序号	**BYoneV2.0 功能菜单**
1	**功能：**首页 **说明：**以图表的形式展示资产，网络，云，安全，告警几大块的概要和统计信息，支持动态的删减概要和统计信息。 **子菜单：** “资产”- 包括资产的可用性，性能，变更，安全，告警等方面的统计图表； “网络”- 包括网络的可用性，性能，变更，安全，告警等方面的统计图表； “云”- 包括云的可用性，性能，变更，安全，告警等方面的统计图表； “安全”- 安全事件数趋势图，安全事件类型统计图，安全事件严重等级统计图，安全事件源统计，安全事件目标统计，资产的安全风险等级统计，安全事件影响统计，安全事件预测，地理位置信息，实时安全事件显示表； “告警”- 告警数趋势图，告警类型统计图，告警严重等级统计图，告警设备/资产统计图，告警处理情况统计图，告警通知情况统计图，告警趋势预测，告警实时显示表等。
2	**功能：**资产管理 **说明：**资产管理是以 CMDB（配置管理数据库）为核心，以可视化的方式管理资产的属性（硬件，软件，接口，位置信息，重要等级，负责人等），资产的健康状况，资产的可用性，性能，变更，风险等级，告警等。 **子菜单：** “资产可视化浏览”- 以图表的形式浏览资产基本属性，资产健康状态，可用性，性能负载情况，相应的告警情况及与告警相关的事件信息，配置变更情况等； “资产配置”- 可配置资产的名称，类型，版本，重要程度，联系信息，地理位置信息，设定维护模式等； “变更管理”- 变更查看、查询，配置备份（定时，手动备份，导入导出备份）； “资产报告”- 包括概览，网络，服务器，虚拟化，与 BYoneV1.0 一致； “运维工具”- 提供方便的运维工具包括：ping, traceroute,browse,telnet,remote desktop 等；
3	**功能：**网络管理 **说明：**以可视化方式对网络相关方面：网络拓扑，设备可用性，性能，变更，接口流量，流数据，IP 地址簿，终端准入进行展示，分析，告警，管理。 **子菜单：** “概览”- 事件统计，告警数统计，告警事件统计，cpu,mem,intf 性能负载情况统计，配置变更事件，流数据分析，Down/Restart，丢包率，响应时间； “拓扑图”- 显示分主图和缩略图，主图与 BYoneV1.0 一致，主图部分新增告警数显示，缩略图显示拓扑全景并支持导航； 位置调整支持，可调整拓扑图元素的位置，并可保存； 打印支持，可支持拓扑图的打印； 编辑支持，可支持编辑节点或线路的名称； 基础操作包括：放大，缩小，分层显示，拖动； 搜索支持，输入设备名称或 IP 地址可在拓扑图上定位具体的设备及周边几台的设备的连接情况； 工具支持，可在拓扑图上直接使用以下运维工具：telnet, ssh, ping,traceroute 命令 “IP 地址簿”- 包括 IP 到设备的定位，IP 盗用监测，IP 地址使用情况统计，非法接入告警； “管理工具”- 包括 telnet, ssh, ping, traceroute 等工具。

4	**功能：**云管理 **说明：**将云和虚拟化纳入 BYoneV2.0，综合管理云虚拟化的架构，资源分配情况，服务运行情况，性能负载情况。 **子菜单：** “概览”- 虚拟化架构，资源分配情况，服务运行情况，性能负载情况 “虚拟化监测”- 总 CPU,Mem,Disk，CPU, Mem,Disk,Intf 接口使用情况，VM 名称，数量，启停状态等 “虚拟化服务监测”- 远程访问，监测虚拟化服务健康状态
