

# 2024年中国威胁情报行业 发展研究报告

## INTRODUCTION

# 引言

**正本清源：明确“威胁情报”的内涵与外延。**随着各类网络安全威胁与日俱增，新型攻击手段层出不穷，各类企业和组织的网络安全策略逐渐由“被动”转为“主动”，由“治疗”转为“预防”，“威胁情报”这一概念因而引发各方聚焦。但网络安全行业覆盖面广，细分类型众多，涉及包括基础架构安全、数据安全、零信任、渗透测试/红蓝对抗等二十余个领域，且各领域彼此相互拓展，领域间边界不清。基于此种背景，本报告将明确“威胁情报”的内涵与外延，“威胁情报”与其他网络安全领域的区别与联系，树立“威胁情报”行业价值。

**市场透视：从供需两端观察中国威胁情报市场发展现状。**报告将对包括微步在线的威胁情报头部企业展开充分调研，了解各企业技术、产品、市场及综合能力。从行业全局视角计算总体市场规模并判断未来走势；从供给端归纳行业主要参与者，讨论威胁情报的基础能力、商业模式与产品能力指标，定量展示中国主要威胁情报厂商市场份额；从需求端展示产品落地情况及实施效果。

**发展洞察：探寻威胁情报行业未来趋势。**报告将以发展的视角观察可能对未来产生重大影响的行业焦点，包括情报出海、AI大模型及漏洞情报三大方向。分析威胁情报在合规、技术与应用方面的演进趋势，并尝试洞悉这些趋势可能导致的行业格局变化，或带来的潜在市场机会。

# CONTENTS

# 目 录

---

## 01 中国威胁情报发展背景与行业界定

---

## 02 中国威胁情报行业洞察

---

## 03 中国威胁情报行业案例

---

## 04 中国威胁情报行业趋势洞悉

01 /

# 中国威胁情报 发展背景与行业界定

# 发展背景：网络威胁现状

## 全球范围内网络威胁呈增长态势，攻击者能力与攻击频率均有上升

从宏观视角看，随着全球数字化进程加速，网络成为企业数字化运营的关键支撑，在网络带来前所未有的便捷和效率的同时，网络威胁也随之增长。根据公开研究报告显示，攻击者数量、攻击速度相较于往年均有上升，大规模勒索行动的受害者数量也增长76%。同时，各主要行业遭受的攻击频率都有所上升，其中科技、咨询、金融业遭受的攻击频率最高，工业工程、房地产、能源行业遭受的攻击频率增长快速，增速最高达102%。

### 全球网络威胁态势增长：从攻击能力到攻击频率

#### 网络威胁相关指标增长



##### 被攻陷时长缩短

交互式电子犯罪入侵活动的平均突围时间从2022年的**84分钟**减少到2023年**62分钟**，最快突围时间仅为**2分7秒**



##### 攻击者增多

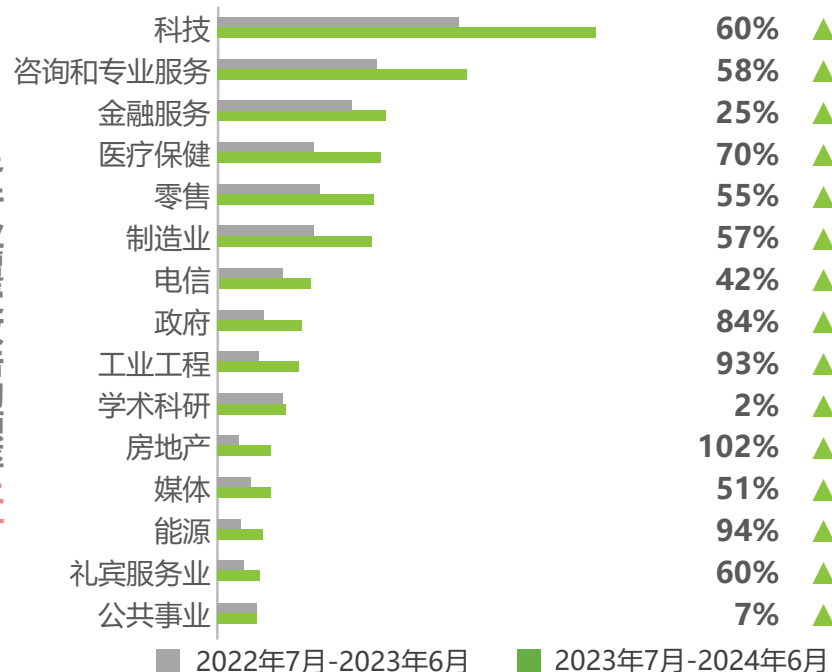
2023年CrowdStrike追踪到**34个**新的攻击者组织，总数达**232个**



##### 受害者增多

大规模勒索行动的受害者数量同比增长**76%**

#### 各行业遭受攻击的频率上升



# 发展背景：企业视角

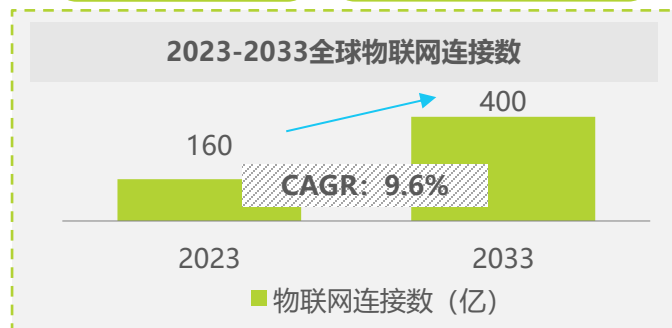
## 数字化转型扩大企业与网络威胁接触范围，亟需更全面、及时的防护能力

从企业视角看，随着数字化转型的推进，企业内部面临的网络风险正不断增加。从2023到2033年，全球物联网连接数预计将从160亿增长到400亿，复合年增长率达9.6%，接入网络的设备显著增多。同时，企业业务不断扩张，远程办公设备增长、多云策略的采用都带来更多连接点。此外，数据资产协同与共享愈发频繁，在数据同步和共享常态化的趋势下，企业更容易因软件漏洞等问题受到攻击，且修复关键漏洞的时间较长。

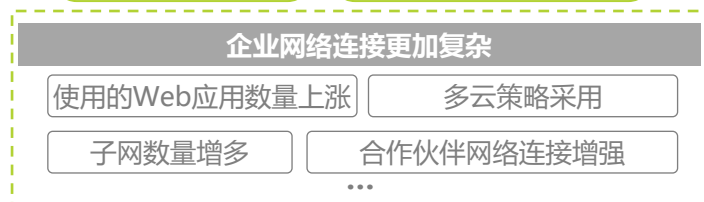
### 数字转型下企业网络风险扩增：从连接泛化到交互递增

#### ● 设备与网络连接增多

- 1 设备数量激增 连接方式更为复杂 ...

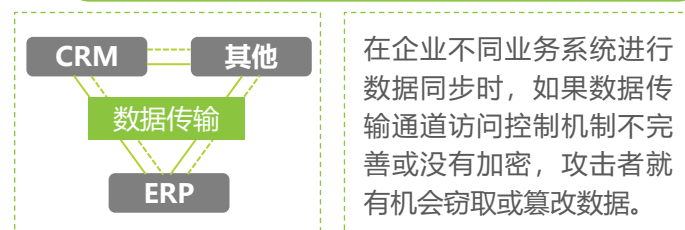


- 2 供应链需协同 与外部网络连接增多 ...



#### ● 数据资产协同与共享频繁

- 1 企业内部不同业务系统间的数据流动增多



- 2 共享数据常态化，企业面临的软件漏洞增多

Verizon在调研中强调，2023年攻击者利用漏洞作为入侵的初始访问步骤的情况增长了180%，这些漏洞主要是包含MOVEit漏洞（文件共享系统漏洞）在内的零日漏洞。

