2023中国网络安全市场

攻击面管理产品用户调研报告

安在 ANZER

数说安全 CYBERSECURITY REVIEWS

2023年3月

2023年3月

前 言

“攻击面管理”是2022年中国网络安全产业热度上升比较快的词，过去从事网络资产管理与网络空间测绘、漏洞扫描与漏洞管理、威胁情报、自动渗透测试工具产品研发的公司纷纷推出自己的攻击面管理产品，或给自己打上“攻击面管理”的标签，攻击面管理市场热度快速上升。

面对供给端呈现起步即爆发的势头，需求端如何看待和理解攻击面管理技术？产品在用户防线中的定位是什么？用户对产品的满意度如何？用户对产品未来的预期是什么？为此，安在新媒体与数说安全联合开展了2023中国网络安全市场攻击面管理产品用户调研活动，力争从甲方用户角度出发，更全面、深入的分析攻击面管理市场现状与未来发展，为产业从业者提供借鉴与参考。

CONTENTS 目录

CONTENTS 目录

攻击面管理产品用户实际使用情况

攻击面管理产品用户未来投入计划

攻击面管理市场概述

攻击面管理的起源

2018 年，Gartner 敦促安全领导者开始减少、监控和管理他们的攻击面，作为整体网络安全风险管理计划的一部分，并且在2021年发布的《Hyper Cycle for Security Operations，2021》中将攻击面管理（ASM，Attack Surface Management)相关技术定义为新兴技术，这被大家公认为是“攻击面管理”这个名词做为一种网络安全产品类别的起源。

攻击面是什么?

美国国家标准与技术研究院（NIST）对攻击面的定义是：“位于系统、系统组件或环境的边界上的一组入口，攻击者可以从这些入口尝试进入、产生影响或从中提取数据。”（The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.）。

攻击面管理是什么?

不同机构对攻击面管理的定义略有区别，但大同小异。

IBM：攻击面管理（ASM）是对构成组织攻击面的网络安全漏洞和潜在攻击向量的持续发现、分析、修复和监控。

Michael Cobb：攻击面管理是对组织的 IT 基础设施的持续发现、清点、分类和监控。

Cycongnito：攻击面管理是发现、分类和评估组织所有资产安全性的持续过程。

CrowdStrike：攻击面管理是对组织 IT 基础架构内的攻击媒介进行持续发现、监控、评估、优先排序和补救。

Mandiant：在当今的动态、分布式和共享环境中发现和分析互联网资产，持续监控已发现资产的风险敞口，并使情报和红队能够实施风险管理并为风险管理提供信息。

Palo Alto Networks：攻击面管理（ASM）是持续识别、监控和管理所有内部和外部互联网连接资产以发现潜在攻击向量、暴露和风险的过程。

国内的赛迪顾问在《中国攻击面管理市场研究报告，2022》中将攻击面管理定义为：攻击面管理是一种从攻击者的角度对企业数字资产攻击面进行检测发现、分析研判、情报预警、响应处置和持续监控的资产安全性管理方法。

数说安全综合以上各方的定义，结合对攻击面管理工作的要点，对攻击面管理的定义为：**攻击面管理（ASM）是持续发现、分析、监控和评估内部和外部所有资产以发现潜在暴露面、攻击向量和风险，并进行优先排序、响应处置的过程。**

攻击面管理解决的主要问题是什么？

- 帮助防御者发现自己的盲区：由于思维方式和所拥有的技术技能的不同，攻击者与防御者往往会存在视角上的重大不同，人不可能对自己认知范围之外的事情做出有效应对，引入攻击者视角，将会很大程度上帮助防御者发现自己所忽略的，或视野之外的安全威胁。

- 帮助防御者合理排定工作的优先级：防御者的工作是纷繁复杂的，所拥有的资源也是有限的，需要对防御工作进行优先级排定、做出取舍与折衷，攻击者视角可以帮助防御者有针对性的防御，提高资源利用效率。

关键发现

关键发现

- 漏洞扫描、漏洞与补丁管理、网络资产管理仍是作为目前企业发现与管理自身攻击面的最主要产品，采购专业CAASM和EASM产品的用户比例仅为11%和15%，市场渗透率远低于传统安全产品。

- 不同于传统安全产品以合规导向为主，攻击面管理产品由技术与合规双轮驱动，现有能力无法持续监测攻击面的变化、符合监管或审计要求是目前企业实施攻击面管理的两大最主要因素。

- 超过50%以上的企业认为IT资产管理和未知资产发现上存在不足，而认为满意的企业比例仅为15%和11%，良好的资产发现与管理仍是企业目前亟待解决的核心问题。

- 办公网、数据中心、公有云、私有云是企业IT资产分布最主要的区域，并且有60%的企业认为目前攻击面扩大的首要原因是将数据和资产转移到云端，因此，未来云上资产识别与管理将成为企业IT风险管理中新的关注重点。

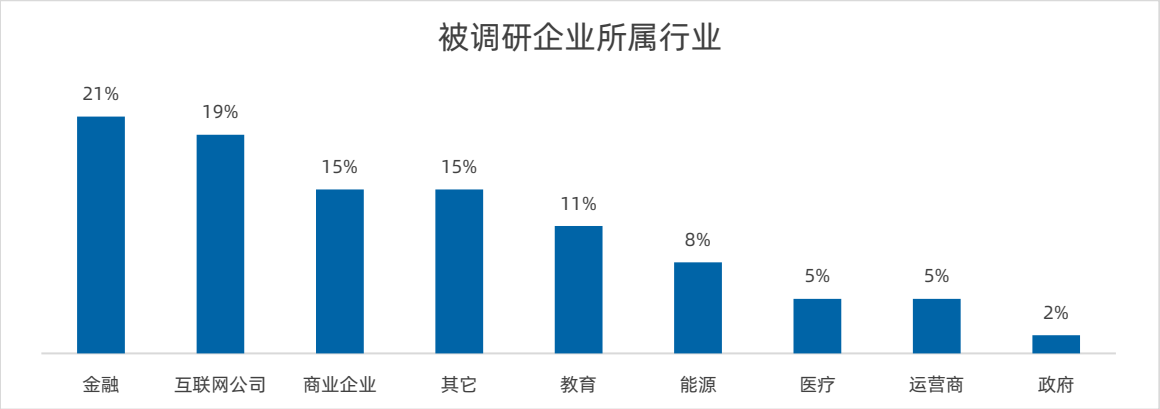
- 全面的资产可见性与动态管理、漏洞发现与优先级管理，这两项能力，既是产品功能层面用户最关注的两个主要特性，也是用户认为现有产品最主要的两个不足。

