网 安 联
Wang An Lian

—— 网安联抗“疫”公益系列活动之十五（二）——

Hillstone
山 石 网 科

远程教育安全解决方案

教育行业售前工程师–钟文健

2020.03

背景

网安联抗“疫”公益系列活动之十五（二）·

政策要求

教 育 部 办 公 厅

教技厅函〔2020〕7号

教育部应对新型冠状病毒感染肺炎疫情工作领导小组办公室关于疫情防控期间以信息化支持教育教学工作的通知

（六）强化网络安全保障。教育部加强对重要信息系统（网站）的网络安全监测通报，组织电信运营商和网络安全服务商为国家体系等重要信息系统（网站）提供重点保障。教育网网络中心应保障教育网安全稳定运行。各地各校要落实网络安全等级保护制度，加强网络安全管理和技术保障能力。重点加强个人信息保护，选用第三方平台和服务的应明确个人信息使用规则，不得借机超范围采集个人信息。

①

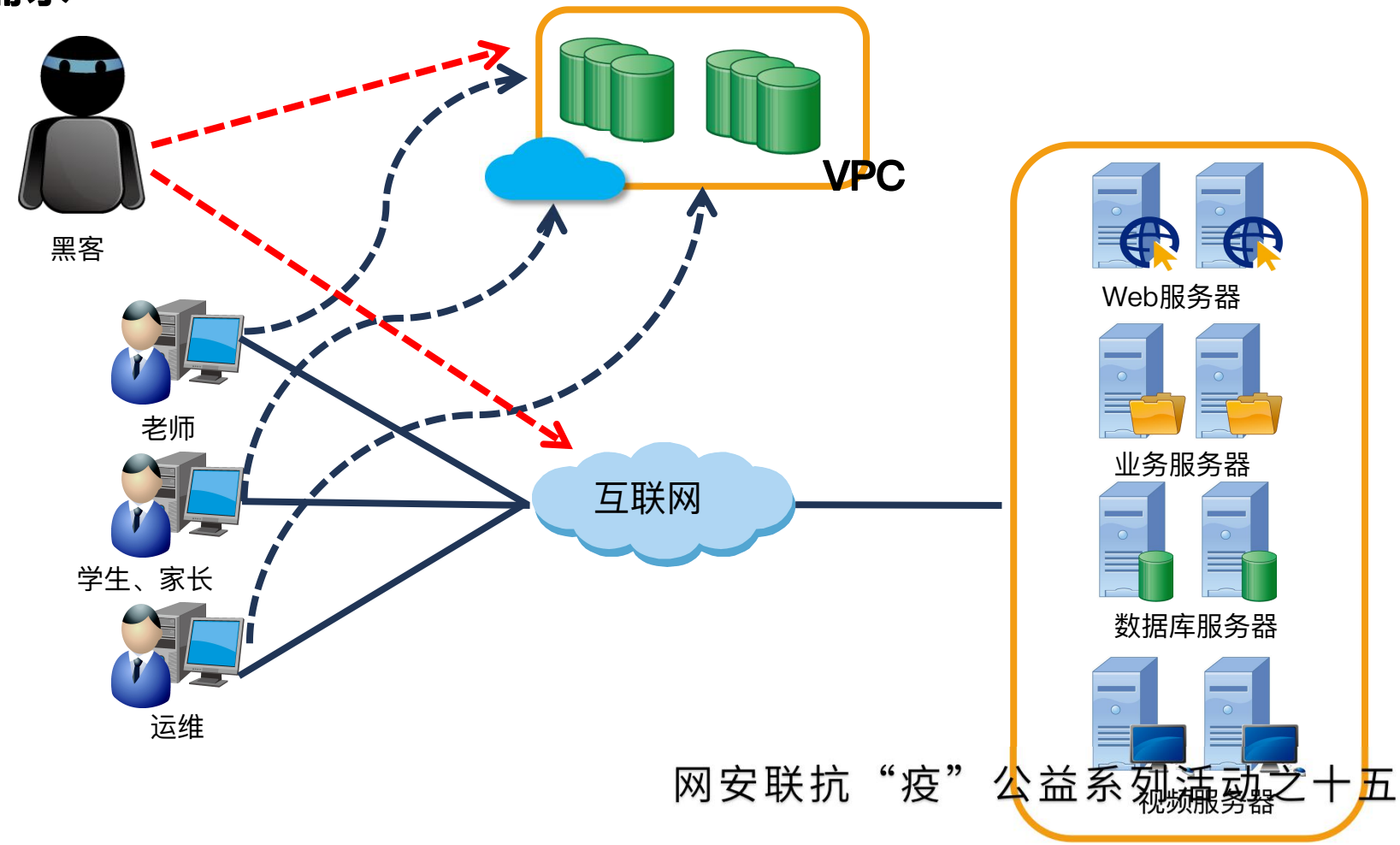
②

③

网安联抗“疫”公益系列活动之十五（二）·

网络黑客攻击

- 基于特征检测的传统防火墙已无法抵御黑客的新型攻击行为
- 远程教育平台门户网站的防篡改需求
- 机构云端业务防护需求



网安联抗“疫”公益系列活动之十五（二）·

远程访问内部资源

- 远程访问校内电子图书馆资源
- 异地登录教学管理系统

远程VPN安全接入、扩展需求

网安联抗“疫”公益系列活动之十五（二）·

登陆界面卡顿

- 师生登录平台时
- 老师直播授课时
- 老师上传课件时
- 学生提交作业时

网安联抗“疫”公益系列活动之十五（二）·

运维管理风险

- 远程运维管理需求
- 登录账号管理混乱
- 运维权限划分不明
- 认证方式过于简单
- 缺乏运维监控措施

员工在家办公用VPN毁掉公司数据 微盟公司市值一天蒸发9亿

凤凰网科技 游侠安全网 今天

2月25日消息，港股上市公司微盟集团今日在港交所公告称，SAAS业务数据遭到一名员工“人为破坏”，故障发生后排查发现大面积服务集群无法响应，生产环境及数据遭受严重破坏。截至2020年2月25日12点，微盟集团报5.660港元，跌幅为4.553%。从2月24日至2月25日员工恶意破坏事件的一天时间内，微盟集团市值约蒸发了约9.63亿港元。