5	**功能：**业务服务管理 **说明：**以业务的视角将设备，应用划分到不同的业务分组，从业务的视角监测整个业务的运行状态，KPI 指标，业务性能等。 子菜单： “业务设定”- 将设备，应用等划分到真实的业务分组中； “业务监测”- 业务的运行状态，KPI 指标，故障，告警，以及故障告警对服务的影响； “业务可视化”- 业务结构图，业务运行状态，使用情况； “业务模拟仿真”- 业务性能，负载模拟仿真测试，通过远程访问，ping 等进行测试。
6	**功能：**安全管理 **说明：**以基础告警为基础，采用基于规则的关联分析，基于情景的关联分析，基于行为的关联分析，动态基线技术，地址熵，热点事件分析，威胁态势分析等技术进行安全分析，同时采用风险评估技术对资产进行风险评估和管理 **子菜单：** “概览”- 安全态势（告警数，安全事件数），安全事件分类统计，组织、单位视角，告警源，目标，地理位置视角，风险视图，攻击视图； “脆弱性管理”- 脆弱性扫描（基础基础的扫描引擎：Snort, Rrd,Nmap,Nessus,Ntop） 第三方扫描（第三方扫描如 Nessus 结果导入分析） “风险评估”- 依据 ISO/IEC 27000 系列信息安全标准，以资产为核心，结合资产价值，脆弱性，威胁评级从而对风险进行评定，并给出相应的建议 “安全分析”- 欺诈检测（实时威胁检测，网络安全取证分析） 攻击分析（攻击识别，攻击路径识别，攻击路径回放） 态势分析（攻击态势，风险态势）
7	**功能：**告警管理 **说明：**告警管理包括可视化显示告警，告警响应方式，以及告警与工单系统的整合 3 个方面。 **子菜单：** “概览”- 告警数趋势统计，告警类型统计，告警严重等级统计，告警源，目标统计等； “告警列表”- 显示当前的告警列表，可指定条件进行过滤查询，同时可以显示触发告警的事件列表； “告警通知策略” – 配置告警以什么样的方式通知给到用户，通知方式包括：邮件，短信，微信，syslog,snmp trap 等； “工单系统”- 包括新建工单，工单过程记录，同时可以将工单处理结果转换成知识库。
8	**功能：**数据分析 **说明：**数据分析是对历史数据根据检索关键词或检索条件进行查询，统计，分析。数据分析分为 2 种模式：全文检索和条件检索

	子菜单： “全文检索”- 根据关键词对所有历史数据的查询 “历史搜索”- 根据条件对给定范围的历史数据进行结构化查询
9	**功能：**报表 说明：BYoneV2.0 默认提供资产，网络，云，业务，安全，告警 6 大块的报表模版，内容涵盖可用性，性能，变更，安全，告警等，用户也可以根据需求自定义自己的报表模版。 **子菜单：** “报表分类模版”- 按照说明中描述的 6 大块以树形结构的方式展示系统默认报表； “报表生成”- 支持手工和自动生成报表，手工生成根据用户指定的时间范围和报表模版进行生成，生成完成后可以 pdf,excel 两种方式导出。自动生成可以根据用户选择的报表模版和时间范围周期性自动生成报表，用户同时可以指定接收报表的邮箱地址，通过邮件接收自动生成的报表。
10	**功能：**知识库 **子菜单：** “漏洞库”- IPS 漏洞库，恶意软件，恶意域名，恶意进程等； “规则” – 包括可用性，性能，变更，安全等方面规则； “QA”- 在线问答，包括系统使用，运维，告警分析，安全分析等方面的内容，同时可转换为知识库； “全文检索”- 根据关键词检索知识库。
11	**功能：**系统 **子菜单：** “安装向导”- 数据采集对象的配置向导； “平台状态”- 实时显示平台的健康状态； “采集器状态”- 实时显示采集器的健康状态； “使用情况”- 实时显示系统当前监测的对象数，EPS 等情况； “角色管理”- 角色及权限配置，包括功能权限和界面权限； “用户管理”- 用户的增删改查，用户角色设定等； “事件数据库”- 事件数据库使用情况信息。