**<FR ## 智·源规划>  
Mini Product Requirements Document**

Product Description（产品描述）

本文档主要阐述 智·源 数据分析平台规划Roadmap Phase1的定义及功能需求规划。

Reviewers （文档审批人）

|  |  |  |
| --- | --- | --- |
| Department （部门） | Name（姓名） | Approval Date（批准日期） |
| PPC （Product Planning Committee） |  |  |
| PPC （Product Planning Committee） |  |  |
| PPC （Product Planning Committee） |  |  |
| PPC （Product Planning Committee） |  |  |
| Marketing （市场） |  |  |
| Marketing （市场） |  |  |
| Marketing （市场） |  |  |
| Software （软件） |  |  |
| Software（软件） |  |  |
| Software（软件） |  |  |
| QA（测试） |  |  |
| QA（测试） |  |  |
| CTO Office |  |  |
| CTO Office |  |  |
| SE （售前） |  |  |
| TAC（售后） |  |  |
| Documentation（文档） |  |  |

Modification History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision | Date | Author | Comments |
| 0.5 | 08/05/19 | Bin Zheng | Create |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Reviewers （文档审批人） 1](#_Toc513557851)

[Modification History 1](#_Toc513557852)

[1 名词解释 4](#_Toc513557853)

[2 Market Analysis（市场分析） 5](#_Toc513557854)

[2.1 市场背景 5](#_Toc513557855)

[2.2 市场发展趋势 6](#_Toc513557856)

[2.3 市场产品品类 6](#_Toc513557857)

[3 Customer analysis（客户分析） 7](#_Toc513557858)

[3.1 概述 7](#_Toc513557859)

[3.2 政府行业 8](#_Toc513557860)

[3.3 教育行业 8](#_Toc513557861)

[3.4 金融行业 9](#_Toc513557862)

[3.5 大型企业客户 9](#_Toc513557863)

[3.6 行业需求汇总 10](#_Toc513557864)

[4 Competitive Analysis（竞争分析） 11](#_Toc513557865)

[4.1 概览 Summary 11](#_Toc513557866)

[4.2 深信服 Sangfor 12](#_Toc513557867)

[4.3 360 Enterprise Security 12](#_Toc513557868)

[4.4 华三通信 H3C 13](#_Toc513557869)

[4.5 安恒 DbAppSecurity 13](#_Toc513557870)

[4.6 Checkpoint （海外） 14](#_Toc513557871)

[4.7 FireEye （海外） 14](#_Toc513557872)

[4.8 竞品分析汇总 15](#_Toc513557873)

[5 Objectives （目标） 15](#_Toc513557874)

[5.1 规划战略目标 15](#_Toc513557875)

[5.2 P1 阶段总体目标 16](#_Toc513557876)

[5.2.1 数据分析平台愿景 16](#_Toc513557877)

[5.2.2 部署场景 16](#_Toc513557878)

[5.2.3 组件架构 17](#_Toc513557879)

[5.3 智·源 RoadMap 17](#_Toc513557880)

[5.4 Expected FCS Dates （正式发布预期） 18](#_Toc513557881)

[6 Functional Requirements（功能需求） 18](#_Toc513557882)

[6.1 Performance and Capacity Requirements（平台性能和容量需求） 20](#_Toc513557883)

[6.2 板卡定义 20](#_Toc513557884)

[6.3 WebUI or CLI Support（WebUI 和CLI需求） 20](#_Toc513557885)

[6.4 License定义 21](#_Toc513557886)

[6.5 Documentation（文档需求） 21](#_Toc513557887)

[6.6 Training Programs（培训计划） 21](#_Toc513557888)

[7 Regulatory Certifications（认证需求） 21](#_Toc513557889)

[8 Known Issues/Risks（已知问题和风险） 22](#_Toc513557890)

[9 Packaging Requirement 22](#_Toc513557891)

[9.1 Hardware Packaging 22](#_Toc513557892)

[9.2 Software Packaging Requirements 22](#_Toc513557893)

[10 Beta Sites（外部客户试用） 22](#_Toc513557894)

# 名词解释

中文名称：山石 智·源 — 智能数据分析平台

英文名称：Hillstone – Data Analysis Center

系列名称（SKU）：

CLI默认主机名称：

WEBUI默认主机名称：

Product Name：

版本编译名称：BDS-iSenor-BaseVersion-产品线版本.bin

（其中BaseVersion 表示该产品线基于StoneOS的版本 比如:5.5R1 R/P版本:

