中安网星
击败每一次网络攻击

ITDR | 白皮书

身 份 威 胁 检 测 与 响 应

目录

CONTENTS

目录

01

身份基础设施安全面临挑战

一、身份基础设施安全面临挑战

1.1当今身份基础设施现状

当下随着整个 IT 基础架构逐渐云化及复杂化，身份成为了企业防护的新边界。过去的 IT 架构相对简单，传统的安全防护模型是以边界设计为核心，安全信任级别跟位置是强关联的。边界设计的网络安全方法是先连接，后信任，在网络边界验证用户身份，如果用户被认定为是可信任的，就能访问该网络内的数据和资源。

过去的很长一段时间内，企业通过对各类边界层层防护拥有了强大的纵深防护能力，但如今 IT 架构的云化和复杂化，身份本身成为了企业新的边界，传统边界类的防护方案开始捉襟见肘，无法防护新 IT 架构下新场景的威胁。承载企业身份相关的身份基础设施逐渐成为主要的攻击对象 , 如 IAM、AD、PAM、4A、vSphere 等。这些身份基础设施通常具有保存密码多、控制节点多、网络权限广的特点，对攻击者而言是核心的攻击对象，对企业而言则需要重点防护。

1.2企业存在身份风险痛点

1.2.1外部身份威胁

企业复杂割裂身份体系，导致企业身份暴露面在爆炸式增长，例如一个员工有多个身份账户等。暴漏在企业外部的身份连接信息成为攻击者打开企业网络边界金钥匙，常常采集企业对外暴露的身份信息分析后针对其进行攻击。

1.2.2内部身份威胁

身份是一个人在数字世界的映射，一旦内部出现心怀恶意的内鬼或疏忽大意的员工必然会出现失陷账号与失陷主机导致的各种内部威胁 ; 身份凭据滥用，账号管理松散，密钥管理混乱极易引发安全问题。

1.2.3身份设施割裂无法集中监控

对于企业内部而言，不同的供应商使用独立的认证源，企业无法做到统一身份基础设施，如企业的公有云、私有云、本地办公设施等身份源存在必然的割裂；集团子企业使用不同的身份源；部分产品无法对接企业身份源，未来这一情况也无法得到根本的改善。

这造成企业内部统一认证身份设施割裂，内部多个身份源无法统一观察与监控，且存在大量独立的认证源存在监控死角，仅仅依靠身份设施自身的安全监控能力是无法满足企业管控需要的，企业如果要进行安全分析与身份溯源往往力不从心。

1.2.4身份威胁监控能力不足，安全团队人员不足或能力有限

身份威胁监控能力不足，安全团队人员不足或能力有限，深陷不对称的“安全战争”

之中。传统的安全威胁是以漏洞为基础，漏洞总是由攻击者掌握，而防守者掌握并加入到企业防护体系中的周期往往是以月记的，这常常会陷入到攻防不对称的状态中。

因此通过对攻击者行为的预测就显得格外重要，身份检测就是这样一个范式，可以预测攻击者行为。但企业身份威胁安全监控缺乏监控维度与规则，企业被攻击之后无法快速溯源，无法回答身份的调用过程是如何扭转的。

1.3攻击趋势逐步转变为针对身份基础设施

为了顺应新的 IT 架构变革，更好地应对云时代的到来，近几年来企业开始应用身份认证和管理类方案，如 IAM、IGA、IDaaS 和 PAM 等，此类方案主要侧重于授权和身份验证，确保合适的人可以访问他们需要的文件和应用资源，但却疏忽了身份威胁检测和响应的能力，同时这些设施本身也带来了巨大的攻击风险。

伴随着身份认证管理方案的普及，越来越多的攻击者将攻击目标转向具有高攻击价值的身份基础设施。攻击者通过窃取身份设施中的合法身份进行利用，在内网中横向移动而不被发现，也能使用身份设施中访问权限来窃取更有价值的数据，例如员工和客户的敏感个人信息或财务信息等。

在大多数的攻击案例中我们可以看出，攻击者会针对企业内重要身份基础设施进行定向攻击，因为其权限及网络权限的特殊性，此类基础设施一旦被利用，将会成为引发重大安全事故的核心节点，而其中的每一个身份都会成为扩展新攻击路径的重要媒介。

02

ITDR 技术应运而生

二、ITDR技术应运而生

2.1ITDR是什么?

Gartner 于《2022 安全运营技术成熟度曲线》报告中正式提出 ITDR 技术概念，Gartner 认为创建 ITDR 这个新类别将有助于企业集中精力并更好地保护其身份系统。换而言之，基于身份的攻击已经成为一种常见的网络安全威胁，以至于需要一种专门的、针对性的方法来对抗身份攻击威胁。

ITDR 即身份威胁检测和响应（Identity Threat Detection and Response），ITDR 是一个新的安全类别，是指保护身份基础设施免受恶意攻击的工具和流程，监测针对身份基础设施的攻击 , 通过结合异常身份请求、UEBA、身份欺骗等方式，可以发现凭据窃取、特权滥用以及其他与身份相关的攻击威胁和潜在风险。

2.2ITDR发展的双轮驱动

2.2.1驱动一：身份是企业防护新边界

云原生时代、企业边界越发模糊和复杂，原有安全防御体系失灵，身份成为企业新边界，也是企业的唯一控制点。

过去 IT 架构简单的时候，网络边界防火墙是刚需，发展到 Web2.0 时代用户开始和大量的互联网应用进行交互，此时 web 应用防护墙（WAF) 开始成为标配。如今万物互联，身份成为企业的新边界新的控制点，那身份威胁检测一定是这个阶段的必然产物。

身份如今变得越来越重要，企业的身份基础设施也开始多元化，例如生产网络使用堡垒机、办公网使用 AD、隔离网用云桌面、服务器用 vCenter、云上应用使用 IDaas 等。攻击者越来越多地将目标对准身份基础设施本身，组织必须更加专注于保护其身份基础设施。ITDR 技术将为身份基础设施部署增加额外的安全层。

