

“数字替身”数据资源防护软件

抵御未知网络攻击、达成危害消解



目标定位

智能化网络渗透攻击已经成为网络攻击的新态势，加剧攻防信息失衡，导致我国重点单位存在大量“检不出”“看不见”的未知网络攻击。现有防御技术过度依赖已知威胁情报，难以抵御高水平未知网络攻击，防护关键资源，实现危害消解。



创新理念

“数字替身”的核心是变“本体受害”为“李代桃僵”，由“替身”无感代替“本体”承受攻击，在业务系统中建立链式诱导防御机制，改变“敌暗我明”的攻防格局，为重点单位抵御未知APT攻击、勒索攻击提供全新的解决方案^{1,2}。



优势技术

“数字替身”数据资源防护系统包括客户端和服务端两部分，客户端在真实业务系统中对关键数据资源建立最小防护面，突破API无感劫持与重定向等关键技术，发现可疑行为，提取未知样本；服务端全面存证客户端替身日志与样本，开展智能化威胁研判。

多模态高拟真替身与认知对抗

自动提取不同模态数据资源“密点”，为数据资源“本体”自动构建脱敏的高仿真“替身”，形成认知欺骗对抗能力

低干扰“零信任”身份认证

建立进程链签名验证、人机交互事件关联等多种身份认证机制，在进程对关键资源访问过程中，快速识别并发现可疑进程与异常访问行为

关键数据资源防护

通过对关键API劫持、验证，放行正常访问，重定向可疑访问至“替身”，在信息系统中同时实现关键资源防护与未知攻击危害消解

全链路存证与智能威胁研判

研制API、进程、网络等多级探针，隐蔽记录可疑样本进程行为等关键证据，开展面向未知网络攻击的全链路取证与智能威胁研判



部署应用

- ◆ 系统已经通过1200余项企业级集成测试，完成与360、安天等头部安全企业产品线的集成和应用验证，提供多形态部署能力
- ◆ 系统已在电力、金融、科研等重点领域单位规模化部署，发现并实证多起重大事件，来函评价“率先形成我国体系化、可落地、具备实战操作性的未知网络攻击危害消解方案”“为核心产品提供技术代差优势”
- ◆ 申请试用详情可访问：<https://digitalscapegoat.cn>