构建企业关键信息资产安全体系

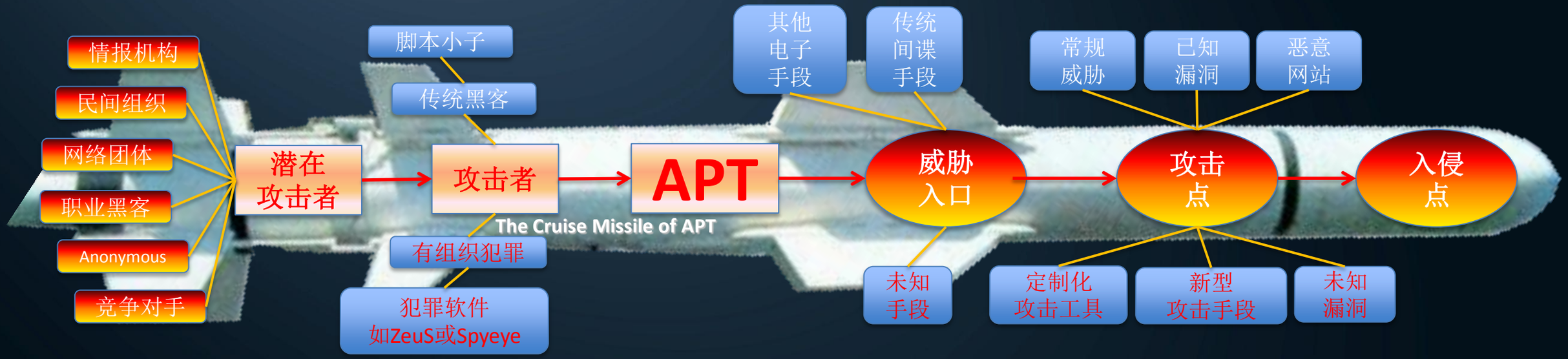
Building Enterprise Key Information Assets Security System