云原生时代催生出很多新的业务及办公场景，对应被攻击的场景也将更加丰富。比如远程办公场景，现在可能一个企业办公软件账户泄露，可能就会导致这个企业的大量业务数据丢失，一个业务应用设计有逻辑问题，可能就会导致被薅羊毛，这样的案例再这几年有很多，新业务场景下其实产生非常多种的风险攻击面。

企业的安全需要，从防火墙、入侵检测和杀毒软件的传统老三样“标配”，逐渐向数据是新中心、情报是新服务、身份新边界的新时代“立体化”网络安全需求演进。

表一　典型的身份基础设施分类

身份设施对象	设施应用场景	设施属性特点	设施主要功能	ITDR 能否保护
IAM	多用于企业应用资源认证管理	身份认证和管理、网络权限广泛	提供给企业的应用统一的身份认证	能
AD	多用于办公网区域认证管理	身份认证和管理、POD 集中控制、网络权限广泛	对办公网 / 服务器的终端提供认证和管控功能	能
vCenter	多用于企业虚拟化资源管理	身份认证和管理、POD 集中控制、网络权限广泛	能够基于用户硬件资源快速构建虚拟化办公平台，支持多操作系统	能
PAM (4A/ 堡垒机)	多用于企业生产网资源认证管理	身份认证和管理、POD 集中控制、网络权限广泛	多用于企业生产网络，能够统一管理和登录审计生产网的服务器	能
K8S	多用于企业容器化资源的认证管理	身份认证和管理、POD 集中控制、网络权限广泛	企业的容器化管理方案，用于构建企业的私有云方案，具备弹性伸缩的特点	能
zabbix	多用于企业的服务器运维机器管理	身份认证和管理、POD 集中控制、网络权限广泛	企业常用的服务器监控方案，管理企业的大多数生服务器	能
CLOUD（IDAAS）/ IDAAS	多用于企业云上应用的身份认证和管理	身份认证和管理、POD 集中控制、网络权限广泛	有云方案，用于业务应用的对外部署，提供对外访问等，基于 IDASS 的功能，实现内外访问的身份统一	能
云桌面	多用于企业办公隔离网的虚拟办公平台	身份认证和管理、POD 集中控制、网络权限广泛	基于虚拟化技术，提供给用户在办公外网的虚拟办公平台	能

2.2.2驱动二：攻击链路中身份是核心要素

频繁的攻防演练、以 APT 为代表的新一代攻击模式中身份攻击利用已成为攻击全链路中被高频使用的技术手段。大量的攻防案例分析，无论多复杂的攻击链路都离不开最核心的三个攻击要素：

第一个要素是要知道攻击对象是谁，比如是一个 IP 地址，是一个应用系统，是一个账户等；

第二个要素是要拿到一个身份信息，比如是一个密码，是一个私钥，是一个凭据或证书等

第三个要素是进行身份的登录验证，验证登录这个对象。

三个要素不断的循环其实就可以形成一个复杂攻击链路。

同时能够发现在现代化的攻击过程中，攻击者也更喜欢拿身份基础设施作为链路中的关键攻击对象，此类身份基础对象都满足三个特点：

第一保存的身份凭据多，攻破之后能够拿到大量的身份密码或凭据等；

第二本身网络权限广，是攻击很好的跳板；

第三是控制机器多，能够让攻击者以此快速拓展战场。

对攻击者而言，这些对象有极高的攻击价值，所以企业应当聚焦精力来保护这些身份基础设施。

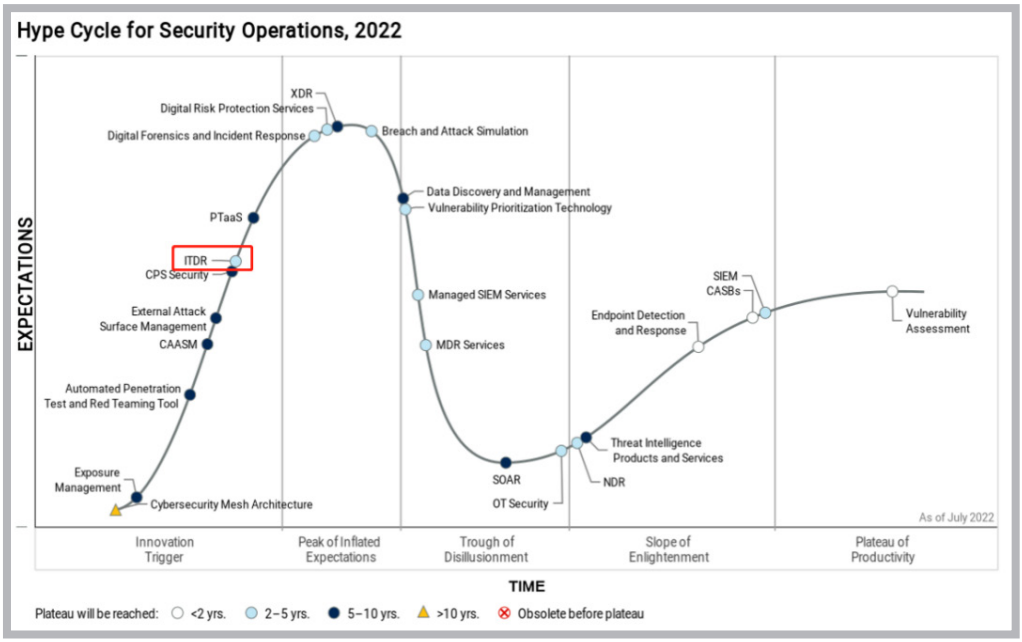
过去我们已经看到国内大量攻击案例中都会去攻击 AD、堡垒机、云平台、vCenter、4a 等身份基础设施，甚至攻击者会攻击利用一些安全厂商的系统，随着零信任在国内的逐步落地，针对零信任组件的攻击在未来也会有增长的趋势。