180%

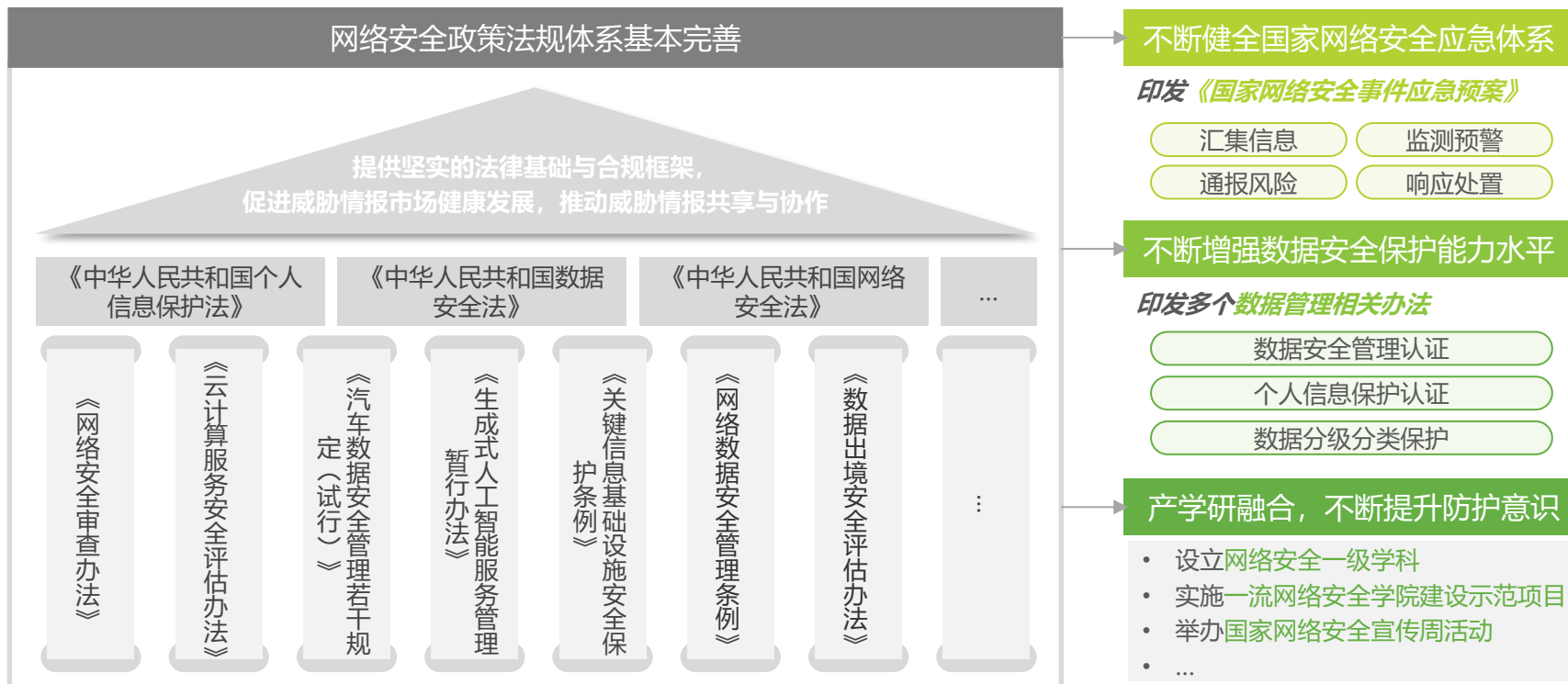


# 发展背景：政策视角

## 政策以“全方位、细粒度”模式推进企事业单位网络安全防护能力提升

在数字化浪潮和网络威胁态势交织的当下，国家高度重视网络安全。国家密集出台政策在全国范围推进企业安全防护能力进阶，从多维度拓展安全要求范围，全面提升企事业单位网络安全防护意识。目前，网络安全防护理念已经从被动防御转为主动防御，企事业单位亟需更先进的防御措施，及时检测、识别，预测安全威胁，加快响应速度，减少网络威胁带来的损失。

### 国内网络安全政策推进方向：从覆盖范围到渗透力度



来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 威胁情报内涵

## 通过收集、分析多源数据得到的威胁表征、攻击对象、攻击方式等情报

威胁情报构建者对各类网络活动监测数据、安全事件详情、恶意软件特征以及来自安全社区与专业平台的共享信息等多维度素材进行系统梳理与深度挖掘，提取出如恶意IP地址、可疑域名、异常文件哈希值等关键威胁指标（IOC），识别出背后的威胁行为者及其动机、技能水平与攻击偏好，明确攻击所采用的战术、技术和程序，从而为网络安全防御者提供全面、精确且具前瞻性的决策依据。根据威胁情报的内容组成和用途，可以分为：1) 辅助技术人员阻拦网络攻击的战术威胁情报；2) 辅助运营人员持续、全面管理组织安全状态的运营威胁情报；3) 辅助安全负责人制定宏观安全策略的战略威胁情报。

### 威胁情报内涵：从技术实践到战略应用

#### 战术威胁情报

##### 【用途】检测和响应正在进行的网络攻击

安全技术人员通过比对战术威胁情报，及时发现恶意攻击，并参考威胁情报所记录的攻击者行为，找到合适的方式切断攻击。

##### 常见战术威胁情报内容

###### 判断指标

文件哈希值  
网络流量  
系统文件  
用户权限  
...

###### 判断依据

文件传输前后不一致  
短时间内异常上升  
频繁修改或大量复制  
不断尝试越级访问  
...

#### 运营威胁情报

##### 【用途】预防攻击，实现可持续安全运营

运营威胁情报除了涉及战术威胁情报，还包括组织内部的安全工具、安全人力、安全预算等更宏观的信息。

##### 常见运营威胁情报内容

###### 判断指标

威胁拦截率  
攻击检出率  
平均响应时间  
安全预算  
...

###### 判断依据

拦截率是否达标  
工具检测是否准确  
防护响应是否灵敏  
是否偏离执行预算  
...

#### 战略威胁情报

##### 【用途】制定宏观安全策略，管理数字风险

战略威胁情报的内容倾向长期、宏观的信息，为安全负责人等高层决策者提供战略支持。

##### 常见战略威胁情报内容

威胁行为者的动机或目标

行业或区域的网络威胁趋势

新兴威胁技术和威胁场景预测

★ 获取难度增加

★ 信息量增大

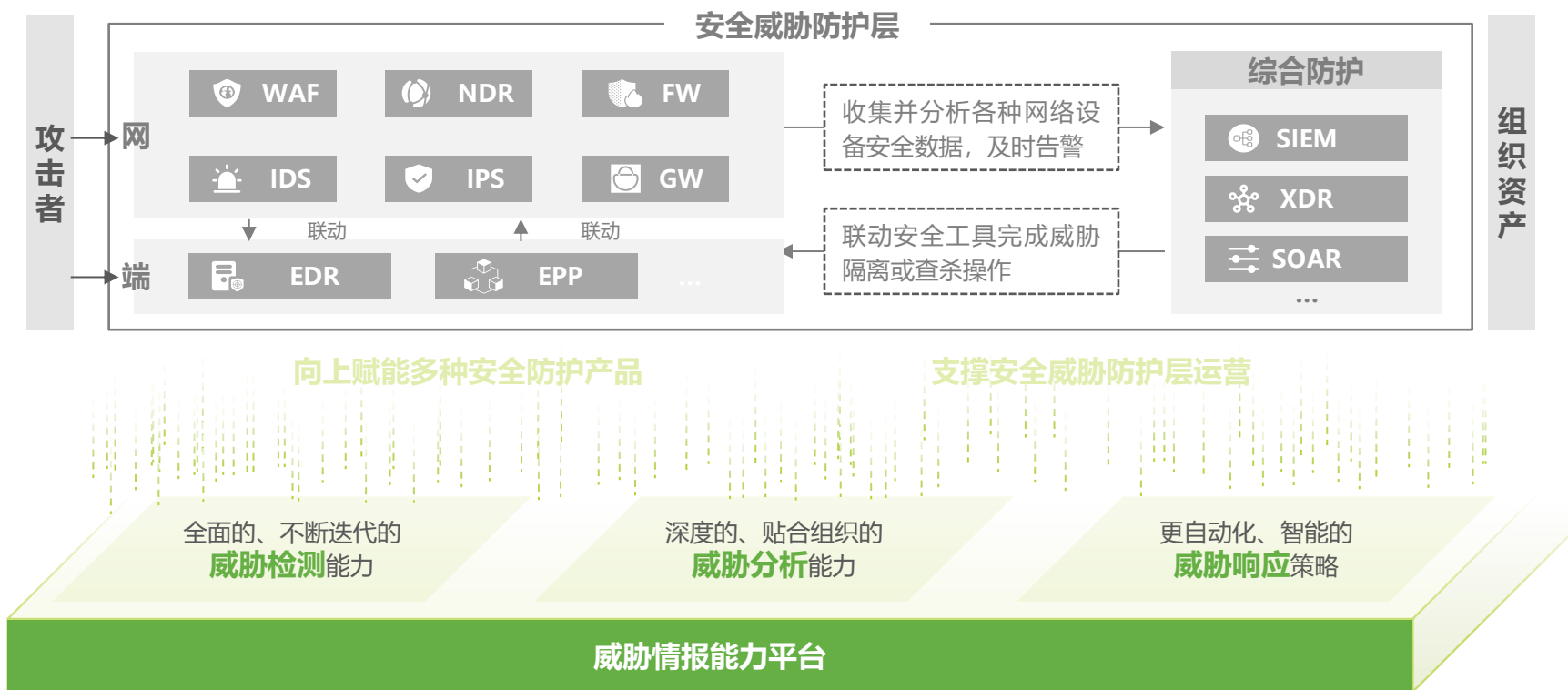


# 威胁情报外延

## 作为网络安全高阶能力，提升安全产品防御主动性与及时性

不同安全产品在网络安全防御中有特定防护对象和应对的威胁类型，威胁情报的能力可以有效提升安全产品防御主动性与及时性。威胁情报能实时收集、分析全球网络威胁信息，精准洞察新型攻击手段。当新威胁出现，安全产品依据自动生成的威胁情报快速精准检测，快速响应处置。如未知恶意软件来袭，产品借助情报预判，主动出击拦截，而非被动等待攻击发生，起到防御关口前移功能，极大增强防御效能。

