
QINGCLOUD
LIVE
青云
LIVE
直播间

青云直播间 LIVE

3月10日 19:00

企业安全合规之等级保护2.0

干货好礼送不停

等保2.0最新政策解读
企业安全合规新挑战

贾忠民

青云QingCloud 信息安全负责人

负责青云网络安全的管理以及等保认证的咨询与实施

- 等保2.0相关的政策法规
- 等保2.0测评介绍
- 等保违法案例

青云直播间 LIVE

网络安全等级保护

A 什么是等保？

为什么要做等保？ C

B 在哪里做等保？

等级保护发展历程

1994年《中华人民共和国计算机信息系统安全保护条例》颁布实施。

1

1994

1999

2

1999年《计算机信息系统安全保护等级划分准则（GB17859）发布。

2008

3

2008年 等级保护1.0元年

《信息安全技术 信息系统安全等级保护基本要求》相关标准发布实施。

2016

4

2016年发布《中华人民共和国网络安全法》

2019

5

2019年 等级保护2.0元年

5月13日正式发布等级保护2.0版本（《信息安全技术网络安全等级保护基本要求》），12月1日正式实施。

网络安全法律法规

中华人民共和国
国家安全法

第二十五条 国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；

中华人民共和国
网络安全法

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改

网络安全等保相关标准

- 《信息安全技术 信息系统安全等级保护基本要求》(GB/T22239–2008)
- 《信息安全技术 网络安全等级保护基本要求》(GB/T22239– –2019)
- 《信息安全技术 网络安全等级保护安全设计技术要求》(GB/T25070–2019)
- 《信息安全技术 网络络安全等级保护测评要求》(GB/T28448–2019)
- 《信息安全技术 网络安全等级保护测评过程指南》(GB/T28449–2019)