所有攻击环节都能看到攻击者使用身份类攻击，攻击者在不同的场景不同的过程都会使用不同的身份类攻击手法。

2.3ITDR的市场认可及趋势

2.3.1Gartner眼中的ITDR：身份优先安全

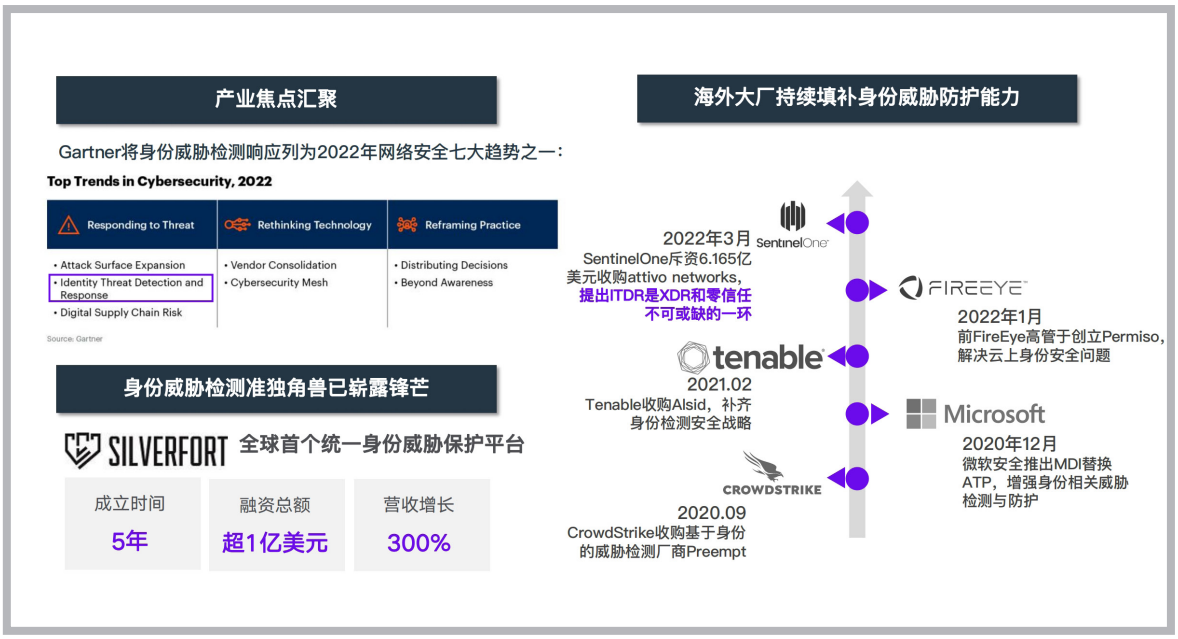
Gartner 今年发布的数份安全趋势报告中曾提及身份优先安全，将其解读为安全管理者在未来必须解决的重要趋势之一。ITDR 在 Gartner《2022 安全运营技术成熟度曲线》报告中被列为新兴技术，其效益等级为高，目标受众有着 5% 至 20% 的市场渗透率，这代表着 Gartner 对这项技术应用价值的潜在认可。从技术成熟度上来看，ITDR 技术本身成熟度较高，Gartner 预期未来 2-5 年即可达到主流应用。



且在今年 3 月 Gartner 发布的 2022 年的七大安全与风险趋势中，Gartner 表示：攻击者正在瞄准针对身份和访问管理（IAM）基础设施，通过凭证滥用发起攻击。Gartner 提出了“身份威胁检测和响应 ITDR（Identity Threat Detection and Response ）”这一术语来描述用于保护身份系统的工具和最佳实践的集合。与此同时，Gartner 预估，到 2023 年，“75% 的安全故障将是由于对身份、访问和特权的监控与管理不足”，而在 2020 年这一比例为 50%。考虑到这一点，需要更强大的身份安全检测能力——尤其是能够利用有效的帐户凭据检测可疑活动。

2.3.2权威机构对Gartner提出ITDR的认可

新威胁领域的一些例子，包括云控制台访问、云授权滥用以及嵌入式 DevOps 和应用程序密钥带来的极端危险。而攻击者完全认识到了这个机会：国际身份安全联盟 IDSA 的一项研究发现，在过去两年中，79% 的企业都经历过与身份相关的攻击。和其他许多攻击一样，最近的 SolarWinds 数字供应链攻击同样涉及了身份盗窃和特权访问操纵。而在国内的护网行动场上甚至有超过 50% 的攻击和弱口令相关，凭据窃取攻击更是数不胜数，面对这些现代威胁，身份显然已成为新的安全战场。



2.3.3ITDR在国内外的发展趋势

ITDR 技术在国外发展还是比较迅速的，涌现了一波独角兽公司，国内 ITDR 发展还属于起步阶段；我们在提出 ITDR 解决方案的同时需要尽快实现在企业中的身份安全落地，要去结合国内企业安全现状去思考实际解决方案，过去企业侧已有的身份基础设施，包括生产网用堡垒机，办公网用 AD，隔离网用云桌面，内部虚拟化用 vCenter 等，这些土壤足够支撑 ITDR 方向企业现阶段的发展；随着零信任的落地浪潮，身份厂商的快速发展，客户的身份设施同样会更加多样化，会让 ITDR 有可预期的第二次业务爆发增长机会。

从市场来看，身份设施是客户侧最基础的管理工具，几乎不存在没有身份管理设施的企业，现在网络安全覆盖的万余家企业一般都是已经部署了 AD 域、堡垒机、4A 中的一种或几种设施作为传统的身份管理。现在更多的应用对接产生了更多的身份场景，衍生出 IAM、IDAAS 这些新兴的身份设施。

终端、流量、身份形成了贯穿公司内行为的三层，终端检测相应形成了 EDR，流量检测响应形成了 NDR，而基于身份检测相应的 ITDR 则会成为未来身份这一层最重要的安全产品。未来无论是零信任方案还是 XDR 方案都绕不开 ITDR 的支持。