演讲人：钱晓斌 alan.qian@huawei.com
职　位：华为企业网络产品线首席安全架构师
日　期：2014年9月25日

ISC 2014 中国互联网安全大会

360互联网安全中心

APT：挑战安全的极限



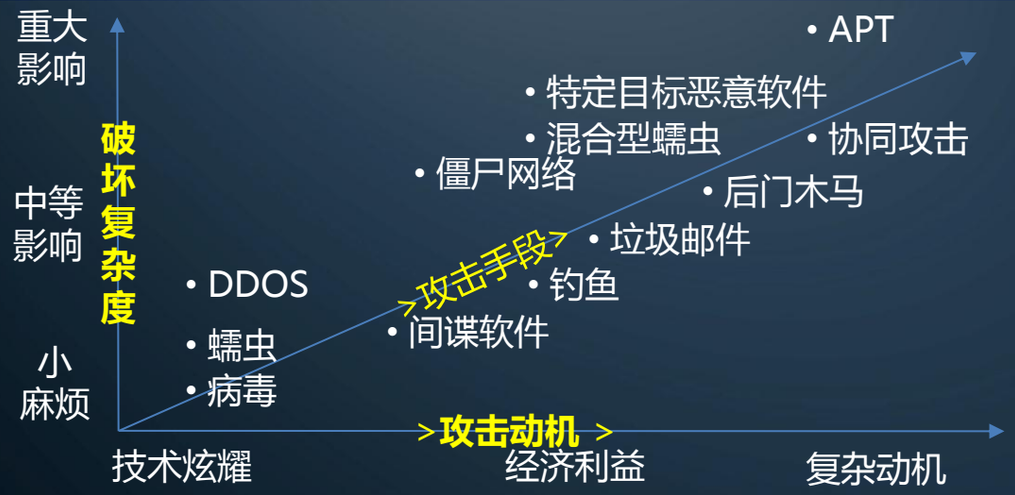
道高一尺，魔高一丈。

APT（Advanced Persistent Threat）正在挑战安全的极限。

目录

企业信息资产的安全挑战

安全形势复杂化



威胁加剧，驱动安全投资力度持续加大

威胁

现在的问题已不是谁遭到了黑客的攻击，而是谁没有受到攻击。

-纽约时报

攻击量庞大：

2011: 5.5Billion

2010: 3 Billion

影响

2011年网络犯罪带来的损失达到3880亿美金

CAGR 2012-2017 ~10%

固定封闭网络 -> 无边界开放的网络

BYOD/云 ▲ 桌面/服务器	精细 ▲ 粗放	开放 ▲ 封闭
无线 ▲ 有线	宽带 ▲ 窄带	虚拟 ▲ 物理

新的安全合规要求，安全投资加速的另一驱动因素

云计算

NIST SP 800-144（云安全性急隐私管理指南）

CSA（云控制矩阵）

……

移动办公

NIST SP 800-124（企业移动设备管理和安全准则）

ISO27000（信息安全管理体系）

信息安全等级保护

……

数据保护

PCI-DSS（支付卡行业数据安全标准）《关于加强工业控制系统信息安全管理的通知》

《商业秘密》

信息安全等级保护

ISO27001

HIPPA/Data Protection Directive-EU/SOX

德国《明镜周刊》披露的NSA入侵手段

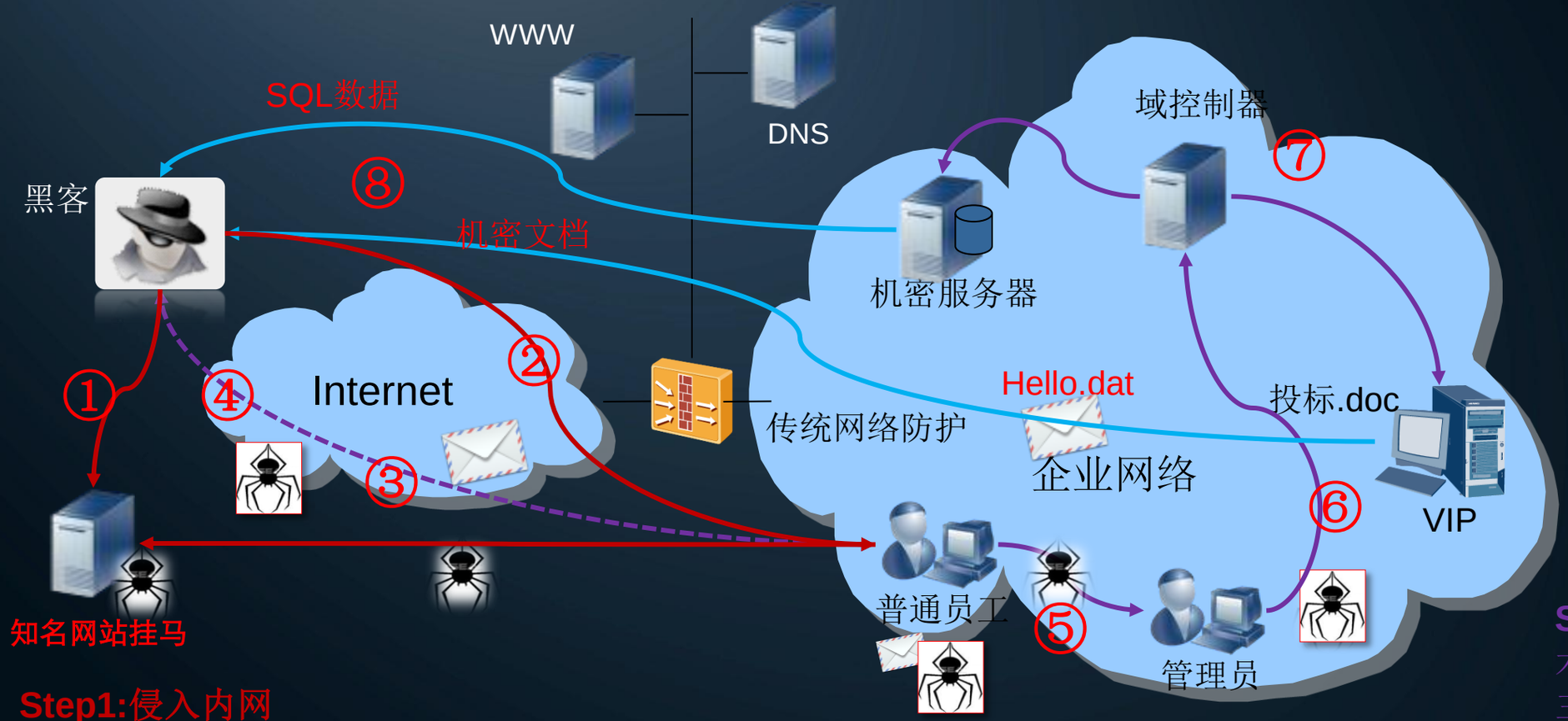
ISC 2014 中国互联网安全大会

360互联网安全中心

#	入侵手段	说明
1	IRATEMONK	硬盘firmware侵入软件
2	BULLDOZER	无线监听器
3	CANDYGRAM	伪造GSM基站
4	COTTONMOUTH-ICOTTONMOUTH	USB、以太木马植入与无线监听二合一工具
5	CTX4000	雷达侦听工具
6	DEITYBOUNCE	针对Dell服务器植入软件
7	DROPOUTJEEP	iPhone入侵软件，读写文件/短信/通讯录/位置/话筒摄像头
8	FEEDTROUGH	Juniper防火墙的攻击工具，用于透过防火墙安装恶意软件
9	FIREWALKFIREWALK	RJ45形状的数据注入、监听、无线传输设备
10	FOXACID	通过中间人手段植入间谍软件的技术
11	GINSU	PCI入侵工具，用于安装恶意bios
12	GOPHERSET	通过SIM卡实现对手机的远程控制
13	GOURMETTROUGH	针对Juniper防火墙的植入软件
14	HEADWATER	通过中间人手段针对华为路由器植入间谍软件的技术
15	HOWLERMONKEYHOWLERMONKEY	用于监听和远程控制的无线传送器
16	HALLUXWATER	华为防火墙后门探测工具
17	IRONCHEF	BIOS入侵技术
18	JETPLOW	针对思科防火墙的植入软件
19	LOUDAUTO	无线窃听设备

#	入侵手段	说明
20	TRINITYMAESTRO-II	微型硬件平台
21	MONKEYCALENDAR	通过短信传送手机位置的软件
22	MONTANA	用于入侵Juniper路由器的工具套件
23	NIGHTSTAND	远程安装windows软件的便携系统
24	NIGHTWATCH	与VGA接口无线监听器配套的解调模块
25	PICASSO	手机窃听软件
26	PHOTOANGLO	雷达侦听工具升级版本
27	RAGEMASTER	VGA接口无线监听器
28	SCHOOLMONTANA	Juniper防火墙永久侵入软件
29	SIERRAMONTANA	Juniper防火墙永久侵入软件
30	STUCCOMONTANA	Juniper防火墙永久侵入软件
31	SOMBERKNAVE	Windows XP 远程控制软件
32	SOUFFLETROUGH	针对Juniper防火墙的BIOS入侵软件
33	SPARROW IISPARROW II	用于WLAN监听的微型硬件
34	SURLYSPAWN	键盘远程监听技术
35	SWAP	针对多处理器系统的刷新BIOS的技术
36	TOTEGHOSTLY	针对windows手机的远程控制软件
37	TRINITY	微型硬件平台
38	WATERWITCH	用于发现附近手机精确位置的移动工具