- 对于攻击面管理产品来说，94%的企业选择将预算投入控制在百万以内，而在这部分企业中，有70%认为预算将不超过五十万。

被调研企业背景情况

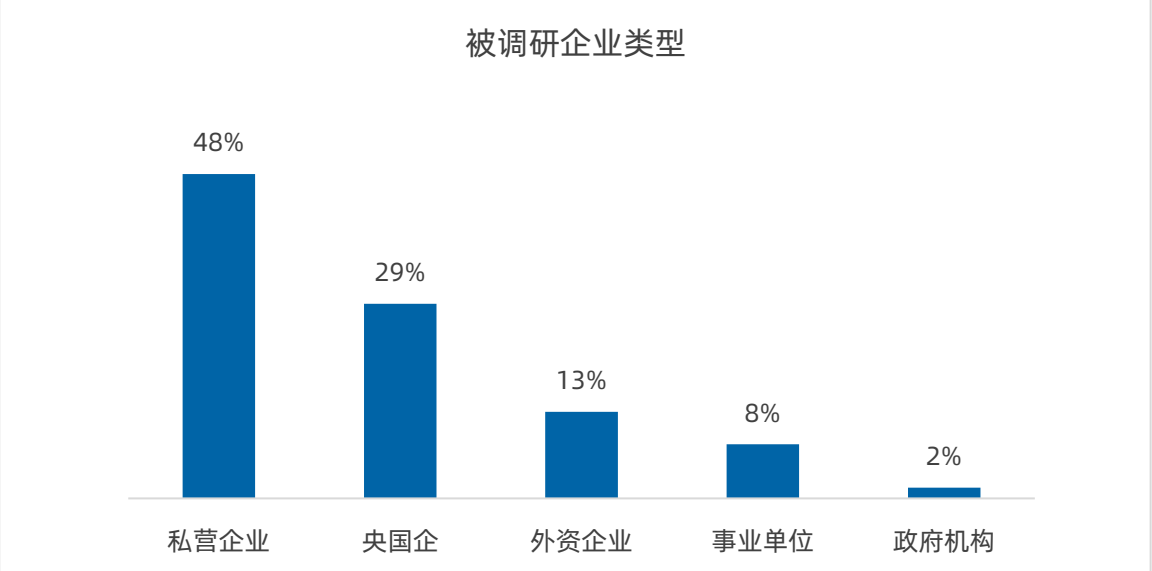
企业所属行业

企业所属TOP3行业分别是：金融、互联网公司、商业企业与其它。



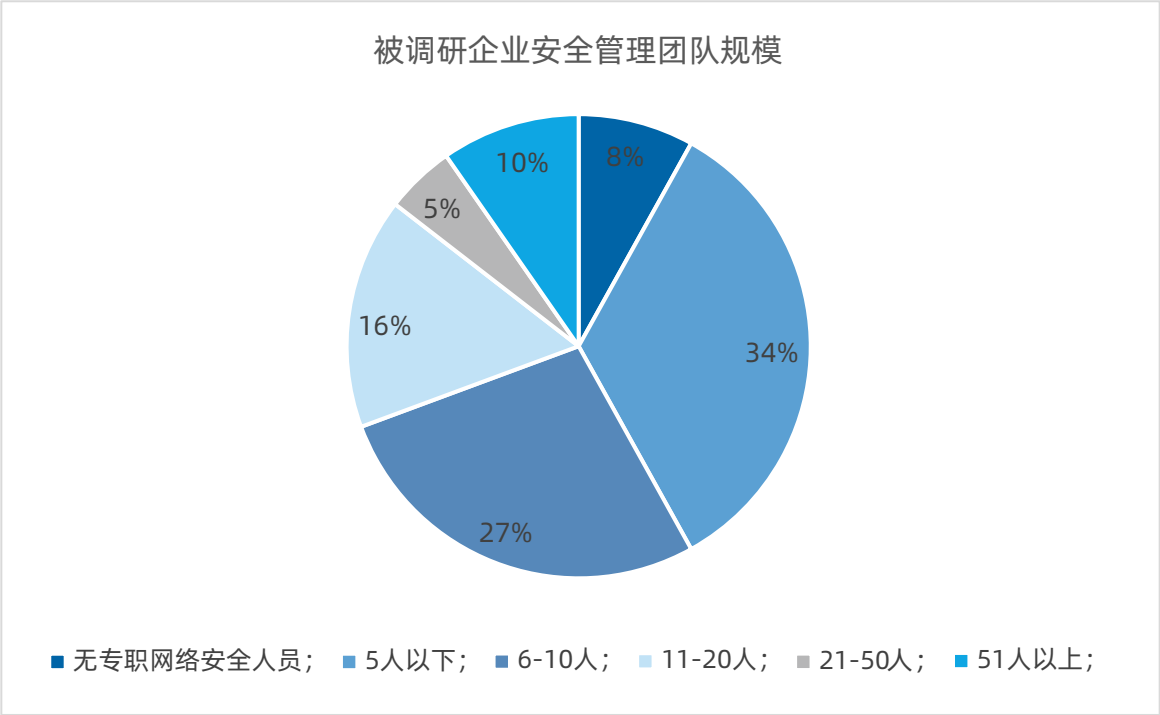
企业类型

企业TOP3类型分别是：私营企业、央国企、外资企业。



企业安全管理团队规模

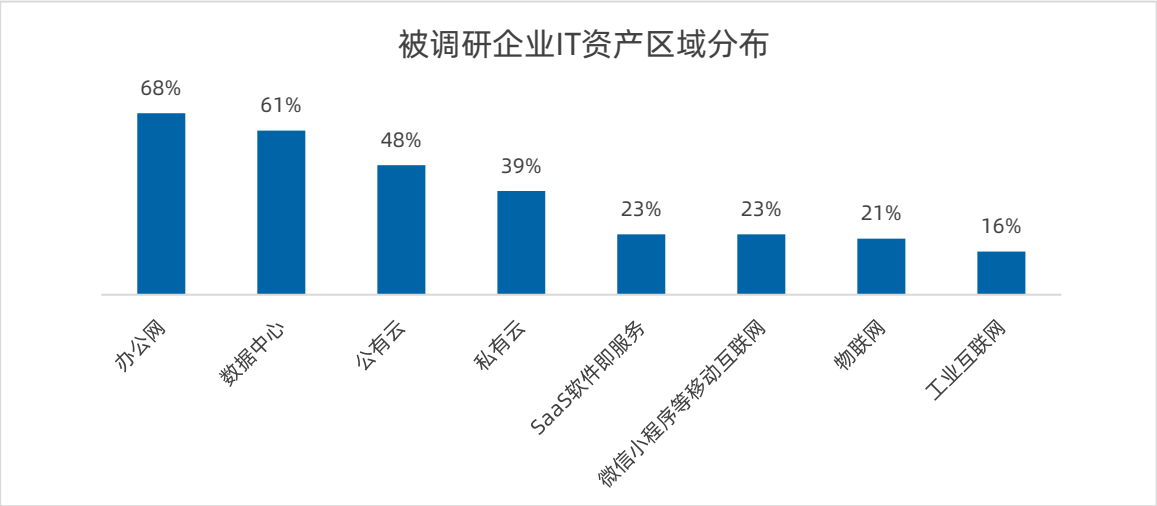
企业安全管理团队TOP3规模分别是：5人以下、6-10人、11-20人，另外有8%的企业无专职网络安全人员。



