基于人工智能的大数据安全

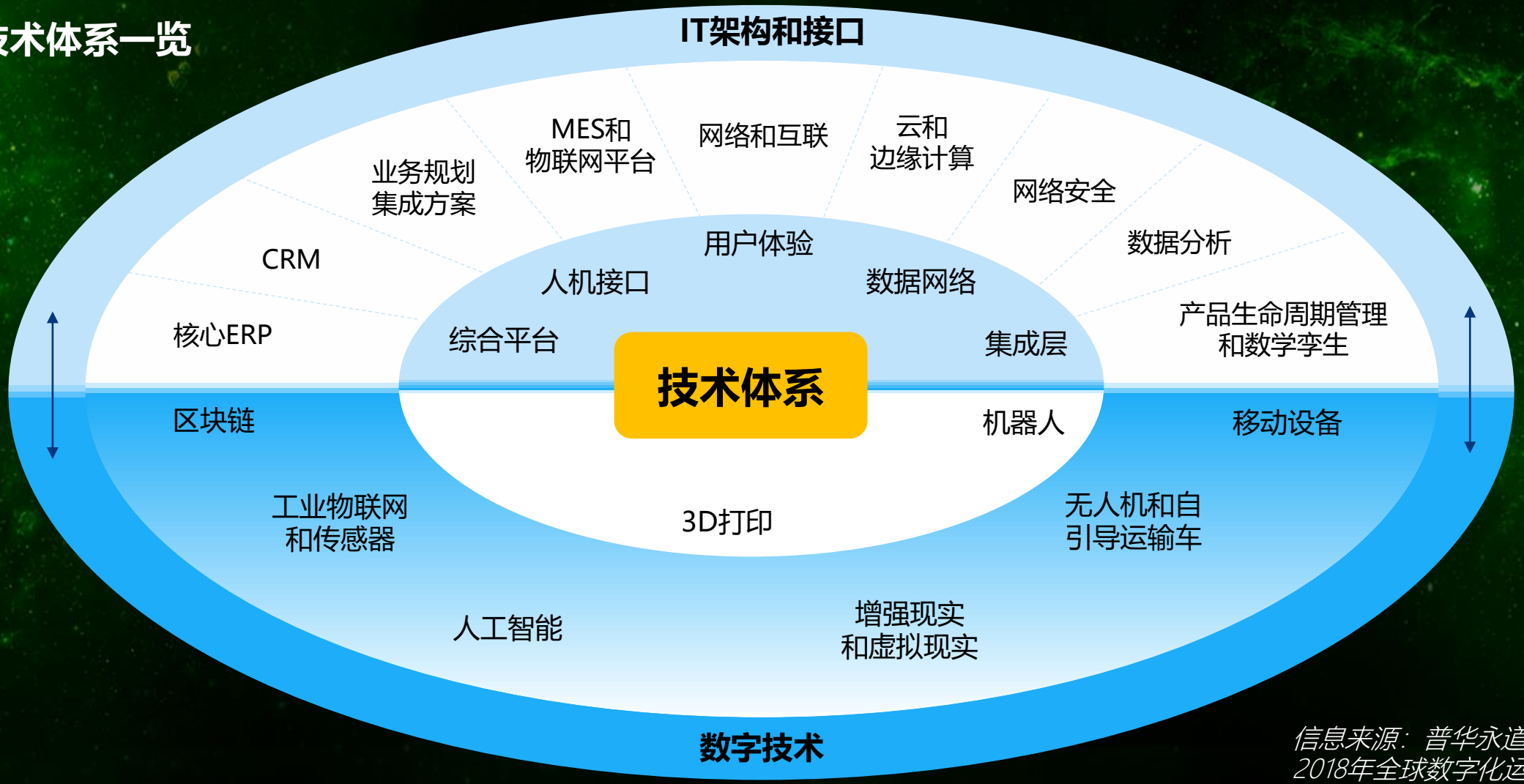
杨明非　天空卫士网络安全技术有限公司 合伙人

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018　Beijing·China
（原中国互联网安全大会）

企业数字化转型趋势

ISC 2018 ISC互联网安全大会 | 360互联网安全中心

技术体系一览



信息来源：普华永道思略特
2018年全球数字化运营调研

企业数字化转型对企业IT安全的挑战

ISC 2018 ISC互联网安全大会 | 360互联网安全中心

大数据应用导致数据更加集中，风险度更高

- 数字化转型中大数据分析技术被更加广泛使用
- 数据集中增大了业务价值，同时也带来更大的风险

企业安全边界消失

- 传统的基于防火墙、IPS构建的企业安全边界失效
- 更多的企业员工、外包、第三方来自于互联网无法有效保护

数据资产安全考虑不足

- 多数企业更关注业务支撑系统的建设，而忽视数据安全建设
- 传统的IT 系统安全建设主要考虑是以网络和威胁为主
- 缺乏原生的数据安全手段对数字化转型带来的海量数据资产进行保护

企业核心数据资产正在承受前所未有的巨大风险

- 内部违规人员的外泄 (accidental insider)
- 内部恶意人员的外泄 (malicious insider)
- 外部攻击者进入企业网后的外泄 (compromised insider)