难以觉察的数据窃密攻击



Step1:侵入内网

伪装业务邮件或网页欺骗普通员工中招，入侵进入内网；建立C&C通道

Step2:层层渗透

木马在本地网络扫描其他主机，发现管理员、VIP、等主机，定向扩散，获得高级核心数据权限

Step3:数据盗取

进入VIP电脑，获取机密文件，篡改文件名，通过总裁邮件外发。

客户登陆核心数据库中导出机密数据时，通过C&C通道将信息外发。

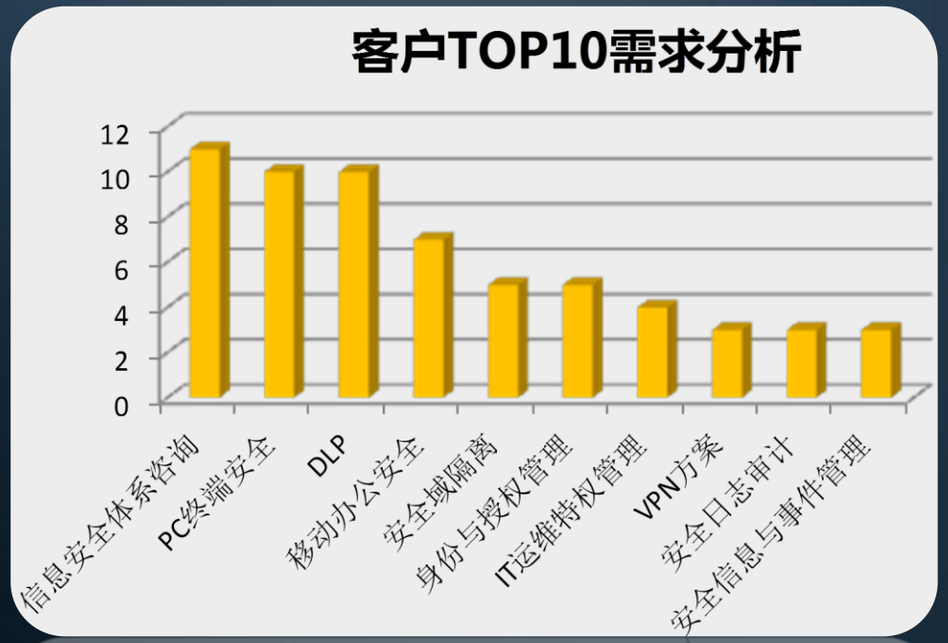
高级窃密攻击所涉及的数据量

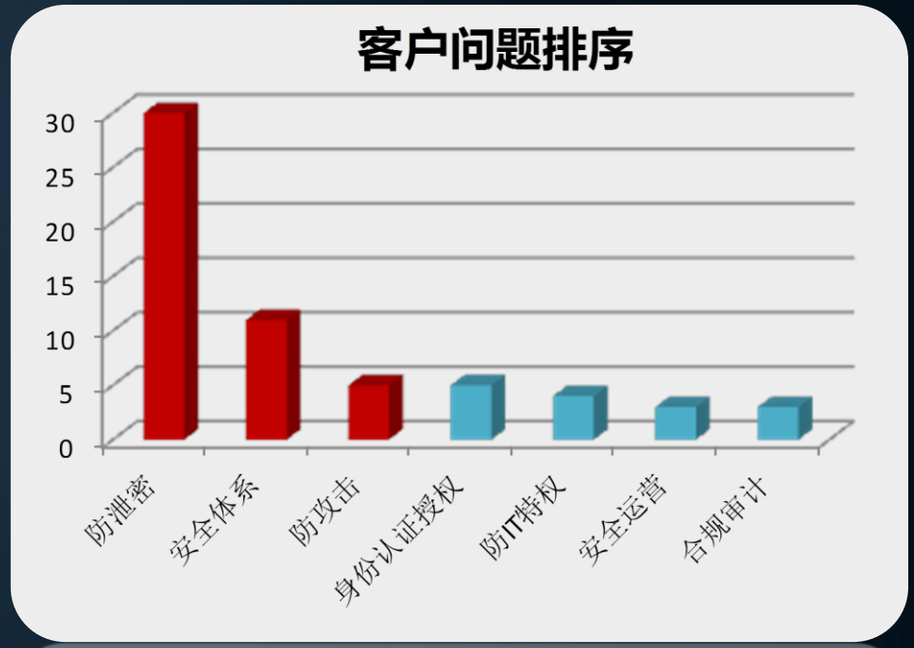
花大量
时间
工具
攻击手法
收集信息

- 社交库
- 接触资料
人员信息
- 密码字典
- 可能的
存储位置
- 攻击对象
网络拓扑
- 目标
资产信息
- 攻击对象
应用环境
- 生产环境
- 攻击对象
组织结构
- 供应链
- 安全设施
- …

A公司
关键
信息资产

企业信息安全TOP3问题





No.1 缺乏整体的信息安全技术体系和管理体系来指导信息安全的规划和建设，信息安全无成功经验可参考，无法确保信息安全方案和措施真正落地。

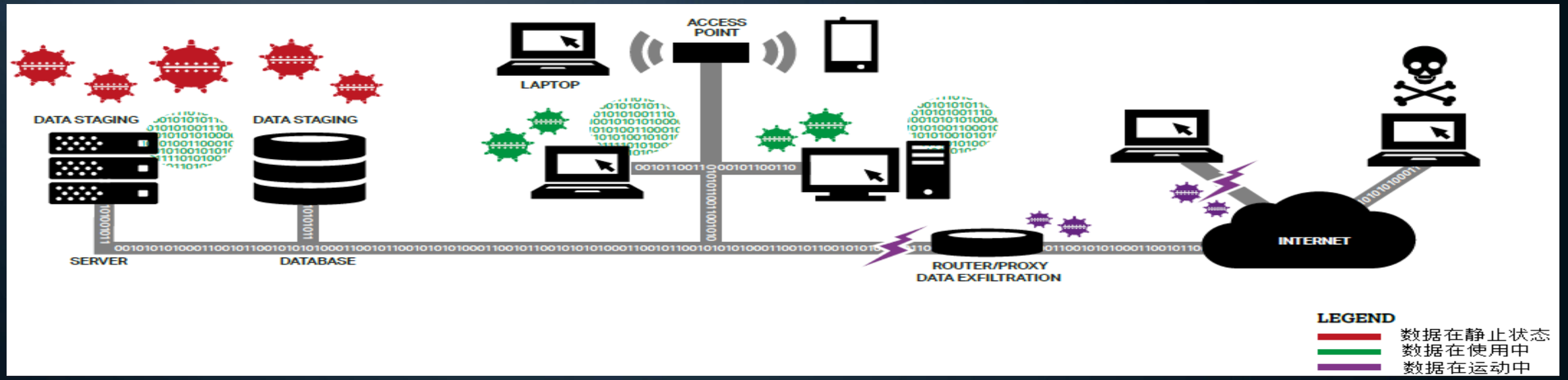
No.2 关键信息泄密，严重危害企业的声誉、竞争力和业务发展。

No.3 企业IT系统受到攻击和入侵，造成业务损失，影响IT效率。

说明：针对来源于20多个行业客户的调研样本，我们根据客户的原始需求提取客户主要痛点，统计识别出TOP客户问题。

目录

数据防窃密：数据三态



静止状态： 指的是非活动数据存储于数据库，数据仓库，电子表格，压缩文件，磁带，离线备份，或移动设备等。

使用状态： 指的是“活动”的数据资产正在被一些应用处理中，经常是存在于非持久的存储介质中，如电脑内存、CPU缓存和CPU寄存器中，数据在数据库的操作表中也属于在使用中的数据。在使用中的数据经常包含了敏感信息，如数字证书、加密密钥等。