企业自身IT与网络安全现状

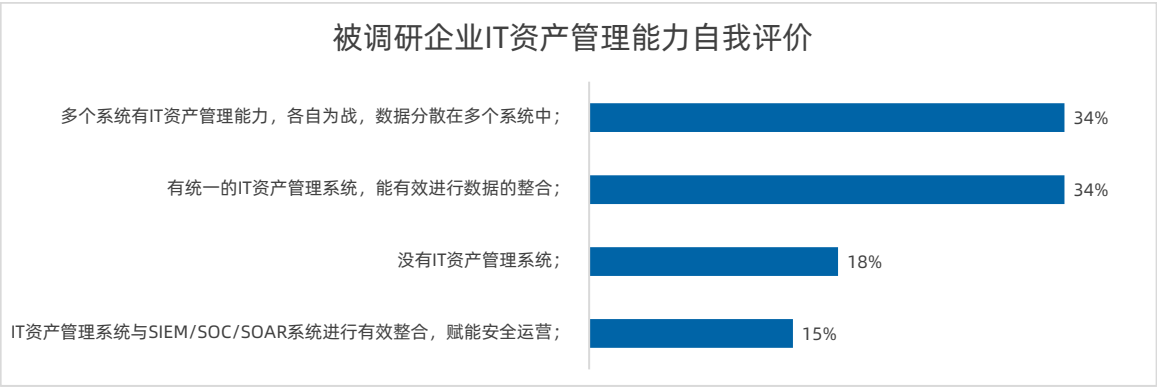
企业IT资产分布

企业IT资产分布最多的3个区域分别是：办公网、数据中心、公有云。



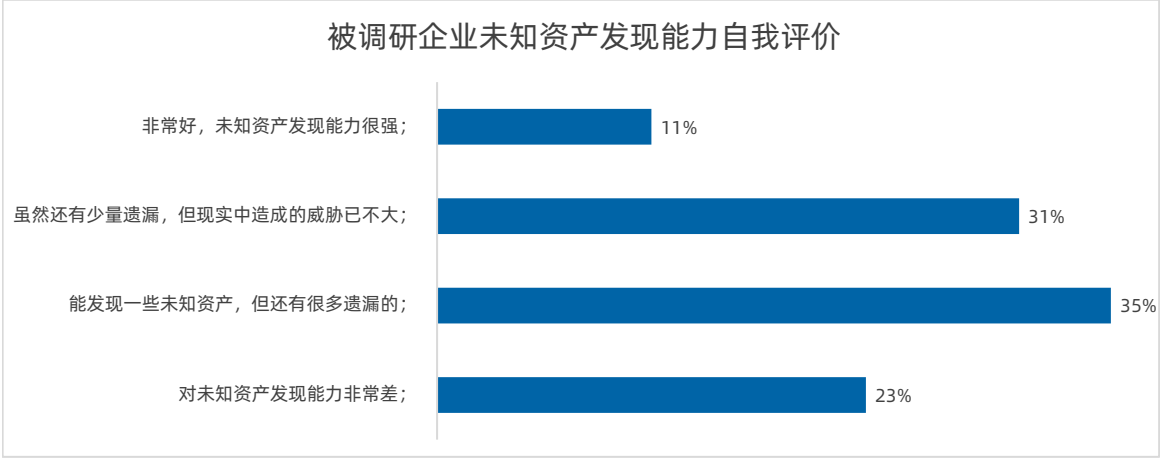
企业IT资产管理能力

52%的企业认为没有或只有较弱的IT资产管理能力，只有15%的企业认为可以将资产管理系统与SOC/SIEM/SOAR系统进行有效整合，赋能安全运营。



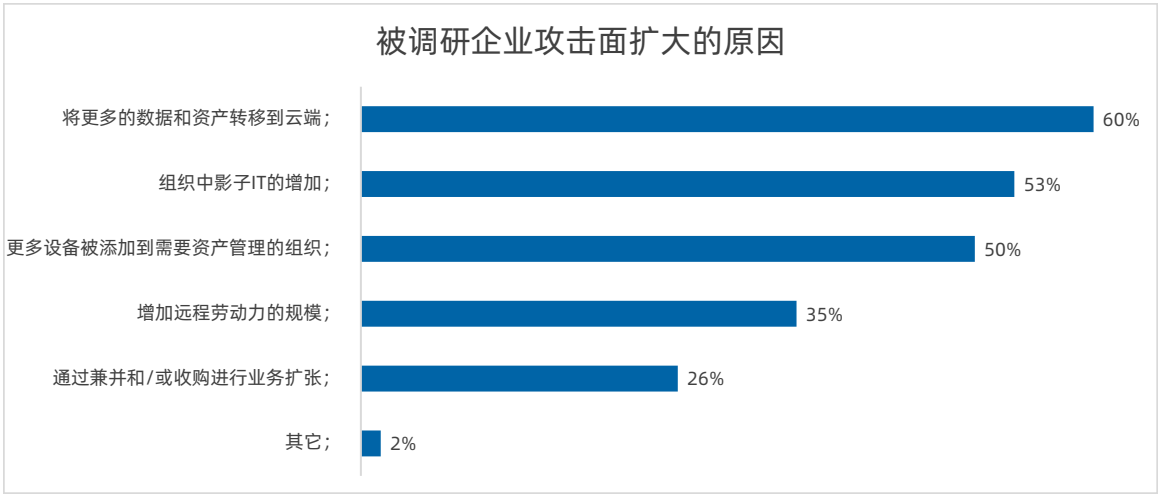
企业未知资产发现能力

