大数据技术

集群+动态扩容

系统采用大数据技术设计，支持集群方式部署，存储集群高可用，可以无限扩展存储节点，扩展存储空间，容灾能力强、具备自动发现集群设备、无需停机

采用业界标准技术

通过授权访问，既保障了保障数据不被厂商绑定，又保障了数据的安全性

大数据检索技术

采用大数据全文检索技术，索引分布式存储，分布式并行查询，类似自然语言，方便使用、快速发现问题

海量数据存储

不仅可存储各类日志信息，对于产生安全问题的原始数据包也能存储并下载

精准解析

利用网络流量分析探针，解析各类主流网络协议，如HTTP、DNS、SMTP等，对相关元数据可进行查询和分析

开放的自有标准化语法解析器，灵活度高、精确度高、快速自定义标准化解析

内置了大M的标准化脚本，适应各类主流设备和系统的精确解析

精确分析

关联场景：基于统计和基于关联

基于统计包含：平均统计、方差统计，支持按天、按周统计，智能机器学习

基于关联包含：状态关联、时序关联、归并关联、筛选关联、端口关联

多维度关联

支持事件与基线关联分析、事件与漏洞关联分析、事件与事件关联分析

丰富展示

丰富的图形化展示：仪表板、业务拓扑图

用户自定义仪表板展现业务数据

实时监控：便于发现异常、随时挖掘分析

热图分布：追踪攻击来源，发现幕后黑手

完整的动态安全问题发现和防御体系

系统可选内置网络流量探针，此处无需第三方提供支持

系统内置了漏洞扫描、基线检查等模块，主动检查，及时加固

通过日志与漏洞等关联分析被动防御，发现威胁，抵御风险