产品线版本 = 两位数字，用'.'分开 比如:1.0 完整的image名称: BDS-iSensor-5.5R1-1.0.bin）

BDS- B（Edge Security）边界安全

中文名称：山石 智·感 — 智能数据分析平台

* 联动设备名称：

BDS（Breach Detection Systems）威胁检测系统

BDS-I（Core Security）内网安全

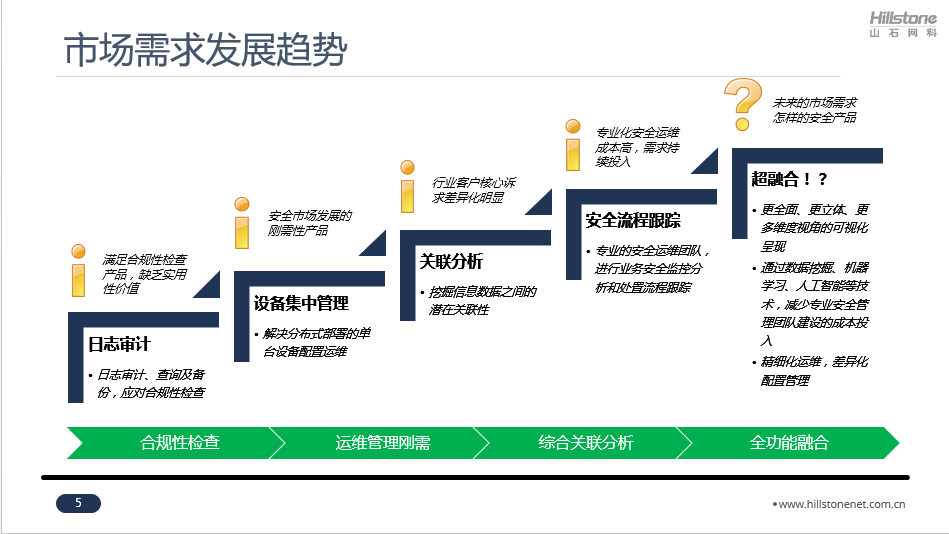
# Market Analysis（市场分析）

## 市场背景

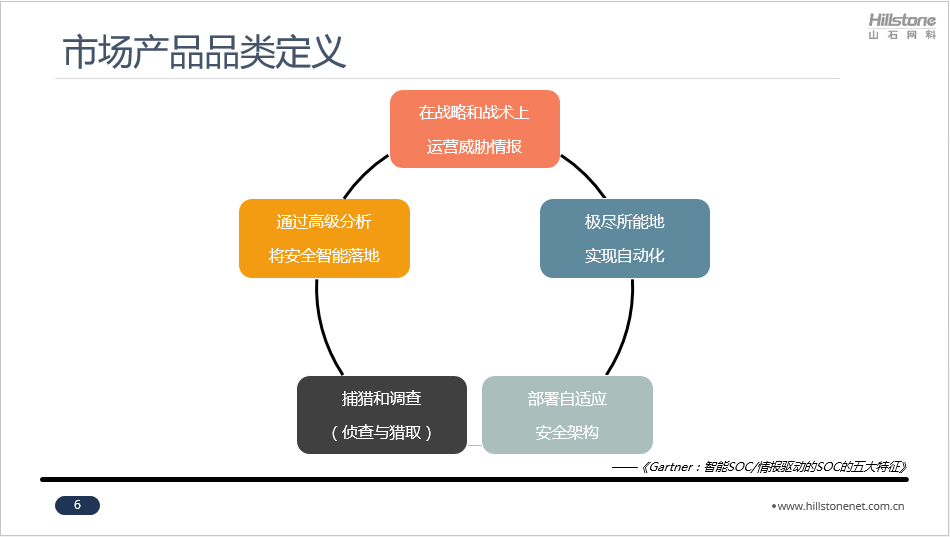


1. 政策导向： 树立网络安全全局观，综合态势能力呈现
2. 技术趋势： 基于分布式，AI技术的海量数据分析，能提升综合安全防护能力
3. 运维能力递进： 更加精细化管理，敏捷，便捷，低成本的运维
4. 安全联合防护： 解决信息孤岛