03

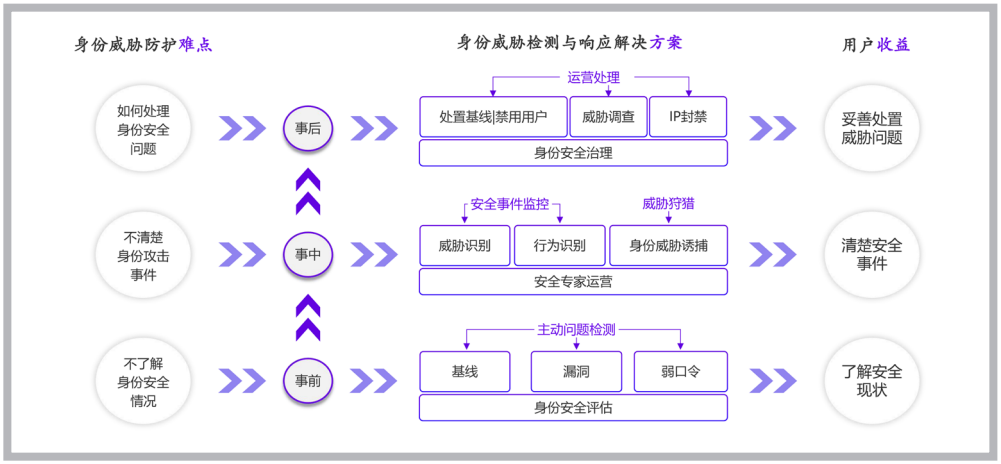
中安网星 ITDR 解决方案的技术架构

三、中安网星ITDR解决方案的技术架构

3.1概述

从运营视角来看，大多数情况下的应急响应或溯源分析过程中仅能碎片式地回答某个来源 IP 攻击某个目标 IP，无法确认每一个网络连接、端点、漏洞、设备背后的联系，但这恰恰是企业安全人员所关注的核心。因此企业需要重视身份在分析与溯源过程中的串联能力。

于是我们融合攻击与运营视角建立了一套身份威胁解决方案



结合现有的身份认证体系构建统一 ITDR 平台来进行落地应用，目标是集中分析企业所有身份数据，以此达到统一审计、统一分析、统一运营的目的。

ITDR 数据集成阶段通过主动或被动的方式采集各类身份数据，目前支持 AD、IAM、PAM、vCenter、Cloud 等多个场景的数据采集。

我们认为企业需要构建覆盖安全事件全生命周期的身份威胁检测和响应能力，基于安全事件的事前、事中、事后三个阶段全方位的解决身份威胁问题。

3.2事前阶段

身份的威胁更侧重于规避、绕过或滥用身份系统，以实现网络攻击。想要降低身份威胁的风险首先要做好预防措施，我们通过如下手段，开展前期的身份安全加固工作：

攻击面管理（减少暴露面）：删除非必要的或过多、过高的权限

漏洞修复：修复身份基础设施存在的漏洞

基线核查：核查身份基础设施的基线配置

弱口令检测：检查身份基础设施内的用户密码健壮性，设置密码复杂度要求

3.3事中阶段

尽管前期的加固工作我们已经做的足够好了，但绝不能认为仅靠基本的预防性控制就足以阻止网络攻击，针对身份的威胁要做到实时监测与防护。威胁检测能力参考 MITRE ATT&CK 和 Kill Chain 模型设计。身份的威胁遍布于杀伤链的各个阶段，能否分辨攻击所处的不同阶段，是威胁检测中重要的一环。精明的攻击者往往可以隐藏自身绕过传统的检测机制，因此我们利用机器学习、欺骗防御、用户和实体行为分析（UEBA）技术进一步加强了检测能力。

欺骗防御：通过在内网构造高权限蜜罐账户的认证凭据，利用攻击者希望隐藏自身位置的心理，攻击者在通过主动信息收集发现高权限凭据后，一般情况都会进行尝试登录或其他手段的利用，此时攻击者对身份认证系统请求蜜罐账户认证，随即暴露所在位置，安全人员即可定位到失陷主机。还可通过流量转发技术，将攻击者对真实业务系统的认证流量转发到提前准备好的蜜罐主机，造成认证成功的假象，拖延攻击进度。以此为安全人员提供充足的时间溯源攻击路径和入口并开展封堵工作，将攻击者重新踢出边界防护的大门之外。

机器学习：设置一定的学习周期，收集大量的身份行为数据，对每个用户进行行为建模，学习结束后形成新的规则模型，当行为超出模型基线便会产生告警。

用户和实体行为分析（UEBA）：将用户或实体行为、告警、风险等信息汇总后，通过算法得出用户或实体的风险评级，发现与用户或实体标准画像或异常行为的活动，有效帮助运维人员发掘潜藏的身份威胁。

3.4事后阶段

ITDR 解决方案中的响应相比检测显得更为重要。事后我们对危险用户可以禁用，同时依托于完整的告警与原始数据存储，我们能对威胁事件进行详细的溯源分析展示。

ITDR 通过对接身份认证基础设施实现阻断规则的配置下发，并且支持手动威胁阻断和自动威胁阻断两种方式。

手动威胁阻断：可添加阻断策略，对指定用户或 IP 进行阻断指令，被阻断的用户及 IP 将会被临时封禁。

自动威胁阻断：可针对每一条检测规则配置自动威胁阻断策略，若规则配置内自动威胁阻断开关打开，则在当前规则告警时，将当前规则告警中的用户和 IP 自动添加到威胁阻断页面的阻断策略中，并执行阻断命令对其进行临时封禁。