### 威胁情报外延：威胁情报赋能安全运营



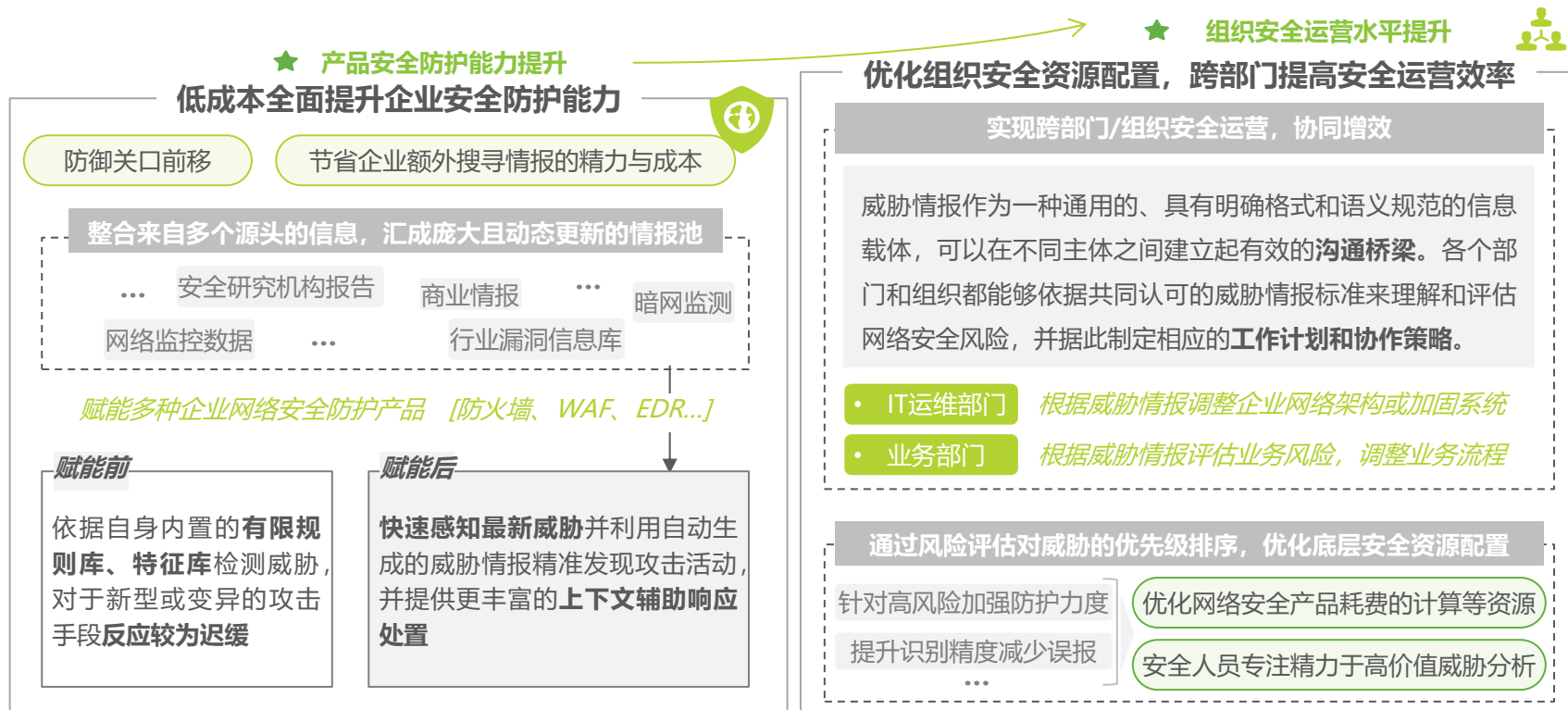
来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 威胁情报价值

## 从提升企业主动防御能力到增进企业全面安全运营效能

在当今复杂多变的网络安全环境中，企业可以通过借助动态更新的威胁情报库或威胁情报赋能的安全产品提前洞察潜在的安全风险，在攻击尚未发生之时就精准布防，实现主动防御，有效防止恶意入侵。在安全协作方面，威胁情报作为一种标准化的信息载体，可以实现跨部门/组织共享安全信息与应对策略、实现最大化利用安全资源，构建起稳固且可持续发展的网络安全体系。

### 威胁情报价值：实现主动防御和协同防护



来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 国内外发展对比

## 基础能力至成熟产品发展趋同，产品融合与使用水平进展有别

海外威胁情报行业的宏观发展路径经历了从基础威胁情报能力的构建，到成熟可调用的威胁情报能力平台的建立，再到威胁情报与其他安全产品的联动融合三个阶段。国内威胁情报行业的发展轨迹与此相似，但由于起步较晚，其发展速度和成熟度与海外相比有所差距。在产品融合与使用水平方面，由于国内外安全需求的差异，国内威胁情报融入的产品类别顺序与海外存在差异。此外，海外由于安全产业起步较早，多数企业的整体安全运营能力相对优于国内，因此海外企业在威胁情报的使用水平上也相对较高。

### 国内外威胁情报发展路线对比



来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

02/

# 中国威胁情报 行业洞察

















# 中国威胁情报行业产品商业模式

## 三类纯情报产品各具优势；多样情报融合方式形成3类综合产品

当前国内市场威胁情报主要以两种方式被用户采用，一种是对威胁情报数据及平台的直接应用与消费，另一种是通过使用安全监测响应类产品，为这类产品中的情报能力或情报模块买单。前者专注提供高质量的情报数据和服务，通常以标准化API接口、TIP平台或是通过威胁情报门户账号订阅方式交付，API及威胁情报门户账号订阅更侧重情报数据交换的便捷与及时性，TIP则更侧重对情报数据的查询、分析、生产、共享及狩猎等全方位情报管理与流程化操作。后者情报主要以三种方式与其他产品融合，形成情报赋能型产品。

### 威胁情报产品落地模式

#### ■ 纯情报产品形式交付

	主要特征	模式图示	收费方式	典型用户
<b>API</b>	<b>外向查询：</b> 需企业将数据输出至情报平台进行检测  <b>便捷易用：</b> API轻量化部署，使用方便，订阅周期灵活	<b>企业</b>  从本地设备、安全平台汇集需要检验的安全类数据  <b>API</b> 安全类数据通过API发送请求，数据在云端与威胁情报碰撞，企业可直接查看结果，判断风险 <div> <div>安全日志</div> <div>资产漏洞</div> <div>可疑文件</div> <div>...</div> </div>	<b>订阅</b>  按照威胁情报查询量向用户收费	<b>画像</b> - 对数据安全性要求适中 - 企业情报查询量较低  <b>用户 中腰企业</b>  互联网  高科技  外企
<b>门户账号订阅</b>	<b>开箱即用：</b> 只需购买门户账号，即可获取最新最全的威胁情报  <b>灵活高效：</b> 威胁情报门户提供各类情报分析、订阅及导出	<b>企业</b>  通过账号获取威胁情报门户提供的以情报数据工具、情报报告等人读情报为主的各类情报分析 <b>账号</b>  <b>账号</b> 获取精选的开箱即用的威胁信息及数据 <div> <div>最新安全事件</div> <div>攻击工具数据</div> <div>热门趋势图表</div> <div>IOC</div> </div>	<b>订阅</b>  一般按年或按次收费	<b>画像</b> - 对情报分析、呈现要求较强  <b>用户</b>  企业安全  研究团队
<b>TIP</b>	<b>本地部署：</b> 威胁情报被汇集至用户本地，保护企业自身数据安全  <b>全面赋能：</b> 本地化部署与企业业务深度结合，可覆盖更多应用场景	<b>企业</b>  与安全组件深度融合，赋能企业精准安全运营 <b>TIP</b>  <b>TIP</b> 威胁情报定向输入至用户本地TIP产品中 <b>平台</b>  <b>平台</b> 最新、多源、海量的威胁情报接入与整合 <div> <div>IOC</div> <div>IP信誉</div> <div>漏洞情报</div> <div>...</div> </div>	<b>硬件+订阅</b> - 硬件费用 部署在用户端的硬件产品 - 订阅费用 威胁情报使用费用，一般每3年付费	<b>画像</b> - 对数据安全、企业隐私要求较高 - 企业情报查询量较大  <b>用户 头部企业</b>  金融  政府  央企  能源

#### ■ 情报赋能形式交付

1 情报作为“高位能力”赋能厂商自身其他安全类产品

XDR SOC FW ...