## 市场发展趋势

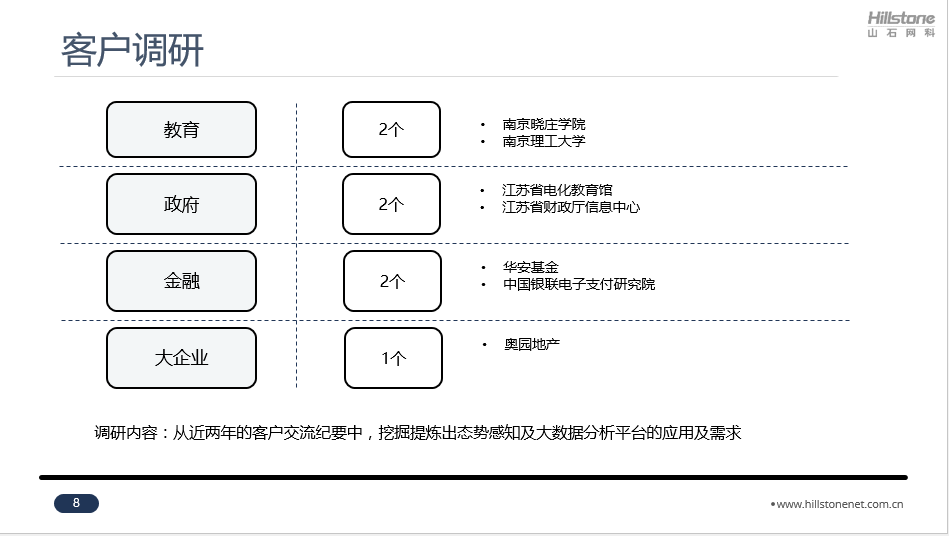


## 市场产品品类

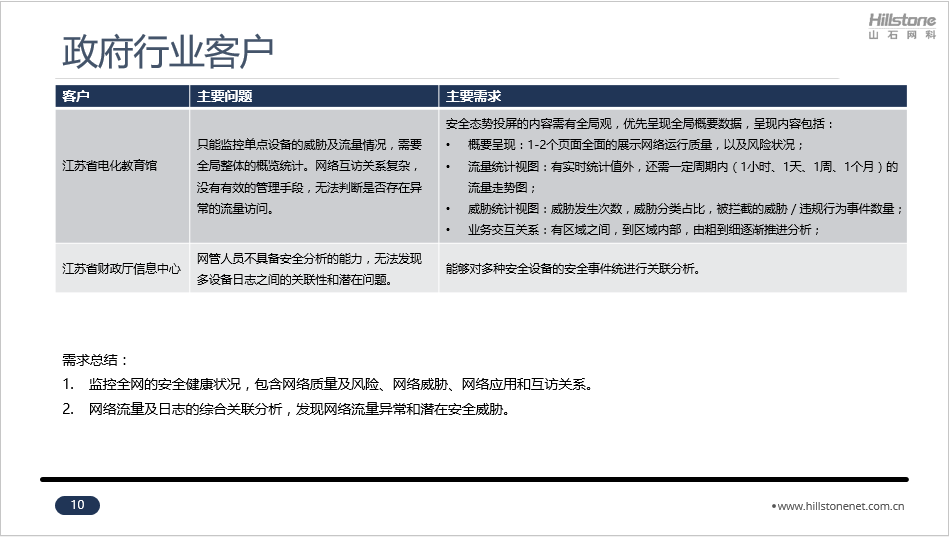


# Customer analysis（客户分析）

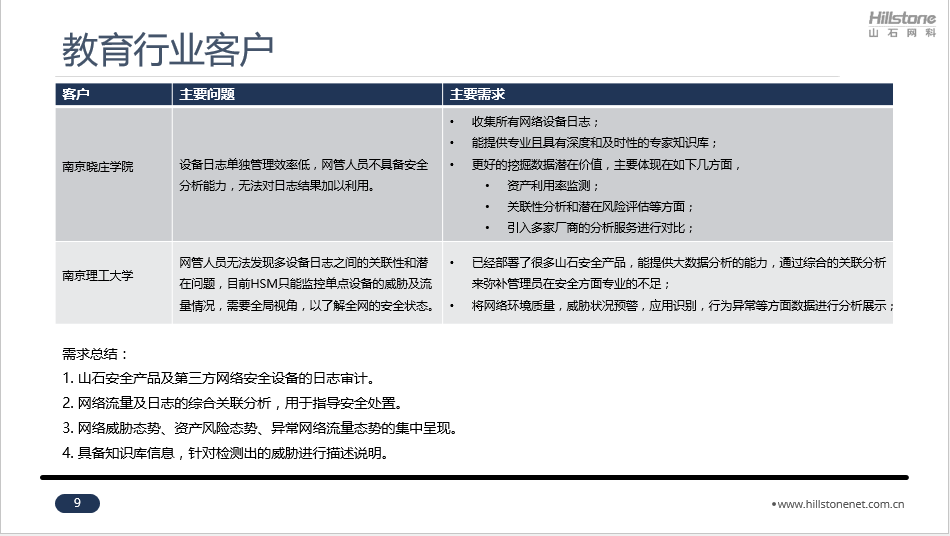
## 概述



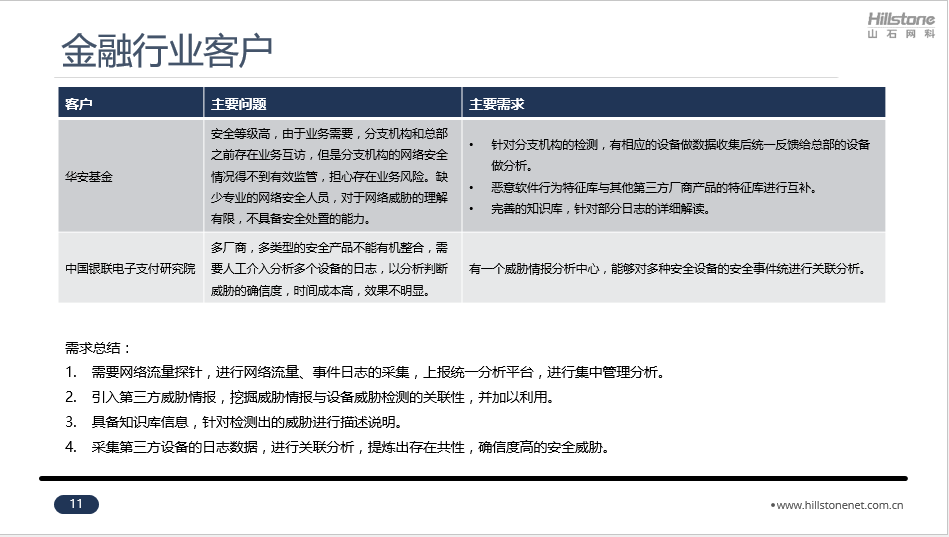
## 政府行业



## 教育行业



## 金融行业



## 大型企业客户



## 行业需求汇总



**主要功能需求总结：**

* 