身份威胁响应模块同时支持对接第三方安全防护产品，实现联动处置，快速支持安全事件应急响应工作。

04

中安网星 ITDR 解决方案的落地实践

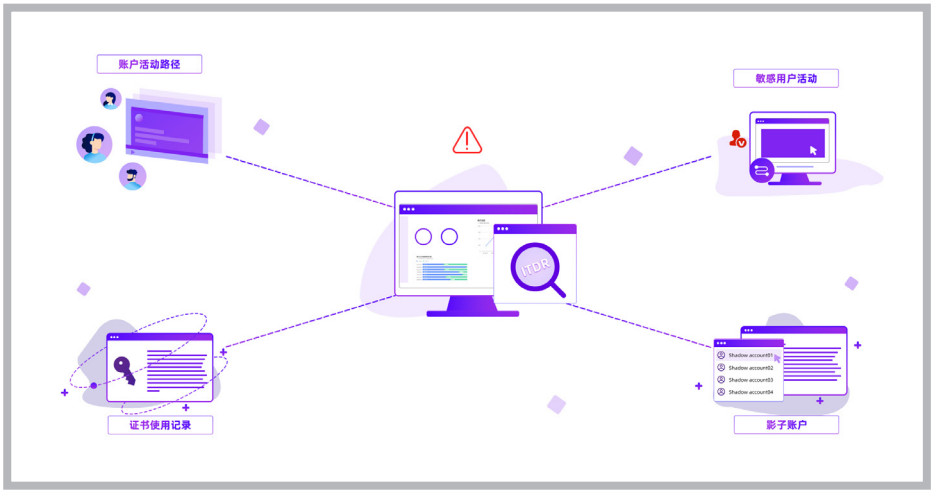
四、中安网星ITDR解决方案的落地实践

4.1三大核心能力

ITDR 平台功能构建围绕着三大能力方向 / 向量进行构建

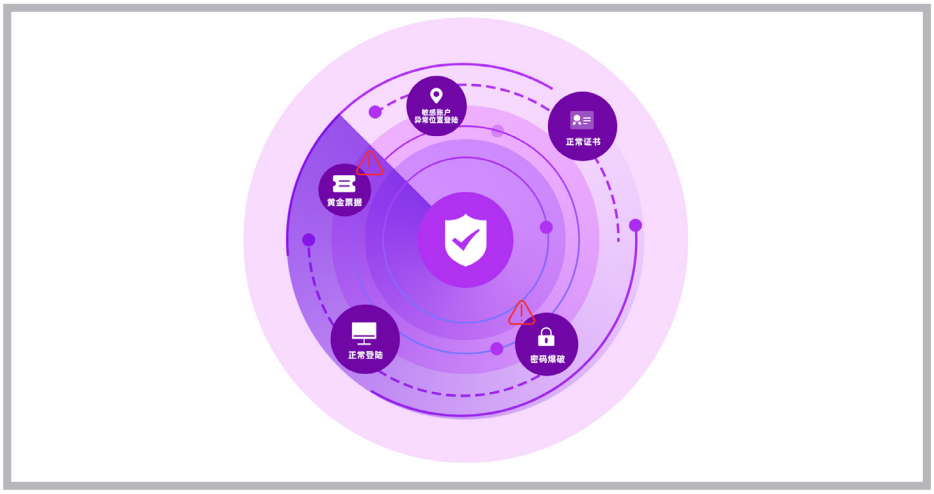
·第一能看到See：最大限度地提高企业各个位置的身份可见性

（通过对多个企业多个身份源的数据进行收集分析，通过大数据处理及图计算技术最大程度的将身份可视化，梳理每一个身份的扭转情况，能够发现其中的影子账号、账号权限过高等隐藏威胁）



·第二能保护Protect：高效、高速、实时监测身份攻击行为

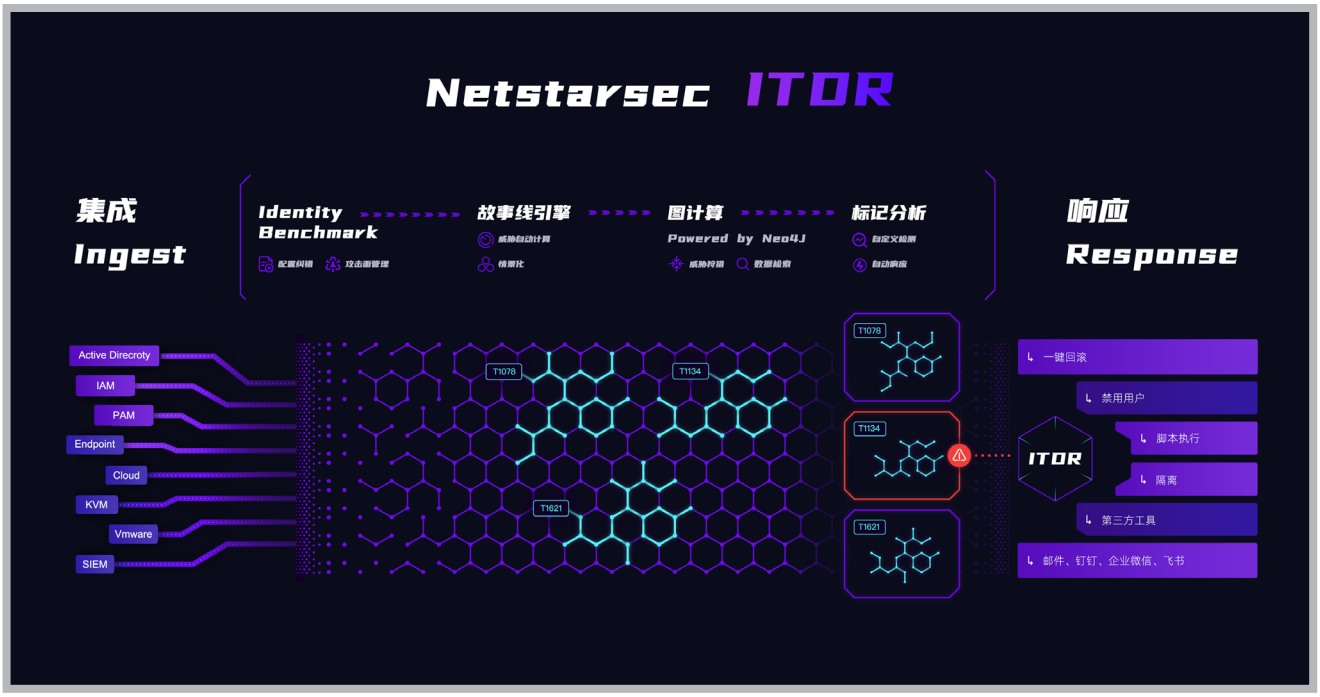
（对身份设施的主动式扫描进行加固保护，基于大数据处理和机器学习的分析能够实施感知到身份类的攻击行为，同时联动身份设施进行威胁诱捕，威胁诱捕一定程度上弥补可能因为数据不全面、数据碎片化造成的检测能力缺陷。