准备离职的运维管理员

不怀好意的第三方接入

马大哈的业务人员

恶意的外部黑客

合规需求在逐步加强


ICS 35.040

L80

GB

中华人民共和国国家标准

GB/T 35273-2017

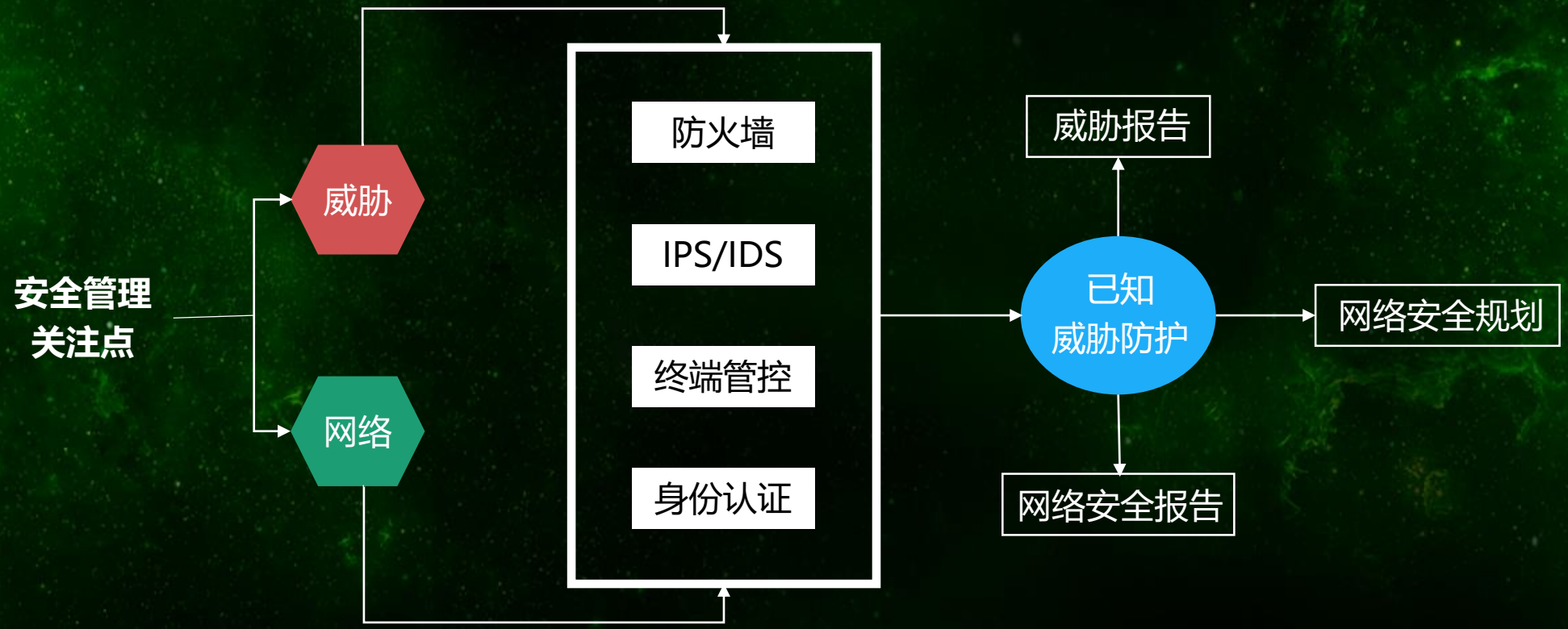
信息安全技术　个人信息安全规范

Information security technology — Personal information security specification