教育、政府、金融和大型企业在网络安全态势的集中呈现和流量、日志、事件的综合分析方面都存在强烈需求。
* 在日志集中管理、单点设备监控和第三方威胁情报方面的需求程度不一。

**行业需求目标总结：**

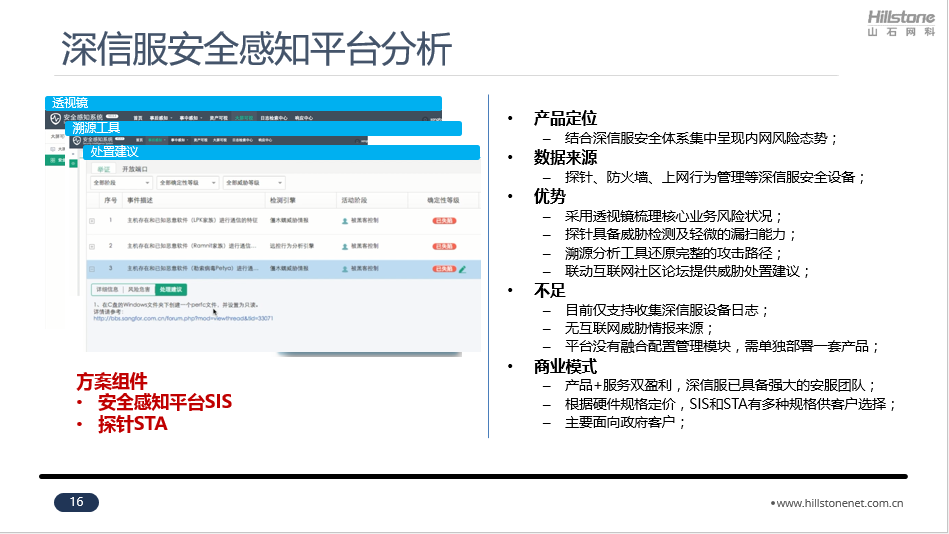
* 教育行业主要结合自身情况进行整体网络安全的建设，部署刚需性安全产品。
* 政府行业主要以政策法规为引导，满足网络安全建设的合规性。
* 金融行业网络安全等级最高，愿意使用新概念、新技术类型的产品，但是看重实用性和时效性，同时也要满足合规性检查。
* 企业成本控制严格，只考虑刚需性安全产品，看重产品所能体现的实用价值。