·第三能阻断恢复Resolve：·在整个安全生态系统中支持自动响应

（通过提供自动化的技术和工具，减少需要企业安全人员手动操作的频率和人为操作出错的概率，提高安全运营效率，ITDR 支持安全响应任务的编排能力，让用户对文件、权限、主机和网络执行经过预先设计编排过的手动和自动的补救措施，提高局部威胁发现、全局快速响应的的能力）

ITDR 整体方案目标是垂直分析企业所有身份数据，集中企业所有身份数据达到统一审计、统一分析、统一运营等目标。通过对企业身份的可见性、保护和响应超越终端与流量的局限视角。



ITDR模型架构图

第一部分 ITDR 数据集成阶段通过主动或被动的方式采集各类身份数据，目前支持 AD、IAM、云、SIEM 等多个场景的数据采集

第二部分会针对采集到的身份系统数据进行身份配置核查与攻击面管理，通过国际规范与攻防经验判断配置错误点并对其修复从而缩减身份攻击面

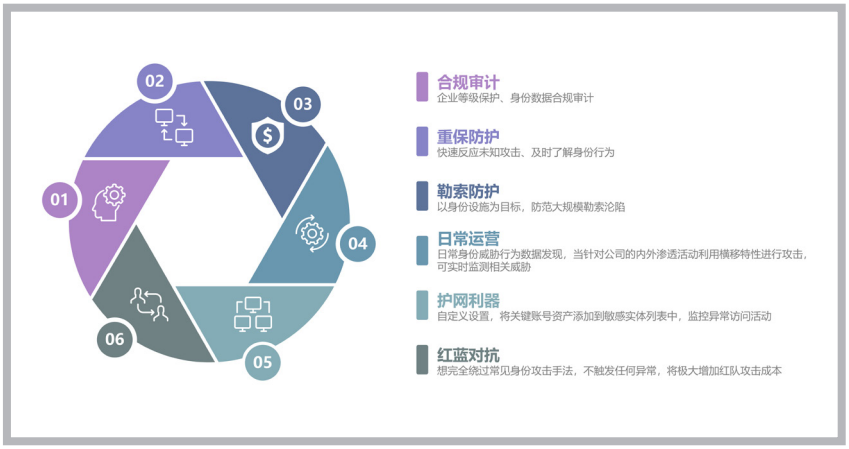
第三部分故事线引擎会通过规则与机器学习结合将身份的多个数据日志结合分析将单个身份日志聚合为一个个故事讲述给客户，达到威胁发现的目的

第四部分图计算通过把身份描述为点，身份权限关系描述为边构建出一个网图进行数据分析与攻击路径管理，从而实现高级身份威胁狩猎与分析

第五部分标记分析可以自定义检测规则并参与到机器学习标记工作中持续运营提高威胁检出率

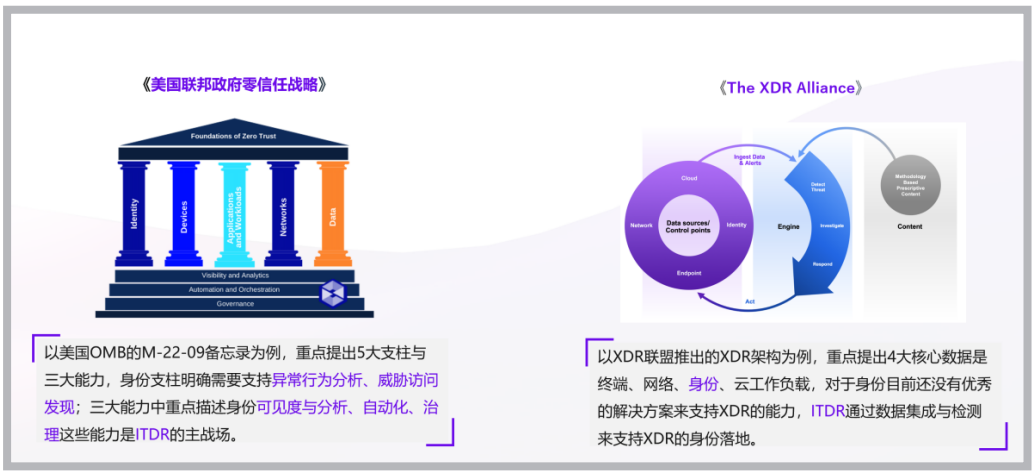
第六部分响应模块支持第三方集成与自定义剧本执行并能一键回滚，快速支持安全事件应急响应