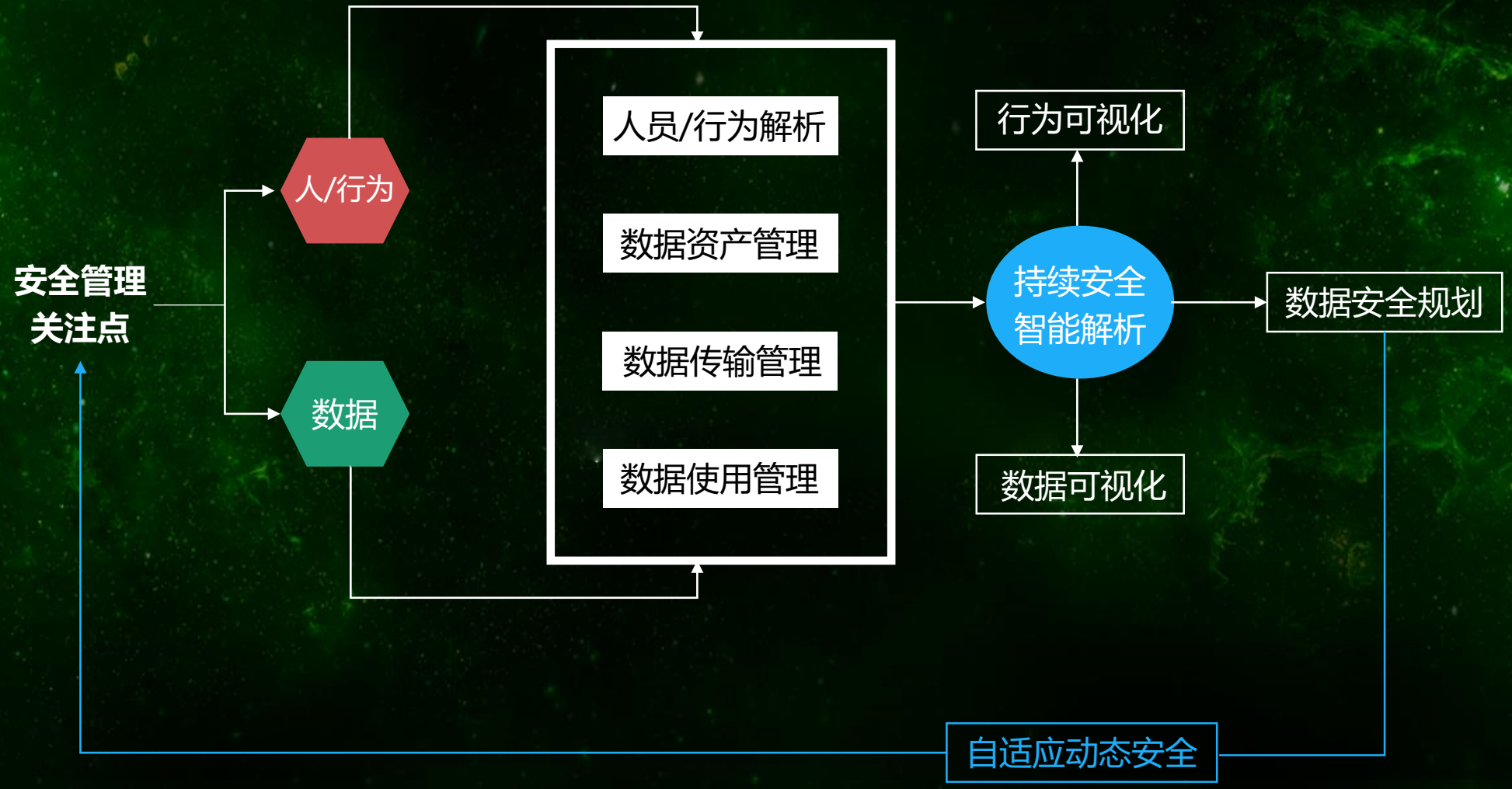
网络安全面临转折点

传统面向边界的安全模型不再成立　　传统基于好坏的鉴别机制不再有效　　传统围绕技术的安全工程不再适用

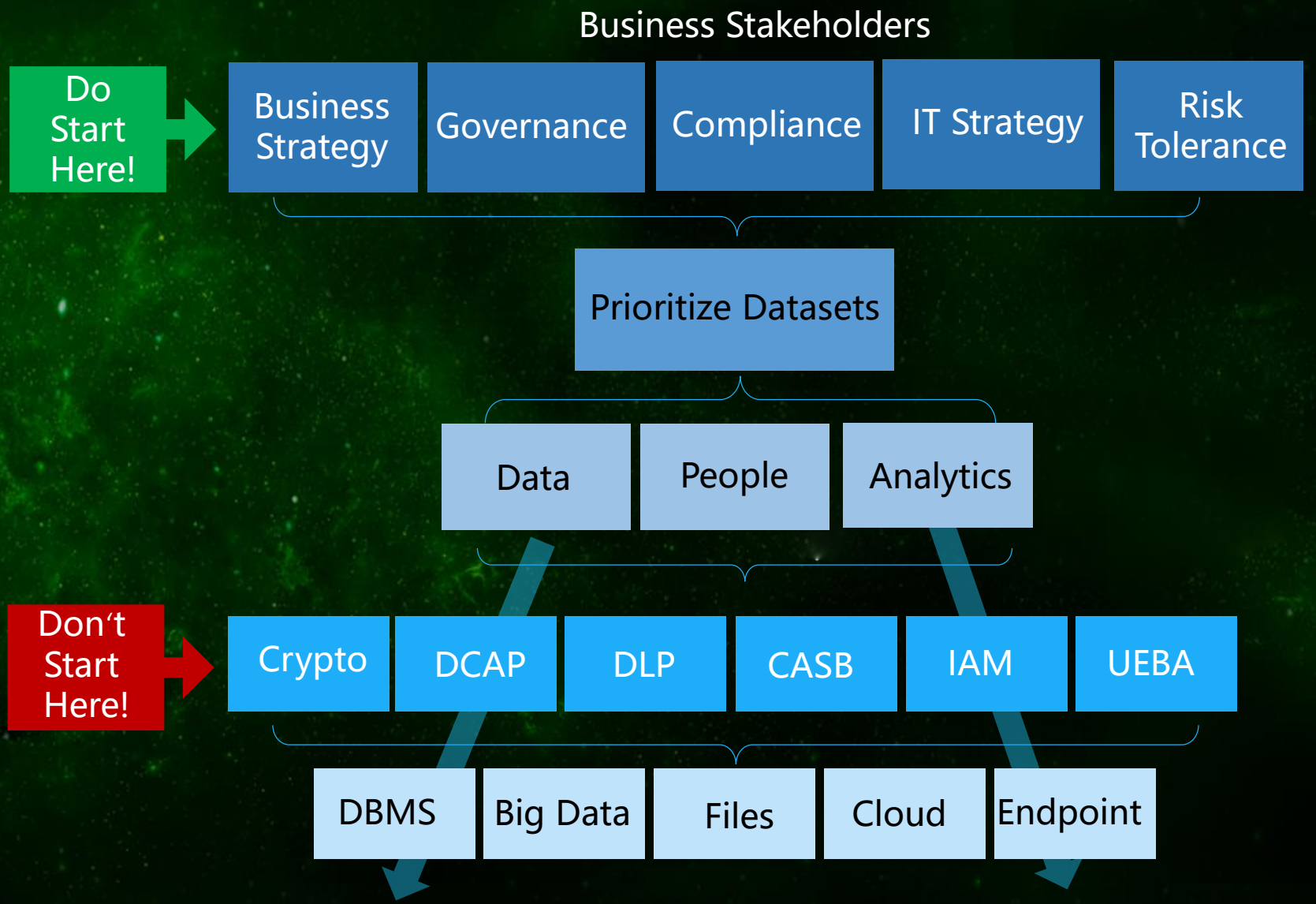
传统面向威胁的安全模型



面向人和数据的新安全模型



数据治理与数据安全



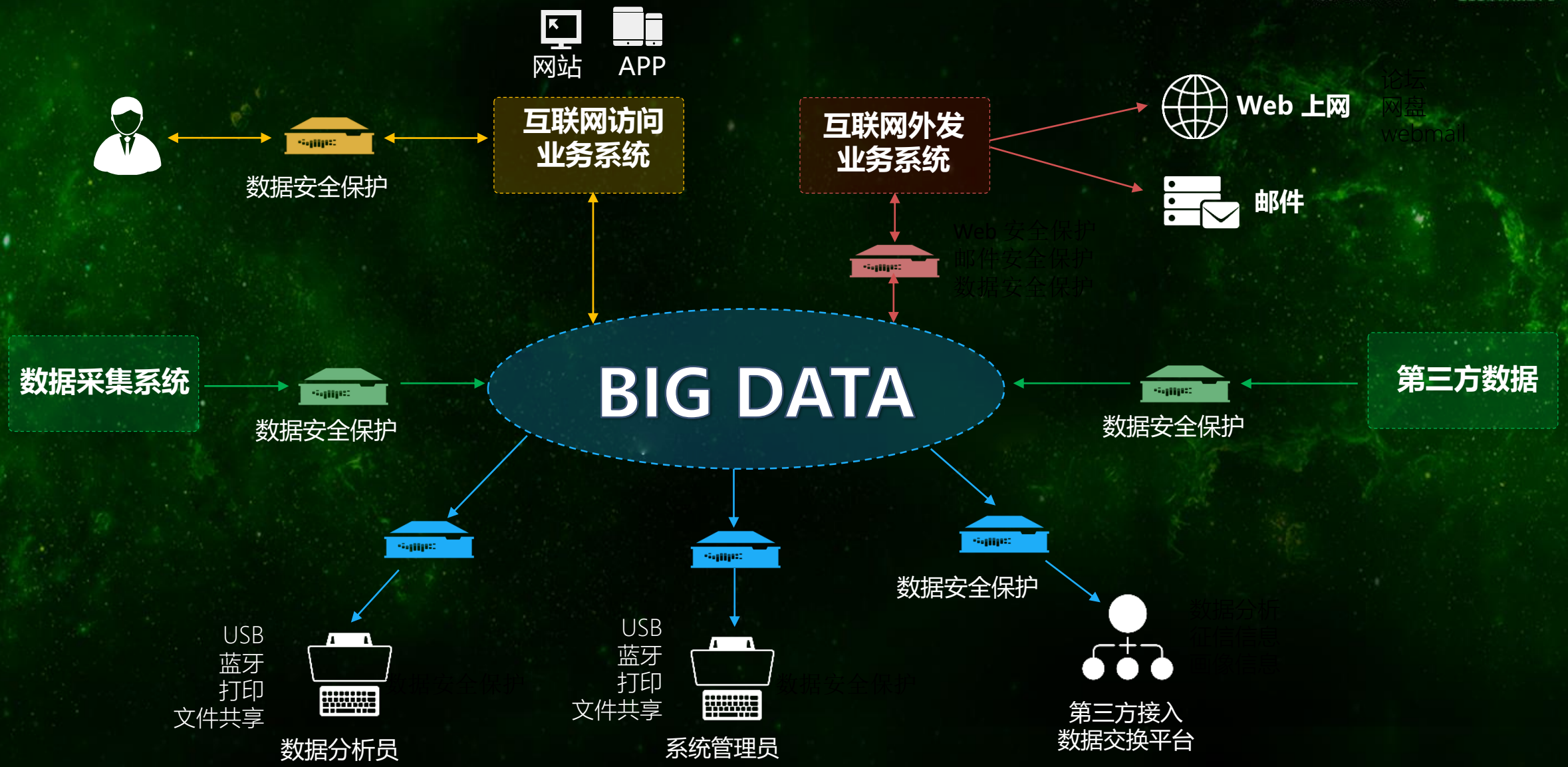
1. 平衡业务需求与风险
