QINGCLOUD

安全知识分享

目录

01 市场背景

企业面临的问题

1

业务上云，资产、业务、数据如何保护?

- 随着云计算，虚拟化，SDN的大力发展，企业逐渐把业务迁移到云上。
- 云端资产和数据存储的增加，其安全保障越来越受到重视。

2

企业如何有效防御复杂多变的攻击?

- 由于基础架构的复杂性。
- 攻击手段纷繁复杂且不断发展演变。
- 据 MCAFEE 对云服务的网络攻击研究，自 2020 年 1 月以来，云服务遭受到的网络攻击增加了 630%。

3

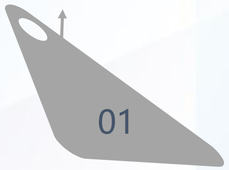
等保2.0 的实施，企业如何满足相关条例要求?

- GB/T 22239-2008 信息安全技术 信息安全等级保护基本要求。
- GB/T 22239.1 信息安全技术 信息安全等级保护基本要求 第1部分 安全通用要求（征求意见稿)。
- GB/T 22239.2 信息安全技术 信息安全等级保护基本要求 第2部分 云计算安全扩展要求（征求意见稿）。

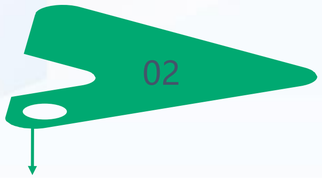
市场需求

有效抵御各种常见的攻击，并满足等保合规要求。

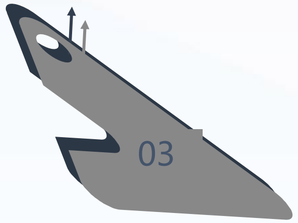
采取可靠的技术手段来隔离重要网络区域和其他网络区域



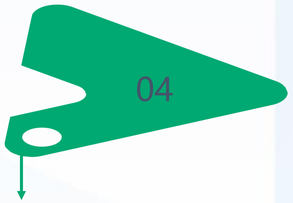
能够对非授权设备私自联到内部网络的行为进行检查或限制



在网络边界区域之间根据访问控制策略设置访问控制规则



提供日志审计，为安全事件分析、策略调整提供数据支撑



02

常见攻击手段

常见攻击手段

- 病毒：利用网络进行复制和传播，盗取用户信息、破坏文件等
- 后门程序：绕过安全性控制而获取对程序或系统访问权的程序方法，达到控住主机的目的
- 间谍软件：在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件
- WEB攻击：SQL注入、系统命令注入、LDAP注入、SSI注入、邮件注入、请求体PHP注入等攻击
- 钓鱼邮件：利用伪装电邮，诱导点击网页，收集账号、口令信息
- 拒绝服务：洪水攻击、慢速攻击等，造成资源被占满，正常请求被拒绝
- 漏洞攻击：应用层漏洞、ODAY漏洞等
- APT攻击：多种复杂攻击手段结合、长期的持续性攻击

云环境中常见的网络威胁

新购主机无法访问

端口被Dos攻击，ssh/rdp应用漏洞被利用等

网页被篡改

主机弱密码被爆破，黑客修改网站源文件

计算资源被异常占用

主机22端口弱密码，或redis服务未授权访问，被植入挖矿病毒

DDos攻击

分布式大流量模拟访问，导致业务带宽被占满

Web、应用漏洞进行入侵

应用漏洞被暴露，黑客利用历史漏洞即可轻松完成入侵

混合云不同区域之间的网络隔离

SDWAN用户对跨区域网络安全防护

跨VPC之间的网络攻击防护

03 常见防护产品

常见安全产品

网络安全

- 云防火墙
- 高防 IP
- 漏洞扫描
- 堡垒机
- 操作审计
- 云安全中心

数据安全

- SSL 证书
- 密钥管理
- 数据库审计
- 加密服务
- 凭据管理

应用/业务安全

- WEB 应用防火墙
- 内容安全
- 风险识别
- 应用安全访问

终端安全

- 主机安全
- 反病毒引擎
- 零信任

常见安全产品

产品	简介
云防火墙	云上边界网络安全防护产品，可提供统一的互联网边界、内网VPC边界、主机边界流量管控与安全防护，包括结合情报的实时入侵防护、全流量可视化分析、智能化访问控制、日志溯源分析等能力，是网络边界防护与等保合规利器。
高防IP	提供针对 DDoS 攻击防护及代理转发服务，用户通过配置高防 IP，将攻击流量引流到高防 IP 进行清洗，确保源站业务的稳定可用。
漏洞扫描	以企业IT资产为核心，提供全面、快速、精准的漏洞扫描及风险监测服务，帮助企业持续地发现暴露在互联网边界上的常见安全风险。
堡垒机	云上统一、高效、安全运维通道，用于集中管理资产权限，全程监控操作行为，实时还原运维场景，保障云端运维身份可鉴别、权限可管控、风险可阻断、操作可审计，助力等保合规。
密钥管理	针对云上数据加密需求精心设计的密码应用服务，为用户的应用提供符合国密要求的密钥服务及极简应用加解密服务，助用户轻松使用密钥来加密保护敏感的数据资产。
WEB应用防火墙	Web应用防火墙对网站或者APP的业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。

常见安全产品

产品	简介
主机安全	基于海量威胁数据，利用机器学习为用户提供资产管理、木马文件查杀、黑客入侵检测、漏洞风险预警及安全基线等安全防护服务，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系。
零信任	依赖可信终端、可信身份、可信应用三大核心能力，实现终端在任意网络环境中安全、稳定、高效地访问企业资源及数据。
数据库审计	是一款基于人工智能的数据库安全审计系统，可挖掘数据库运行过程中各类潜在风险和隐患，为数据库安全运行保驾护航，等保合规利器。
日志审计	日志审计产品通过对网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，并进行全维度、跨设备、细粒度的关联分析，透过事件的表象真实地还原事件背后的信息，从而协助用户全面审计信息系统整体安全状况。通过安装 Agent 采集主机产生的日志信息，并进行汇总展示。


QINGCLOUD青云