# Competitive Analysis（竞争分析）

## 概览 Summary



## 深信服 Sangfor



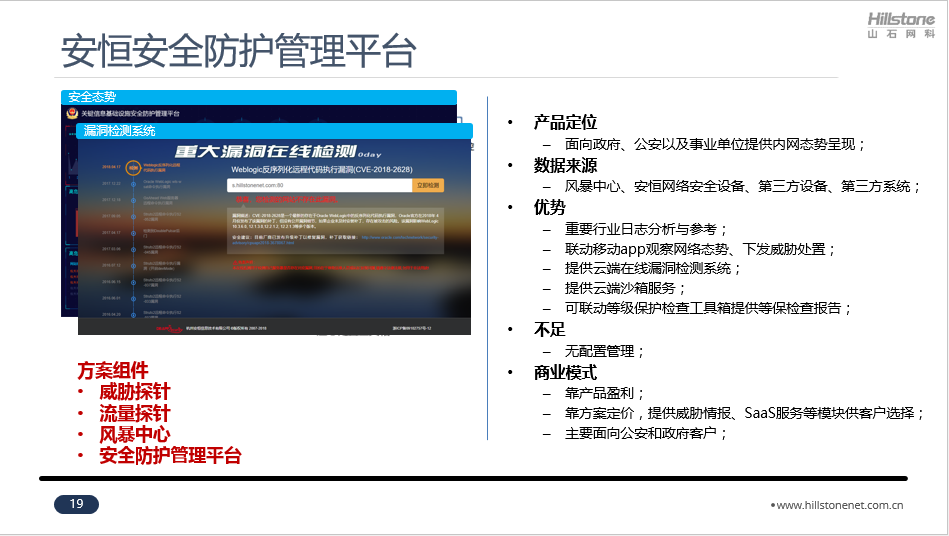
## 360 Enterprise Security



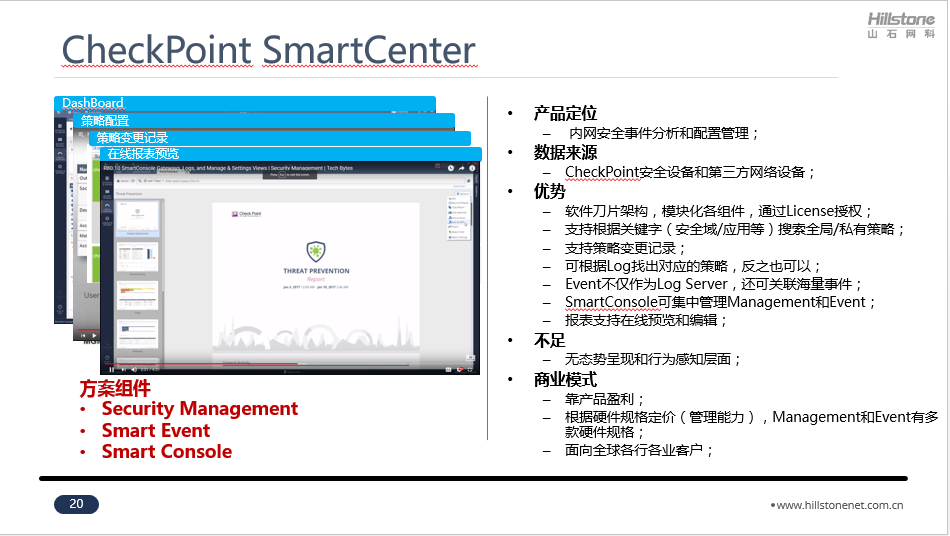
## 华三通信 H3C



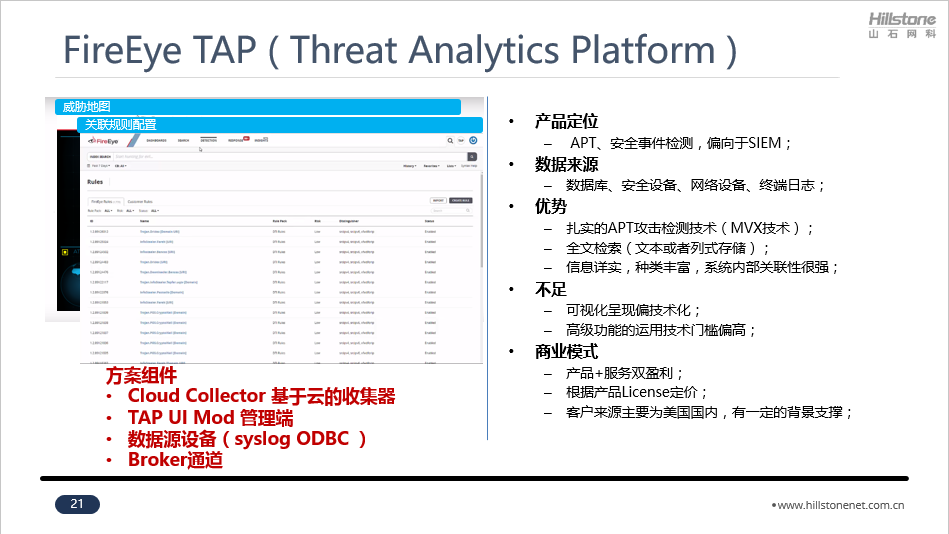
## 安恒 DbAppSecurity



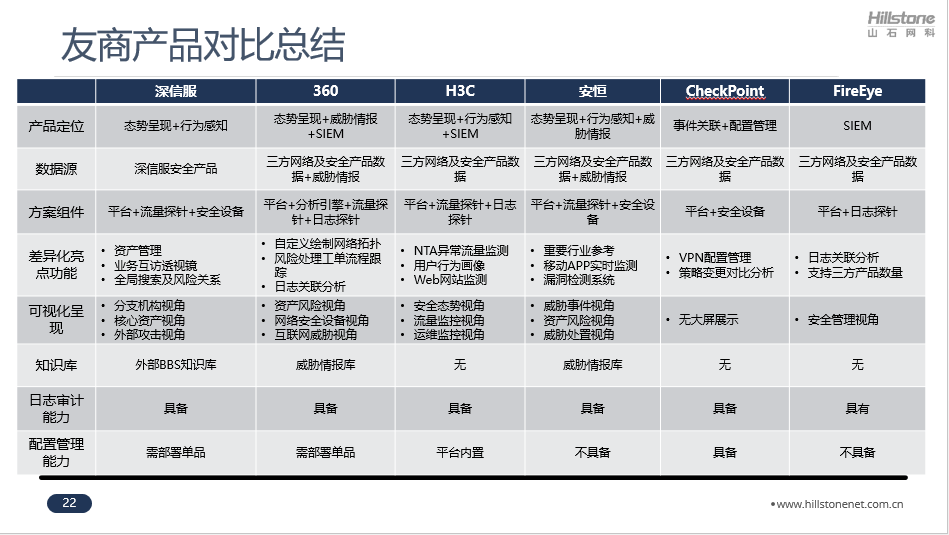