2. 标识、优先级排序和管理数据集的生命周期
3. 定义数据安全策略
4. 部署数据安全产品
5. 为所有产品编排统一策略

Gartner Data Security Governance Framework

应对：建立行为+数据的新安全体系

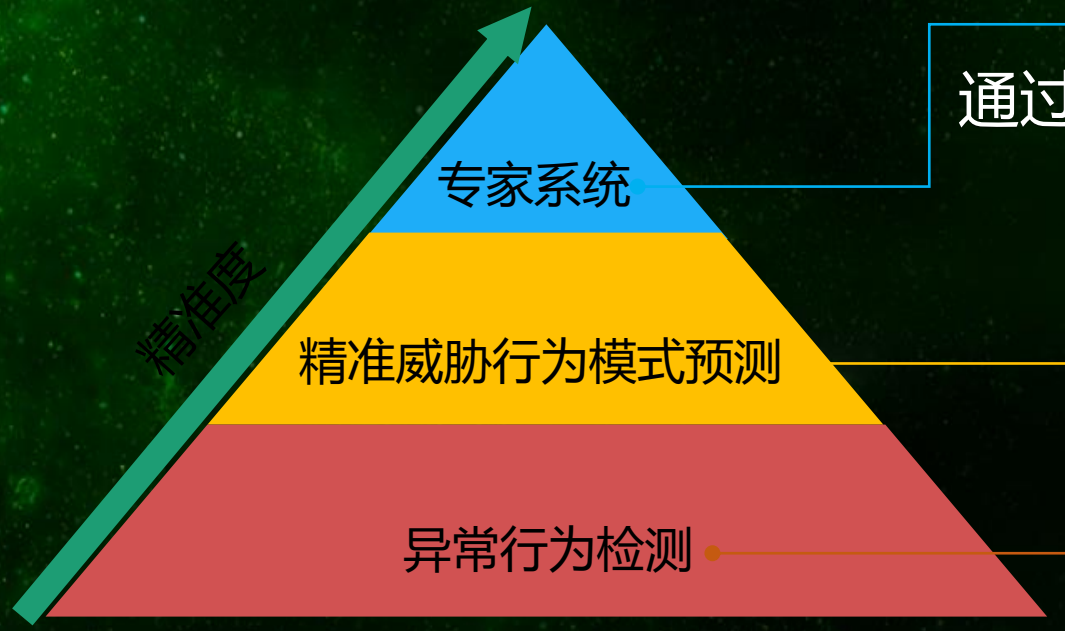
- 综合行为与数据
- 建立基于人的策略而不是基于组的策略
- 对数据的存储、使用和传输进行全面管理和控制
- 基于大数据分析、机器学习和DLP作为技术支持点