运动状态： 指的是数据在企业网络中传输，或者临时在电脑内存中准备进行读取、更新、或发送到另外的数据处理服务。数据总是不断在进行处理、加密、存储到磁盘或数据库中。

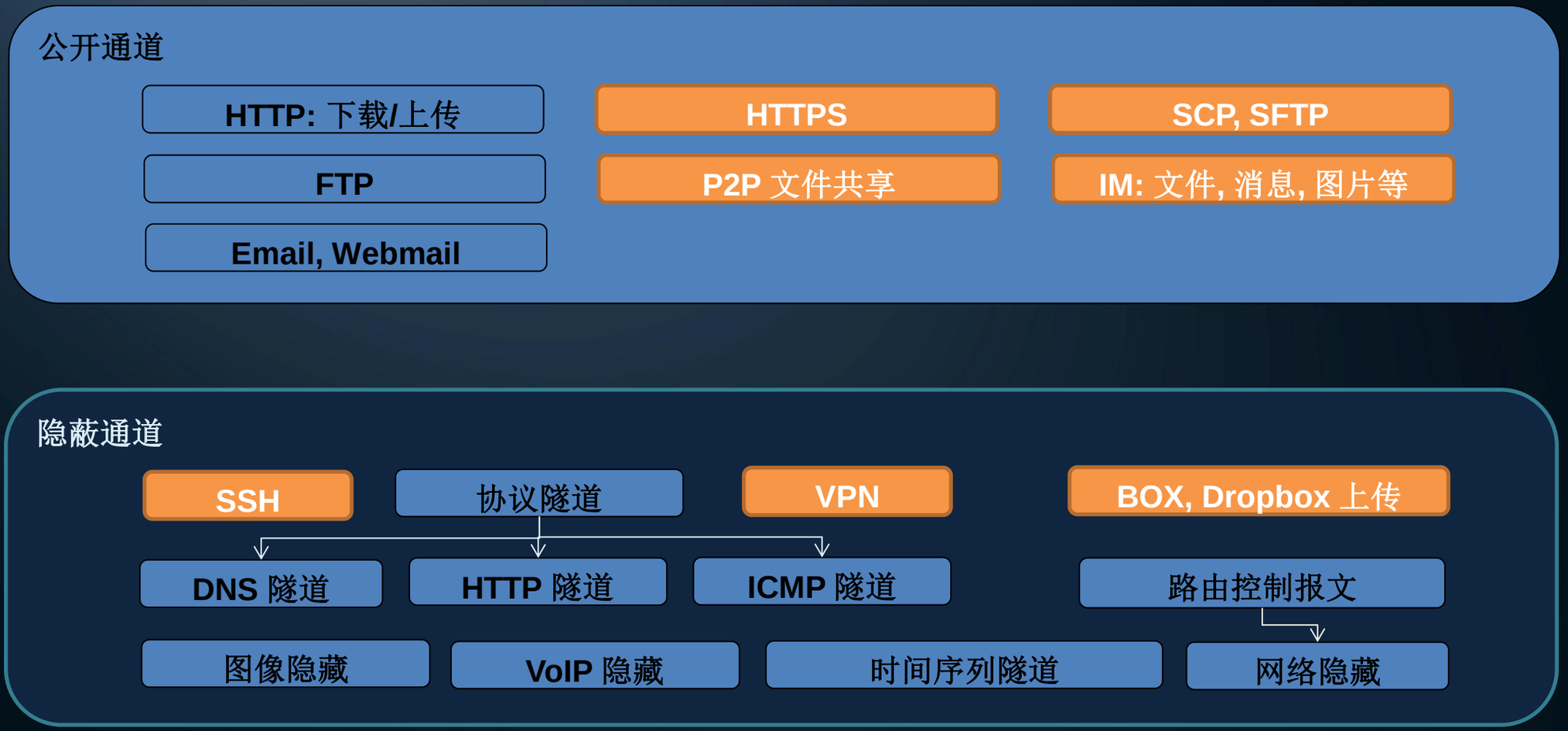
数据在三种状态下都有可能被攻击获取，需要针对三种状态的数据进行保护。

数据防窃密：攻防分析

	攻	防
静止状态	●SQL注入攻击 ●C&C, 远程管理攻击, 后门 ●提权 ●恶意代码感染：钓鱼，恶意email附件，0day攻击，跨站脚本攻击，恶意网站下载攻击	●周期性服务器、终端、存储设备扫描发现内容，产生内容匹配内容规则 ●对主机存储的敏感信息进行硬盘和数据库加密 ●合理的密钥管理体系 ●基于主机的DLP控制 ●数据库中的仿造数据
使用状态	●冷启动攻击 ●Rootkits，bootkits ●内存信息获得恶意代码，远程管理攻击，C&C ●恶意代码感染：钓鱼，恶意email附件，0day攻击，跨站脚本攻击，恶意网站下载攻击，缓冲区溢出攻击	●采用安全认证的加密机制在网络上移动数据 -保证在网络上移动数据端到端的加密 ●数据库的仿造数据，攻击则只能获取仿造数据 ●基于主机的DLP控制 -限制敏感信息拷贝到移动存储介质中 -限制访问敏感信息的应用，只允许允许的企业工具进行加密
运动状态	●报文嗅探 ●Rootkits, bootkits ●C&C, 远程管理攻击, 后门	●数据传送中保证网络会话必须进行加密 -使得数据截获跟难获取 ●使用硬件进行加密 -避免在加密之前在内存中使用明文