## Checkpoint （海外）



## FireEye （海外）



## 竞品分析汇总



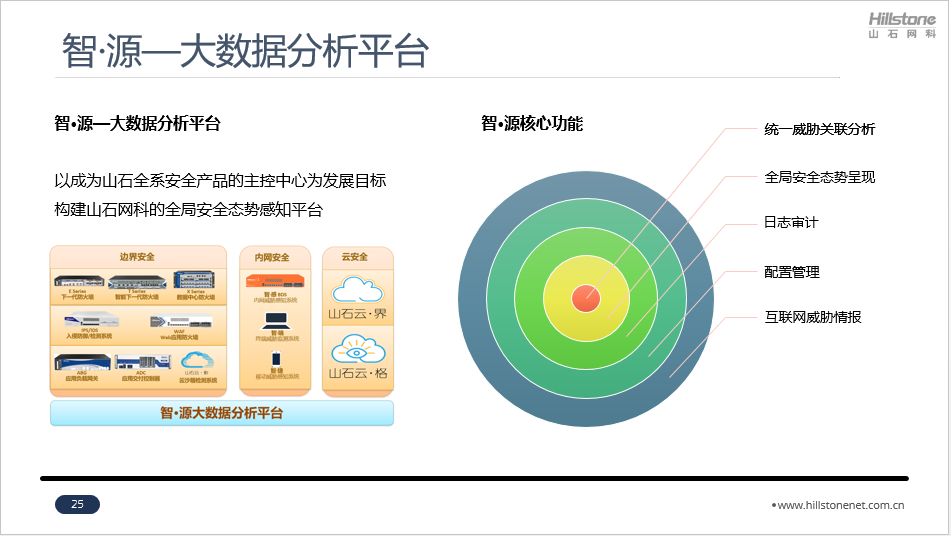
# Objectives （目标）

## 规划战略目标

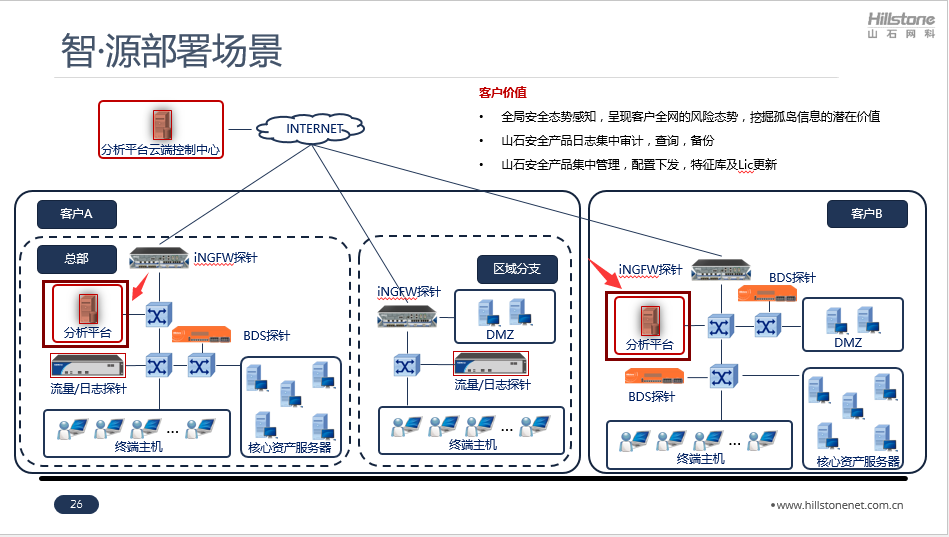
* 关联分析： 行业客户核心诉求，挖掘信息数据之间潜在关联性；
* 进阶运维：持续的降低运维成本，通过过滤计算有效数据，监控分析与处置流程；
* 集中管理： 融合HSM的设备集中管理能力，解决分布式部署单台设备配置；
* 日志审计： 融合 HSA 的日志审计能力，解决审计，查询，合规能力 ；