网络安全等级保护

分等级实行安全保护

➢对国家重要信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行**安全保护和监管**

实行按等级管理

➢对信息系统中使用的信息安全产品实行**分等级管理**

分等级响应、处置

➢对信息系统中发生的信息安全事件实行**分等级响应、处置**

等保建设的目的


满足国家相关
法律和制度的要求
降低信息安全风险
提高定级对象的
安全防护能力
合理规避或降低风险
履行和落实网络
信息安全责任义务

QINGCLOUD | LIVE

等保2.0的特点及新变化

青云 LIVE 直播间

等保2.0相对1.0的关键变化

对象变化

信息安全

↓

网络安全

引入云计算、移动互联、工控、物联网等新领域

结构调整

一个中心

三重防御

防御理念

被动防御

↓

主动防御

等保2.0涉及的行业

政府单位

- 各大部委、各省级政府机关、各地市县级政府机关、各事业单位等

金融行业

- 金融监管机构、各大银行、证券、保险公司等

医疗行业

- 医院、疫病控制中心、医疗卫生管理机构、医疗卫生研究机构等

教育行业

- 高校、职校、普教、互联网教育、APP等

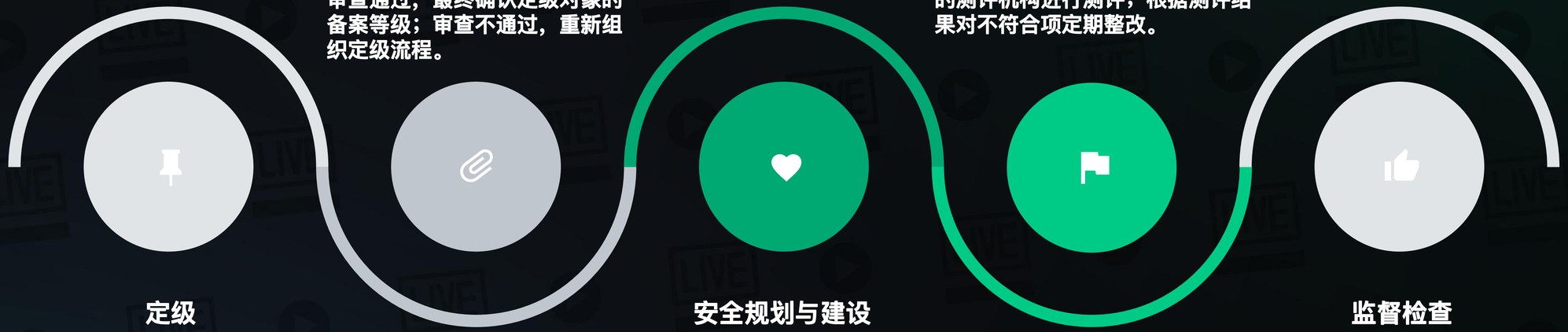
能源行业

- 电力公司、石油公司、天然气公司、煤碳公司等

企业单位

- 大中型企业、央企、上市公司等，其他有信息系统定级需求的单位和行业

等保2.0涉及的行业



定级

确定定级对象
初步确认等级
专家评审
主管部门审核
参考定级指南：
http://www.djbh.net

备案

公安机关根据备案材料进行审查
审查通过，最终确认定级对象的备案等级；审查不通过，重新组织定级流程。

安全规划与建设

需求分析，
总体设计建设方案规划

安全等级测评+整改

根据信息系统等级，选择国家认可的测评机构进行测评；根据测评结果对不符合项定期整改。

监督检查

出具测评报告，并向公安机关提交一份公安机关每年对网络运营 者开展网络安全等级保护 工作的情况和网络的安全 状况实施执法检查。

提交备案材料 至 备案证明

纸质版：

1. **信息系统安全等级保护备案表**一式两份（封面单位名称处盖章）。应填写完整、无漏项，不得改动备案表版面格式。机打，不可手写，单面打印。
2. **信息系统安全等级保护定级报告**一式两份（定级表格处盖章）。机打，单面打印。
3. **信息安全承诺书**签字盖章。法人亲笔签字
4. **相关证件复印件**各一份：工商营业执照(或执业许可证、事业单位证书、非盈利性机构证书等许可证明)、法人代表身份证、组织机构代码证（如三证合一，省略）。
5. **法人授权书**（被授权人需携带本人身份证原件及复印近）。
6. **实际办公地的房产证或租房合同复印件**。
7. **主机托管合同或云主机租用合同的复印件**。
8. **企业内部信息安全部门、技术部门组织架构人员登记信息表**，左上角盖章（表格中确定两位24小时应急处置网络安全事件联系人）。
9. 从事互联网金融的企业（如网贷P2P平台、证券交易系统等），备案时需提交纸质版**《信息安全等级保护备案证明使用承诺书》**法人亲笔签字，加盖单位公章。其他行业无需提交。

（备案面审提交时请按照以上顺序排列材料）

安全建设内容

主要工作内容

- □系统构成分析
- □安全保护现状分析
- □差距分析
- □安全技术体系建设规划
- □安全管理体系建设规划

交付成果

- ✓基本信息调研
- ✓安全现状分析报告
- ✓差距分析报告
- ✓安全技术体系建设方案
- ✓安全管理体系建设方案

等保测评技术要求

安全通用要求

技术要求

- 安全物理环境
- 安全网络通信
- 安全数据应用
- 安全计算环境
- 安全管理中心

管理要求

- 安全管理制度
- 安全管理机构
- 安全管理人员
- 安全建设管理
- 安全运维管理

安全扩展要求

- 云计算安全扩展要求
- 移动互联安全扩展要求
- 物联网安全扩展要求
- 工业控制系统安全扩展要求

等保测评结果

主要工作内容

- □辅助客户开展测评
- □安全整改规划
- □技术体系整改实施
- □管理体系整改实施
- □辅助正式测评

交付成果

- ✓预测评报告
- ✓安全整改计划
- ✓技术体系整改方案
- ✓管理体系整改方案
- ✓测评报告

说明

- 标准项目约为50工作日
- 需要进行整改建设的系统，时间周期根据系统规模、整改程度进行调整

QINGCLOUD | LIVE

等保咨询服务

定级

- 等级保护导入培训
- 业务系统安全域划分
- 安全需求分析
- 信息系统辅助定级
- 专家论证最终定级

备案

- 系统调研
- 完善安全管理制度
- 安全方案设计
- 辅助系统备案
- 系统等级整改

建设

- 系统自查
- 差距分析
- 安全建设规划
- 安全技术体系建设
- 安全管理体系建设

测评

- 辅助客户开展测评
- 安全整改规划
- 技术体系整改实施
- 管理体系整改实施
- 辅助正式测评

运行检查

- 月度安全巡检
- 安全状态监控
- 年度等级保护自查
- 协助主管部门现场检查
- 5x8应急响应服务

青云直播间 LIVE

网络安全违法案例

重庆某私立医院被罚款1万元

重庆永川某私立医院服务器突然陷入瘫痪，医院业务全面“停摆”，重庆永川公安接警后立即按照“净网2019”工作要求，启动网络安全应急响应预案。。经过民警和技术专家调查核实，该私立医院因未按照网络安全等级保护制度的要求履行安全保护义务。

公安机关按照公安部“一案双查”工作要求，对医院未按照网络安全等级保护制度的要求履行安全保护义务的行为进行查处，并按照《中华人民共和国网络安全法》第五十九条之规定，对医院处以罚款一万元，对直接负责的主管人员处以罚款五千元的行政处罚。

经开区某卫生管理部门未履行网络安全保护义务案

张家口市经开区某卫生管理部门未按网络安全等级保护要求履行安全保护义务，致使其官方网站存在网络安全漏洞的违法行为，今年8月，依据《网络安全法》第21条、第59条之规定对其处以警告行政处罚。

张家口市某交易中心未落实网络安全等级保护制度案

网警在检查中发现，张家口市某交易中心网签系统未按照《信息网络安全等级保护管理办法》进行定级测评工作，且经过多次检查督导仍未落实，存在较大的社会影响和风险隐患。今年8月，依据《网络安全法》第21条、第59条之规定对其处以警告行政处罚。

QINGCLOUD | LIVE

竞答红包

Question

Q：标志着等保法律地位的是哪部法律？什么时间开始正式实施？

A、《国家安全法》，2015年7月1日
B、《网络安全法》，2016年11月7日
C、《网络安全法》，2017年6月1日
D、《国家安全法》，2017年6月1日

青云 LIVE 直播间

QINGCLOUD | LIVE

Thank you.