在未知资产发现方面，58%的企业认为存在较大不足，只有11%的企业认为可以很好的发现未知资产。



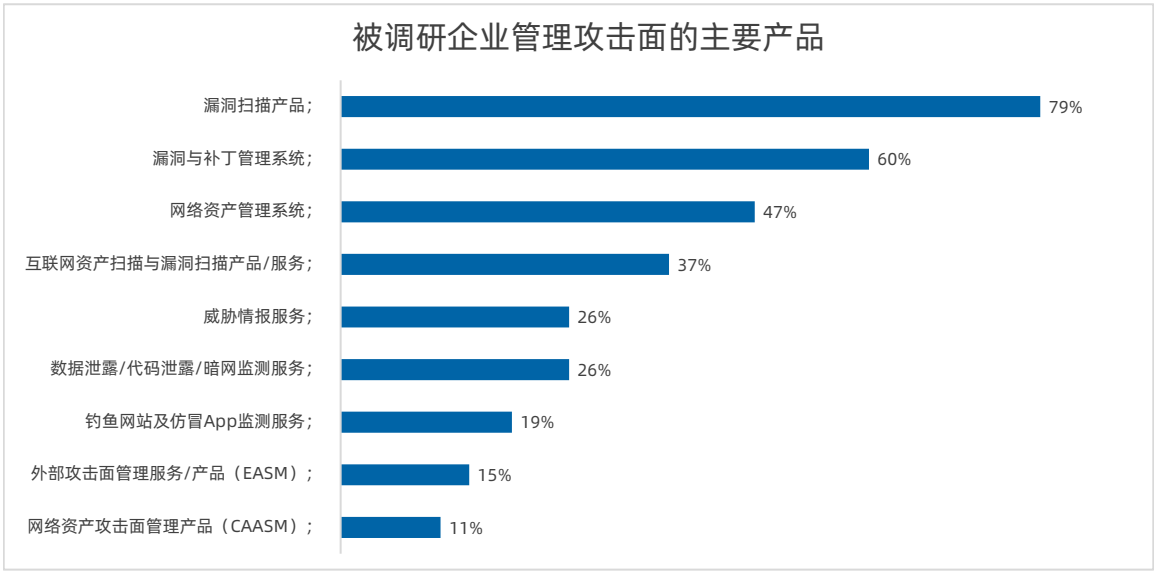
企业攻击面扩大的原因

组织攻击面不断扩大，企业认为最主要的3个原因是：将更多的数据和资产转移到云端、组织中影子IT的增加、更多设备被添加到需要资产管理的组织。



企业管理攻击面的主要产品

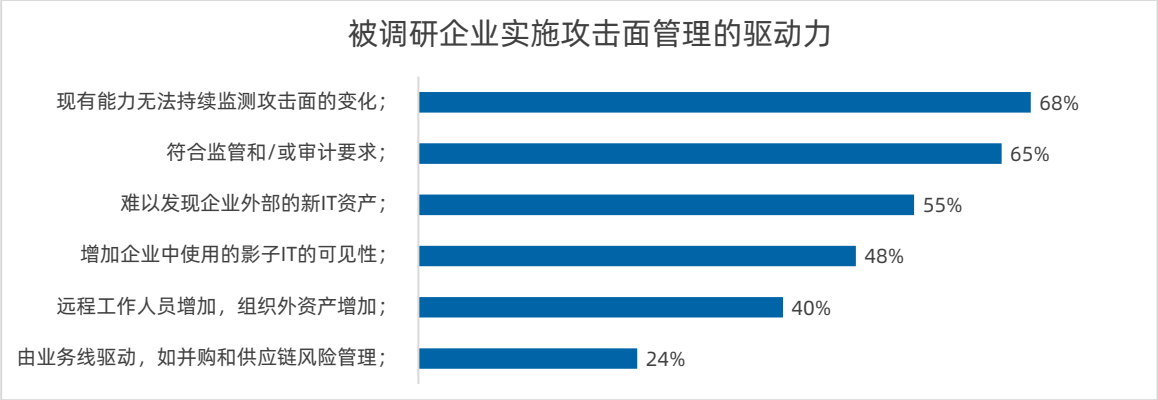
企业通过资产识别与漏洞发现，实现攻击面管理，购买最多的3个产品是：漏洞扫描产品、漏洞与补丁管理系统、网络资产管理系统。而对于CAASM和EASM，购买的比例仅有11%和15%。



