论关键信息基础设施的实用保护技术

守 | 护 | 工 | 业 | 命 | 脉　　保 | 障 | 关 | 键 | 安 | 全

网藤科技

网藤科技团队组建于2015年，公司位于北京高新技术软件园区内，汇集了国内知名的工业互联网安全专家，投资方包括基石基金、信泰投资、深创投、动平衡资本等国内知名机构。

网藤科技以“守护工业命脉，保护关键安全”为服务宗旨，以维护关键信息基础设施安全为目标，以工业信息安全技术为核心，致力于成为国内工业互联网安全领军企业。

1 公司亮点 核心技术突出 发展潜力巨大

发展速度快

三年时间从无到有，百人团队，十余款产品

明星创投企业

被行业内多家资本大佬看中，深创投、基石基金、360安全等明星创投机构入股。估计3亿人民币。

技术、产品的优势

多元化的产品，深度防护技术，彰显公司实力；参与多项标准制定，形成业内最完善的工控安全解决方案

公司定位准确

公司产品切入石油石化和电力领域，该领域对于工控安全属刚性需求，定位准确；在石化等行业客户铺占率领先于同行业

重点客户200余家

公司已深度跟踪石油、石化、电力行业重点客户200余家，储备大型项目100余个，18年合同金额超3000万元，19年合同金额8000万元

2 核心客户 项目覆盖大部分央企能源集团

能源行业 →

中国石油 | 中国石化 | 大唐集团公司 CHINA DATANG | 国家电网 STATE GRID | 华电国际 HUADIAN POWER INTERNATIONAL | China Coal | 中核集团

高端制造 →

京港地铁 | 中国中车 CRRC | ANSTEEL 鞍钢集团 | DAE 东安动力 | AVIC | 大连市自来水集团有限公司 DALIAN WATER SUPPLY GROUP LIMITED COMPANY | 深圳地铁 SHENZHEN METRO

部委协会 →

ETIRI | ICSISIA 工业控制系统信息安全产业联盟 | CNCERT/CC 国家互联网应急中心 | NISIA | CNITSEC

技术合作 →

China unicom中国联通 | ANDRITZ | CEC 中国电子 CHINA ELECTRONICS | 东北大学 NORTHEASTERN UNIVERSITY | ESI | CNITSEC