zhongminjia@yunify.com

QingCloud-IaaS

青云QingCloud

www.qingcloud.com

青云 LIVE 直播间

青云直播间 LIVE

3月10日 19:00

企业安全合规之等级保护2.0

干货好礼送不停

等保方案分享　青云
如何助力企业通过等保测评

方明

青云QingCloud 安全顾问产品经理

负责安全产品惯例以及等保相关咨询工作

- 等保2.0要求解读
- 青云解决方案分享

青云直播间 LIVE

一、等保2.0要求解读

QINGCLOUD | LIVE

等保2.0框架解读

青云 LIVE 直播间

云计算安全拓展要求
第三级（技术）分析

责任分担模型

《网络安全法》
网络营者应当遵循等级保护指导要求

GB/T 22239
谁主管谁负责
谁运行谁负责

《云等保护草案》
租户等级保护要求

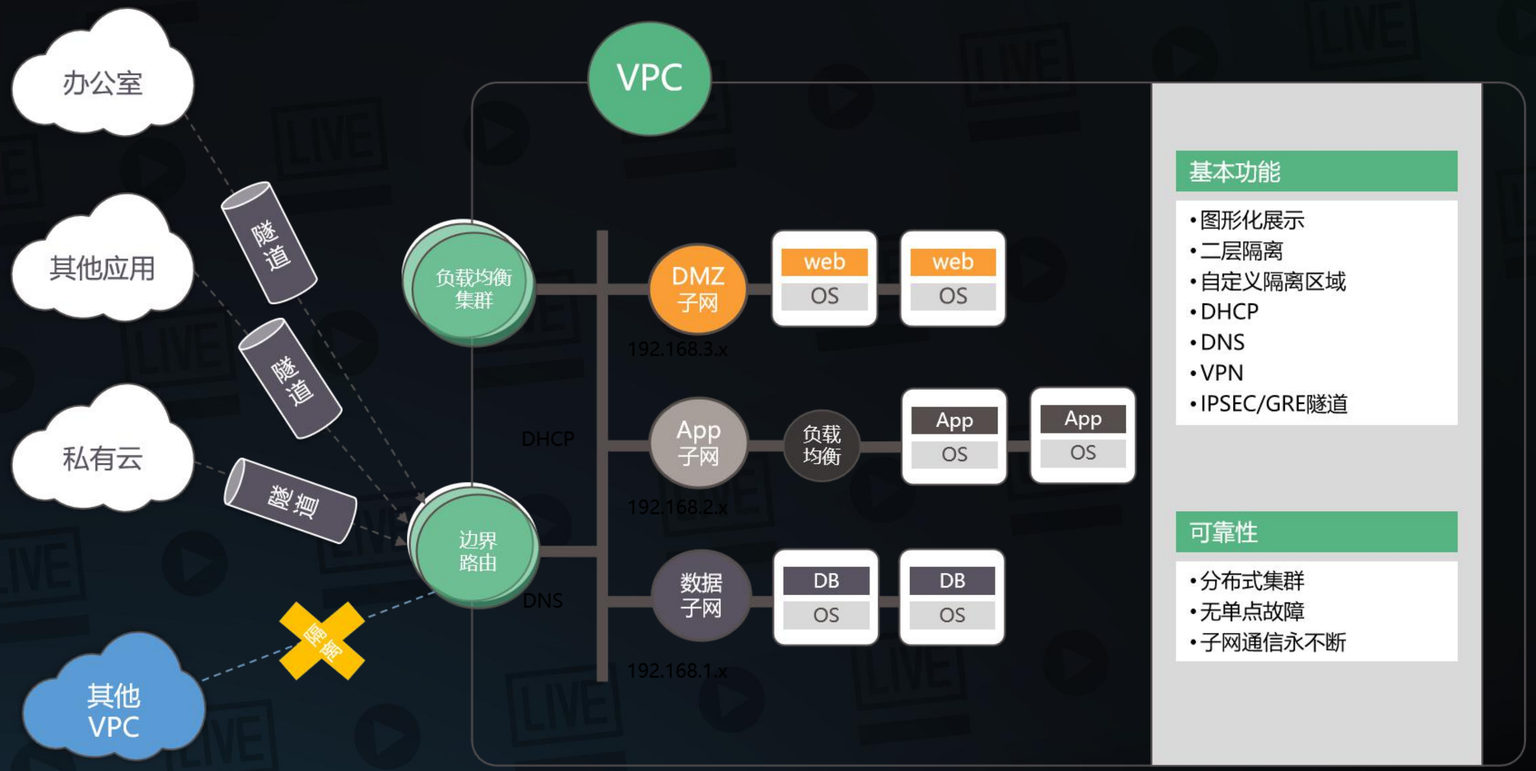
等保测评工作职责划分

参与方	定级	备案	建议整改	等保测评	监督检查
客户	确定系统或者子系统的安全等级，准备定级报告	准备备案材料，到当地公安网监，递交备案	基于等保的安全技术和管理要求进行建设和整改，以符合等保要求	准备和接受测评机构的测评	接受公安网监定期的检查，主动开展每年的定期测评
云平台	协调第三方为客户提供辅导服务	协调第三方为客户提供辅导服务	提供符合等保相关要求的安全产品和服务	提供云平台相关通过等保的证明材料	–
咨询机构	辅导客户定级，准备定级报告并组织专家评审	辅导客户准备备案材料和备案	辅导客户进行定级相关系统和组件的安全加固，并协助建立安全管理体系	协助并指导客户进行测评整改	协助客户接受检查并指导整改
测评机构	提供等保定级指导	提供等保备案指导	–	对系统等级符合性状进行测评，并出具测评报告	–
公安监测	–	审核受理备案材料	–	–	监督检查单位开展等级保护工作情况