全面的大数据安全保护体系



建立以人为中心的数据安全体系

将安全防护模型从策略驱动转向面向用户驱动

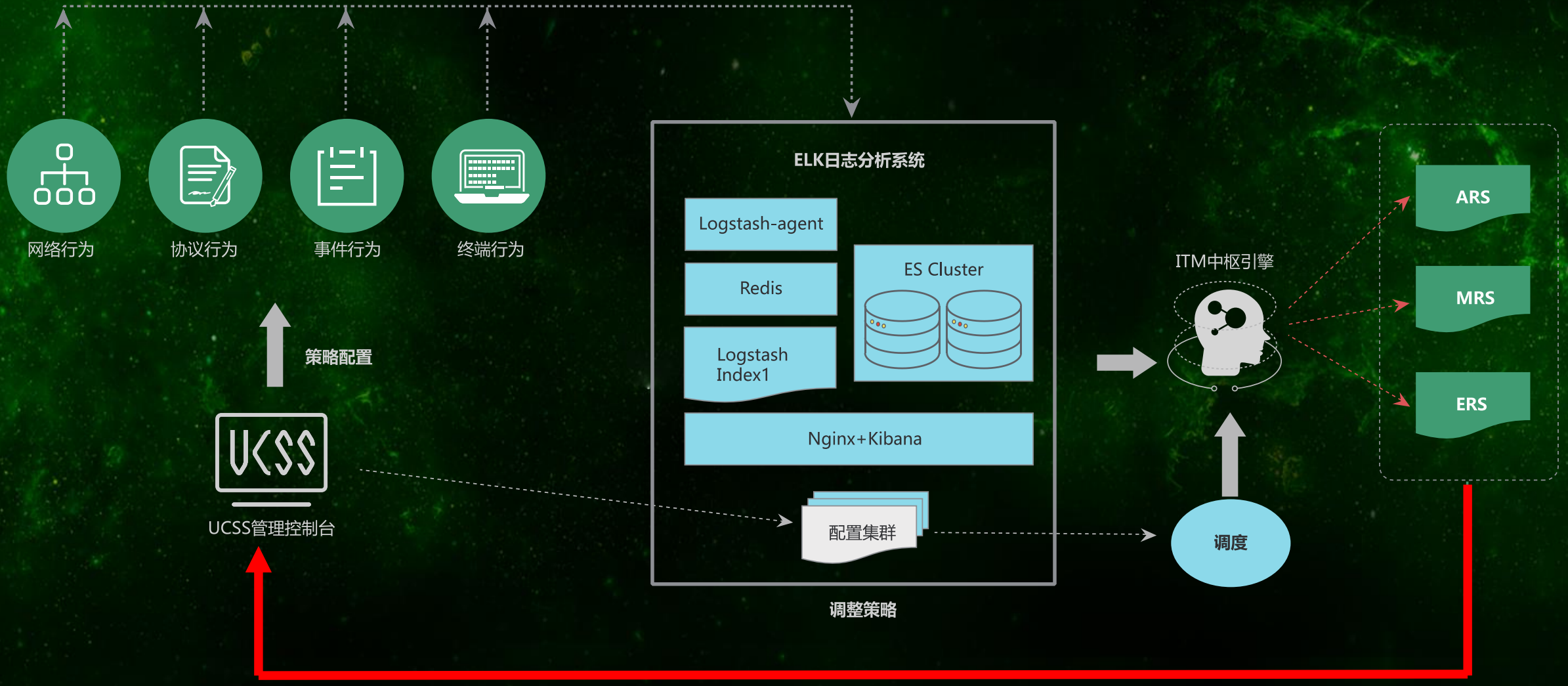


通过综合分析模型确认用户的威胁概率

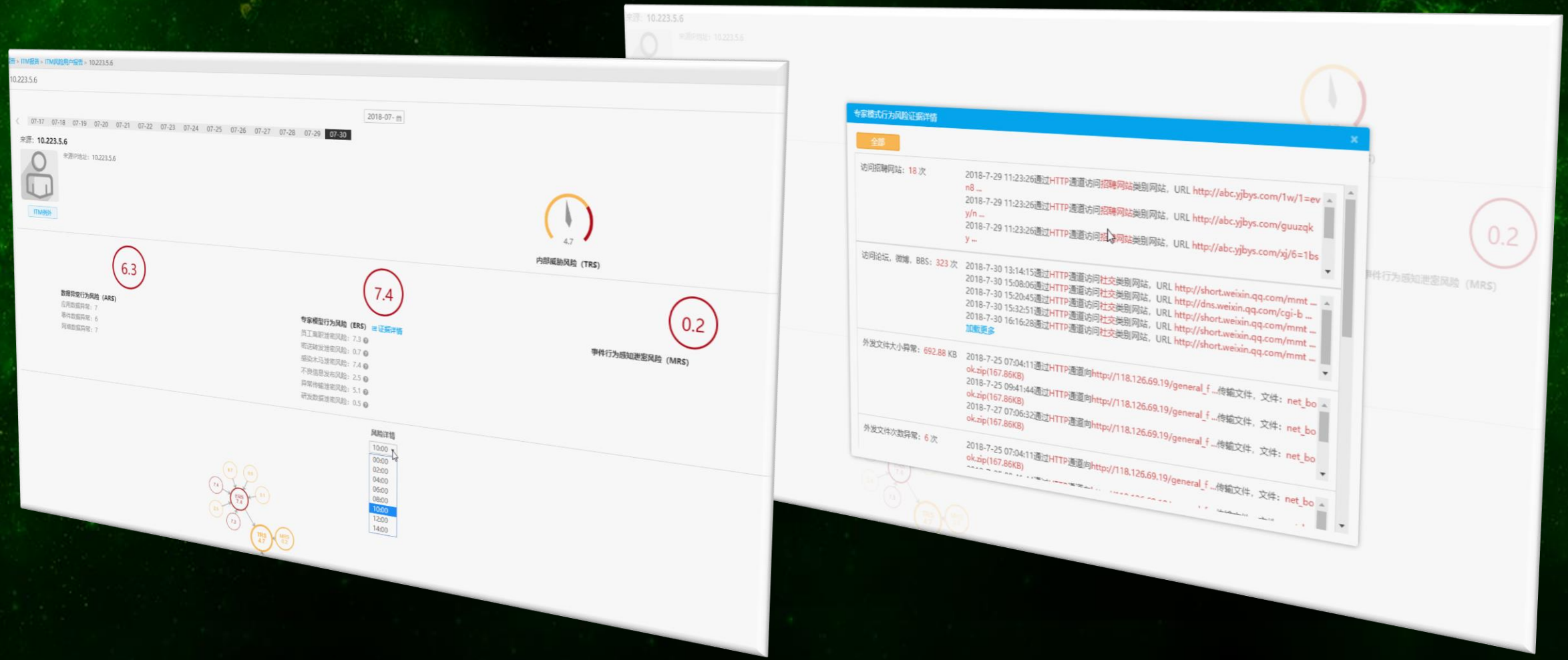
通过对准确定义的策略场景进行基于用户行为的深度分析

通过对大量数据的学习和分析找出异常行为用户

以人为中心的内部威胁防护系统

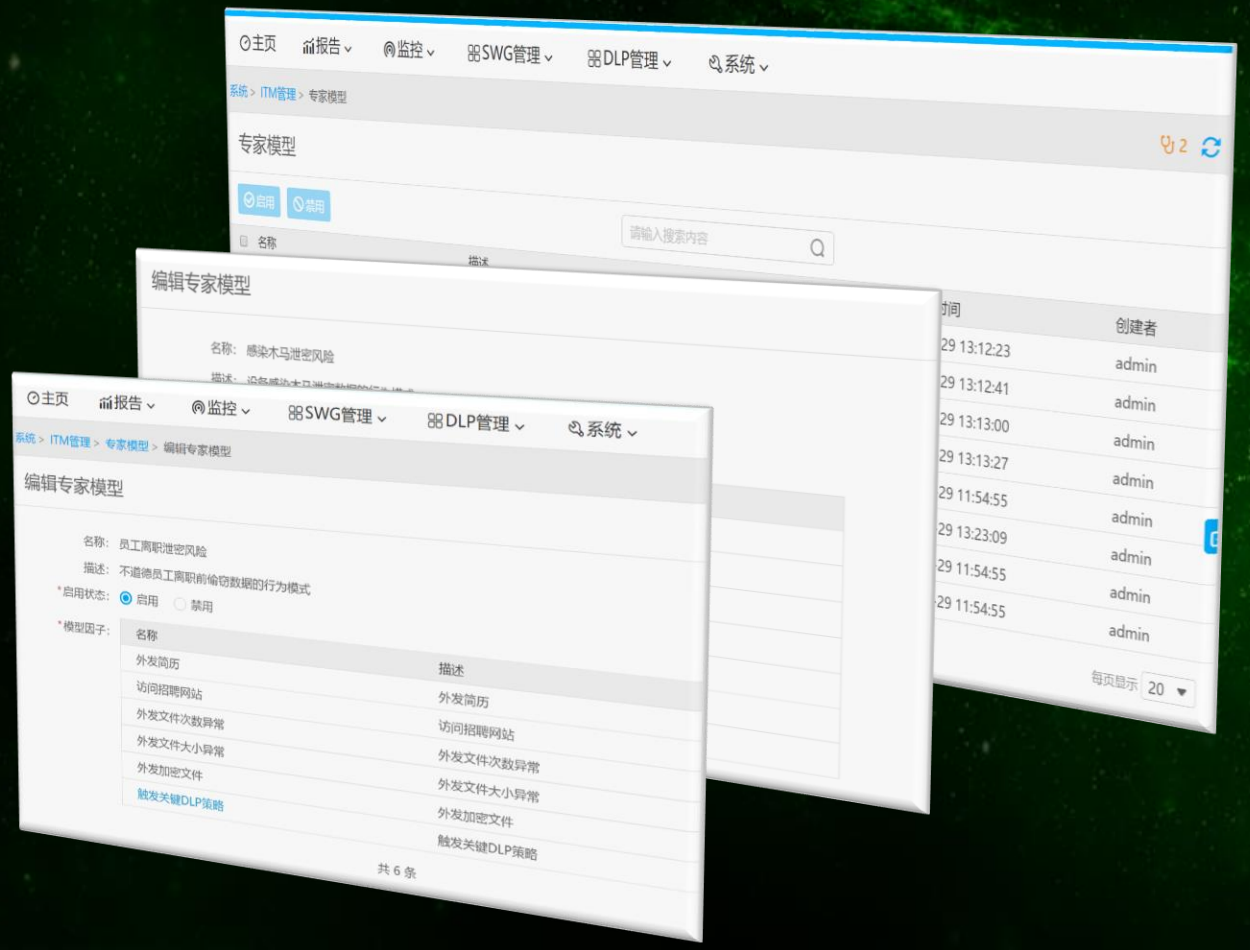


用户风险报告


10.223.5.6
2018-07-
07-17 07-18 07-19 07-20 07-21 07-22 07-23 07-24 07-25 07-26 07-27 07-28 07-29 07-30
来源：10.223.5.6
来源IP地址：10.223.5.6
ITM例外
6.3
数据异常行为风险（ARS）
应用数据异常：7
事件数据异常：6
网络数据异常：7
7.4
专家模型行为风险（ERS）
证据详情
员工离职泄密风险：7.3
远程破坏泄密风险：0.7
感染木马泄密风险：7.4
不当信息发布风险：2.5
异常传输泄密风险：5.1
研发数据泄密风险：0.5
4.7
内部威胁风险（TRS）
0.2
事件行为感知泄密风险（MRS）
风险详情
10:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
专家模式行为风险证据详情
全部
访问招聘网站：18 次
2018-7-29 11:23:26通过HTTP通道访问招聘网站类别网站，URL http://abc.yjbys.com/1w/1=ev
n8 ...
2018-7-29 11:23:26通过HTTP通道访问招聘网站类别网站，URL http://abc.yjbys.com/guuzqk
y/n ...
2018-7-29 11:23:26通过HTTP通道访问招聘网站类别网站，URL http://abc.yjbys.com/xj/6=1bs
y ...
访问论坛，微博，BBS：323 次