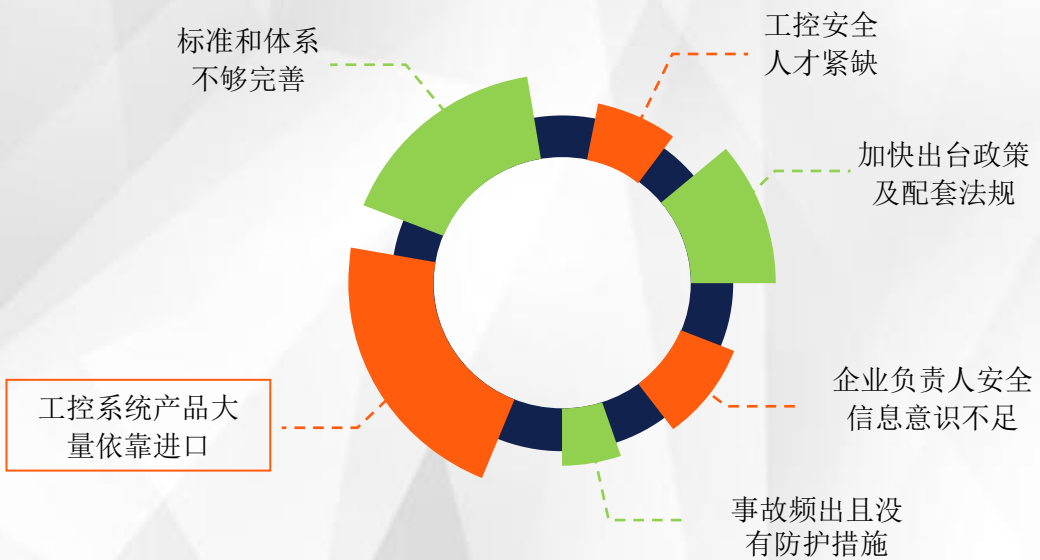
3 荣誉资质

- ISO9001质量体系管理认证证书
- ISO14000环境管理质量体系认证证书
- ISO27000信息安全管理体系认证证书
- 中国网络空间安全协会副理事长单位
- 国家信息安全风险评估服务资质
- 国家信息安全系统集成服务资质
- 中关村“雏鹰人才计划”支持单位
- 中关村“金种子企业”
- 中关村高新技术企业
- 高新技术企业证书
- 国家工业信息安全发展研究中心技术支撑单位
- 工业信息安全标准工作组（WG7）单位
- 2016年度中国工控网络安全领域创新企业奖
- 2018年度自动化领域优质工业安全服务商
- 2018年工信部工业信息安全优秀案例

4 网络安全"合规性"促使市场爆发

1 我国工业控制处于起步阶段、市场渗透率低、行业集中度低

我国工控系统核心控制模块从国外引进，而国外工业控制芯片、工业控制系统产品设计和配置等都存在漏洞。这些漏洞的存在将给予不法分子利用病毒进行攻击的机会，从而造成严重后果。另外，国家层面的威胁也有可能由于我国工业控制系统被硬件设备生产国操控而加剧，标准和安全体系尚未完善。