二、青云解决方案分享

QINGCLOUD | LIVE

云上网络架构
构建安全通信网络



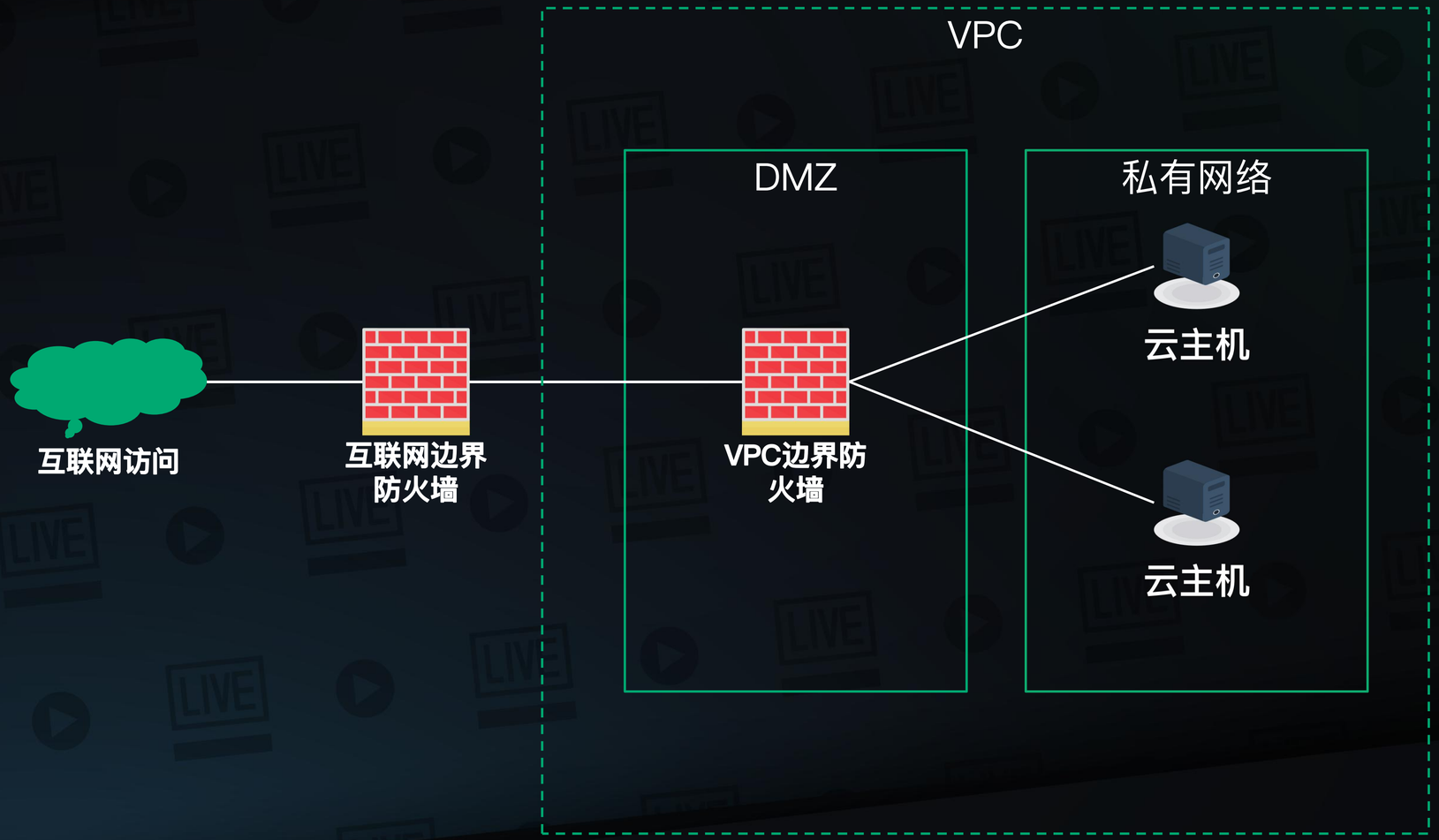
青云QingCloud 网络SDN技术

- 单VPC 256个子网
- 单VPC 65000+主机
- 智能自学习算法，点对点直接路由
- LB 支持集群模式
- 主机直接分配EIP
- 防火墙可绑定任意资源
- 性能线性水平扩展，支持超大规模数据中心