防数据窃密方案主要采用保护主机免受恶意攻击、加强数据管理及数据加密的方法。

数据防窃密：外传通道和控制方法



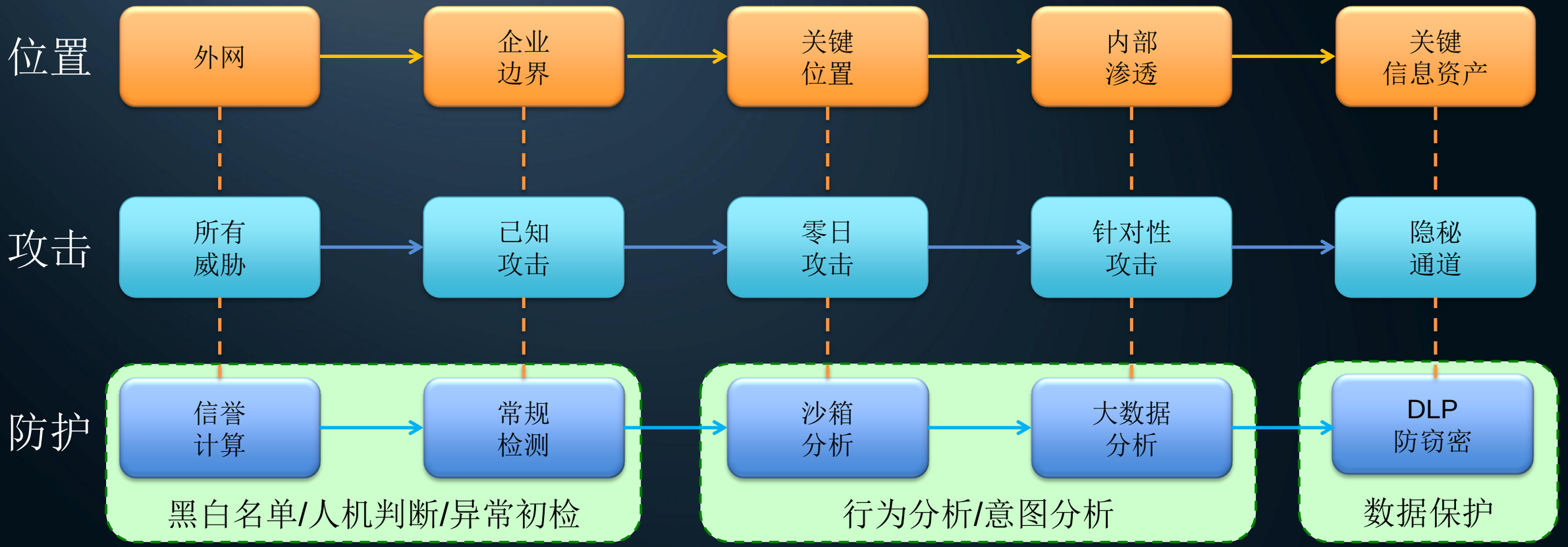
数据防窃密：外传通道和控制方法

通道	外传方法	窃密安全控制
公开通道	HTTP下载（SQL注入攻击）	1. SQL注入攻击检测，使用IPS或WEB应用防火墙
	公开通道: HTTP, FTP, IM, P2P, email, webmail	1. HTTP Proxy或防火墙上根据信誉进行阻断 2. Proxy上对通道进行DLP内容检测； 3. 在设备上进行内容检测。
	加密通道：HTTPS, SCP, SFTP, VPN, 公开通道上的第三方加密	1. Proxy上对通道进行DLP内容检测； 2. 检测并终止非授权的加密通道； 3. 网络异常行为检测 4. 主机行为检测

通道	外传方法	窃密安全控制
隐蔽通道	协议隧道，如DNS, HTTP, ICMP	1. 网络异常行为检测 2. DNS请求/响应报文分析 3. DNS流量分析
	图像隐藏，VOIP隐藏，网络隐藏	1. Proxy上对通道进行DLP内容检测； 2. 在每个特定隐蔽通道上对隐藏分析过滤； 3. 在设备上进行内容检测。
	1. 云存储上传	1. 禁止云存储上传服务
	1. 时间序列通道	1. 暂无

对数据窃密上传通道的控制需要采取对外协议控制、IPS/WAF检测、DLP内容检测、网络异常行为检测、主机行为检测以及对特定隐蔽通道分析过滤的多种方式。

洞察信息资产泄露规律


位置
外网
企业
边界
关键
位置
内部
渗透
关键
信息资产
攻击
所有
威胁
已知
攻击
零日
攻击
针对性
攻击
隐秘
通道
防护
信誉
计算
常规
检测
沙箱
分析
大数据
分析
DLP
防窃密
黑白名单/人机判断/异常初检
行为分析/意图分析
数据保护

转变信息资产保护思想

#	前APT时代	APT时代
保护思想	敌人在外部	敌人在外部，但更危险的敌人在内部
保护对象	所有	重点（关键信息资产、关键基础设施、关键VIP人员）
保护策略	以堵为主：千方百计防止进入	以围为主：千方百计防止做坏事
保护位置	围绕边界	围绕KIA数据
安全事件	形式：碎片化、离散化 用途：合规报表	形式：多维关联、可视化 用途：高级威胁检测
检测手段	技术：独立作战，缺少协作 内容：文件与流量	技术：基于行为模型与大数据，智能协同 内容：内部环境信息、外部威胁情报与信誉数据、分层分析全流量样本

选择KIA安全设施


引诱最终用户阶段
渗入系统阶段
安装后门阶段
建立隐秘通道
尝试窃取机密
应用管控
信誉过滤
入侵防御
木马检测
病毒查杀
DLP内容过滤
沙箱行为分析
大数据分析
阻断高危APP
阻断已知恶意网站
阻断漏洞攻击
阻断已知恶意软件
阻断偷渡下载
检测未知恶意软件
检测未知恶意流量
检测未知恶意软件
阻断C&C链接/异常链接
阻断恶意软件恶意域名
阻断Spyware/C&C链接
阻断非法外传
阻断未知C&C流量
智能协同：基于特征信誉行为，检测阻断活动攻击

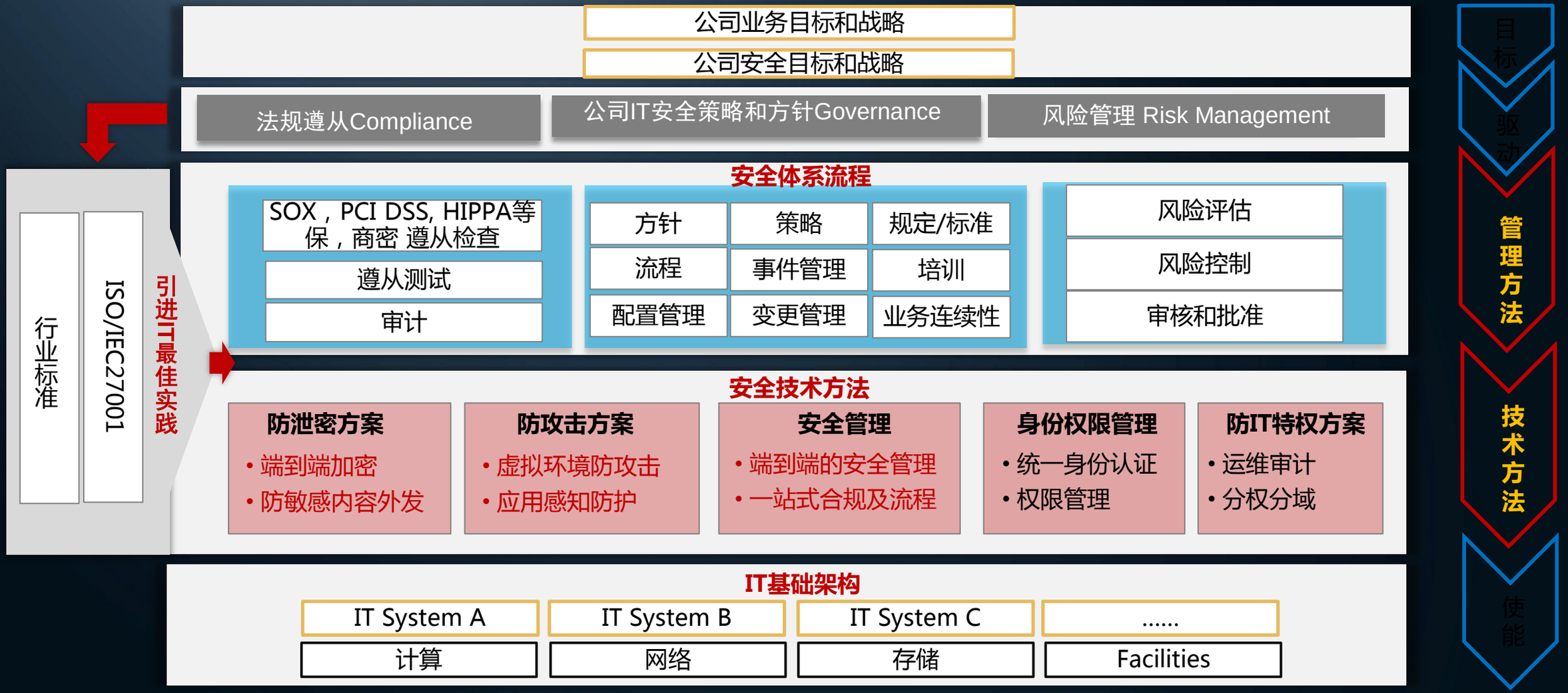
选择信息资产安全设施


信息安全管理
防IT特权滥用
身份安全
防泄密
防攻击
安全组织
安全运作
安全策略
运维管理
日志审计
操作视频
权限控制
审计回放
PKI
SSO
SOC
防移动泄密
防内网外发
防云环境泄密
网络隔离
APT
虚拟化防入侵
安全咨询厂商
网络安全厂商1
终端安全厂商1
终端安全厂商2
网络设备厂商1
网络设备厂商2
Feature present
Feature present but limited
Feature missing

