1.行业背景

在互联网快速发展中，金融行业的网络安全建设过程中也在不断的提高防护等级，在终端设备上部署基于签名式和规则检测的安全产品，但这种终端安全产品无法捕获目前新型的未知威胁的网络威胁，并且只能体现在事中环节，事前威胁和事后溯源都不能完全体现。

金融行业的网络安全人员在面对 APT 攻击时各个安全系统产生的大量告警数据不能进行统一的呈现，告警产生海量的数据会形成信息孤岛。网络安全人员对整个网络被攻击的发展态势不明了，响应措施往往不够彻底并且滞后。如果攻击再次袭来，网络安全人员只有被动做出无效响应，如此循环，机构内部的网络安全防护就形同虚设，投入的人力、物力、财力也相当的昂贵。

2.痛点及需求

目前以 APT 攻击为代表的高级未知威胁给金融机构的网络安全带来全新的挑战，通过长期潜伏金融机构的重点部门，收集情报，获取重要数据，并长期潜伏，重点部门所有终端需要面临的风险也越来越大，本期建设主要围绕安全咨询和终端安全开展，用户的主要关注点在于：

1. 边界防御体系面对 APT 攻击存在被绕过的风险

网络边界部署防火墙和 IPS/IDS 是必要的，但是远远不够的。通过分析攻击链可以知道，黑客绕过防火墙等边界防护设备后，在内网还会进行长期而且危害巨大的潜伏及窃密活动。而这些恶意活动，边界防护设备是根本无能为力的。

2. 传统终端安全检测单一，APT 攻击难以发现

依靠特征检测曾经是终端安全的首选，但是深入内网的 APT 攻击让这些技术手段也束手无策。APT 攻击由于有巨大的利益驱动，所使用的技术和利用的漏洞都是非常先进的，一般安全厂商根本无法捕获样本，因而采集不到这类威胁的特征。所以，传统的终端安全无法应对未来的挑战。

3. 海量威胁告警数据，但难以溯源完整事件

一次 APT 攻击通常分为很多步骤，也会持续较长时间。一次成功的 APT 攻击会让很多安全系统产生大量告警，包括防火墙，IDS/IPS，终端安全软件等，而且告警的维度也相当多，IP、域名、文件 MD5、签名、注册表、流量等等都有可能触发告警。如果任由这些来源的告警全面展示给管理员，让客户进一步落实确认告警的工作是不切实际的也是不负责的。