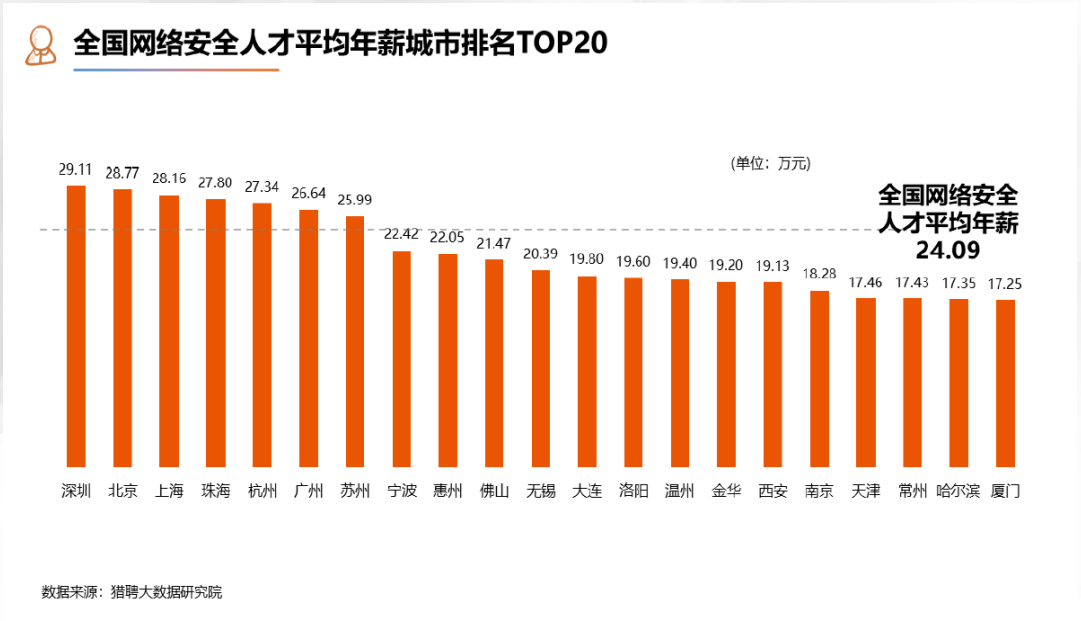
2 工控安全政策频出，具有指导和实操意义，驱动工控安全发展

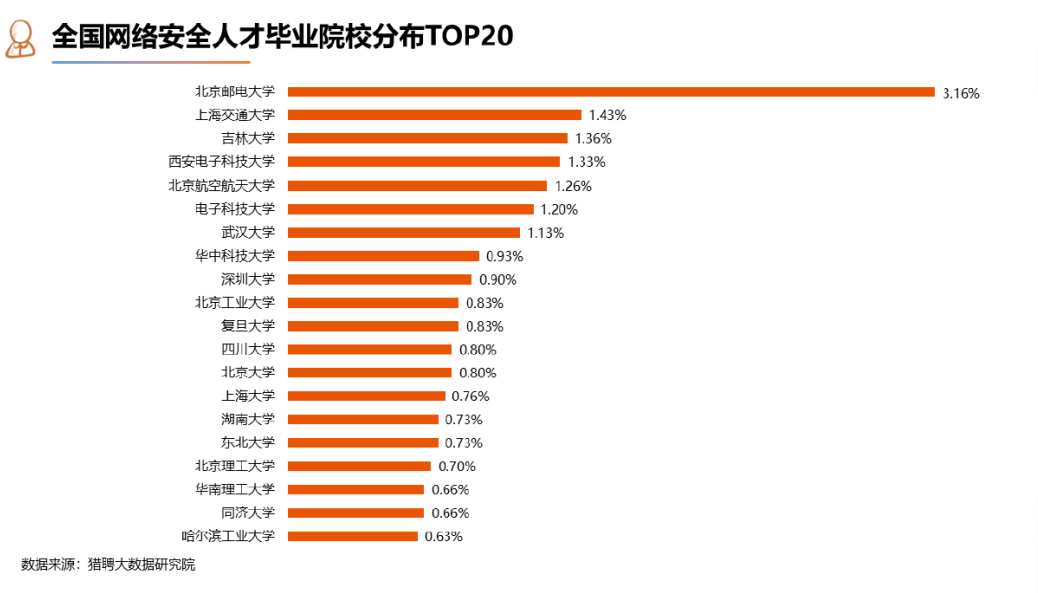
在2011年，工信部发表了《关于加强工业控制系统信息安全管理的通知》，强调加强工业信息安全的重要性，其中特别提到了与国计民生紧密相关领域的控制系统。自此，工控安全开始受到政府的高度重视，国家发改委开展工业控制系统信息安全专项的工控安全试点

2012	国务院发布《关于大力推进信息化发展和切实保障信息安全的意见》明确推进工业控制安全
2015	国务院印发《中国制造2025》明确加强工业控制安全保障能力建设
2016	公安部将工业控制系统纳入国家安全执法工作，明确高度重视工业控制安全
2017	工信部印发《工业控制系统信息安全防护指南》制定离开防护实施方案提供指导。
2019	公安部颁发《网络安全等级保护条例》（等保2.0）

5 人才短缺 急需培养实用型工程技术人才

早在2016年，教育部高等学校信息安全专业教学指导委员会副主任李建华就曾指出，当前中国重要行业信息系统和信息基础设施需要各类网络空间安全人才70万，预计到2020年这个数字会增长到140万。