现实中的DLP


70%
30%
网关DLP：失窃密通信通道与行为检测
内容过滤/通信行为检测/恶意软件检测
终端DLP：防失窃密软件
特马检测/躲避行为检测/隐密通道检测
传统DLP
防止合规性数据泄露

构建关键资产安全系统


公司业务目标和战略
公司安全目标和战略
法规遵从Compliance
公司IT安全策略和方针Governance
风险管理 Risk Management
安全体系流程
SOX，PCI DSS, HIPPA等保，商密 遵从检查
遵从测试
审计
方针
策略
规定/标准
流程
事件管理
培训
配置管理
变更管理
业务连续性
风险评估
风险控制
审核和批准
行业标准
ISO/IEC27001
引进IT最佳实践
安全技术方法
防泄密方案
• 端到端加密
• 防敏感内容外发
防攻击方案
• 虚拟环境防攻击
• 应用感知防护
安全管理
• 端到端的安全管理
• 一站式合规及流程
身份权限管理
• 统一身份认证
• 权限管理
防IT特权方案
• 运维审计
• 分权分域
IT基础架构
IT System A
IT System B
IT System C
.....
计算
网络
存储
Facilities
目标
驱动
管理方法
技术方法
使能

企业信息安全产品与技术体系架构

安全管理

- 安全策略管理
- 合规审计
- 安全管控中心（风险及运营管理）

身份认证解决方案

- 身份认证产品
- 证书体系
- 接入控制NAC

防泄密解决方案

- 终端防泄密
- 文档，磁盘 防泄密
- 网络防泄密
- 安全数据传输
- 安全域

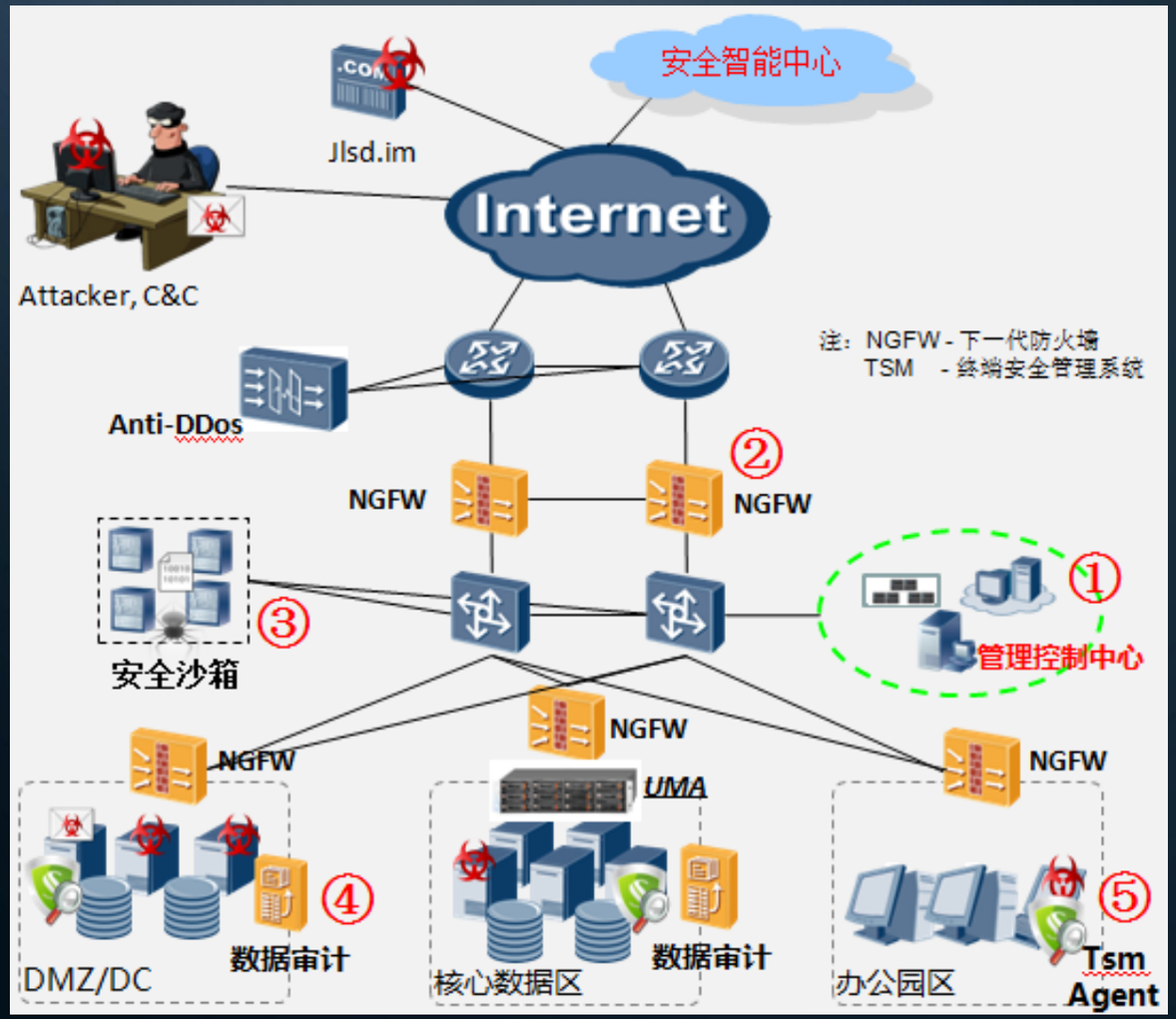
防攻击解决方案

- 终端防攻击