青云 LIVE 直播间

云上下一代防火墙

构建云平台的安全区域边界



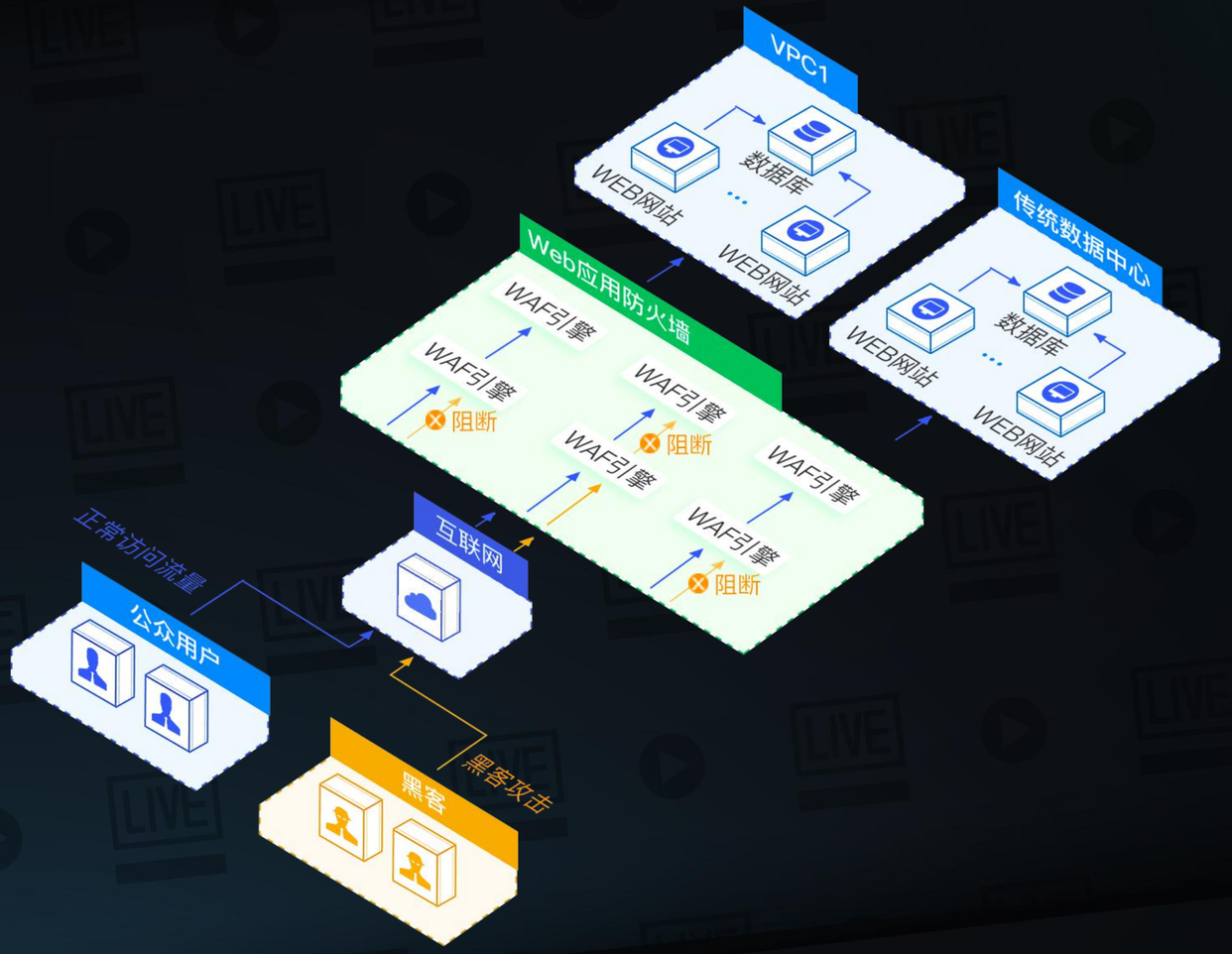
青云QingCloud SaaS下一代防火墙

- SaaS化下一代防火墙服务
- 提供应用防火墙、入侵防护、防病毒、反APT、VPN、智能带宽管理、多出口链路负载均衡、内容过滤
- 以资产为视角，构建全流程防御防火墙

QINGCLOUD | LIVE

云上WEB应用防火墙

守护WEB应用安全 安全区域边界



Web应用防火墙 守护网站应用安全

- 对网站或者APP的业务流量进行恶意特征识别及防护，将清洁的流量回源到服务器
- 避免网站服务器被恶意攻击和入侵，保障核心数据安全，实现防入侵、防扫描、防攻击、防数据泄露、防CC等攻击防护