2018-7-30 13:14:15通过HTTP通道访问社交类别网站，URL http://short.weixin.qq.com/mmt ...
2018-7-30 15:08:06通过HTTP通道访问社交类别网站，URL http://dns.weixin.qq.com/cgi-b ...
2018-7-30 15:20:45通过HTTP通道访问社交类别网站，URL http://short.weixin.qq.com/mmt ...
2018-7-30 15:32:51通过HTTP通道访问社交类别网站，URL http://short.weixin.qq.com/mmt ...
2018-7-30 16:16:28通过HTTP通道访问社交类别网站，URL http://short.weixin.qq.com/mmt ...
加载更多
外发文件大小异常：692.88 KB
2018-7-25 07:04:11通过HTTP通道向http://118.126.69.19/general_f ...传输文件，文件：net_bo
ok.zip(167.86KB)
2018-7-25 09:41:44通过HTTP通道向http://118.126.69.19/general_f ...传输文件，文件：net_bo
ok.zip(167.86KB)
2018-7-27 07:06:32通过HTTP通道向http://118.126.69.19/general_f ...传输文件，文件：net_bo
ok.zip(167.86KB)
外发文件次数异常：6 次
2018-7-25 07:04:11通过HTTP通道向http://118.126.69.19/general_f ...传输文件，文件：net_bo
ok.zip(167.86KB)
0.2
事件行为感知泄密风险（MRS）

预置专家模型ERS（持续更新扩展）

- 预测员工离职倾向 和 离职泄密风险
- 预测员工感染木马的机率 和 恶意感染泄密风险
- 预测员工主动故意泄密风险
- 预测员工针对核心知识产权数据的窃密 与 泄密风险
- 预测员工异常数据传输倾向 和 异常数据泄密风险
- 预测员工邮件转发或密送恶意泄密风险
- 预测员工不良信息发布机率 和 不良信息扩散风险