4.2六大应用场景

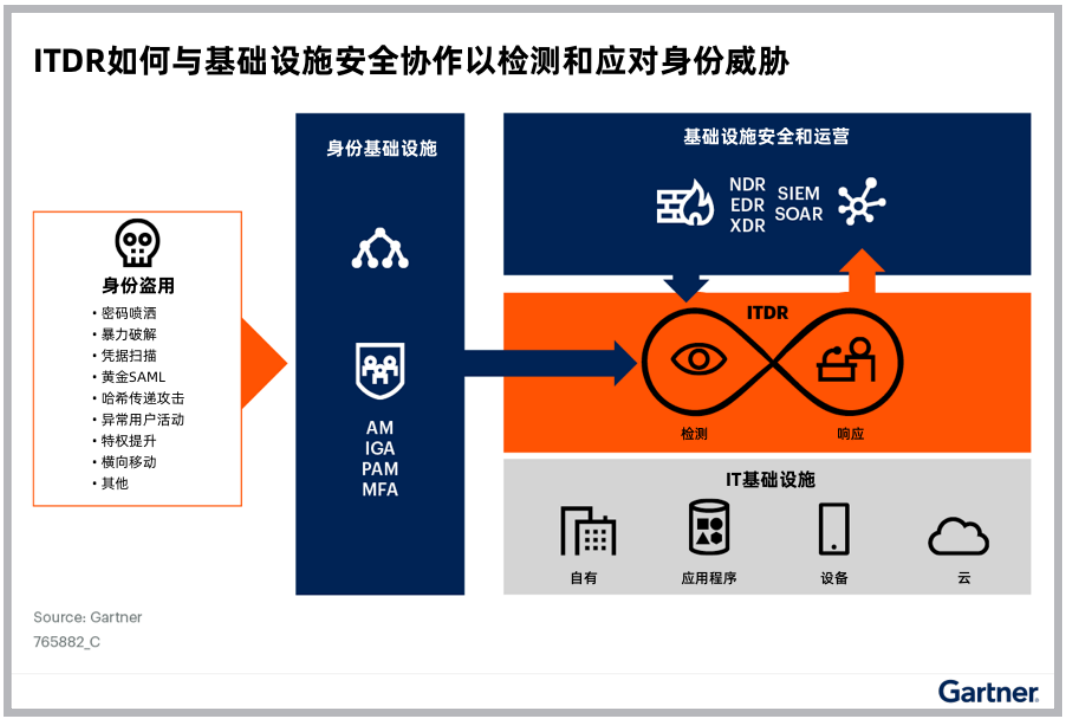


4.3ITDR与企业原有基础设施完美配合

2022 年 10 月 Gartner 发布 ITDR 详细解读，明确 ITDR 在整个网络安全中的生态位。中安网星完全认可 Gartner 的架构分类。ITDR 与 XDR 以及零信任体系有交集，且作为底层支柱的身份亟需 ITDR 来增强安全性。