- 网络防攻击
- 服务器防攻击
- Web防攻击
- Email防攻击

防IT特权滥用方案

- 防越权（ITOC）
- 防偷窥
- 防特权滥用

企业信息安全解决方案部署



入侵早发现→重点布控→应急响应&取证

管理控制中心
- 负责行为统一分析、关联分析、策略控制，安全可视化显示

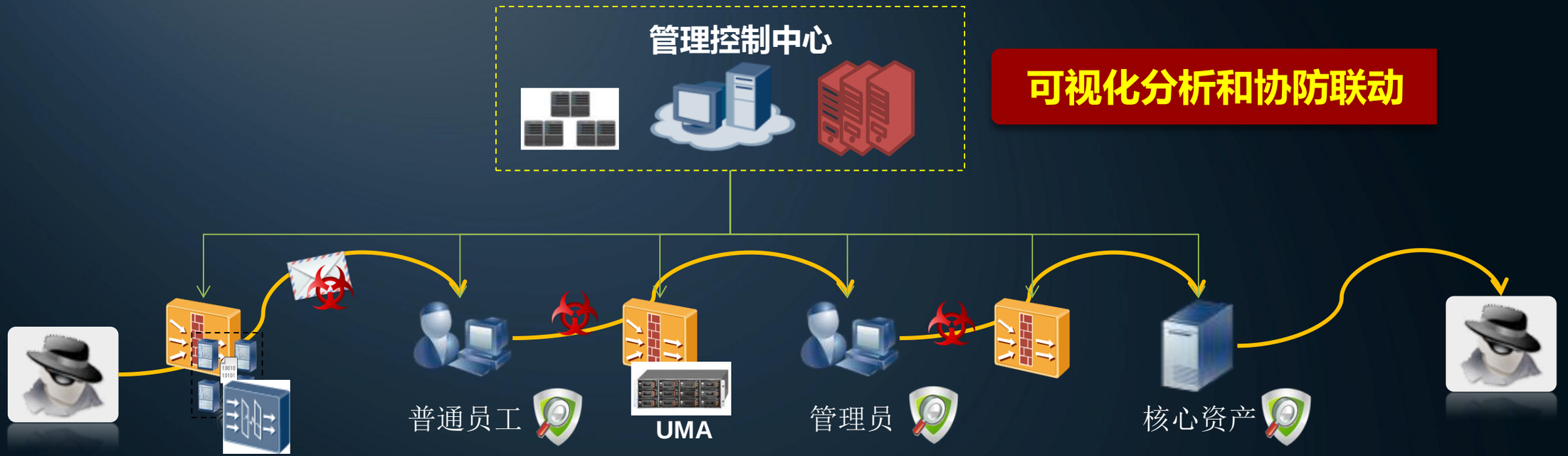
NGFW威胁行为感知
- 网络用户感知、应用识别、IPS、AV、DDOS防御、内容感知、内网布控
- Anti-DDos流量清洗，防御Ddos

安全沙箱
- 可疑样本静态分析
- 可疑样本动态仿真运行、行为分析

数据库审计
- 大数据的数据库审计，支持核心数据库的各类操作行为跟踪、告警

终端管控
- 用户终端应用黑、白名单管控
- 终端用户行为审计、恶意分析

企业信息安全解决方案总结



进不来

检测并及时隔离钓鱼邮件，在第一时间防御APT攻击

监控中

重点监控，实时分析用户应用及网络行为，鉴别可疑行为，跟踪记录

拿不走

可疑或确认的恶意行为，全网协同，用户随时阻断

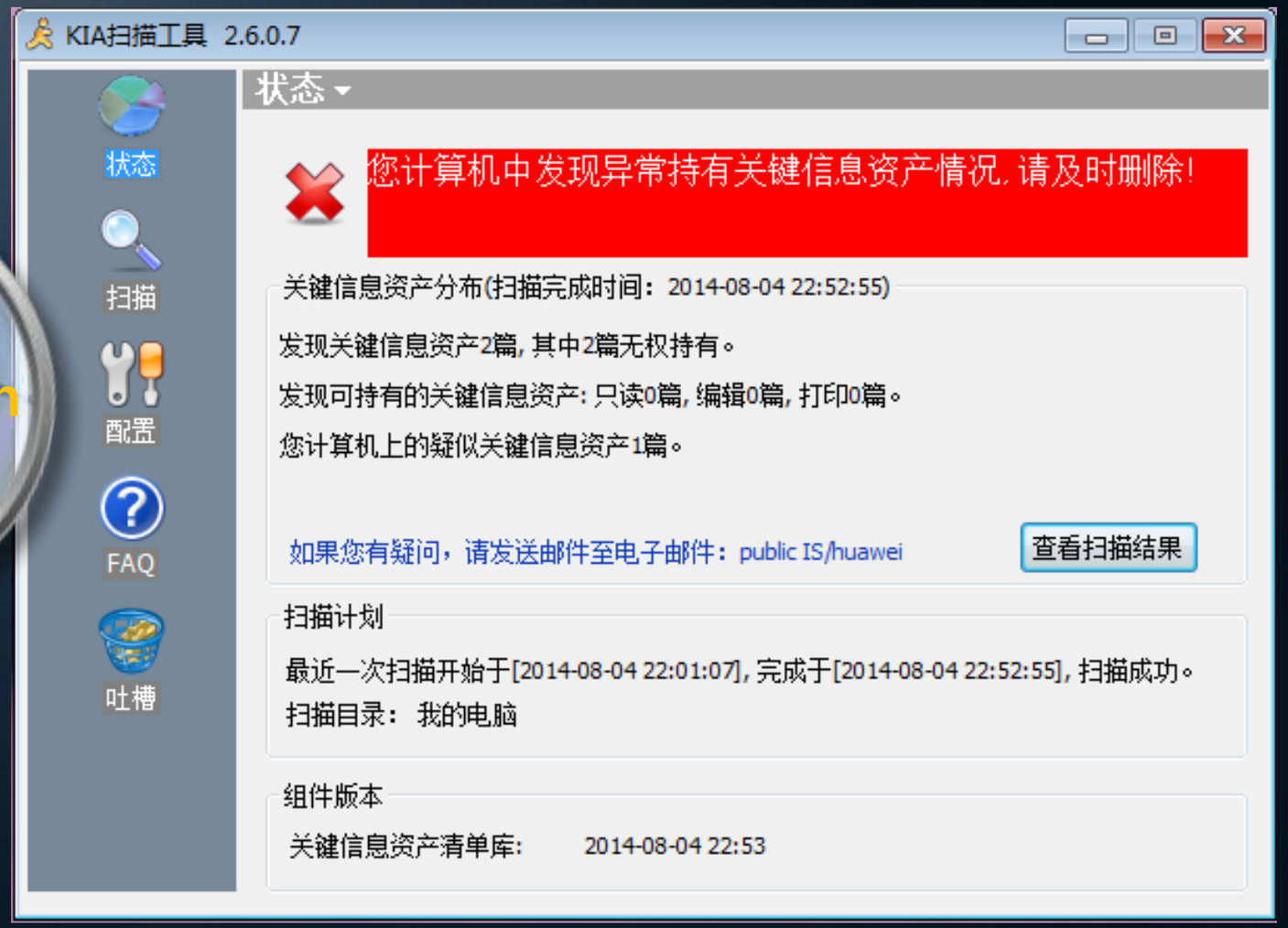
打不开

端到端加密
漏网之鱼，行为可还原、取证

目录

- **企业信息资产的安全挑战**
- **构建面向未知威胁的防御体系**
  - 洞察信息资产泄露规律
  - 转变信息资产保护思想
  - 选择信息资产安全设施
  - 构建关键信息资产安全体系
- **企业关键信息资产安全的几个重要建议**
  - 识别关键信息资产
  - 加强研发流程安全
  - 保证供应链安全
  - 建立PSIRT团队
  - 积极融入安全组织与标准