新安全体系的业务价值 – Insider Threat Protection

真正的内部威胁防护

- 通过行为分析发现潜在和正在发生的内网威胁事件
- 可以对威胁进行阻止的人工智能分析系统
- 真正理解“内容”行为的大数据分析系统

降低管理难度

- 初级使用对管理难度较低，系统自动运行并发现可疑事件
- 专家模式可以协助用户降低误报

整体企业安全边界保护

- 全面覆盖企业边界
- 对数据资产实现全面保护

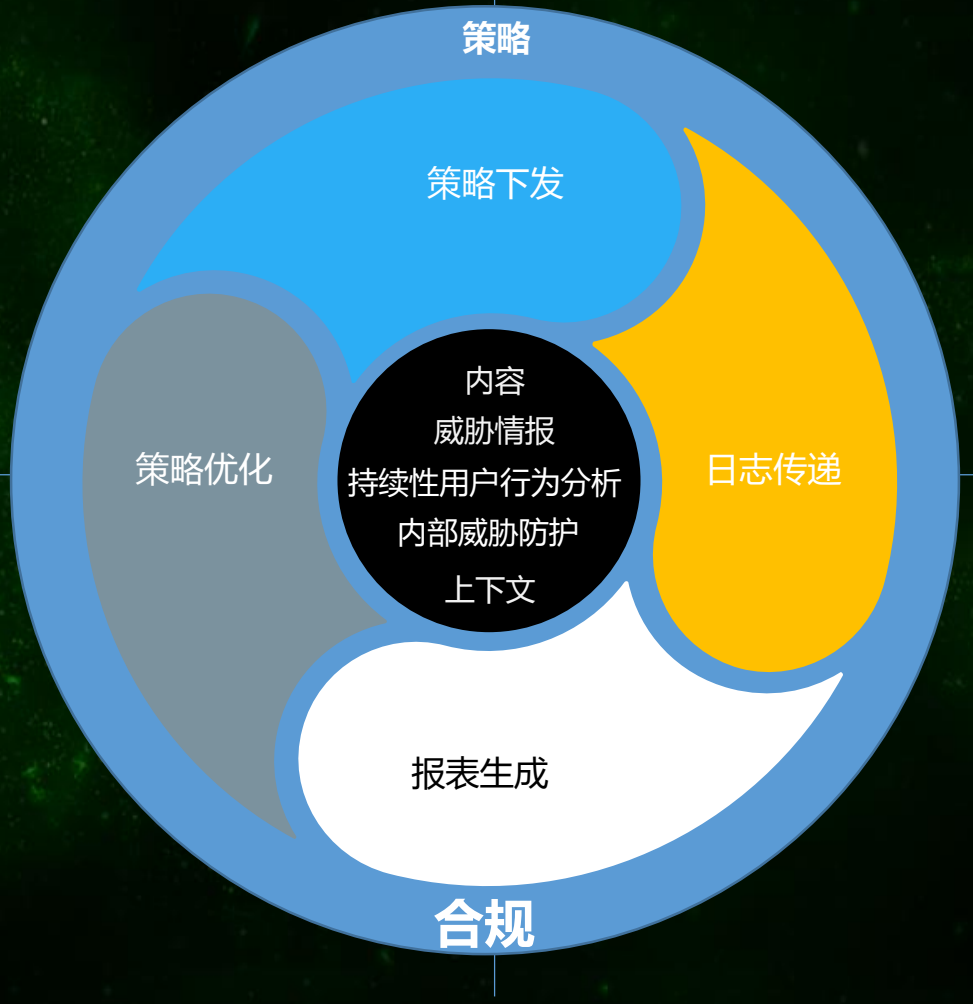
以人为中心的持续性数据安全模型

Discover

- 数据分类分级
- 数据保护基线
- 数据保护范围
- 合规需求

Prevent

- Web安全网关
- 邮件安全网关
- 终端安全防护
- 数据防泄漏系统
- 用户行为采集



Respond

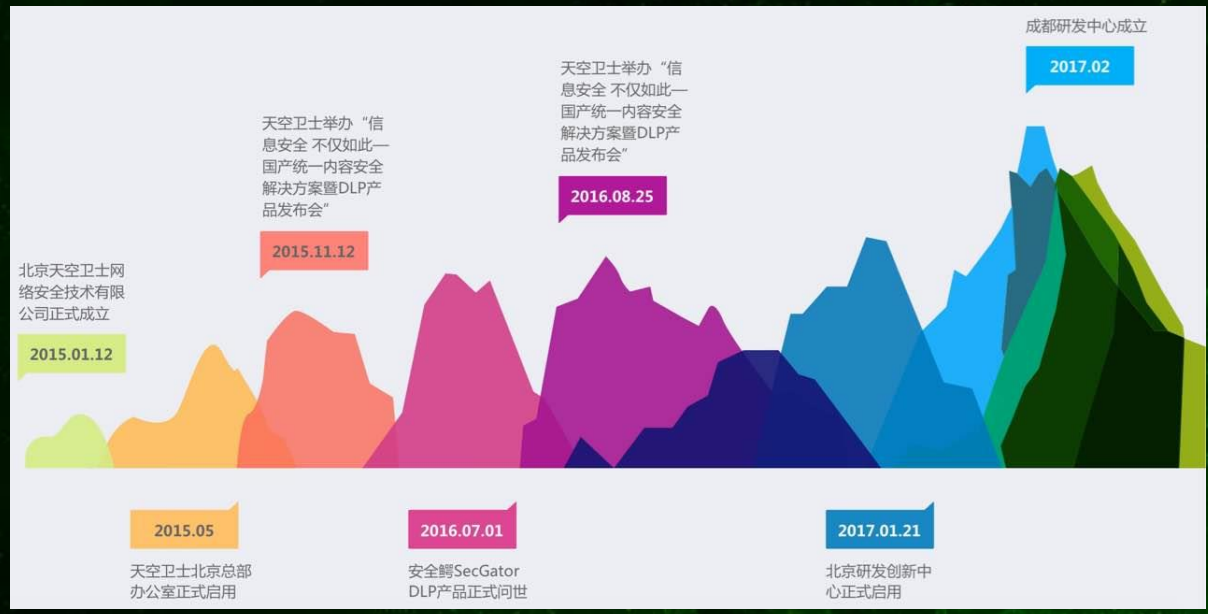
- 策略优化
- 行为判定优化
- 态势分析
- 可信度分值反馈

Detect

- 异常行为发现
- DLP事件分析
- 威胁情报分析
- 用户可信度分值计算

关于天空卫士

- **专注于信息资产安全的创新技术公司**
  - 2015年1月成立, 员工总数近200人，研发与售前咨询团队比例超过85%
- **由国际信息安全领导厂家研发和管理团队创立**