## P1 阶段总体目标

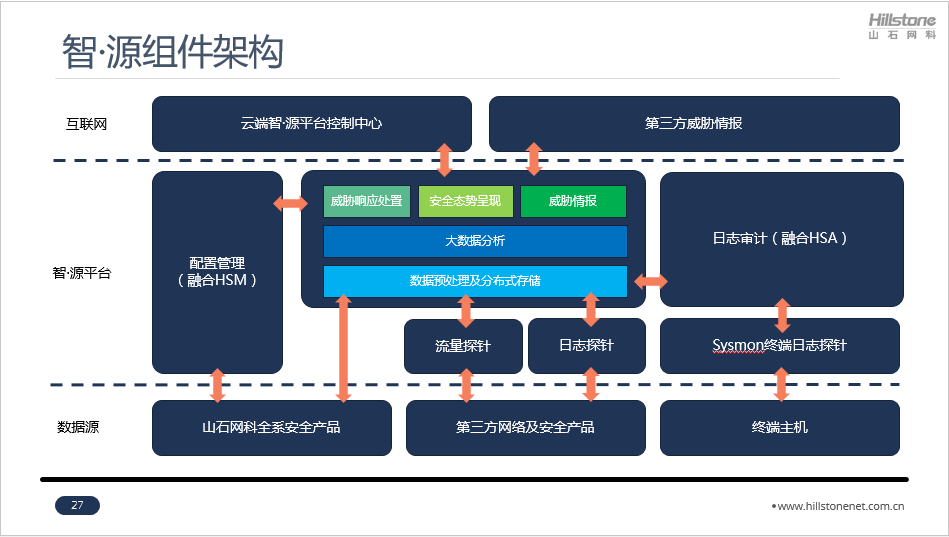
### 数据分析平台愿景

* 

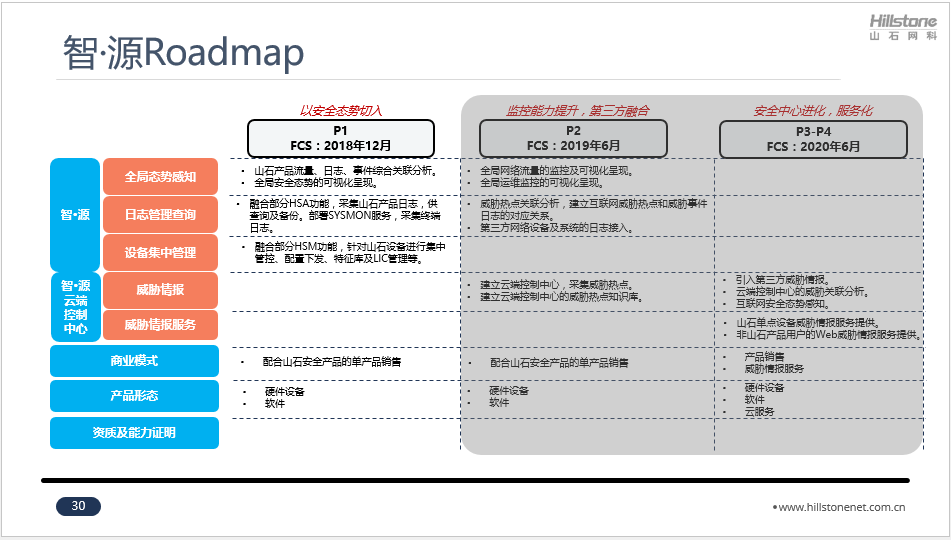
### 部署场景



### 组件架构



## 智·源 RoadMap



本次涉及的版本是 P1 阶段。

## Expected FCS Dates （正式发布预期）

EC： 2018年10月31日

Beta：2018年11月30日

FCS： 2018年12月31日

# Functional Requirements（功能需求）

BDS（违规检测系统）整体规划主要分为BDS-I（Core Security）内网安全和BDS- B（Edge Security）边界安全两部分：

其中R1版本（Compass）推出BDS-I，BDS-I通过智能安全的ABD、ATD、Killchian、iCenter实现，并遵循以下原则：

1.  BDS的定位是边界威胁防护和内网威胁检测，其中BDS-B定位于边界防护，BDS-I定位内网威胁检测。

2.  BDS-I部署在内网，但仍然需要支持串接模式，支持简单的Block IP控制，进行可确认威胁的拦截。

3.  安全策略裁剪掉，因此无法实现恶意URL过滤的功能，后续根据需求整合基于Zone配置的URL过滤。

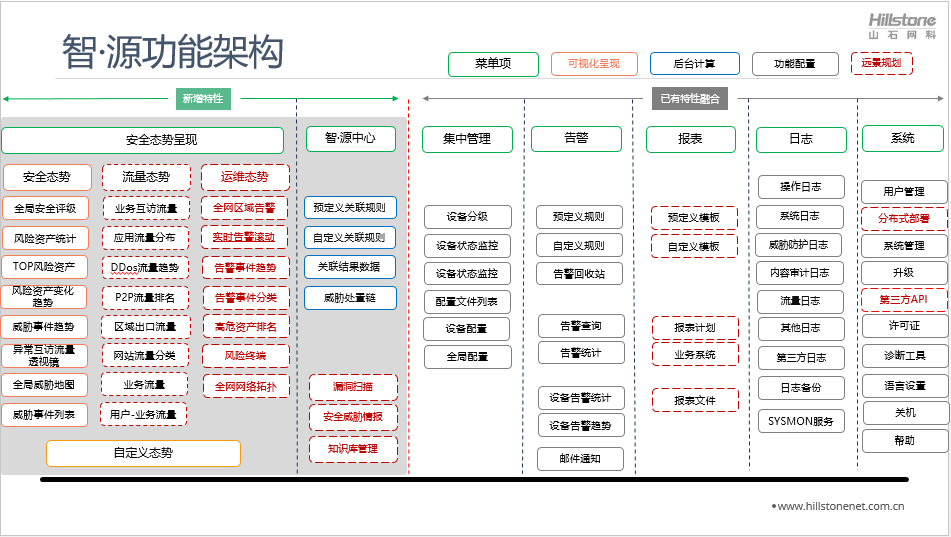
4.  其他控制需求如主机应用行为控制的功能，由于安全策略裁剪掉，无法基于Zone实现多维度的主机行为控制，根据后续需求，通过联动NGFW进行实现。

5.  BDS-I支持零配置旁路部署，出厂配置即插即用。配置如下

|  |  |  |  |
| --- | --- | --- | --- |
| 接口 | 安全域 | 安全域配置 | 其他配置需求 |
| Eth0/2 | Tap | 高级威胁检测：开启  异常行为分析：开启 | * 初始预置常规地址薄，用于识别内网风险主机 * 默认开启ABD、ATD检测引擎 |

其中R2版本（Wrangler）推出BDS-B，BDS-B则通过OEMin沙箱进行规划。

## 智·源功能架构



补充描述：

* 智·源是一个融合型的安全管理中心soc，融合已有的HSM设备集中管理特性，与HSA的日志审计特性为基础，并依靠多网元的数据，新增数据关联分析，数据态势呈现的功能。
* 近景规划： 已有特性的融合，以及态势呈现
* 中期规划： 融入第三方安全威胁情报能力，以及报表功能
* 远景规划： 安全运维，以及运维服务能力

### 详细功能结构表：

|  |  |  |  |
| --- | --- | --- | --- |
| **一级菜单** | **二级菜单** | **三级菜单** | **备注** |
| 首页仪表盘 |  |  |  |
| 安全态势 |  |  | 按Deefay 的设计实现 |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 系统 | 系统信息 |  |  |
| 设备管理 |  |  |
| 配置文件管理 |  |  |
