包括通信透明、测试、防护及旁路模式

**运行稳定安全可靠**
- ✓ 支持BYPASS、接口冗余、热备等机制，确保系统持续运行

**工业级硬件标准**
- ✓ 采用抗干扰、防震宽温设计，适应复杂严苛环境

## 启明星辰工业防火墙功能优化

| | |
|---|---|
| 车联网与交通领域的广泛应用 | • 在车联网中提供车辆信息系统的边界防护，防止黑客攻击，保障通信安全和用户隐私。<br>• 应用于城市轨道交通、高速公路等场景，确保交通信号控制、收费系统等关键业务的稳定运行。 |
| 工业协议支持与深度检测能力 | • 支持S7-NCK、FOCAS、NC-Link等数控协议的识别与控制，可防止数控机床数据泄露、非法操作。<br>• 具备深度数据包检测（DPI）、自适应动态防御、机器学习辅助规则生成功能。<br>• 可自定义非加密协议的内容级检测，结合工业IPS引擎和工业攻击事件库，实现精准入侵防御。 |
| 设备可靠性与连续运行保障 | • 导轨式防火墙支持串口BYPASS功能，在设备故障时自动旁通，保障PLC等关键设备持续运行。 |
| 用户体验优化 | • WEB管理界面支持中英文双语，涵盖所有功能模块，方便国际化部署。 |
| 协议审计与安全告警提升 | • 优化了工业协议审计能力与威胁分级机制，提高指令审计准确性和有效性。 |

来源：专家访谈，头豹研究院

# Chapter 4
# 中国工业防火墙行业分析

- 需求分析
- 发展趋势

# 中国工业防火墙行业分析——需求分析

工业防火墙复购率较高，目前需求主要源于新建工厂的首次部署、新能源项目的经济效益、设备更新换代、国产化替代政策、等保整改要求及企业自身需求扩展

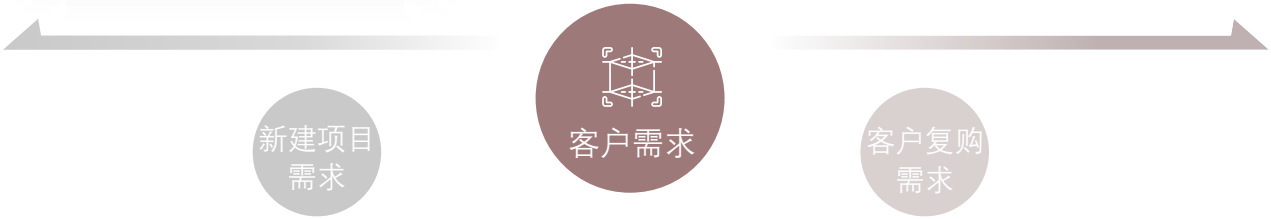
## 工业防火墙需求分析

### 为什么工业防火墙的复购率高

- ICS对安全防护依赖性强
- 部署规模大，需分阶段采购
- 稳定性要求高，转换成本大
- 合规性推动统一采购
- 厂商提供延续性的服务

### 工业防火墙复购常见模式

| 类型 | 特征描述 | 复购周期 | 示例场景 |
|---|---|---|---|
| 批量复购 | 随着业务扩展持续新增设备 | 6-18个月 | 工厂新产线上线 |
| 替换复购 | 替换老旧或不稳定防火墙设备 | 2-5年 | 原系统稳定性不足 |
| 多区域部署复购 | 同一企业不同工厂、园区逐步推广部署 | 12-24个月 | 集团级信息安全标准推广 |
| 升级复购 | 防火墙功能升级，如从L2升级到L7 | 2-3年 | 新增工业物联网安全需求 |




- **新建工厂：**以电力行业为例，无论是新能源电厂（如风电、光伏）还是传统能源电厂（如火电、水电），在并网发电前均需满足网络安全等级保护（等保）要求。因此，新建电厂项目在建设初期就存在明确的工业防火墙首次部署需求。
- **行业趋势：**以电力行业为例，五大四小发电集团正在积极建设新能源电厂。相较于传统火电，新能源项目具备更高的经济效益，这也为工业防火墙提供了新的市场需求。
- **设备更新换代：**现有设施中已安装的工业防火墙经过几年使用后需要更新换代。
- **国产化替代：**国家政策与集团内部政策推动使用国产化的网络安全产品，导致旧有的非国产设备需要替换。
- **等保整改：**每年的等保测评可能导致企业需要增加或升级某些安全设备以符合最新的保护等级标准，例如堡垒机和备份系统的引入。
- **自身需求扩展：**企业的系统扩展或改进（如DCS改造、燃料智能化区域的安全建设）也可能产生新的安全防护需求。

来源：专家访谈，头豹研究院

# 中国工业防火墙行业分析——发展趋势

工业防火墙发展呈现两大趋势：一是向多协议深度检测发展，融合语义解析与威胁情报实现全维度防护；二是AI赋能，通过实时检测、行为分析优化，显著提升对网络威胁的防御效率