↑ 对内赋能

情报中台

2 以技术服务的方式为其他厂商产品提供情报支持

情报技术 → 厂商A 厂商B ...  
对外支持

3 以组成模块的方式与其他厂商模块共同构建解决方案

情报模块 + 模块A 模块B ...  
方案打包 → 用户

来源：结合专家访谈、公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 中国威胁情报行业产品能力与厂商竞争力

产品能力指标：准确性、丰富性、及时性；厂商竞争力指标：数据、技术

**【产品能力指标】**从用户视角看，威胁情报产品能力可拆分为情报准确性、丰富性与及时性三方面。准确性指威胁情报的精准度，能够有效帮助客户减轻安全运营成本；丰富性对应威胁情报的覆盖度与颗粒度，体现了情报的信息含量；及时性指威胁情报在其生命周期结束后快速更新，保证情报信息的高可用。这三方面也是用户订购威胁情报产品的核心考量因素。

**【厂商竞争力】**从情报生产侧观察，安全大数据的采集以及对数据的分析挖掘能力成为企业的核心竞争力。安全大数据采集包括利用社区、沙箱、蜜罐等多种方式获取公开情报、恶意样本特征、基础网络信息等安全类基础数据，为威胁情报的生产提供“原料”。同时，各厂商借助大数据处理、人工智能等一系列技术手段，采用自动化方式将以上基础数据进行标准化、关联与拓线，并由专业分析师参与重点情报的定向分析，持续生产高质量、多维度的威胁情报。

## 威胁情报产品能力及厂商竞争力指标



来源：结合专家访谈、公开资料整理，艾瑞咨询研究院自主研究及绘制。



# 中国威胁情报行业厂商能力特点

## 基于基础数据、服务经验、业务特征等自身禀赋，差异化构建情报能力

威胁情报对于安全类产品的能力提升已经成为行业共识，业内主要厂商均已着手构建情报能力。但由于企业DNA所造就的在基础数据、服务经验、业务特征等方面的差异，因而各厂商的威胁情报产品能力也各有特点。下表列举了5家威胁情报主要厂商代表以及中小型企业威胁情报厂商的能力差异，我们可以看到各厂商如何基于自身禀赋及战略目标，规划设计威胁情报产品，以及产品落地情况。

### 中国威胁情报厂商能力特点

厂商名称	能力特点
微步在线	<b>多样化数据来源：</b> 除通过威胁情报社区、云沙箱、蜜罐等平台获取安全数据及威胁信息，更多以安全产品检测及自研高质量商业情报为主 <b>情报准确度：</b> 情报准确度高，独有的情报生产和品控机制，百万级别的失陷检测情报，能大幅降低企业告警噪音 <b>情报深度与全面性：</b> 具备威胁情报生产与共享的闭环能力，融合高风险漏洞情报、态势情报，全面的情报能力，为企业安全运营赋能
奇安信	<b>B端服务经验：</b> 长期服务于政府机构、央企以及大型集团，具备丰富的安全服务经验，同时积累高质量的威胁情报数据，也可以捕捉一些针对B端企业的更为刁钻的攻击手法 <b>产品覆盖范围：</b> 具备全域产品设计能力，已将威胁情报与自身的包括XDR、SOAR、SOC等安全产品融合，提升产品能力
360安全	<b>C端安全软件：</b> 360安全卫士装机量达数亿，通过此类安全终端广泛地获取C端安全数据（包括病毒、DNS反向链接等） <b>云沙箱部署：</b> 360云沙箱对社会开放，可免费使用。由于360安全装机量较大，因此攻击者更多选择在其沙箱内做病毒免杀测试，因此厂商可以最快时间发现新型攻击
腾讯安全	<b>C端互联网软件/APP：</b> 基于自身互联网业务，对于旗下的强隐私性软件/APP（如交易、支付、社交等）配置安全组件，维护用户数据安全；同时在C端获取网络安全信息（非用户个人隐私），形成自身威胁信息的基础数据 <b>云基础设施：</b> 自身公有云服务为腾讯积累了服务不同业务类型B端用户的安全经验
绿盟科技	<b>纯安全理论与技术：</b> 老牌综合安全服务厂商，威胁情报的理论研究较强，威胁情报主要作为其他类安全产品的能力模块存在
中小安全厂商	<b>体量及数量：</b> 据不完全统计，我国现有中小型情报厂商数十家，年收入区间处在数百万至千万水平 <b>区域属性：</b> 多数小型威胁情报厂商属于地方性质，情报信息比较单一，且专供于某些机构/客户使用

来源：结合专家访谈、公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 中国威胁情报产业图谱



注释：

1. 由于威胁情报特有的行业特点，以上图谱中多数厂商的主营业务并非威胁情报，但他们均具备威胁情报能力，并将威胁情报单独或与其他安全类产品融合后对外提供服务，因此我们将具备此类特征的厂商纳入到图谱中。
2. 多数威胁情报厂商自身具备基础数据获取能力，因此上游情报数据供应商并不必要；但为了提升情报覆盖度与准确性，威胁情报厂商选择情报数据供应商合作，特别是海外数据供应商，以拓宽数据收集范围。

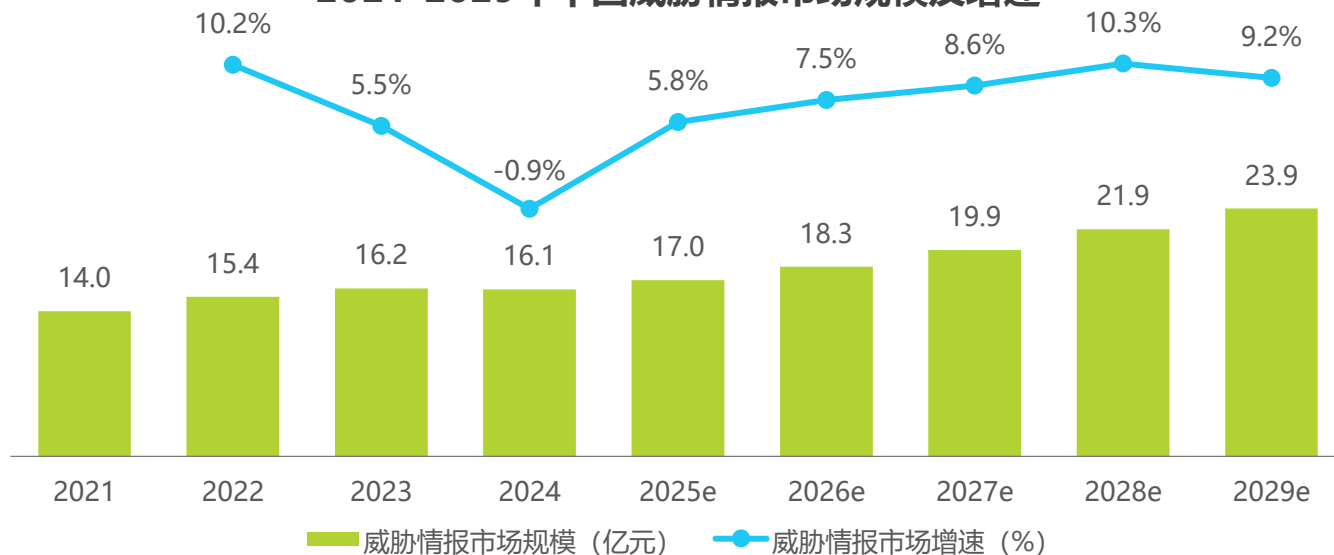
来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 中国威胁情报市场规模

## 受疫情影响市场规模短期下跌，安全需求及产品融合推动行业长期增长

2020年疫情爆发后，宏观经济不确定性增加，各行业均在努力削减成本，而网络安全项目实施周期较长，往往容易被客户率先搁置，受此影响，我国威胁情报市场规模增速有所下降，从2022年底疫情防控结束至2024年底的2年时间，网络安全行业重在“清库存”，后疫情时期的影响短期内限制了行业的进一步增长，2024年中国威胁情报市场规模达到16.1亿元，较23年小幅下跌0.9个百分点。未来，在宏观层面，随着疫情的影响逐渐淡去，国家为促进经济增长于2024年下半年采取了一系列积极的宏观调控动作，同时地缘政治的不确定因素仍然存在，加之国家对网安的重视程度日益增长，推动网安攻防演练常态化，鼓励企业加大以“威胁情报”为代表的实战化能力建设投入。在微观层面，从需求端看，生成式人工智能显著降低攻击门槛，新的攻击工具及新型攻击手法日益增多，勒索软件攻击日益猖獗，需要企业依靠最新威胁情报来增强自身检测防护能力，对威胁情报类安全产品的需求预计将有所增强；从供给端看，威胁情报与其它各类安全产品的融合持续加深，作为网络安全高阶能力，已实现在网、端、综合防护等各类安全模块中的部署。因此，在供需两端的共同推动下，我们预计未来行业将进入稳步发展期。

### 2021-2029年中国威胁情报市场规模及增速



注释：如同本报告对于威胁情报的定义，市场规模可拆分为两部分，一部分是以提供API、TIP、情报查询账号等情报分析、生产与情报管理为主的纯威胁情报服务规模，另一部分则是融入进其他安全产品中的威胁情报服务规模（通常占该安全产品总收入的一定比例），报告对这两部分分别统计并加总后绘制本图。