青云直播间 LIVE

QINGCLOUD | LIVE

数据安全与访问鉴权

KMS 密钥管理服务与IAM 身份与访问权限管理

Identity and Access Management

身份识别与访问管理

通过使用 IAM ，可以统一管理和控制其接入实体（用户）的认证（登录）和授权（具备的权限）

定义

- 在线数据加解密
- 不必共享密码或访问密钥，直接为接入实体创建仅属于该实体的访问凭证
- 密钥保存管理，自动密钥轮转周期

Key Management Service

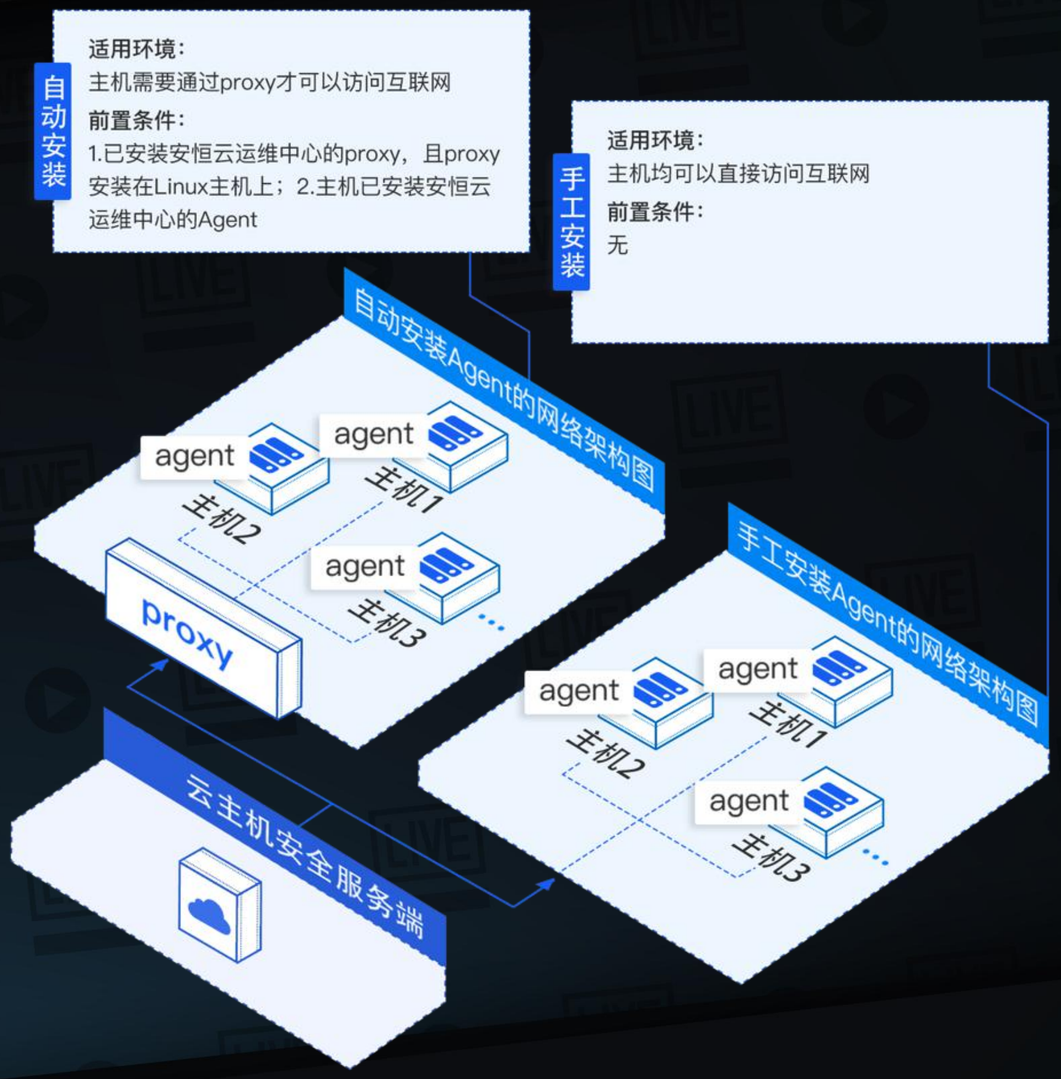
密钥管理服务

密钥管理	密钥轮转	云产品加密
对称密钥	非对称密钥	密钥别名

密钥API

青云 LIVE 直播间