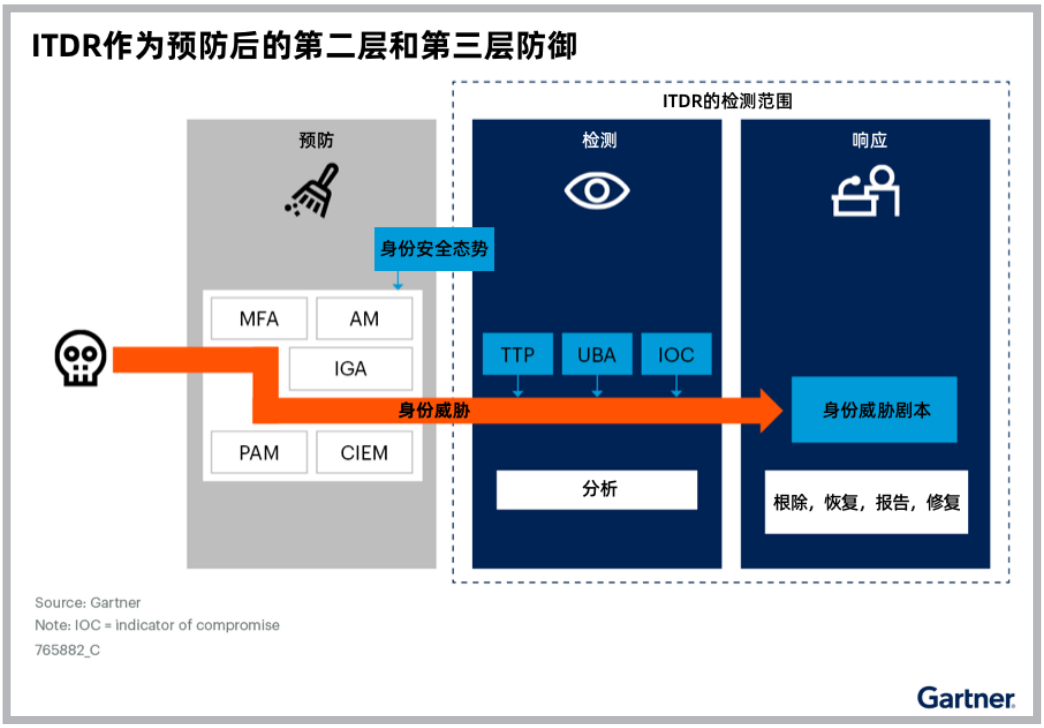


ITDR 方案会与现有的 IT 基础设施以及安全设备配合完成企业整体的安全防御任务。



图一　ITDR如何与基础设施安全协作

同时，在身份层面 ITDR 与已有的基础设施互相协作，形成第二和第三层防御。

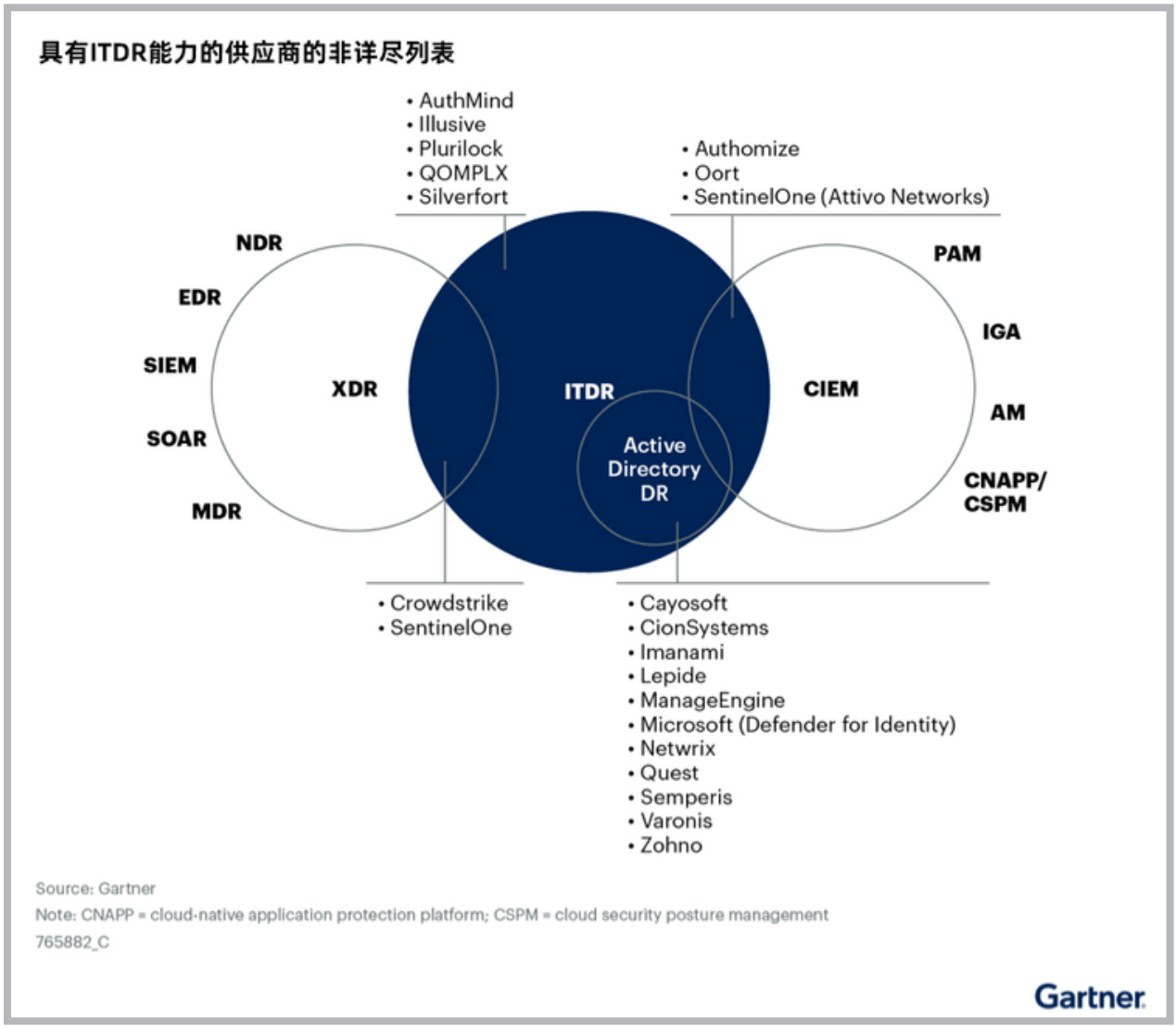


图二　ITDR作为预防后的第二层和第三层防御

身份威胁可以绕过或破坏 IAM 预防性控制。因此，重要的是要了解预防（攻击前进行身份安全态势监控）与

检测和响应（监视攻击并在攻击进行时阻断攻击）的分离。通过了解这种分离，企业可以制定更好的计划来实施“纵深防御”，重点放在身份上。如果企业采用 IAM 这样的单一工具，而不是综合防御方法，他们存在的风险是较高的。

针对非中国市场中的 ITDR 市场的企业我们做了如下的分类，基于 ITDR 发展出了 XDR 趋向、CIEM 趋向、ADDR 趋向、整体 ITDR 方案四大类，可以观察出当前 ITDR 在重要领域的应用趋势非常快速，应对此趋势我们应当快速反应与应对。



图三　具有ITDR能力的供应商非详尽列表

身份是企业的基础。企业依赖其身份基础设施来实现协作、远程办公和客户对服务的访问，这已将身份系统转变为攻击者的主要目标，而凭证滥用是近几年最常见的安全漏洞途径。

05

中安网星 ITDR 解决方案为企业带来的价值体现

五、中安网星ITDR解决方案为企业带来的价值体现

5.1基于业务视角

5.1.1身份基础设施统一监控

统一认证身份设施割裂，内部多个身份源无法统一观察与监控；同时也能对这些身份基础设施进行加固

5.1.2内部风险控制

大量企业在内部威胁管控上常常头疼，例如员工离职或商业间谍行为往往对公司核心知识产权造成严重影响，ITDR 通过对员工身份验证及其所访问的资源信息进行实时监控，可做到事前预防，事中监控和事后取证，助力企业管理内部安全威胁。另外当前多数企业存在大量业务风险，部分风险（如薅羊毛、刷单等）虽然没有 SQL 注入漏洞利用直接影响系统，但长期被羊毛党、刷单党光顾的企业生存下来的几率很低。ITDR 可通过对通用业务账号的多种数据维度自动建立基线持续调优助力业务风控安全。

5.2基于攻防视角

5.2.1黑客入侵

入侵检测是每一个大型互联网企业都要面对的严峻挑战。价值越高的公司，面临入侵的威胁也越大，从身份角度入手的安全检测能够从登陆验证的角度发现安全问题，以此为检测核心可极大的提高安全检测能力。

5.2.2护网演习

由于身份基础设施在办公网络中掌握了大量的关键凭据，使得身份权限在多数情况下会成为红队攻击的主要目标，而一旦身份基础设施遭到攻陷，也会造成防守方的大量失分。ITDR 不仅能对身份进行监控还能对身份凭据进行安全防护，防止凭据落入攻击者手中。

5.3基于运管视角

5.3.1当前运管存在相关痛点

身份威胁安全监控缺乏监控维度与规则；

身份凭据滥用，账号管理松散，密钥管理混乱极易引发安全问题；

MFA 只能应用于特定的系统，无法大规模或基于行为触发；

5.3.2满足合规的需求

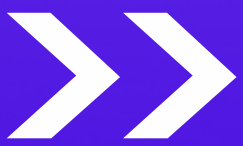
等保等各行各业的独立网络安全合规都指出有针对身份需要进行相关的防护与检测，ITDR 可以针对这些合规提供自动化合规手段，解决企业身份数据与平台合规问题。

5.3.3检测滥用的权限

通过使用身份分析和智能并监控使用情况并将其与已识别的用户任务配置文件相关联，可以确定用户任务所需的适当权限级别，并且可以删除任何过多的权限。这消除了具有过多特权用户的滥用机会。

06

结语



六、结语

随着身份成为企业安全的新边界，您会开始意识到企业需要解决更多的新型网络安全攻击，本书将为您提供一个心智模型，为您更好地建立一个身份安全防护体系。同时，您可以利用本书内的知识并传播到您的团队中，组建一个“Identity security team”，来专注于规划发展您的身份安全体系建设。

更为重要的是，中安网星 ITDR 解决方案将会为您提供多维度的综合防御能力，持续保护您的身份基础设施免受侵扰。

阻止今天、明天和未来的威胁

电话：010-53671735

官网：www.netstarsec.com

邮箱：public@netstar.cn

地址：北京市朝阳区酒仙桥东路18号1号楼四层A405