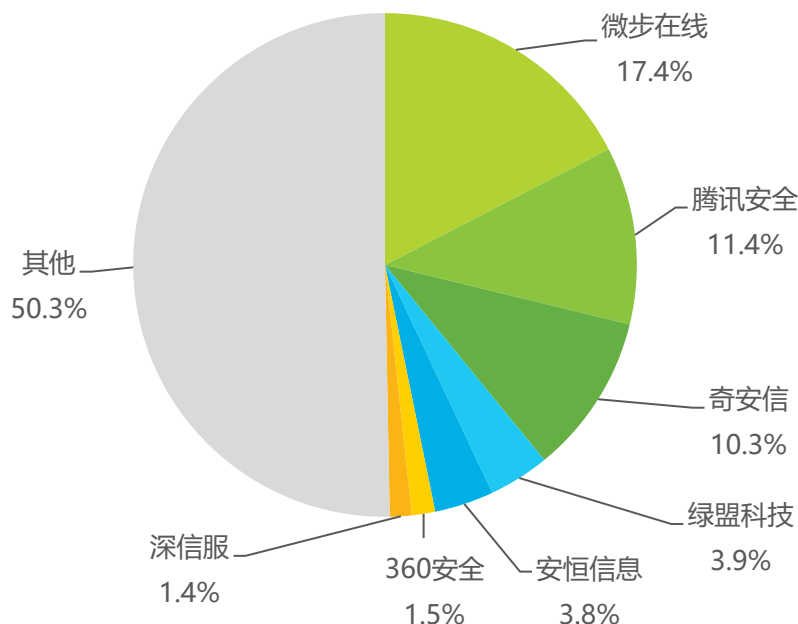
来源：结合专家访谈、公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 中国威胁情报行业市场份额

头部厂商已积累一定行业优势，积极的竞争与创新是未来行业的主基调

目前，中国威胁情报属于低集中寡占型市场（CR4=43.0%，CR7=49.7%）。一方面，微步在线、腾讯安全、奇安信等行业领导厂商基于自身差异化能力，积极丰富产品矩阵，覆盖更广泛的需求场景，不断夯实企业竞争力，在行业中已形成一定优势。另一方面，以AI大模型、大数据开源组件为代表的新技术被持续融入威胁情报中；同时各厂商仍在探索情报能力与其他安全产品的融合方式与商业捆绑模式，因此以发展的视角看，积极的竞争与创新将成为行业的主基调。

2024年中国威胁情报市场份额



注释：如同本报告对于威胁情报的定义，各厂商的市场份额可拆分为两部分，一部分是以提供API、TIP、情报查询账号等情报分析、生产与情报管理为主的纯威胁情报服务，另一部分则是融入进其他安全产品中的威胁情报服务（通常占该安全产品总收入的一定比例），报告对这两部分分别统计并加总后绘制本图。

来源：结合专家访谈、公开资料整理，艾瑞咨询研究院自主研究及绘制。

03/

# 中国威胁情报 行业案例

# 微步在线 (1/2) 情报产品

累积海量高质情报，专注于精准、高效、智能的网络威胁发现和响应

微步成立于2015年，专注于精准、高效、智能的网络威胁发现和响应，开创并引领中国威胁情报行业的发展，打造了精准的威胁情报、高质量的漏洞情报、实时感知的态势情报为核心的下一代威胁情报，业务遍布国内外企业，在主流行业头部企业覆盖率超过90%。基于威胁情报TI及AI大模型分析能力，微步在线形成了包括安全情报、端点安全、流量安全、边界安全、云上安全、安全服务和安全工具的完整产品和服务矩阵。

## 微步在线威胁情报产品矩阵





# 微步在线 (2/2) 情报解决方案 微步在线® 艾 瑞 咨 询

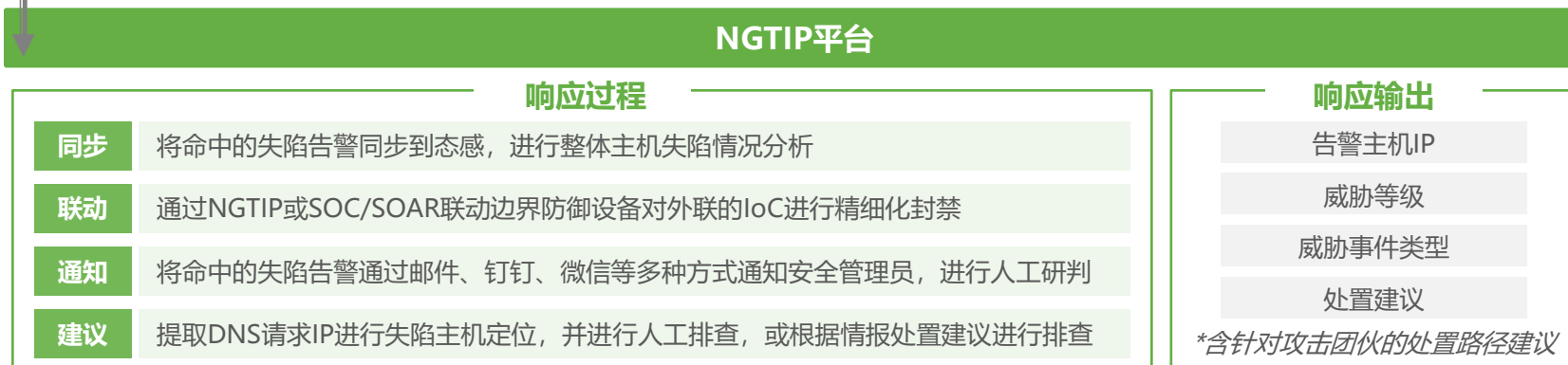
## NGTIP基于日志和IOC情报进行失陷检测，实现检测、分析、处置闭环

在网络安全领域，黑客常通过DNS隧道侵入企业内部，使传统边界安全设备失效，迫使企业陷入被动防御的窘境。针对这一问题，微步在线的下一代威胁情报平台NGTIP通过对比收集到的多源日志（尤其是DNS日志）与平台内置的高质量情报库，实现对远控、挖矿、恶意软件等多类威胁的及时检测，将企业的防御关口提前。除了检测功能外，微步在线的下一代威胁情报平台NGTIP还能与SOC等安全产品协同，实施精确的防护措施，并通过多种渠道向安全管理人员通报威胁事件信息，提出处理建议，形成安全防护的闭环，助力企业有效应对网络安全挑战。

### 步骤① <检测> 微步在线失陷主机检测与自动化响应场景解决方案



### 步骤② <响应>



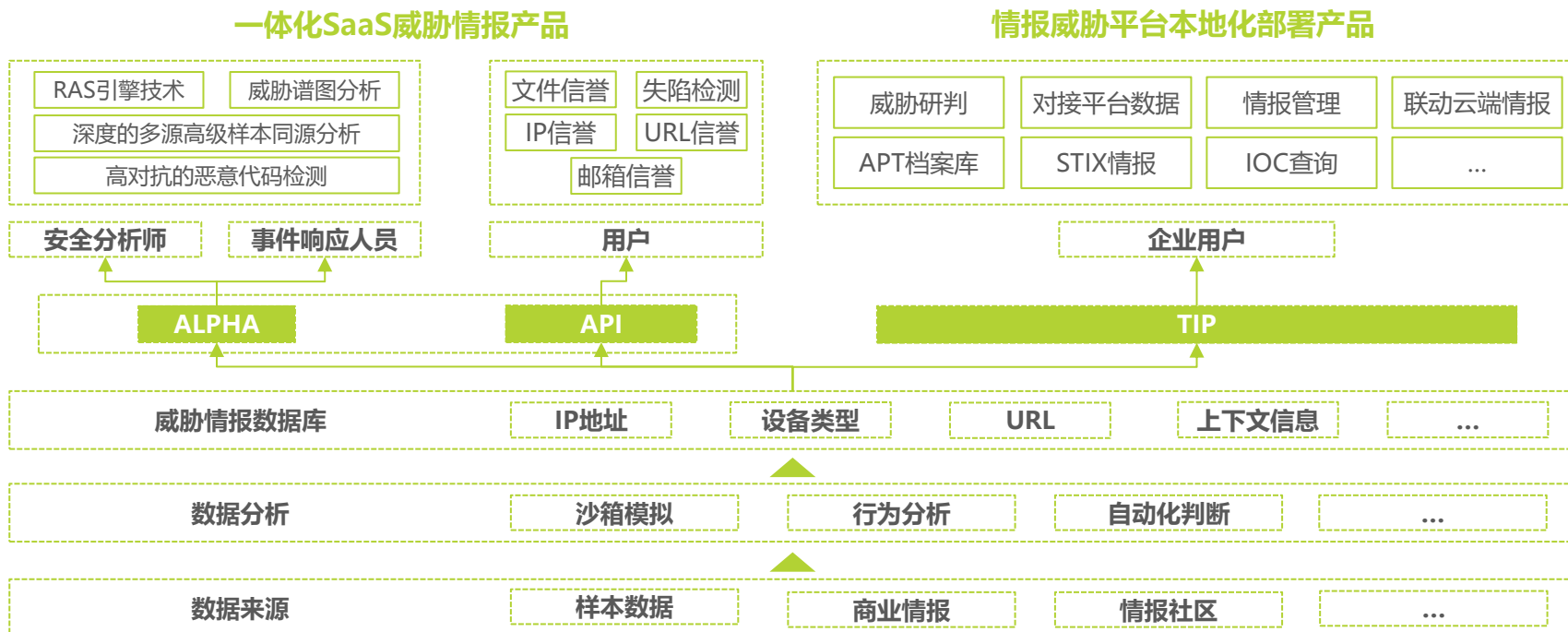
来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 奇安信（1/2）情报产品