攻击面管理产品与用户需求的匹配度

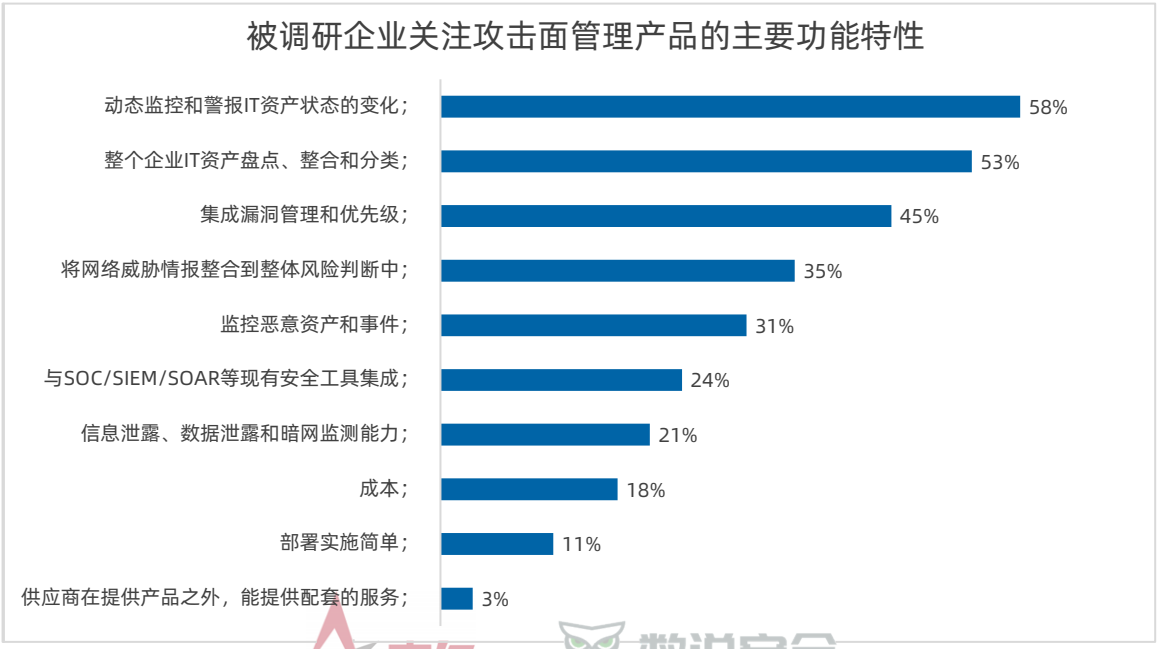
企业实施攻击面管理的驱动力

驱动企业实施攻击面管理的最主要3个原因是：现有能力无法持续监测攻击面的变化、符合监管和/或审计要求、难以发现企业外部的新IT资产。



企业关注攻击面管理产品的主要功能特性

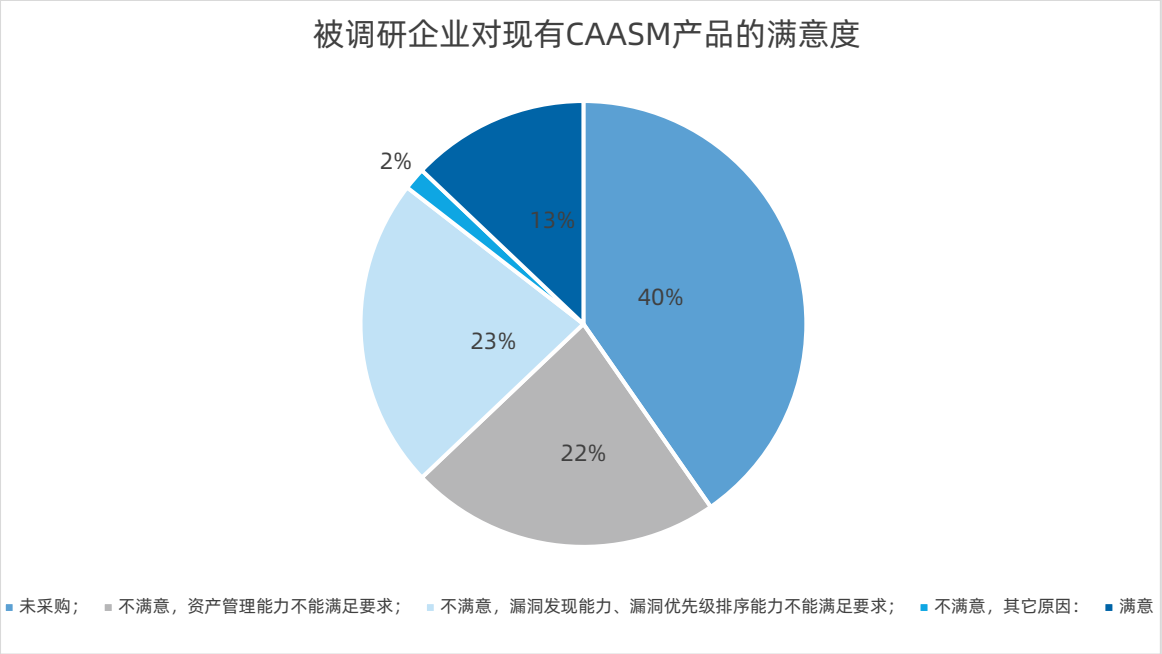
如果选购攻击面管理产品，企业最关注的3个功能特性是：动态监控和警报IT资产状态的变化、整个企业IT资产盘点、整合和分类、集成漏洞管理和优先级。



攻击面管理产品用户实际使用情况

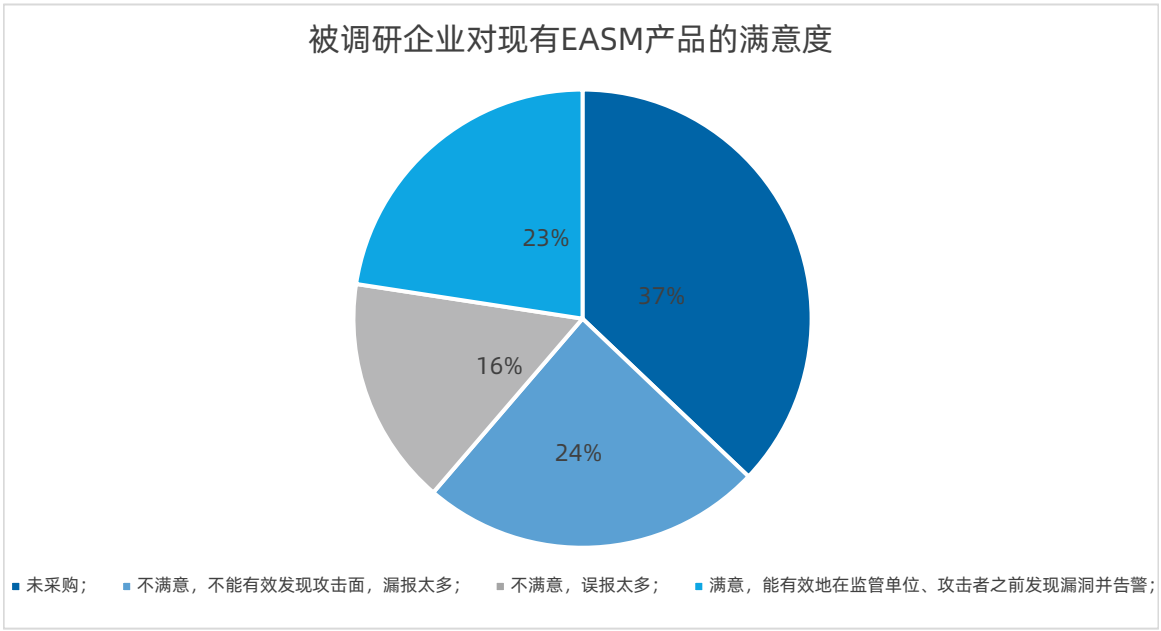
企业对现有CAASM产品的满意度

47%的企业对已购买的CAASM产品不满意，主要原因是资产管理、漏洞发现、漏洞优先级排序方面不能满足企业要求。仅有13%的企业对已购买的CAASM产品满意，另有40%的企业还没有购买CAASM产品。