| ~~SNMP~~ |  |  |
| 升级管理 |  |  |
| 许可证 |  |  |
| 邮件服务器 |  |  |
| 短信发送参数 |  |  |
| 系统调试 |  |  |
| 诊断工具 |  |  |

## 平台性能和容量需求Performance and Capacity Requirements

## 产品型号 Product Model Define

### 硬件 Hardware

|  |  |  |
| --- | --- | --- |
| **参 数** | **智·源 500** | **智·源 100** |
|  | 2U | 1U |
| **支持设备数量（最大）** | 500 | 100 |
| **存储容量** | 4T | 2T |
| **网络接口** | 2 \* 千兆电口 | 2\* 千兆电口 |
| **RAID** | RAID 5 | RAID 0 |
| **电源** | 单/双电源 495W | 单电源 250W |
| **外观尺寸(W × D × H, mm)** | 2U (440 ×520 × 88) | 1U（434x394x43） |

### 虚拟化 vSys

默认P1阶段不支持， 待进一步确定。

## WebUI or CLI Support（WebUI 和CLI需求）

默认无，待补充或可补充。

## 授权定义License

License定义及授权以时间维度、功能维度进行管理，具体实现方式如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **License类型** | **功能授权** | **时间授权** | **备注** |
| 出厂Lic | Hillstone Soc 全功能：   * 开启 日志审计与数据分析(hsa) * 开启 设备集中管理(hsm) | 30天 |  |
| 试用Lic | Hillstone Soc 全功能：   * 开启 日志审计与数据分析(hsa) * 开启 设备集中管理(hsm) | 90天 |  |
| 正式Lic | Hillstone Soc 全功能：   * 开启 日志审计与数据分析(hsa) * 开启 设备集中管理(hsm) | 1~5年 | License销售 |

## 文档需求Documentation

数据分析平台：

* 产品主打胶片（用于给用户/代理商介绍整体价值）
* 安装手册
* 产品手册
* 用户手册
* DataSheet

## 培训计划Training Programs

* 智·源 安全大数据分析技术

*抛离防火墙概念，却分内网检测和边界防护*

* 智·源 产品功能培训

*学习掌握山石网科数据分析产品功能，及优劣势*

# Regulatory Certifications（认证需求）

暂无

# Known Issues/Risks（已知问题和风险）

# Packaging Requirement

## Hardware Packaging

## Software Packaging Requirements

# Beta Sites（外部客户试用）

End of Document