## 依靠多源威胁情报，提供一体化SaaS+本地化的威胁情报追踪产品矩阵

奇安信在威胁情报产品领域为客户提供一体化SaaS威胁情报产品（API）及本地化部署服务（TIP）。ALPHA威胁分析平台是面向安全分析师、事件响应人员的综合性威胁情报分析平台，以海量多维度网络空间安全数据为基础，实现报警研判、攻击定性、黑客画像以及威胁持续跟踪；API提供面向客户的接口查询服务，能够提供文件信誉、失陷检测、IP信誉、URL信誉和邮箱信誉等情报。TIP则能够帮助企业本地化部署，实现情报落地，帮助企业高效地利用情报发现威胁，增强自身的安全防护能力。

### 奇安信威胁情报产品



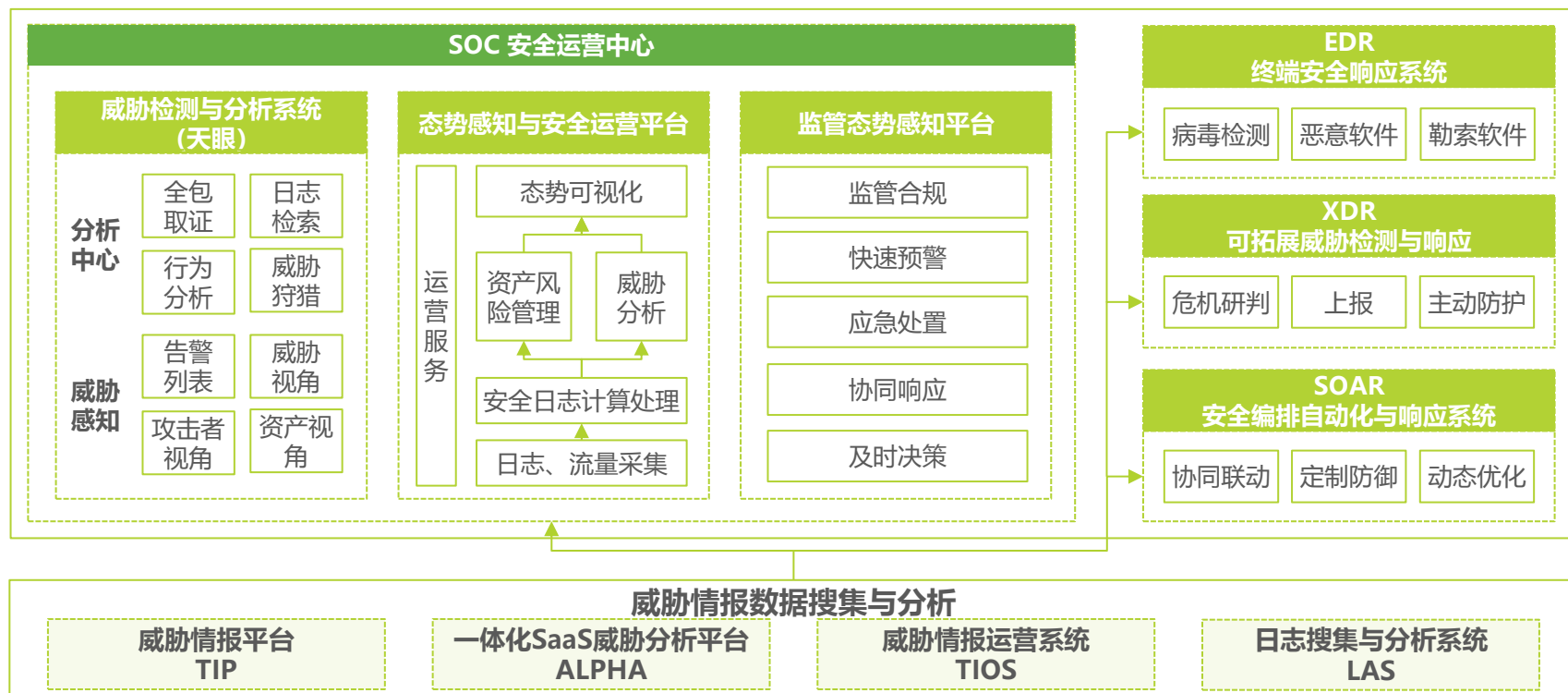
来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 奇安信（2/2）情报解决方案

## 基于ALPHA平台能力，威胁情报赋能奇安信六大主要应用产品

基于领先的情报威胁数据收集与分析能力，奇安信推出了一系列威胁情报应用产品，包含SOC、EDR、XDR、SOAR四类主要产品，SOC类产品包括聚焦攻防渗透和数据分析的威胁检测与分析系统（天眼）、更多分析维度和数据基础的态势感知与安全运营平台（NGSOC）及专为政府监管打造的监管态势感知平台；终端安全响应系统（EDR）能够基于威胁情报检测终端病毒、恶意软件和勒索软件，威胁检测率显著提高；XDR扮演平台中枢的角色，进行危机研判、自动上报和主动向防火墙推送策略达到防护阻断功能；SOAR根据威胁情报自动生成安全策略，形成可灵活调整的定制化防御方案。

### 奇安信威胁情报解决方案



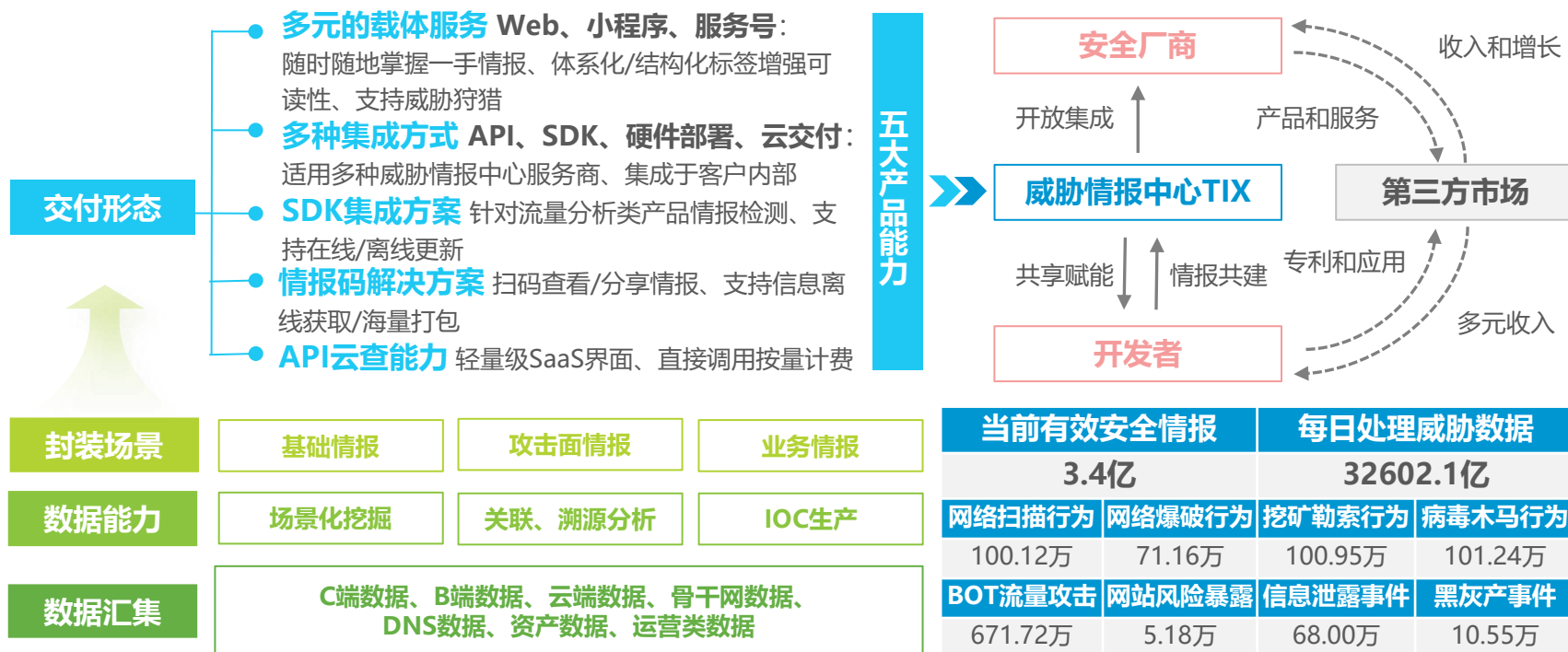
来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 腾讯安全（1/2）情报产品