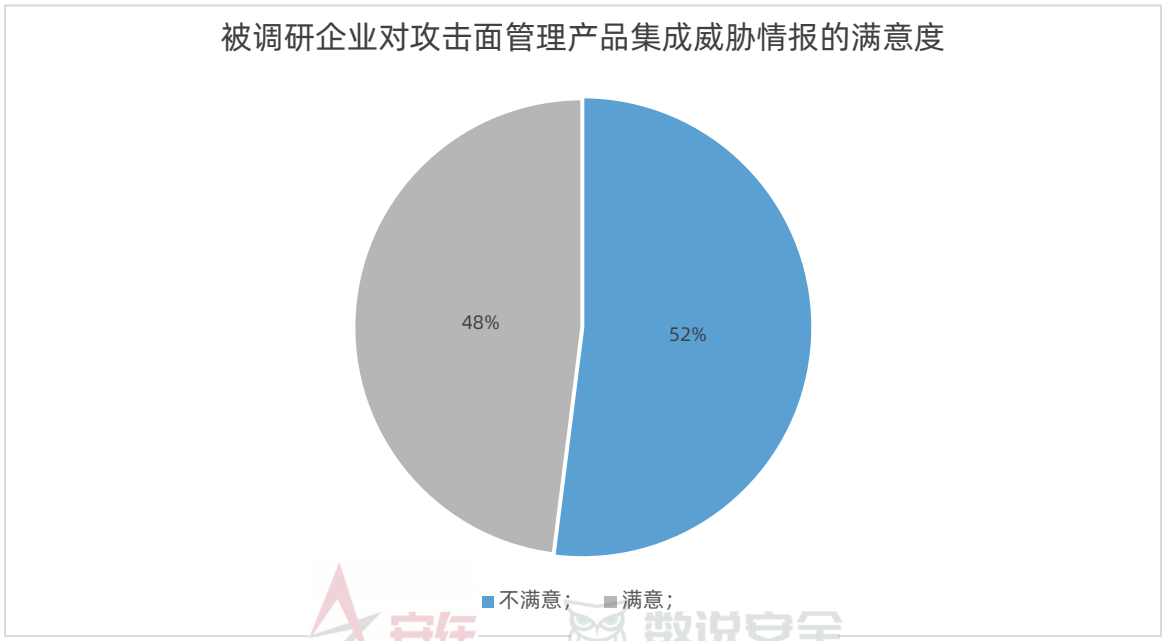
企业对现有EASM产品的满意度

40%的企业对已购买的EASM服务不满意，主要原因在于较多的漏报和误报，有23%的企业对购买的EASM服务满意，而另有37%的企业还没有购买EASM服务。



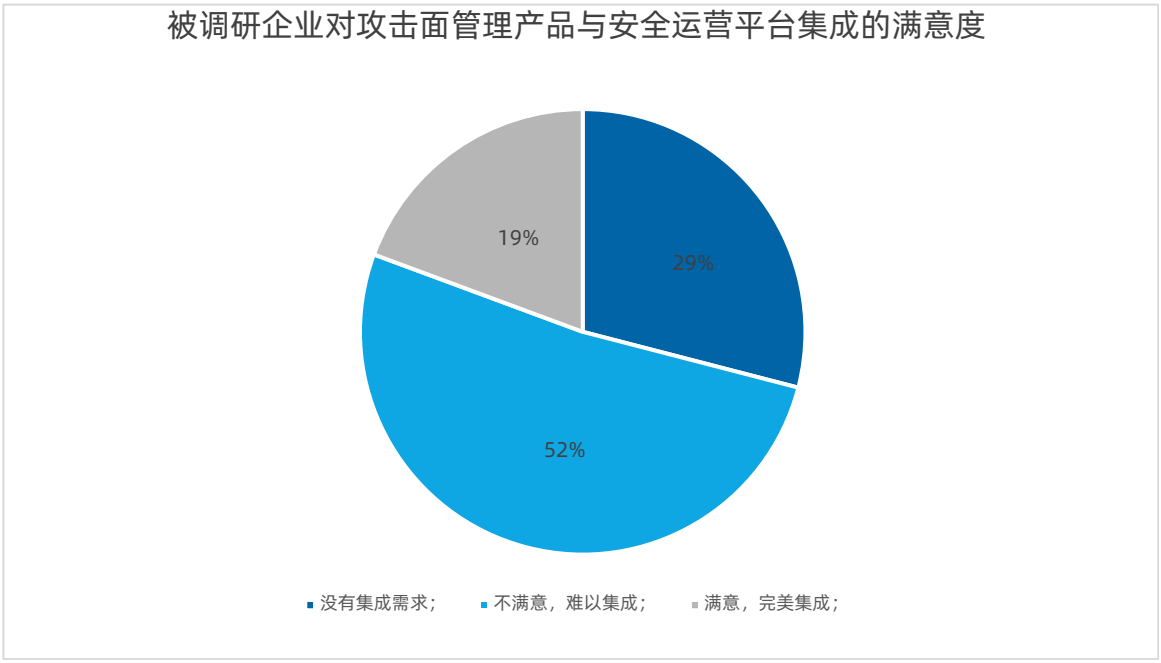
企业对攻击面管理产品集成威胁情报的满意度

52%的企业对攻击面管理产品集成威胁情报的效果不满意。



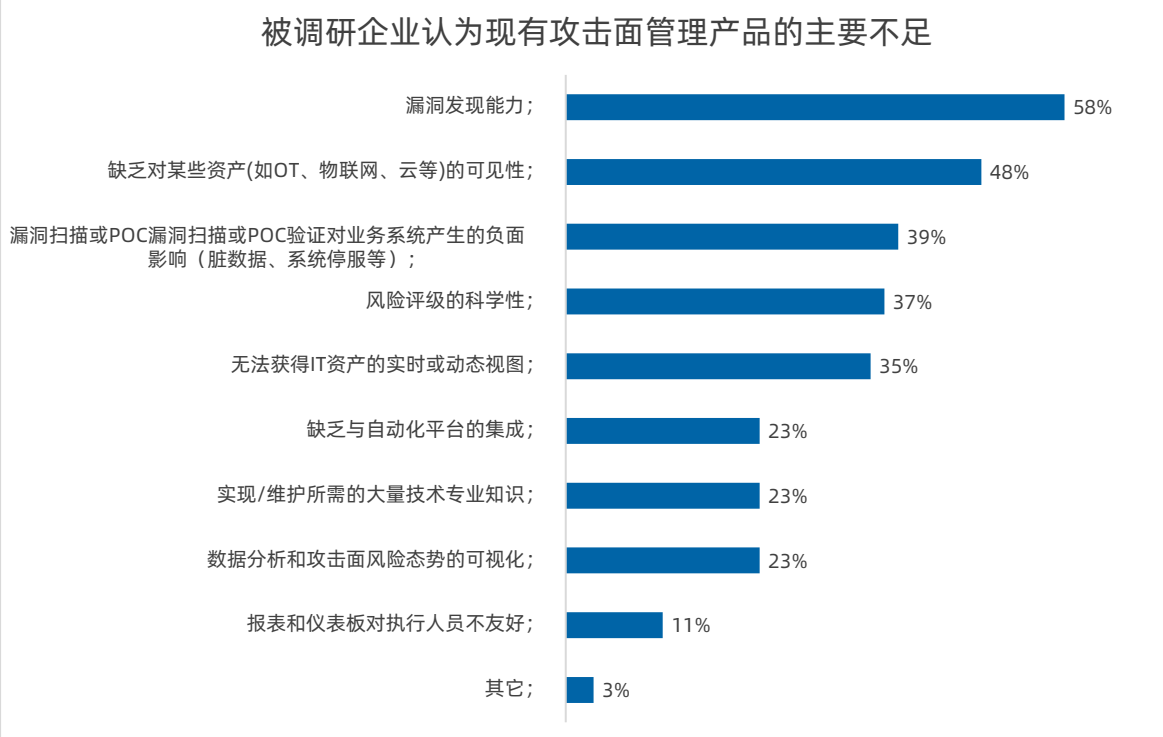