  - 核心团队均来自全球领先数据安全厂商的中国及全球研发中心与顶级安全厂商与咨询公司
  - 数十位顶级国内数据安全研发、大型项目实施经验团队
  - 在数据安全领域研发投入与规模最大的中国公司

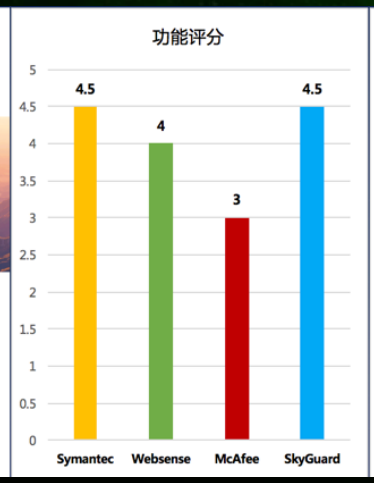


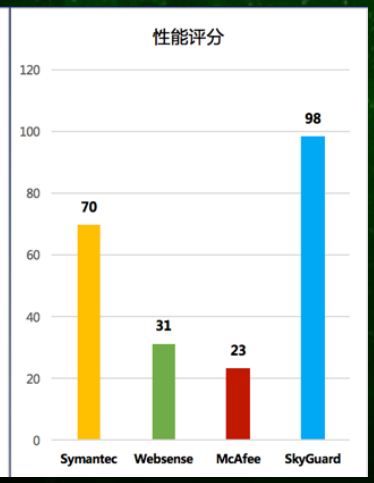
天空卫士2016年度北京钓鱼台国宾馆发布会

我们的使命与愿景 保护中国企业信息资产安全

ISC 2018 ISC互联网安全大会 | 360互联网安全中心

- **真正国产“自主、安全、可控”**
  - 唯一可以直面国际领先同类产品的中国公司
  - 同时具备公安部与军队产品销售资质
- **基于人和数据安全创新与超越**
  - 数十项针对国际领先技术产品
    - 基于人工智能的内部威胁防护体系
    - 国内领先的Web安全代理，全功能对标国外顶尖产品
    - 强大的邮件外发审查保护产品，支持邮件回溯分析
    - 多种部署模式，本地、云、混合云等全面支持新IT架构
    - 创新型应用数据安全保护体系
    - 丰富的外部支持工具降低数据治理和安全实施成本





*来源：2016年8月计世资讯 《中国DLP评测报告》

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原中国互联网安全大会）