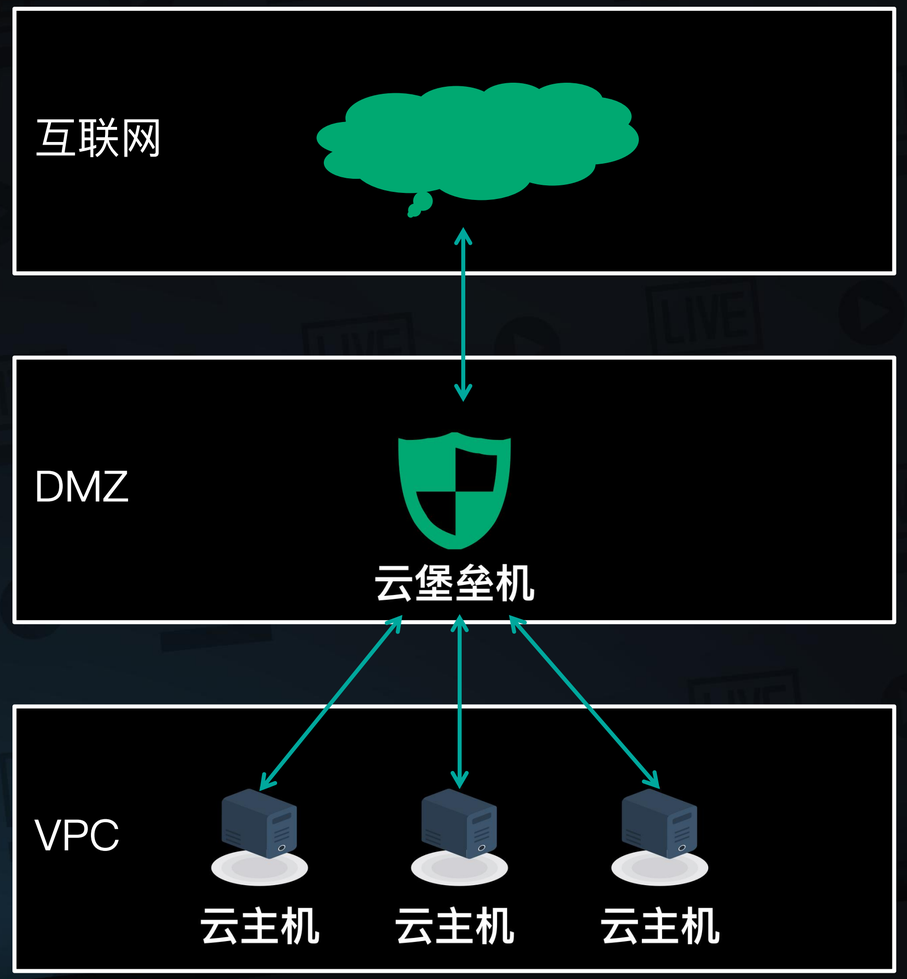
云上主机安全合规



青云QingCloud 主机安全

- 提供主机系统防护与加固、主机网络防护与加固等功能
- 业界领先的勒索专防专杀、网页防篡改、网络隔离与防、补丁修复、外设管控、文件审计
- 违规外联检测与阻断等主机安全能力,帮您快速发现网站潜在安全隐患

身份管理识别与安全审计

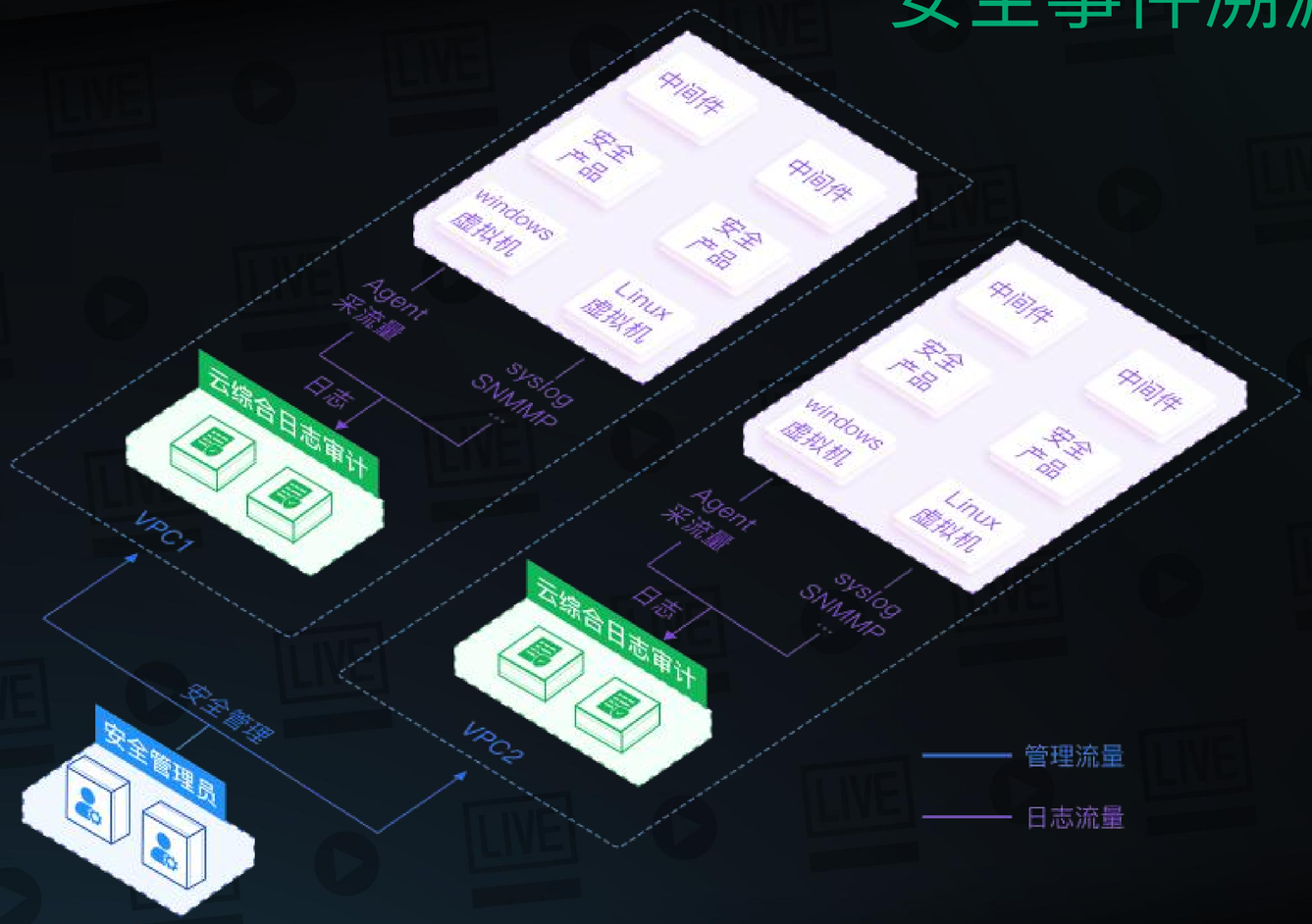


云堡垒机

- 提供多云主机资产的运维审计功能
- 覆盖SSH、RDP、VNC、Telnet、FTP/SFTP等多种协议
- 支持通过浏览器Web页面和本地C/S客户端工具的方式访问主机，为用户提供包含事前授权、事中监察、事后审计等完整的运维闭环