企业对攻击面管理产品与安全运营平台集成的满意度

52%的企业认为不满意，难以将攻击面管理产品集成到企业安全运营平台中，有19%的企业认为可以完美集成，而有29%的企业则认为没有将两者集成的需求。



企业认为现有攻击面管理产品的主要不足

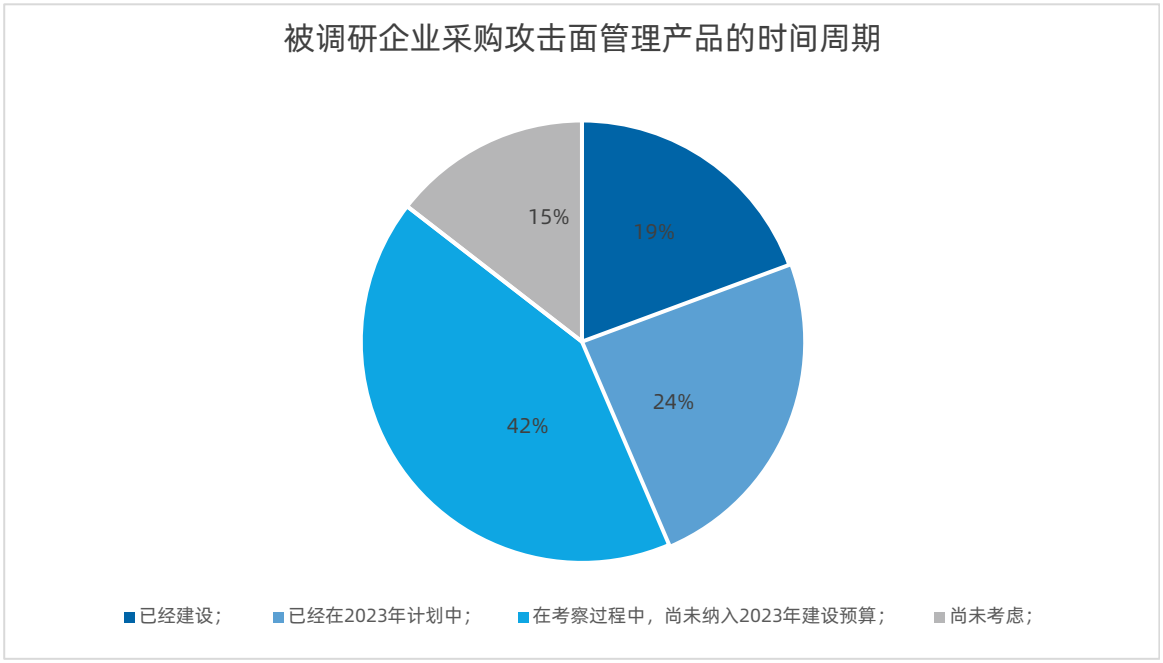
企业认为目前使用的攻击面管理产品，最主要的5个不足分别：漏洞发现能力、缺乏对某些资产(如OT、物联网、云等)的可见性、漏洞扫描或POC验证对业务系统产生的负面影响（脏数据、系统停服等）、风险评级的科学性、无法获得IT资产的实时或动态视图。



