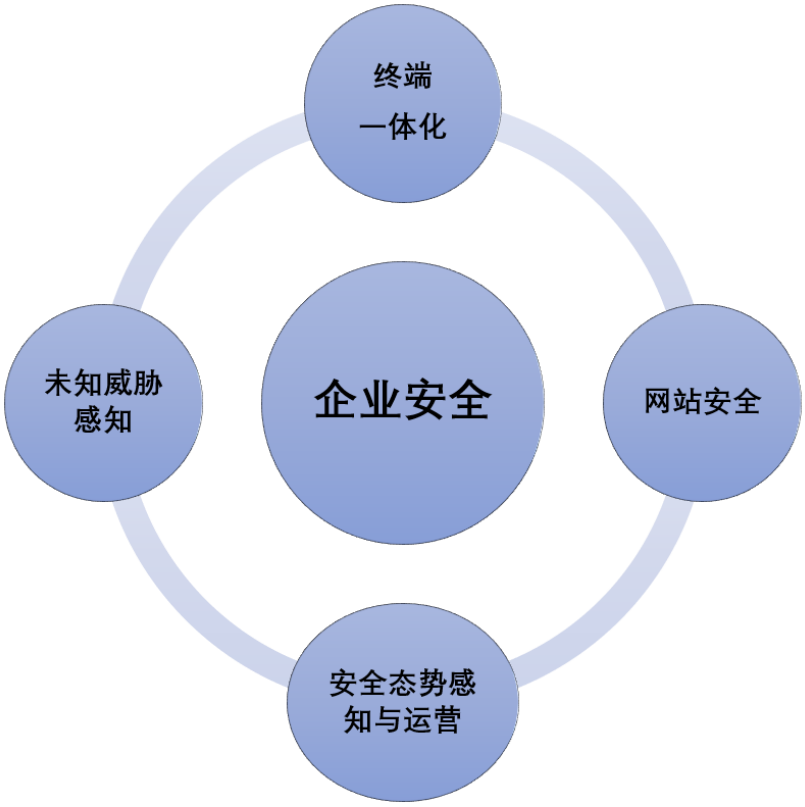
# 大型企业整体安全解决方案

在当前信息安全已经上升到国家安全层面的形势下，来自国外具有国家背景的攻击者已经针对多家央企，通过免杀、鱼叉、水坑攻击等新技术手段进行高级可持续性攻击。然而大量未知威胁攻击手段可以绕过以特征检测为核心检测手段的传统安全防护设备，企业难以有效发现未知威胁，也就无法抵御未知威胁，如何检测未知威胁成为企业面临的挑战。

奇安信集团提出的解决思路即以数据为核心取代以技术为核心，以云端分析取代设备分析，以情报线索取代技术对抗，并提出了一套完善的安全解决方案，包括终端一体化、未知威胁感知、网站安全、安全态势感知与运营等，来提升企业网络安全能力，主要包括以下几个方面。




一是提升终端安全管理能力。全集团集中部署天擎终端安全管理系统，并结合Windows 10 政府版的安全可控操作系统，建设统一防病毒体系、统一计算机安全管理体系；利用管理和技术有效结合，可以完美解决终端系统所面临的病毒、恶意软件、补丁缺失、配置不规范问题，保障全集团的终端安全。

二是获得未知威胁感知能力。通过部署天眼未知威胁感知系统，通过进行云端大数据计算和挖掘，结合专家分析所形成的威胁情报数据与本地流量进行关联分析，最大限

度地发现企业内未知威胁，从而使企业获得一般企业所不具备的未知威胁感知能力，使企业的安全检测能力处于行业领先地位。

三是具备安全态势感知能力。部署安全态势感知与运营系统将能使企业管理人员能够准确和直观的了解集团安全态势，集团信息安全状况一目了然。

四是极大提高网站综合防护能力。安域云安全防护平台集成了网站加速、安全监控、云 WAF、抗海量 DDOS、抗 CC、DNS 防护、WEB 攻击防护等，可以为企业建立一套完整且功能强大的网站安全防御体系，极大提高网站的综合防护能力。

五是具有安全溯源能力。当发生安全事件后，可以快速对历史流量数据进行检索，结合云端的海量互联网数据进行多维可视化关联，快速定位攻击、还原攻击路径和追溯攻击者，从源头上控制安全风险，降低攻击再次发生的可能性。