云上安全管理中心

安全事件溯源



安全管理中心 综合日志审计

- 对网络日志、安全日志、主机日志和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件
- 为运维提供全局的视角，一站式提供数据收集、清洗、分析、可视化和告警功能

QINGCLOUD | LIVE

竞答红包

Question

Q：云主机内部的恶意代码、病毒防范可以使用什么类型的安全产品？

A、EDR 终端安全响应系统
B、堡垒机
C、下一代防火墙
D、Web应用防火墙

青云 LIVE 直播间

QINGCLOUD | LIVE

Thank you.

mattfang@yunify.com

QingCloud-IaaS

青云QingCloud

www.qingcloud.com

青云 LIVE 直播间

青云直播间 LIVE

3月10日 19:00

企业安全合规之等级保护2.0

干货好礼送不停

QINGCLOUD | LIVE

等保三级 案例分享

郑锐

青云QingCloud 公有云业务售前技术顾问

负责青云华东区公有云售前技术支持工作。5年公有云架构设计及交付经验，帮助交通、医疗、教育、跨境电商等行业的多家客户完成了云化转型。

- 为什么要做等保?
- 这是一个怎么样的过程?

青云直播间 LIVE

- 为什么要做等保?
- 这是一个怎么样的过程?

WHY

依据《网络安全法》，各个行业的业务系统均需要进行等级保护备案；

该案例系统为某物流公司的运营管理系统，包括下单，物流信息管理，物流查询等功能，属于一个独立的业务系统，因此需要过等保。

- 为什么要做等保?
- 这是一个怎么样的过程?


等保流程
1 系统定级
2 系统备案
3 预测评
4 正式测评
5 定期检查
1.如何确定级别?
2.如何选择咨询机构?
1.需要准备哪些材料?
2.具体找哪个部门?
3.需要花费多长时间?
1.哪些测评项需要整改?
1.如何选择测评机构?
2.时间周期?
3.验收材料有哪些?
1.有固定周期吗?
专家评审报告
备案证明
等保差距分析报告
测评报告

如何确定系统等级

指标	被侵害的客体		对客体的侵害程度	级别		
确定系统服务安全等级（A）	系统中断会影响到	□国家安全	□造成一般损害（A3） □造成严重损害 （A4） □造成特别严重损害（A5）	系统服务安全等级A： □（A1） □（A2） □（A3） □（A4） □（A5）	系统等级： **□一级** □（S1A1G1） **□二级** □（S1A2G2） □（S2A1G2） □（S2A2G2） **□三级** □（S1A3G3） □（S2A3G3） □（S3A1G3） □（S3A2G3） □（S3A3G3）	**□四级** □（S1A4G4） □（S2A4G4） □（S3A4G4） □（S4A4G4） □（S4A1G3） □（S4A2G4） □（S4A3G4） **□五级** □（S1A5G5） □（S2A5G5） □（S3A5G5） □（S4A5G5） □（S5A5G5） □（S5A1G5） □（S5A2G5） □（S5A3G5） □（S5A4G5）
		□社会秩序、公共利益	□造成一般损害（A2） □造成严重损害（A3） □造成特别严重损害（A4）			
		□公民、法人和其它组织的合法利益	□造成一般损害（A1） □造成严重损害（A2） □造成特别严重损害（A3）			
确定业务信息安全等级（S）	系统数据被篡改被泄漏影响到	□国家安全	□造成一般损害（S3） □造成严重损害 （S4） □造成特别严重损害（S5）	系统业务安全等级S： □（S1） □（S2） □（S3） □（S4） □（S5）		
		□社会秩序、公共利益	□造成一般损害（S2） □造成严重损害（S3） □造成特别严重损害（S4）			
		□公民、法人和其它组织的合法利益	□造成一般损害（S1） □造成严重损害（S2） □造成特别严重损害（S3）			


等保流程
1 系统定级
2 系统备案
3 预测评
4 正式测评
5 定期检查
1.如何确定级别?
2.如何选择咨询机构?
1.需要准备哪些材料?
2.具体找哪个部门?
3.需要花费多长时间?
1.哪些测评项需要整改?
1.如何选择测评机构?
2.时间周期?
3.验收材料有哪些?
1.有固定周期吗?
专家评审报告
备案证明
等保差距分析报告
测评报告

系统网络拓扑图


接入缓冲区
业务处理区
WEB服务器-1
WEB服务器-2
Postaresal
RabbitMQ
Memcache
internet
缺省防火墙
VPC网络
虚拟网络
下一代防火墙
防火墙跳板机
Syslog服务器

QINGCLOUD | LIVE

竞答红包

Question

Q：部署在青云公有云上的业务系统过等保，只需要青云提供（ ）和（ ）两份证明材料即可满足安全物理环境的要求。

A. 专家评审报告、云平台备案证明
B. 云平台备案证明、云平台测评报告
C. 等保差距分析报告、云平台测评报告
D. 云平台测评报告、专家评审报告

青云 LIVE 直播间

QINGCLOUD | LIVE

Thank you.

ryanzheng@yunify.com

QingCloud-IaaS

青云QingCloud

www.qingcloud.com

青云 LIVE 直播间

QINGCLOUD | LIVE

问卷调查

扫码填写问卷调查，参与最终抽奖

QingCloud-IaaS

青云QingCloud

www.qingcloud.com

青云 LIVE 直播间