## 腾讯安全威胁情报中心，以五大产品能力助力政企提升数字安全免疫力

腾讯安全专注AI、威胁情报、攻防对抗三大原子能力，聚焦数据安全治理、业务风险控制、安全运营管理、边界安全、端点安全、应用开发安全六大领域，助力政府及企业的数据、系统、业务安全。其中，腾讯威胁情报中心（TIX）依托腾讯安全二十余年网络安全实战经验和大数据智能分析能力，以多元的载体服务、多种集成方式、API云端查询服务、情报码解决方案、SDK集成方案五大产品能力，打造覆盖业务情报、攻击面情报和基础情报的威胁情报大数据平台，助力企业低成本获得全面情报能力，并全面提高产品预警和回应速度。目前TIX已覆盖金融、互联网、高科技企业、政府运营商、安全生态厂商等各行业用户。

### 腾讯安全威胁情报中心产品功能及生态圈



注释：TIX情报数据来源TIX官网，截至2024年12月。

来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 腾讯安全（2/2）情报解决方案



腾讯安全  
Tencent Security

iResearch  
艾瑞咨询

## 基于TIX威胁情报能力，构建攻击面管理服务，帮助客户全面监测风险

攻击面管理是一款致力于解决用户互联网风险监测难题的SaaS化订阅服务产品，基于腾讯威胁情报能力，提供面向政企用户的互联网资产漏洞风险、内容风险与信息泄露风险等维度的监测服务，同时基于企业多维度信息关联测绘，实时监测互联网暴露面，发现暴露资产、端口、服务与潜在风险。

### 腾讯威胁情报解决方案——攻击面管理

#### 腾讯安全威胁情报中心攻击面管理7大应用场景

- |   |               |   |
|---|---------------|---|
| 1 | 行业安全监管        | 挂图作战，适用于测绘、监测、专项、指挥，提供全局、单机构、风险事件、资产视角，了解机构风险详情趋势   |
| 2 | 企业安全监测        | 多维度数据融合分析关联呈现，主动情报+被动测绘持续感知并测绘资产，SaaS+人工运营，7×24监测处置 |
| 3 | 重点时期监测服务      | 提供重点时期的安全专家服务，包括但不限于渗透测试、安全巡检、安全加固、威胁溯源等            |
| 4 | 发现高危风险资产和服务   | 基于高危漏洞、敏感端口、弱密码入口等维度，预警用户高风险互联网暴露面                  |
| 5 | 识别未纳管关联资产和服务  | 监测影子资产，识别用户违规上线，脱离管控资产以及相关假冒服务（网站、IP、App、小程序等）      |
| 6 | 追踪外网信息泄露事件    | 定位用户出现的员工信息外泄，客户信息售卖，源代码泄露、企业敏感文档传播等信息源             |
| 7 | 监测内容合规性和服务健康度 | 发现业务发布敏感信息，满足合规要求；实时监测核心网站资产与服务状态，识别对外服务异常          |



#### 腾讯安全威胁情报中心攻击面管理6大产品功能

资产威胁面

社工入侵面

信息合规面

机构管理

资产管理

报告中心



#### 腾讯安全威胁情报经验储备及核心技术

7大安全实验室、100+位安全专家、多名顶尖白帽黑客、日均处理**万亿**源数据、**20+**年攻防经验

##### 云端安全大数据

沉淀海量云业务防护经验  
捕获最新威胁情报大数据

##### 测绘技术

网络空间测绘、无感知半连接技术  
丰富的指纹库、DNS数据发现技术

##### 智能分析流程

##### 算法算力平台

##### Web2.0威胁检测引擎

##### 深度机器学习

来源：结合公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 天际友盟（1/2）情报产品



## 以威胁情报技术研究能力为支撑为客户提供多种安全防护产品

天际友盟于2015年成立后，创建烽火台安全威胁情报联盟，并陆续发布RedQueen威胁情报中心、SIC威胁情报平台、TIG威胁情报网关等产品，致力于为客户提供全生命周期的数字风险防护。目前，天际友盟在北京、上海、深圳、广州、珠海、江苏、西安、沈阳、长春、哈尔滨、长沙、石家庄、太原、香港、澳门等多地设有分支机构，并在2024年于新加坡设立了东南亚业务中心，开展亚太市场。

### 天际友盟威胁情报产品

#### 威胁情报中心-RedQueen

##### RedQueen产品内容

###### 情报订阅服务

威胁情报

事件情报

漏洞情报

资产情报

基础信息

...

多种类型情报均可通过**标准API接口**实现情报数据的下载

###### 溯源查询能力

为使用者提供基于域名、URL、IP、哈希值、Email、字符串等威胁信息的溯源分析查询，协助企业用户强化其对安全事件的快速扩展分析能力和多重溯源能力

#### 威胁情报平台-SIC

##### SIC产品定位与优势

便捷第三方情报接入，建立私有情报能力

精细化情报管理应用，提升检测防护效能

构建多样情报运营体系，打造智能安全运营

#### 威胁情报网关-TIG

与天际友盟威胁情报中心RedQueen、天际友盟威胁情报平台SIC等天际友盟全系列威胁情报产品**协同联动**，实现对威胁的**及早发现、及时阻断及全网预警**，并可对告警中的威胁指示器进行有效**溯源分析**

内网失限  
主机发现

内部挖矿  
主机发现

风险访问  
行为发现

##### RedQueen情报数据全景概览



注释：指标数据来源于官网，统计时间截至2024年12月。  
来源：公开资料整理，艾瑞咨询研究院自主研究及绘制。



# 天际友盟 (2/2) 情报解决方案



## 持续自动监测数字风险，保障用户与企业品牌每一步互动的安全

为保护企业品牌价值，天际友盟发布DRP数字风险防护服务。DRP通过调用威胁情报平台等能力，持续自动监测互联网存量数据和流量数据，及时发现存在的钓鱼欺诈、非法使用品牌标识等行为，并针对威胁行为采取下线措施，实现对网络欺诈和品牌滥用的打击，协助企业保护数字时代品牌价值。

### 天际友盟一站式DRP数字风险防护服务

#### DRP数字风险应用场景

网站钓鱼欺诈	山寨仿冒APP	社交媒体与VIP防冒	钓鱼邮件欺诈	搜索引擎恶意排名	威胁误报
数据泄露	代码泄露	知识产权保护	相似域名风险	历史域名滥用	暗网威胁

#### DRP数字风险服务

##### 监控服务

监控覆盖范围

 Web服务	 应用商店
 代码站点	 社交媒体
 知识社区	 深网暗网

##### 持续监控

对客户的品牌或资产对象，在互联网上进行连续监控

##### 实时预警

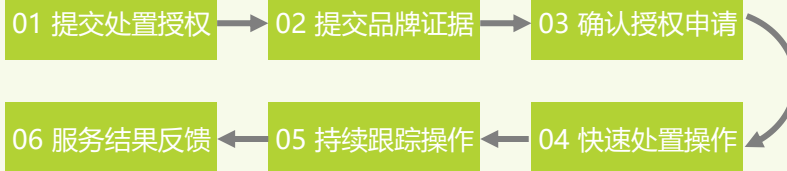
对发现的品牌事件，通过短信、邮件、电话预警

##### 分析报告

风险分析、处置结果汇总等自动化能力和人工报告

##### 处置服务

通过与覆盖全球的VPS提供商、域名注册商、网络提供商及各国CERT、应用商店、社交媒体、代码托管、内容分享平台等各类管理机构的通力合作，可对已确认的风险处置目标进行全球快速处置



04/

# 中国威胁情报 行业趋势洞悉

# 洞悉一：威胁情报+企业出海

## 情报企业正积极探索出海业务，情报标准与数据安全成为两大焦点

【威胁情报标准】我国于2018年推出《信息安全技术网络安全威胁信息格式规范》，以推动技术发展与产业化应用。该规范虽然以国际标准为重要参考依据，但在国际通用与兼容性、技术细节与深度、情报共享与协作效率以及对新技术和新威胁的适应性方面与国际规范尚有差距；未来随着行业标准的完善并进一步与国际靠拢，我国威胁情报企业出海路径将更加通畅。

【数据安全合规】数据是威胁情报行业的重要基础资源，各个国家及地区对于本地数据的保护要求纷繁复杂。对各国当地法律法规的了解与遵守是威胁情报出海的重点和难点。我们看到，一些中国情报厂商已经在探索海外数据合法合规的使用方式，包括但不限于设立海外实体、处理敏感信息以及建立共享协议。