识别关键信息资产，确保合法使用



强化研发流程安全


IPD
概念
TR1
计划
TR2
TR3
开发
TR4
TR4A
TR5
验证
TR6
发布
GA
生命周期
安全需求
安全设计
安全开发
安全测试
安全交付和维护
安全需求分析
安全威胁分析
架构和系统安全设计
代码检视
静态代码扫描
端口扫描
漏洞扫描
安全验证和测试
漏洞管理和补丁开发（包括第三方组件）
配置管理
开源及第三方组件管理
安全基线、规范、标准、指导书

确保供应链安全

- ISO28000供应链安全体系运作与第三方认证
- 支撑全球客户快速和弹性交付的多供应中心布局
- 完善的条码系统支持多维度追溯

供应导入	计划	制造	订单履行	逆向	管理供应运作

来料安全

- 检核实送料人身份
- 货物包装检查
- 货物检查
- 功能性测试
- 软件完整性检查
- 物料上产线前检查和记录

工厂安全（含EMS）

- 员工安全培训
- 敏感区域管控
- 测试网络隔离并受控
- 软件和文件方面执行管控
- 软件加载及校验、QC检验
- 数字证书加载及检验
- 产品100%病毒扫描及检验
- 设备定期校验
- 个人测试账号及系统权限管控

物流安全

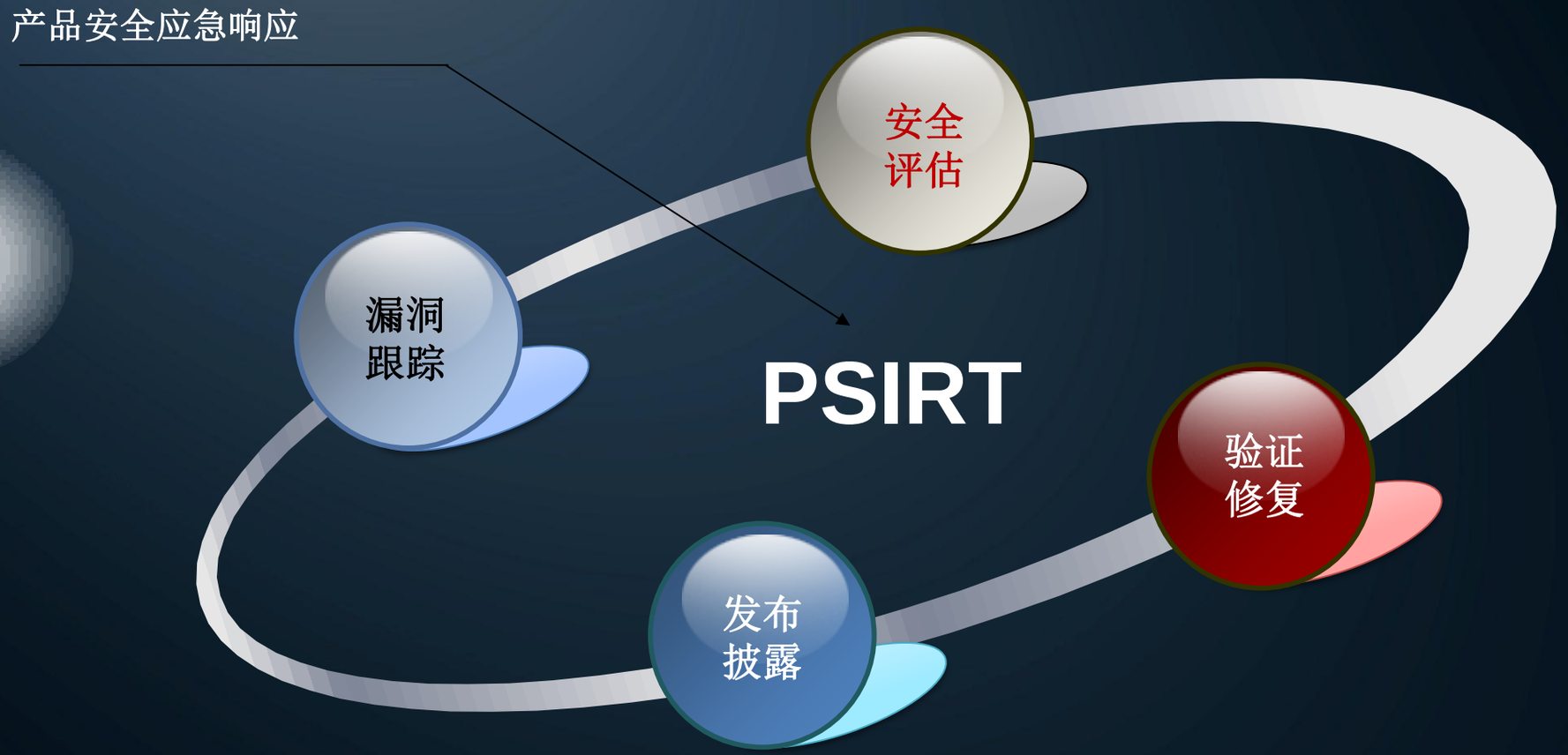
- 运输线路规划及监督，
- 通过IT系统管控物流过程
- 电子报关
- 货物、集装箱完整性检查，监控货物装卸过程。
- 封条管理以及正确施封

基础设施管理及门禁准入控制：7*24保安值守、CCTV监控、电子门禁识别系统

ISO28000 证书

C-TPAT 第三方审核报告

建立PSIRT团队



积极融入安全组织与标准

标准组织中的安全小组

ISO ITU WiMAX 3GPP IETF 中国通信标准化协会 DSL FORUM TeleManagement FORUM IMS Forum TRUSTED COMPUTING GROUP oma THE Open GROUP

安全产品和解决方案提供商

RSA symantec. TREND MICRO CITRIX Microsoft Novell IBM SPIRENT

安全认证和审计组织

MANAGING RISK Common Criteria @SECE EWA Applus

CERT（Computer Emergency Response Team）合作组织

FIRST CERT Software Engineering Institute Carnegie Mellon US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM CNCERT/CC

THANK YOU

中国互联网安全大会

360互联网安全中心