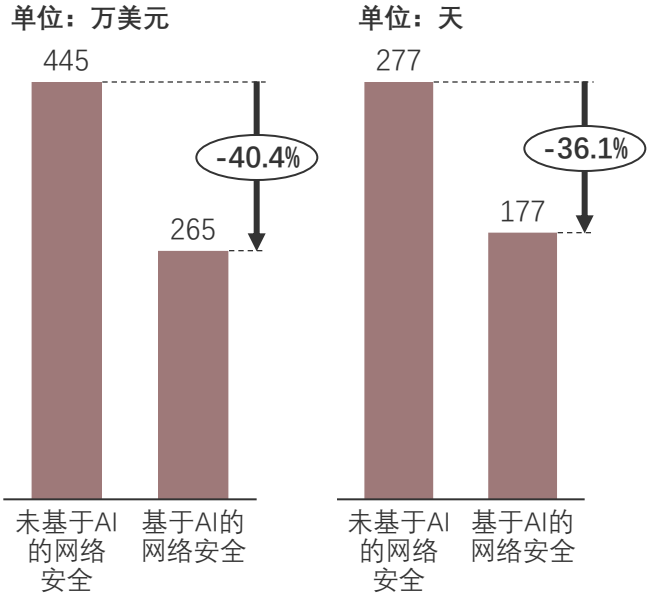
## 工业防火墙厂商可识别的工业协议数量，2025年

| 厂商 | 工业协议识别数量（种） | 工业协议深度解析 |
|---|---|---|
| 启明星辰 | 100+ | 能够对OPC、Modbus、IEC 60870-5-104、IEO61850 MMS、Siemens S7、Ethernet/IP(CIP)等主流工控协议做深度报文解析 |
| 威努特 | 100+ | 支持OPC、Modbus TCP/RTU、S7、EIP、DNP3、IEC104等常用工业协议的深度过滤解析 |
| 天融信 | 60+ | 支持 OPCUA、OPCDA、Modbus TCP、S7、IEC104、DNP3、MMS、EIP、Profinet等多种主流工业协议深度解析 |
| 绿盟科技 | 100+ | 对OPC、Modbus、MQTT、EthernetIP、IEC104、DNP3等协议进行值域级控制 |

**工业防火墙向多协议深度检测发展，融合语义解析与威胁情报，实现多维度防护**

随着工业互联网的深化和OT/IT融合加速，工业防火墙正朝着支持支持更多工业协议（如Modbus、DNP3、OPC UA、PROFINET等）的深度包检测方向发展，实现协议字段级过滤和异常行为识别。目前，启明星辰、威努特和绿盟科技等厂商均能识别100多种工业协议，深度解析OPC、Modbus、MMS多种工业协议。未来，工业防火墙将进一步融合协议语义解析、行为建模与威胁情报，实现对复杂工业协议的全维度安全防护，成为保障关键基础设施安全的核心防线。

## 全球公司数据泄露平均成本、威胁识别时间，2023年




**AI赋能网络安全，显著提升威胁识别与响应效率，降低数据泄露成本和误报率**

面对日益复杂的网络威胁，传统人工分析已难以应对工业场景中海量的安全数据。据IBM Global，2023年企业AI网络安全预算较2021年激增51%，并预计2025年将再增长43%，反映出行业对AI赋能的迫切需求。在AI驱动的网络安全实践中，数据显示，2023年应用AI技术的网络安全方案可将数据泄露成本从445万美元降至265万美元，威胁识别时间从277天缩短至177天，展现出显著优势。在工业防火墙领域，AI技术通过实时威胁检测、异常行为分析和自适应策略优化，显著提升对零日攻击、高级持续性威胁（APT）的防御效率，同时降低误报率。

来源：专家访谈，头豹研究院

# 业务合作

## 会员账号

可阅读全部原创报告和百万数据，提供PC及移动端，方便触达平台内容

## 定制报告/词条

行企研究多模态搜索引擎及数据库，募投可研、尽调、IRPR等研究咨询

## 定制白皮书

对产业及细分行业进行现状梳理和趋势洞察，输出全局观深度研究报告

## 招股书引用

研究覆盖国民经济19+核心产业，内容可授权引用至上市文件、年报

## 市场地位确认

对客户竞争优势进行评估和证明，助力企业价值提升及品牌影响力传播

## 行研训练营

依托完善行业研究体系，帮助学生掌握行业研究能力，丰富简历履历

## 报告作者


**袁栩聪**
**首席分析师**

**林若薇**
**行业分析师**

- service@leadleo.com


## 业务咨询

- **客服电话：400-072-5588**
- **官方网站：www.leadleo.com**

**商务咨询与深度合作**


**深圳办公室**

广东省深圳市南山区粤海街道华润置地大厦E座4105室

邮编：518057

**上海办公室**

上海市静安区南京西1717号会德丰国际广场 2701室

邮编：200040

**南京办公室**

江苏省南京市栖霞区经济开发区兴智科技园B栋401

邮编：210046

# 方法论

- 头豹研究院布局中国市场，深入研究19大行业，持续跟踪532个垂直行业的市场变化，已沉淀超过100万行业研究价值数据元素，完成超过1万个独立的研究咨询项目。
- 研究院依托中国活跃的经济环境，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。
- 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

# 法律声明


# 诚邀

## 2025沙利文新投资大会

**第十九届沙利文全球增长、科创与领导力峰会暨第四届新投资大会**

**THE 19TH FROST & SULLIVAN GROWTH, INNOVATION AND LEADERSHIP SUMMIT AND THE 4TH NEW INVESTMENT EVENT**

2025年8月27日–28日 中国·上海
August 27th-28th, 2025, Shanghai · China

2025年9月2日 中国·成都
September 2nd, 2025, Chengdu · China

## 开幕倒计时

期待与您再度携手

共赴增长之旅、共创美好明天

大会咨询热线：021-3209-6800 转 8672

大会咨询邮箱：gil@frostchina.com