6 关键信息基础设施成为网络安全重灾区

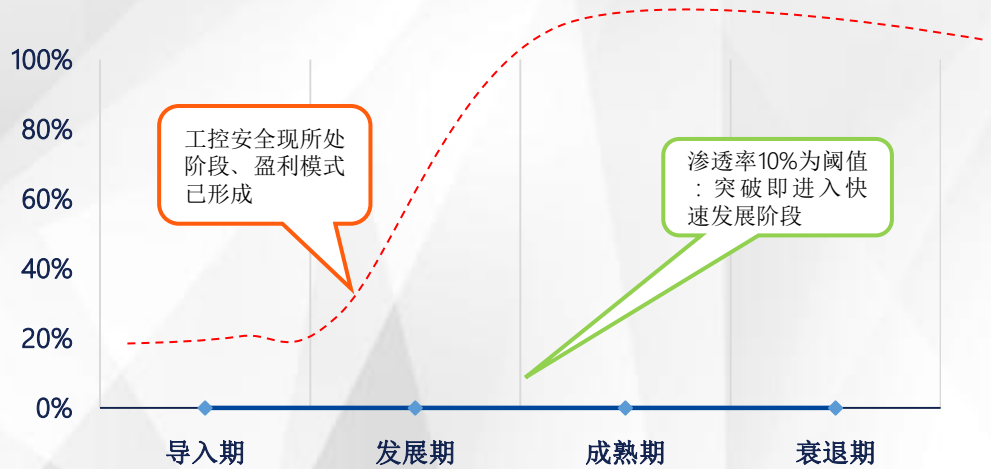
3 加快推进信息基础设施安全保障体系，工控安全发展爆发在即

1、政策角度：2015年以来三大国家政策对工控安全推进明显。这三个重要的政策表明了国家对工控安全的重视，并对工控安全建设提供关键性的指导。

2、用户角度：石油石化、电力、轨道等领域公司对于工业控制安全需求明晰。

3、企业角度：工控安全厂家迅速增加，产品种类不断完善。

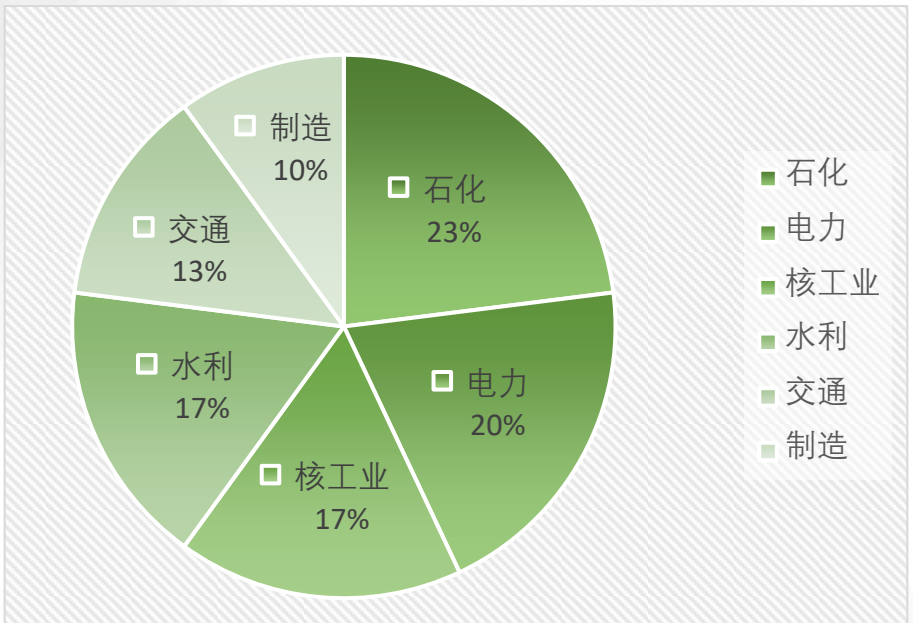
工控安全市场渗透率分析图



4 石油石化、电力行业成为工业控制安全的焦点

我国工控安全事件增长快速，且主要集中在石油石化行业（23%）与电力行业（20%）。

各行业系统被攻击比例



7 工业互联网安全催生千亿级市场

工业互联网安全涉及能源、智能制造、轨交、燃气、化工、烟草等多领域。未来五年国内工信安全市场规模将达到300-500亿级，预计催生5-8家具备上市体量的工信安全公司。

- **石油行业**：按照等保2.0和工信部的要求，需要安装工控安全系统企业。石油石化设计工业互联网的企业预计超过400家，**以中石油辽阳举例**：100套装置,整体投入预算大约8000万元。
- **电力行业**：目前全国发电企业（不算电网公司）大约6000家，每家按照200万预算，则市场规模超过100亿元。
- **轨道交通**：16年底全国轨道交通开通了130多条，每条工控安全投入1000万元，预计市场空间不低于20亿元。
- **智能制造**：国内有450万制造企业，未来10年左右时间预计有10%-20%的企业会实现工业互联网。工信部百万企业上云计划，工业企业30万家。

★ **网藤科技在产品技术储备、市场铺占、解决方案质量等方面都处于行业领先地位，有更大的机会率先跑赢。**

石油石化	分公司	备注
中石化	84家	油田15家、炼化厂39家、销售公司30家
中石油	95家	油气田16家、炼化企业28家、销售公司35家、管道16家

A	石油石化行业	**超值100亿元**
B	电力行业	超值100亿元
C	智能制造	**超50亿元**
D	轨道交通	超20亿元

8 蓝海市场 涉及领域广泛

9 痛点及需求 工业互联网安全形势日益严峻

2010年

Stuxnet

伊朗Natanz核设施受到Stuxnet病毒攻击，导致20000台离心机被摧毁，浓缩铀被毁。

01

2014年

Havex

该恶意程序用来感染SCADA和工控系统中使用的工业控制软件。 这种恶意软件在有效传播之后完全有能力实现禁用水电大坝、使核电站过载、甚至有能力关闭一个地区和国家的电网。