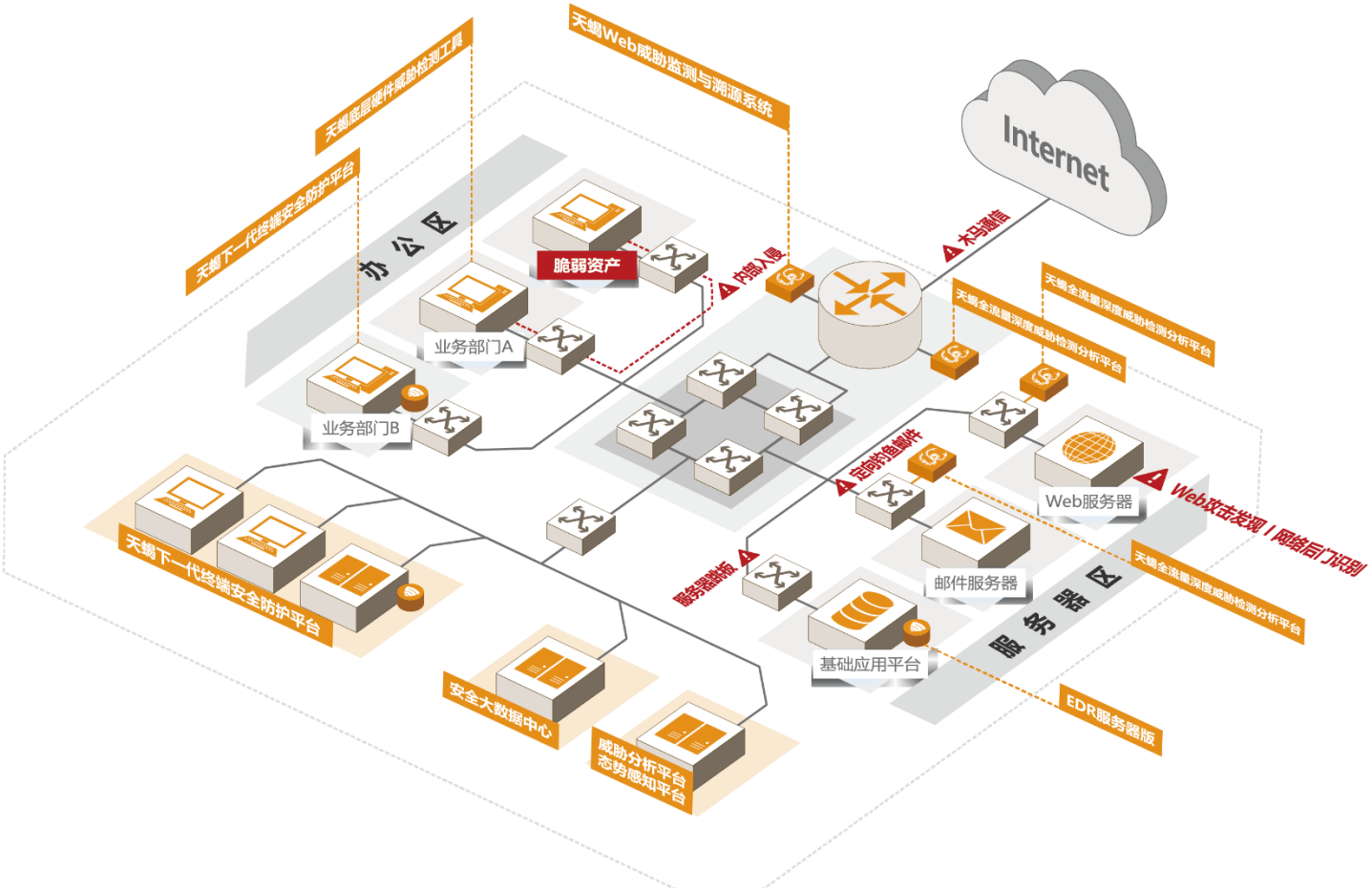
4. 面对高级未知威胁，应急响应低效滞后

金融行业都很注重网络安全方面的投入，但是很多情况下，往往在危害已经产生了，响应团队才会加班加点地去处理问题，而且由于对整个网络的态势不明了，响应的措施往往也不彻底。如果攻击再次来临，又要等到危害产生才再一次的去做无效响应。如此循环，安全方面的防护就形同虚设了。

行业需求：

1. 监控要实时：对网络中的数据和行为进行实时监控和分析。在第一时间发现威胁，就可以把攻击造成的危害降低到最小。
2. 态势要清楚：对网络的状态和趋势要能够看得到，网络的流量趋势、主机数量规模、有哪些程序在运行、一般的网络行为是怎么样的。
3. 信息要关联：孤立的信息其实是无效的、重复的，以至于不能很好地利用。响应团队在定位攻击时，其实就是从各个系统查询数据并将信息关联起来，这不但会解放安全团队的生产力，也能更大限度地发挥所有安全设备的作用。
4. 响应要彻底：应急响应工作的目的是定位攻击威胁，解决安全问题，阻止危害继续扩大。但是不彻底的应急响应工作会导致攻击很快卷土重来。企业需要拥有事后处理的能力和技术。
5. 操作系统要安全：当前 Windows7 已停服，标准版 Windows10 不符合国家安全需求，采用安全可控的 Windows10 神州网信政府版桌面操作系统，是保证操作系统安全的第一层屏障。