攻击面管理产品用户未来投入计划

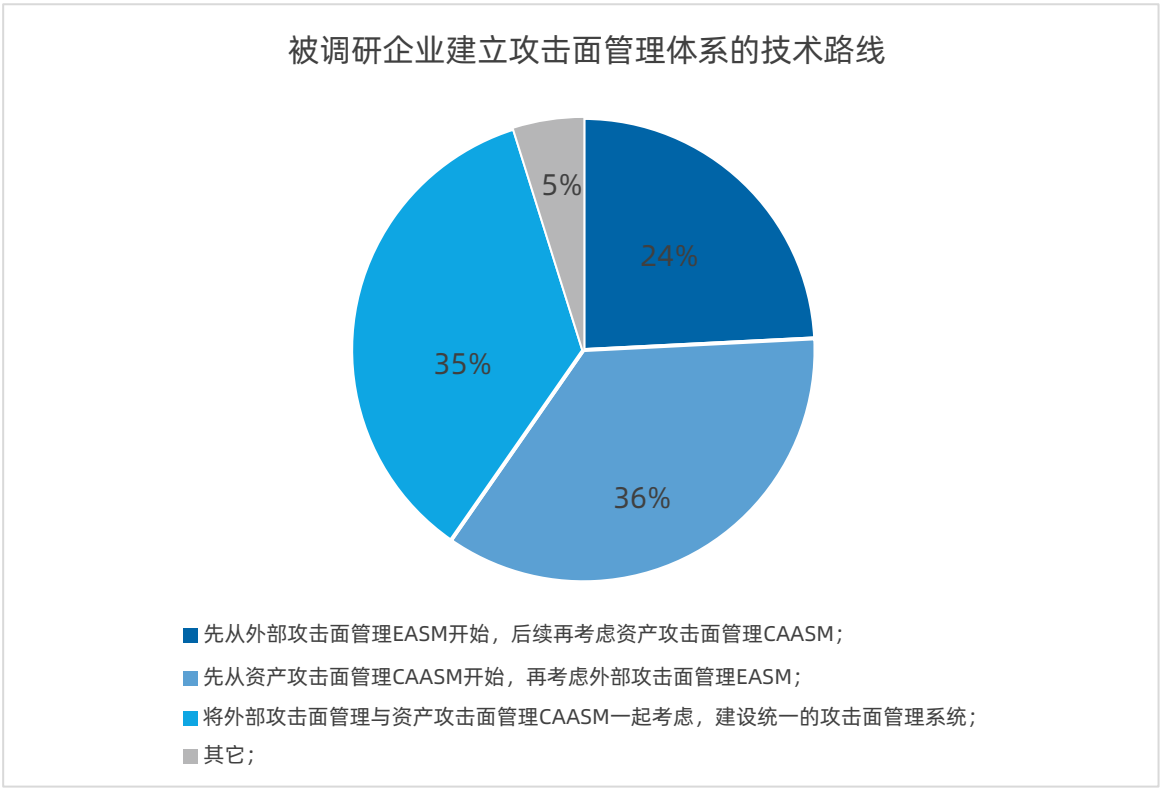
企业采购攻击面管理产品的时间周期

24%的企业表示将在一年内采购攻击面管理产品，42%的企业表示虽在关注产品但未列入当年预算，15%的企业则表示尚未考虑。



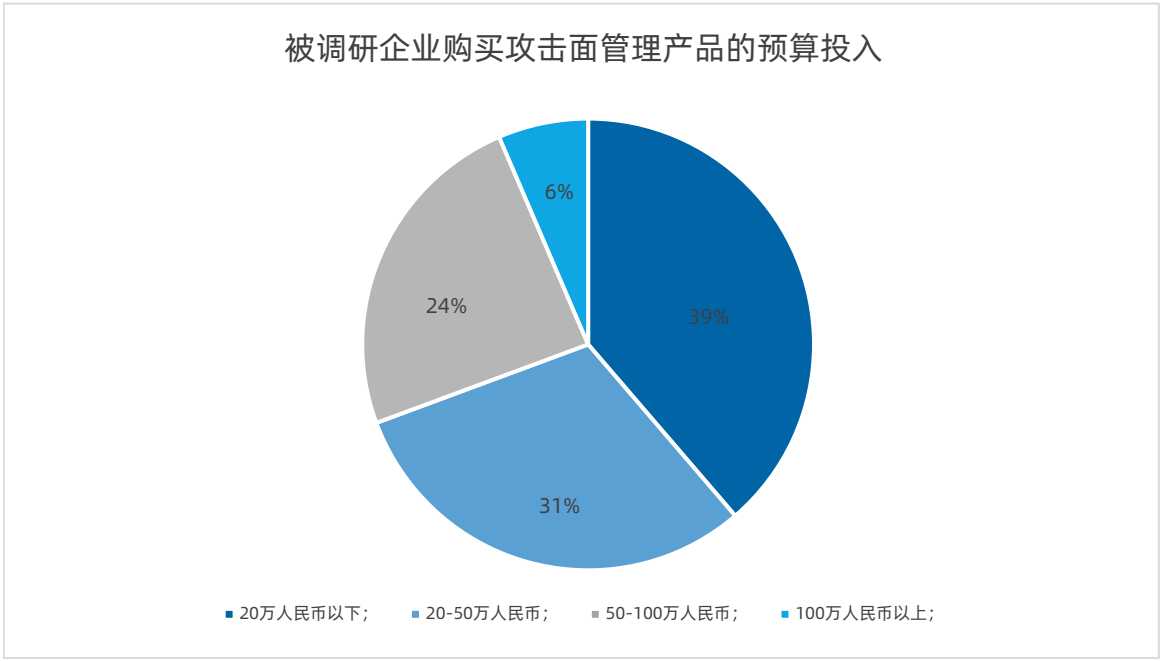
企业建立攻击面管理体系的技术路线

35%的企业希望建立CAASM+EASM一体化的攻击面管理系统，36%的企业认为应该先从CAASM入手，而有24%的企业认为先从EASM开始。



企业购买攻击面管理产品的预算投入

在成本投入方面，即每年可用于攻击面管理产品的预算范围，70%的企业选择了50万人民币以下，24%的企业表示可以在50万-100万人民币，只有6%的企业认为可以在100万人民币以上。



COPYRIGHT NOTICE
版权声明

数说安全隶属于北京赛博英杰科技有限公司，是中国第一家为网络安全企业提供全生命周期顾问服务的公司，为客户提供战略规划、产品管理、数字化营销、卓越运营、投资与并购、媒体传播等服务，立足于让网络安全创业少走弯路，为创业企业对接合作资源，创造良好的安全创业小环境。

安在新媒体隶属上海安阖在创信息科技有限公司，是一家网络安全领域的专业媒体服务机构，致力于为客户提供全面、精准、专业的一站式互联网新媒体服务。自2016年成立发展至今，已成为国内最具影响力的专业媒体品牌之一。

DISCLAIMER
免责声明

本报告所用调研数据均采用样本调研方法获得，数据分析和相关结论因受样本来源和数量的影响，未必能够完全或唯一反映真实的行业及市场现状。所以，本报告只提供给个人或单位用于必要参考，安在新媒体不对任何依据本报告所作的其他分析研究和判断决策负责。

THANKS
致谢

本报告的数据采集工作得到了各界的大力支持，各项调查工作得以顺利进行，在各相关单位、调查支持网站以及媒体等的密切配合下，基础资源数据采集才能及时完成。在此，谨对他们表示最衷心的感谢！

安在 ANZER　数说安全 CYBERSECURITY REVIEWS

数说安全介绍

最专业的网络安全产业研究平台,以数据为基础，为网络安全监管部门、网络安全企业、网络安全产品与服务客户、网络安全资本市场等受众提供研究报告、顾问咨询、媒体传播、数字化营销工具等服务。

关注公众号

数说安全合作邮箱：ssaq@geniuscybertech.com
赛博英杰合作邮箱：connect@geniuscybertech.com

安在新榜介绍

“安在新榜”是网络安全领域的“大众点评”，力求提供全面精准的网络安全市场数据。

码寻求商务合作

扫码加入诸子云