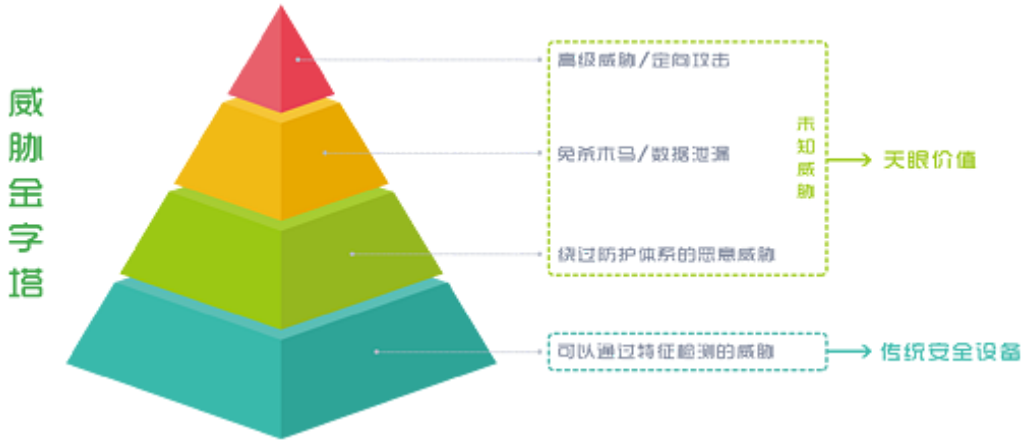
产品简介

360天眼新一代威胁感知系统（SkyEye，以下简称天眼系统）是新一代高级威胁定位发现产品，可为政府、金融、能源、运营商、大型企业等客户提供未知威胁的发现、分析与溯源功能。天眼系统可对本地流量进行全量还原、存储与深度分析，从流量、文件以及终端日志多个维度，结合360云端大数据平台与威胁情报中心推送的专属威胁情报，快速发现高级威胁与定向攻击等恶意行为，并对受害目标和攻击源头进行精准定位。



产品功能

云端持续分析

360能够基于云端多年积累的互联网海量安全基础数据，通过数据挖掘、机器学习等人工智能算法和持续的安全专家运营对互联网全网每天新增的新型木马、流行木马甚至是高级定向威胁（APT攻击）进行发现和跟踪。所有分析结果都将以可机读威胁情报（MRTI）的形式单向推送至客户处的天眼系统中。

本地实时发现

天眼系统可通过一整套本地硬件系统对企业网络流量进行还原与记录，并能接入360天擎的终端行为日志，使用传统检测引擎+人工智能引擎+虚拟执行检测引擎的多引擎检测架构，架构通过动静态检测、漏洞利用检测和大数据技术发现异常网络流量、恶意行为和文件威胁，并结合360云端的威胁情报进一步发现企业内网的高级威胁。

威胁精准溯源

利用云端丰富的实时威胁情报和企业本地翔实的网络行为、终端行为、文件信息，天眼系统可以为企业客户呈现一次攻击的完整过程，它将覆盖攻击的源头、手段、目标、范围等相关信息，可对被发现的未知威胁进行快速溯源和定性，并轻松分辨高级威胁和普通网络攻击。

特色价值

多维度威胁检测

企业客户使用天眼系统后可直接获得天眼的多维检测能力，其检测能力将涵盖网络异常行为检测、漏洞利用检测、虚拟执行检测、终端行为检测、威胁情报关联检测、大数据分析等多个层面。多种技术相互交织形成一个多维度立体防护体系，对流量、文件和终端实现威胁发现的全覆盖。任何一次可疑行为均会触发整个防护体系的多维检测机制，多种检测技术将分别在各自层面输出检测结果，最终形成综合性结论。使用多维度检测技术，天眼系统可进一步提高未知威胁发现成功率，降低威胁告警的误报率。

数据驱动安全

360天眼系统创新的将大数据技术应用于威胁发现领域，在云端通过多纬度跨域分析、深度数据挖掘、可视化分析和人工智能技术，对海量数据进行深度分析以实时获知未知威胁的发展动态。为支撑相关分析，360云端威胁情报中心使用了超过1EB的数据资源，其中包含近百亿样本、数万亿主动防御日志、数十亿域名解析记录以及各类恶意行为相关的漏洞、网址、域名等信息，且所有数据均实时更新。云端所有数据分析成果都将以可机读威胁情报的形式推送到企业侧，再结合天眼系统的高速数据计算能力，可对数以千亿的日志进行快速分析，帮助企业客户发现并定位未知威胁。

全面的数据采集

在企业客户本地，天眼系统可通过高性能硬件设备对各类常用流量协议进行解码和还原，同时针对未知协议进行有效发现，对流量中的关键信息进行截取与存储，确保所有的流量行为、网络访问行为、邮件行为、文件传输行为都在天眼系统的监管之下，帮助客户获取高价值安全数据。同时天眼系统可结合360天擎终端安全管控系统，对客户端行为进行采集记录。全面的网络和终端行为可以保证任何一次恶意活动都无法逃脱天眼系统的检测，并能支撑整个安全事件的取证、溯源工作。为保证数据采集和存储的全面性，天眼系统还可支持采集点的分布式部署和存储计算能力的水平扩展。

使用场景

天眼系统可以轻松部署于企业网络的任何位置，对网络流量进行解析和记录，也可以通过在客户端部署的天擎终端安全管控产品，对客户端日志进行采集记录。同时天眼系统可分析本地采集到的所有信息，并结合来自360威胁情报中心的可机读威胁情报，快速发现企业内部的未知威胁。

产品介绍