### 中国威胁情报出海焦点：情报标准与数据安全



来源：结合专家访谈、公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 洞悉二：威胁情报+大模型

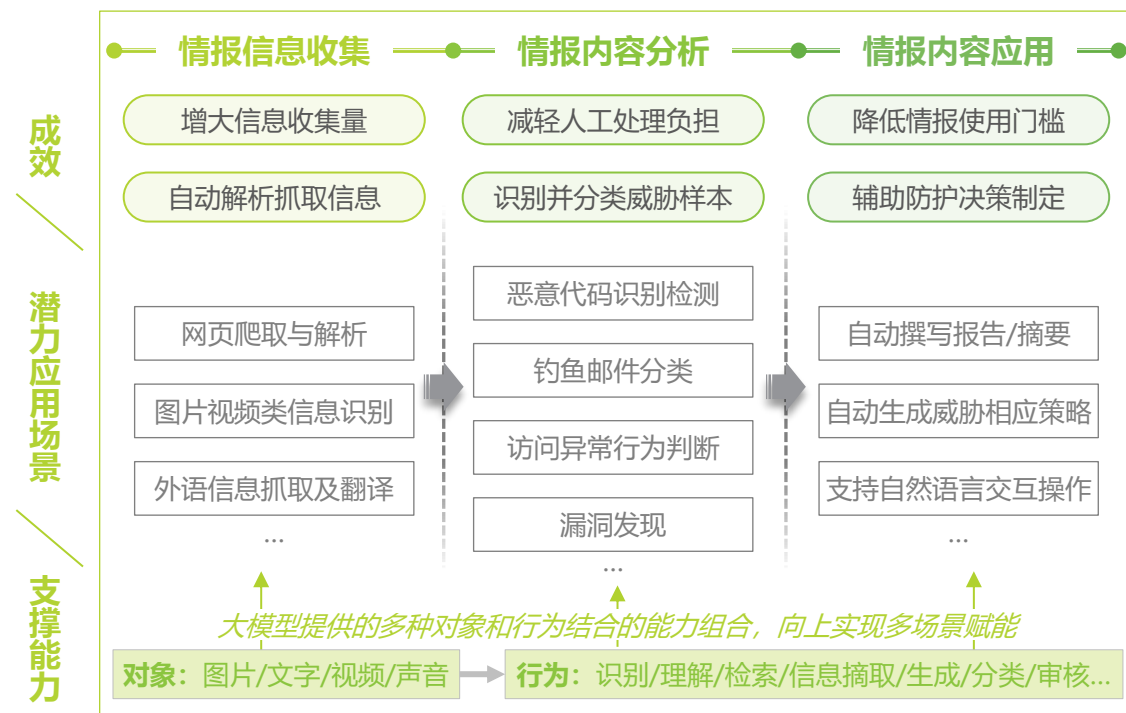
## 大模型时代的AI能力将支撑威胁情报实现更高效的运营和更广泛的应用

大模型出现后，人工智能在自然语言处理、知识学习与整合、泛化和迁移学习方面的能力实现了跃升。对于威胁情报行业，大模型在威胁情报生产与运营的多个环节均有赋能，提升专业人员产出威胁情报的效率、降低威胁情报的应用门槛、支撑其面向更多场景，赋能更多岗位的人员。目前，多数大模型赋能威胁情报的应用场景还在概念验证的阶段，未来，企业可以在例如大模型行业适配、大模型落地效率、性能优化、合规应用等多个角度发力，实现大模型在新应用场景的快速落地，提升自身竞争力。

### 大模型在威胁情报处理中的关键应用与赋能

#### 大模型的应用将进一步提升威胁情报的获取和应用效率

#### 大模型赋能威胁情报的关键着力点



#### 增强大模型的行业适配效能

高质量情报数据源训练

检索增强生成

多模型集成

...

#### 提升大模型落地效率与实践性能

借助MaaS减轻底层资源配置成本

针对自研大模型进行算法优化

...

#### 规避大模型“幻觉”风险

优化数据质量把控与模型验证机制

增强人工审核流程与员工风险意识

...

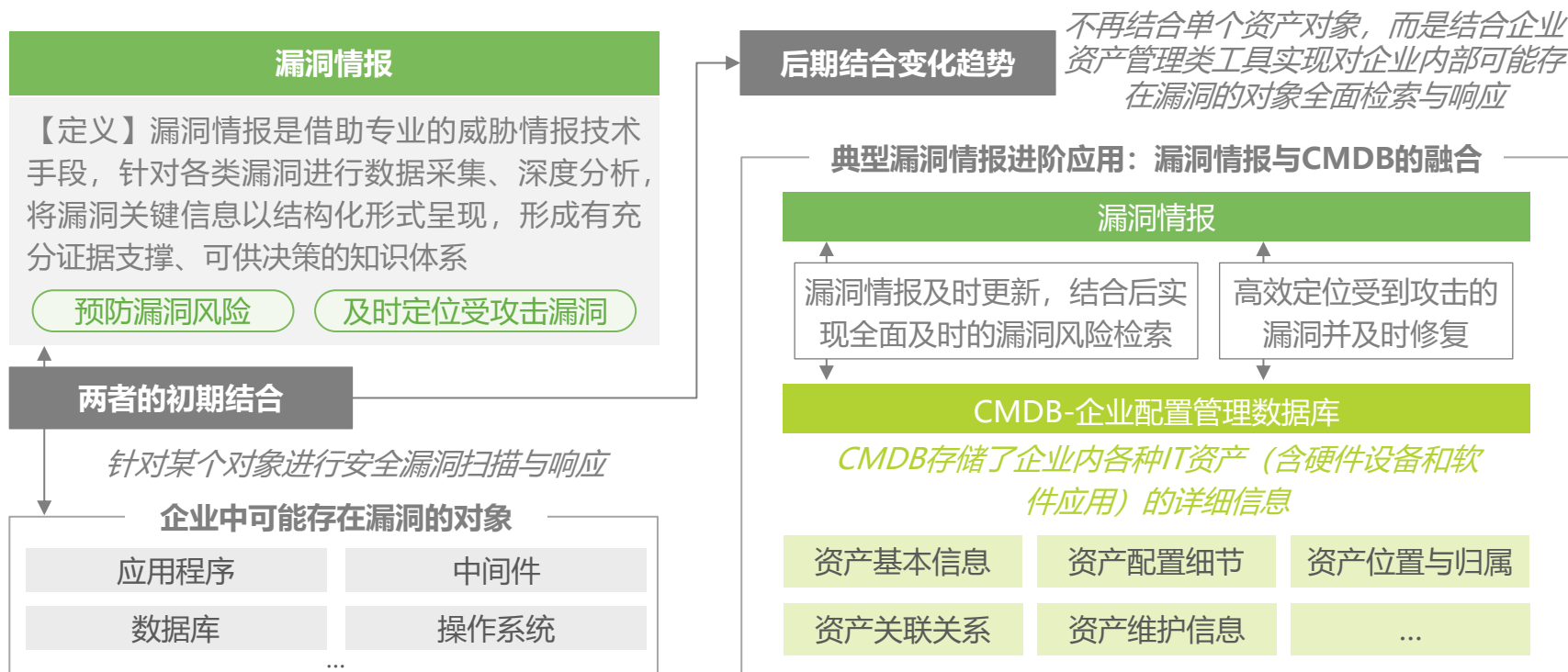
来源：结合专家访谈、公开资料整理，艾瑞咨询研究院自主研究及绘制。

# 洞悉三：漏洞情报价值日益凸显

## 漏洞情报与企业资产不断加深融合，以提升防护主动性与御损能力

目前，漏洞成为攻击者的重点利用方向，公开报告显示，2023年攻击者利用漏洞作为入侵初始步骤的情况增长180%，对企业带来较大危害。因而，结合威胁情报技术，以漏洞为主要防护对象的漏洞情报对企业安全防护的发展更具意义。如今，漏洞情报与企业资产结合紧密度不断上升。企业面临越来越多的资产存在漏洞，需具备的漏洞管理能力要求也越来越高，通过漏洞情报全面及时掌握最新漏洞信息，打通内部资产平台第一时间发现漏洞，并建立科学漏洞评估模型优先处置真正的高危漏洞对于企业变得尤为重要。

### 漏洞情报与企业资产结合紧密度提升



来源：结合专家访谈、公开资料整理，艾瑞咨询研究院自主研究及绘制。

BUSINESS  
COOPERATION

# 业务合作

联系我们



400 - 026 - 2099



ask@iresearch.com.cn



www.idigital.com.cn

www.iresearch.com.cn

官 网



微 信 公 众 号



新 浪 微 博



企 业 微 信





## LEGAL STATEMENT

# 法律声明

### 版权声明

本报告为艾瑞数智旗下品牌艾瑞咨询制作，其版权归属艾瑞咨询，没有经过艾瑞咨询的书面许可，任何组织和个人不得以任何形式复制、传播或输出中华人民共和国境外。任何未经授权使用本报告的相关商业行为都将违反《中华人民共和国著作权法》和其他法律法规以及有关国际公约的规定。

### 免责条款

本报告中行业数据及相关市场预测主要为公司研究员采用桌面研究、行业访谈、市场调查及其他研究方法，部分文字和数据采集于公开信息，并且结合艾瑞监测产品数据，通过艾瑞统计预测模型估算获得；企业数据主要为访谈获得，艾瑞咨询对该等信息的准确性、完整性或可靠性作尽最大努力的追求，但不作任何保证。在任何情况下，本报告中的信息或所表述的观点均不构成任何建议。

本报告中发布的调研数据采用样本调研方法，其数据结果受到样本的影响。由于调研方法及样本的限制，调查资料收集范围的限制，该数据仅代表调研时间和人群的基本状况，仅服务于当前的调研目的，为市场和客户提供基本参考。受研究方法和数据获取资源的限制，本报告只提供给用户作为市场参考资料，本公司对该报告的数据和观点不承担法律责任。



# THANKS

艾瑞咨询为商业决策赋能