3. 解决方案



一期方案	二期方案	三期方案	四期方案
安全服务	天蝎Web威胁监测与溯源系统	安全规划及驻场服务	APT威胁感知系统 多引擎扫描分析系统（Robin） 天蝎下一代终端安全防护平台
• 安全监控值守 • 威胁情报共享 • 风险评估 • 信息安全应急响应 • 渗透测试 • 安全加固 • 安全宣传培训 • 入网安评	• 在发生网络调整系统升级扩容新系统上线等变更时，进行评估，给出明确的、可实施的安全建议及建设规划，配合相关安全工作开展。 • 在日常工作中，协助安全人员开展定期的自查评估工作，设备或系统上线时实施上线前的安全评估和反馈相关的制度、规范和流程的落实情况。 • 保障日常工作中的网络安全。 • 应急响应及安全事件分析。 • 对重要系统（网络安全整合平台）进行协助运维。	• 建立信息安全防御基础，实现针对企业整体的安全技术规范。 • 对高难度的威胁分析工作进行指导，并根据分析结果验证架构的可行性。 • 7*24小时对网络安全设备进行监控。事前的监测预警、事中定位及应急处置、事后能够安全审计、日志分析、追踪溯源。 • 在用户网络发生变更时，进行评估，给出明确的、可实施的安全建议。 • 对网内的疑似恶意代码进行分析和评估，快速通过技术工具和人员分析准确定位在主机及系统中的恶意代码和木马，并迅速提出解决方案。 • 通过黑盒子测试的方式验证系统的脆弱性并提出解决方案；配合网络安全主管部门和金融监管机构的监管审计。	围绕下一代终端安全防御目标，完善对服务器等终端的高级恶意代码的检测，针对终端的异常连接、进程、指令等异常服务进行重点监测。同时，借助之前阶段的安全经验，形成适合用户实际环境的安全防范体系、安全策略，初步形成终端层的大数据分析和疑似攻击分析能力，为后续的安全防护提供可靠支持。同时推进原有安全产品的安全信息的集中，打通应用、网络和系统各层安全事件。建设以安全信息为主的大数据平台原型，形成符合企业应用的安全分析模型。

4.客户认可的价值

- 通过初期阶段的技术服务和定向培训，优先排查出机构内部系统普遍存在的安全问题，并根据现网发生的安全事件以及针对银行系统的脆弱性分析，进行安全策略调配，安全设备调优，强化机构网络系统在实际环境中的安全防御能力。
- 通过用户实体行为分析技术（UEBA）实现自动化的建模，将多个异常活动相互关联，分析检测机构内部网络的多种高级威胁，以实现对网络中已知和未知威胁的检测。
- 通过对终端活动的持续性监测和记录，可以让安全人员获得对抗攻击者的关键优势，转被动为主动，从而使安全人员重新掌控其局势，并将记录的数据作为威胁溯源的佐证。
- 通过对所有信息系统及安全设备进行定期安全监控，及时发现并解决安全问题。
- 实现了金融企业系统以及网络安全环境的优化。完成了企业在应用层的安全监管问题，加强了网络入侵方面的检测；准确判断威胁事件的发生时间、来源、以及攻击行为是否成功等。
- 开展特殊重点时期信息安全保障工作，保证了安全设备、信息系统稳定、安全运行。
- 通过专业的渗透测试手段能更直接地展示企业信息系统安全现状，通过全方位的搜集、检测、发现敏感信息、实验、攻击等措施，尽可能地突破现有安全防范体系，获得对信息的越权操作。实现了安全监控加强及评估加固，保证业务系统的连续性、安全性。
- 紧急响应企业网络被入侵事件，在指定时间内响应或处理紧急安全事件，包括黑客攻击、故障查因、事件跟踪等，使公司网络信息系统在最短时间内恢复正常工作。
- 在发生攻击或环境事件时，保证了关键基础设施所支持功能的业务连续性。 提高了企业的网络安全防御体系的网络安全感知能力，并通过各种宣传方式和手段加强了员工的安全意识。

- 通过专业的培训提高业务人员、运维人员的安全技能和意识，以此来完善整体安全解决方案的基础设计工作，为后期的安全建设提供宝贵经验。
- 解决机构内部应用系统的高级恶意代码攻击、威胁溯源、应急响应等急迫问题，利用已有的技术平台提升应用系统的监测服务能力。