02

2015年12月

Blackenergy

乌克兰电网遭黑客攻击，约70万户家庭供电被迫中断。

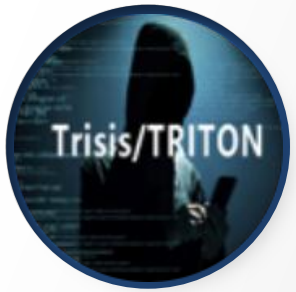
03

2019年3月

委内瑞拉停电事件

电力系统遭到网络攻击，18个州停电，全国交通瘫痪，打砸抢发生，多人受伤死亡。

04



2019年4月

国内某炼化厂

200多台DCS上位机遭遇挖矿病毒攻击，导致厂区大面积停产；网藤科技应急服务小组紧急驻厂处置。

05

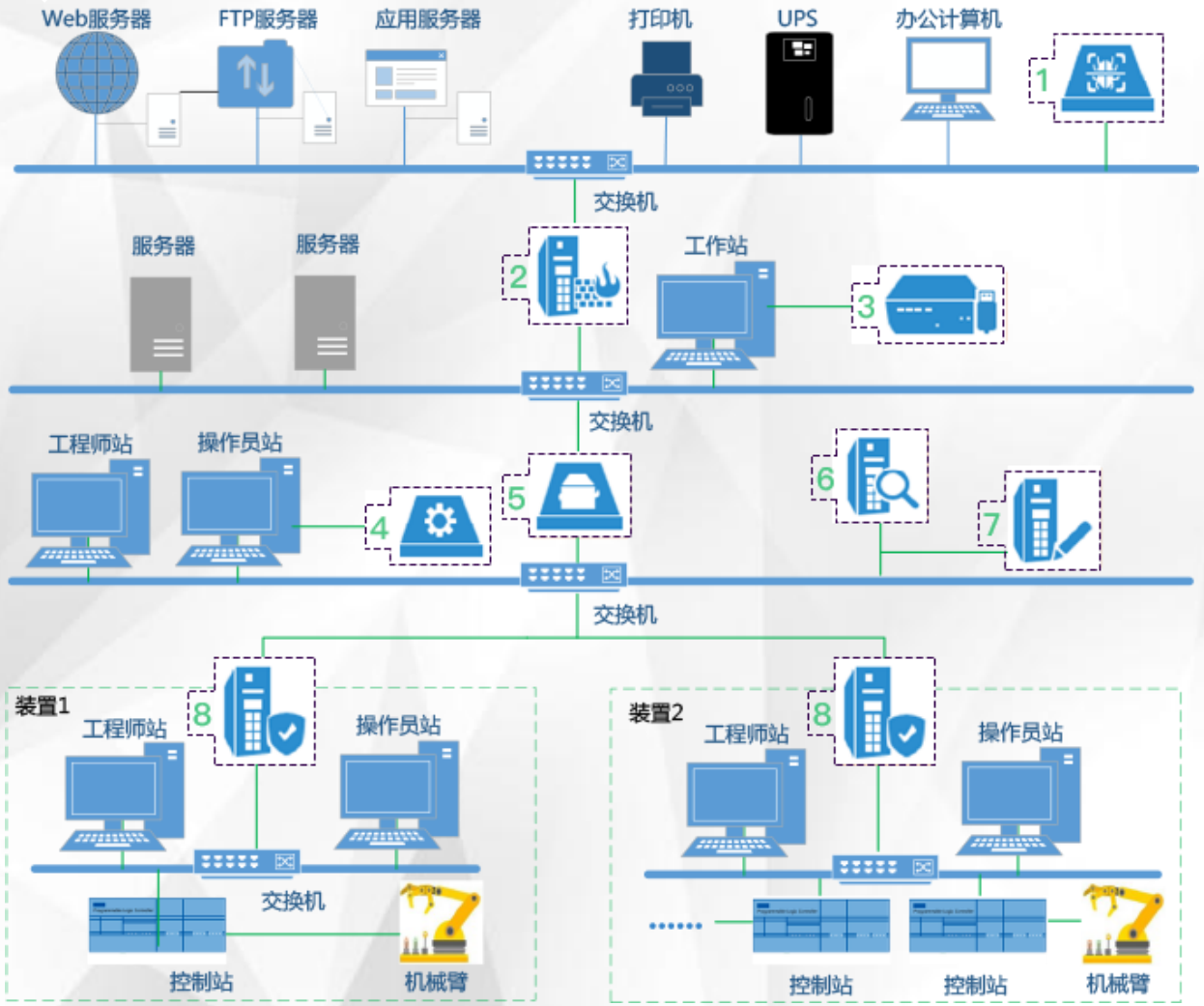
10 痛点及需求 来自于网络安全合规的强制性要求

时间	发文机构	规范要求
2014年8月	发改委	《电力监控系统安全防护规定》（发改委14号令）
2015年3月	能源局	《电力二次系统安全防护总体要求》（36号文）
2015年2月	轨交协	《城市轨道交通信号系统用户需求书》
2016年11月	人大立法	《中华人民共和国网络安全法》（“关键信息基础设施保护”）
2016年10月	工信部	《工业控制系统信息安全防护指南》
2017年6月	工信部	《工业控制系统信息安全事件应急管理工作指南》
2017年10月	工信部	《工业控制系统信息安全防护能力评估工作管理方法》
2017年12月	工信部	《工业控制系统信息安全行动计划（2018-2020年）》
2017年11月	烟草标委TC144	《烟草行业工业控制系统网络安全技术规范》
2019年5月	信安标委TC260	《信息安全等级保护管理办法》 （等保2.0,2019年5月13日发布）

公司名称	上市时间	2017年 收入/亿	过去5年 复合增长率
美亚柏科	2011年3月16日	13.37	30.74%
任子行	2012年4月25日	10.77	41.04%
启明星辰	2010年6月23日	22.79	25.64%
蓝盾股份	2012年3月15日	22	44.85%
北信源	2012年9月12日	5.15	22.07%
绿盟科技	2014年1月29日	12	17.89%
立思辰	2009年10月30	21.61	32.81%

- 网络安全是强政策影响行业；
- 08年等保1.0出台后，11年前后有大批网络安全公司上市；
- 随着《网络安全法》以及等保2.0的推行，工业互联网安全迎来大的爆发。

11 工业互联网安全整体解决方案提供商



1、网御威胁预警系统（增强级）

5、工业安全隔离网关

2、工业防火墙（增强级）

6、工控安全审计系统（增强级）

3、USB安全隔离装置（独家专利）

7、工业行为追溯系统

4、账户集中管理系统

8、工业安全防护系统

12 部分产品形态

工业防火墙

工业防火墙

工业安全隔离网关

工业安全隔离网关

工控安全审计系统

网御威胁预警系统

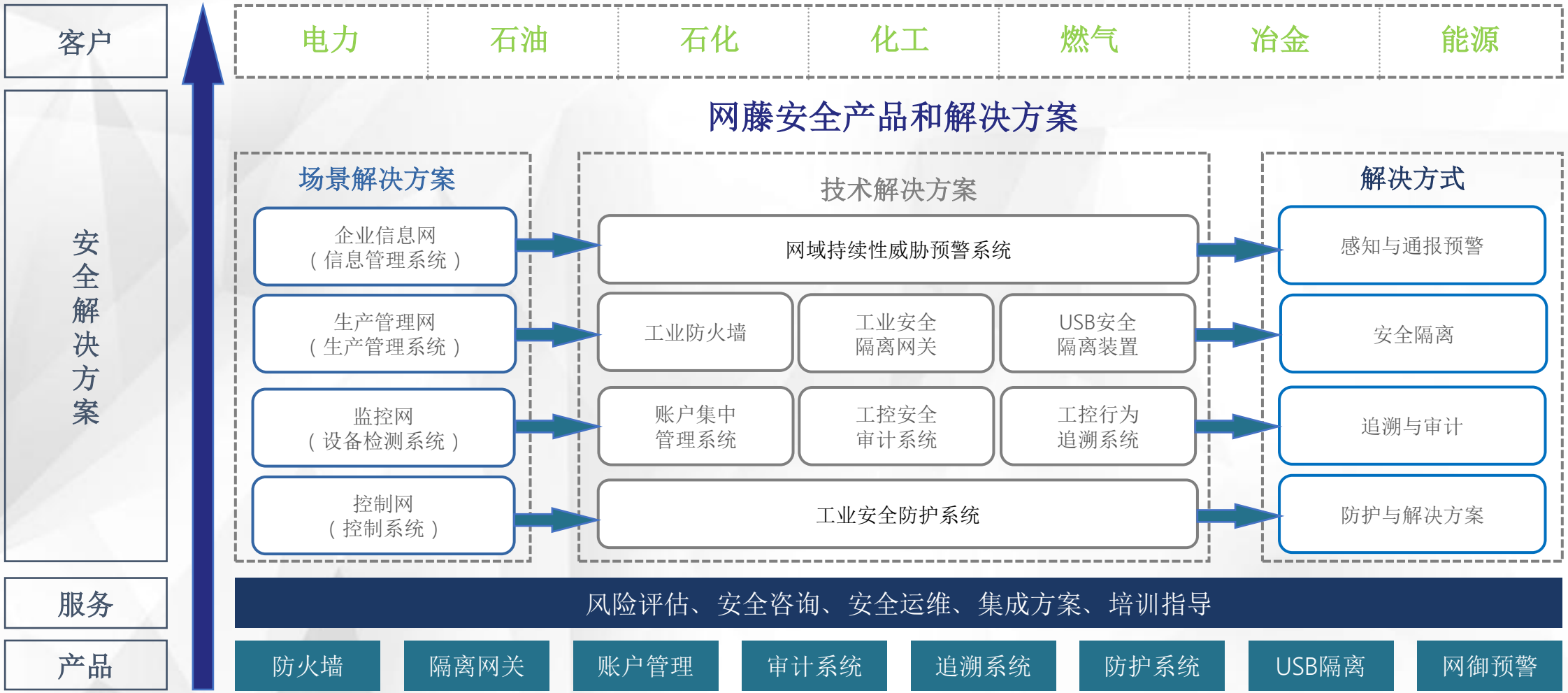
账号集中管理系统

USB安全隔离装置

工业行为追溯系统

工控安全防护系统

核心安全能力支撑全体系安全产品



14 核心安全能力

60+工控协议融合

可对超过60种工控协议进行深度分析，基本覆盖各个领域工厂应用场景需求，通过采集工控协议的控制参数，能准确的构建不同工控生产业务模型，制定工控安全方案。

600万+恶意代码库

自研病毒查杀引擎，能处理600万+的病毒、木马等恶意代码。覆盖现在所有工控相关病毒，同时行为判断引擎具备识别未知病毒的能力。

木马追踪和地址定位

对各种已知和未知木马的通信行为进行实时监控、分析、识别预警，通过可疑流出流量、动态域名等木马行为对未知木马进行检测。一旦发现木马行为，则可以对内网的主机和外网的目标地址进行准确定位，并获取与木马相关的深度信息。

操作还原技术

自动识别被管理设备系统，对终端的输入输出进行解析，解析出用户使用的逻辑意图。将用户在系统中的操作行为以真实的环境模拟显现出来，审计管理员可以利用操作还原技术还原出运维管理员的真实操作。

病毒处置方式

网藤科技独特的"体外"查毒，在线升级病毒库。通过定制的硬件设备完成恶意代码的查杀处置。

百余种工控安全攻击知识库

支持200以上的已知工控攻击方式识别，基本覆盖当前已知所有攻击方式，有效的提高了安全事件的预警识别能力。

打造产学研一体化平台 孵化新产品新技术

关键基础设施安全保护技术两大趋势

基于国产自主芯片打造全新安全产品

开辟新的产品线，基于国产芯片研制开发全新的安全产品。

更联合了国内知名自动化设备生产厂商、国内知名芯片设计商
共同打造国内首台套采用国产芯片的火力发电DCS机组
计划于12月底正式投产试点，网藤科技配套提供全面
的采用相同国产芯片的安全解决方案。

Thanks!

4001-552-663

北京网藤科技有限公司
Beijing Net Teng Technology Co., Ltd.
www.inetvine.com

守护工业命脉，保障关键安全