网安联抗“疫”公益系列活动之十五（二）·

数据泄露隐患

- 个人隐私信息
  - 老师
  - 学生
  - 家长
- 机构教学资产
  - 课件
  - 授课视频
  - 押题考卷
  - 。。。

在线教育服务商部分名单

2012-2022 年中国在线教育市场规模（亿元）

资料来源：艾瑞咨询、东兴证券研究所

2012-2022 年中国教育用户规模（万人）

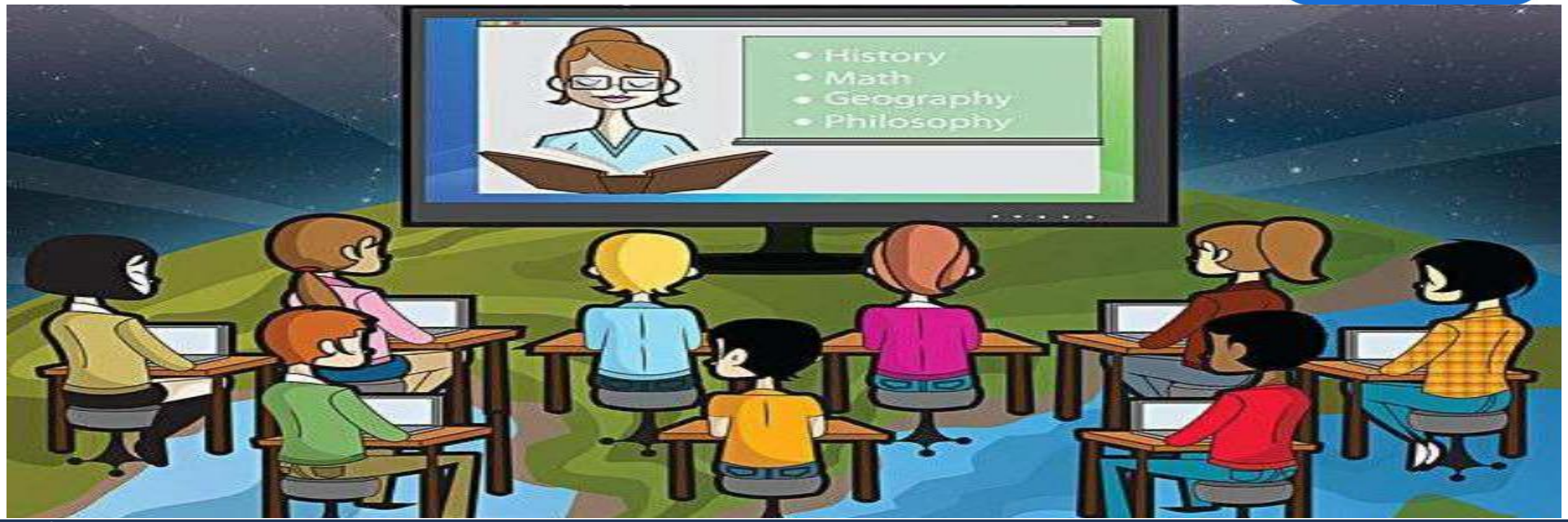
资料来源：艾瑞咨询、东兴证券研究所

阿里巴巴集团	旗下优酷、钉钉联手发起“在家上课”计划，提供免费课程，湖北省近 50 所中小学已加盟
腾讯	开展多条业务线联动，免费提供平台基础云资源
好未来	提供直播系统、课程内容、运营陪护等支持
网易教育	中国大学 MOOC、网易有道智云将免费提供在线教学服务
爱学习集团	免费开放优质内容与直播工具
VIPKID	将会免费开放旗下在线直播平台
麦奇教育科技	也将免费开放在线授课平台
7EDU	将向全国中学提供 SAT/AP 等系列学习资源
科大讯飞	表示向全湖北中小学免费提供智慧空中课堂
ClassIn	表示对非营利教育机构实施完全免费的政策
学堂在线	免费为全国教师提供线上培训，组织混合式教学名师开设示范课
北京猿力教育科技	为全国中小学生提供免费的巩固预习课；同时开放旗下猿辅导网课、猿题库、小猿搜题、小猿口算、斑马 AI 课等产品的核心功能，在寒假延长期内为学生提供系列支持
承承网络科技	在线英语启蒙 App 叽里呱啦向全国儿童免费开放在线英语启蒙资源

机构	主要援助措施
新东方	向湖北省红十字会捐款2000万元，向医护人员子女免费开放班课
好未来	设立1亿元抗疫情基金，免费提供在线教育技术和解决方案支持
精锐教育	捐赠超2000万价值在线课程，免费提供在线素质教育课程
跟谁学	捐赠课程，免费提供直播工具
尚德机构	捐赠500万元现金采购物资，免费提供在线课程
网易有道	免费提供课程，增设500万元全勤奖学金
掌门教育	捐赠价值2000万元的1对1课程
猿辅导	捐款1000万元，免费提供教学服务
松鼠AI	捐款1000万元，提供免费在线学习账号
VIPKID	捐赠课程和直播平台
一起教育科技	免费开放在线教育直播平台
叽里呱啦	免费开放启蒙英语资源
小盒科技	免费开放机构在线教学服务
轻轻教育	免费开放在线教育平台和工具
弘成教育	捐赠课程，开放在线学习平台
流利说	捐赠课程
正保远程教育	提供多项免费职业教育课程
学大教育	免费提供教学服务
爱学习集团	免费开放在线平台
洋葱学院	捐赠课程
作业帮	捐赠课程
麦奇教育	捐赠课程，开放在线教育平台
钉钉	免费开放“在线课堂”功能
腾讯	联合多家企业推出“不停学联盟”，捐赠课程
科大讯飞	捐赠1000万元医用物资，免费提供直播教学系统

适用场景

- 中小学、高校的远程教学
- 普通企业内部的线上培训
- 互联网企业的网络教育：VIPKID、学而思、沪江等
- 间接教育机构的知识共享：得到、喜马拉雅FM、短书等

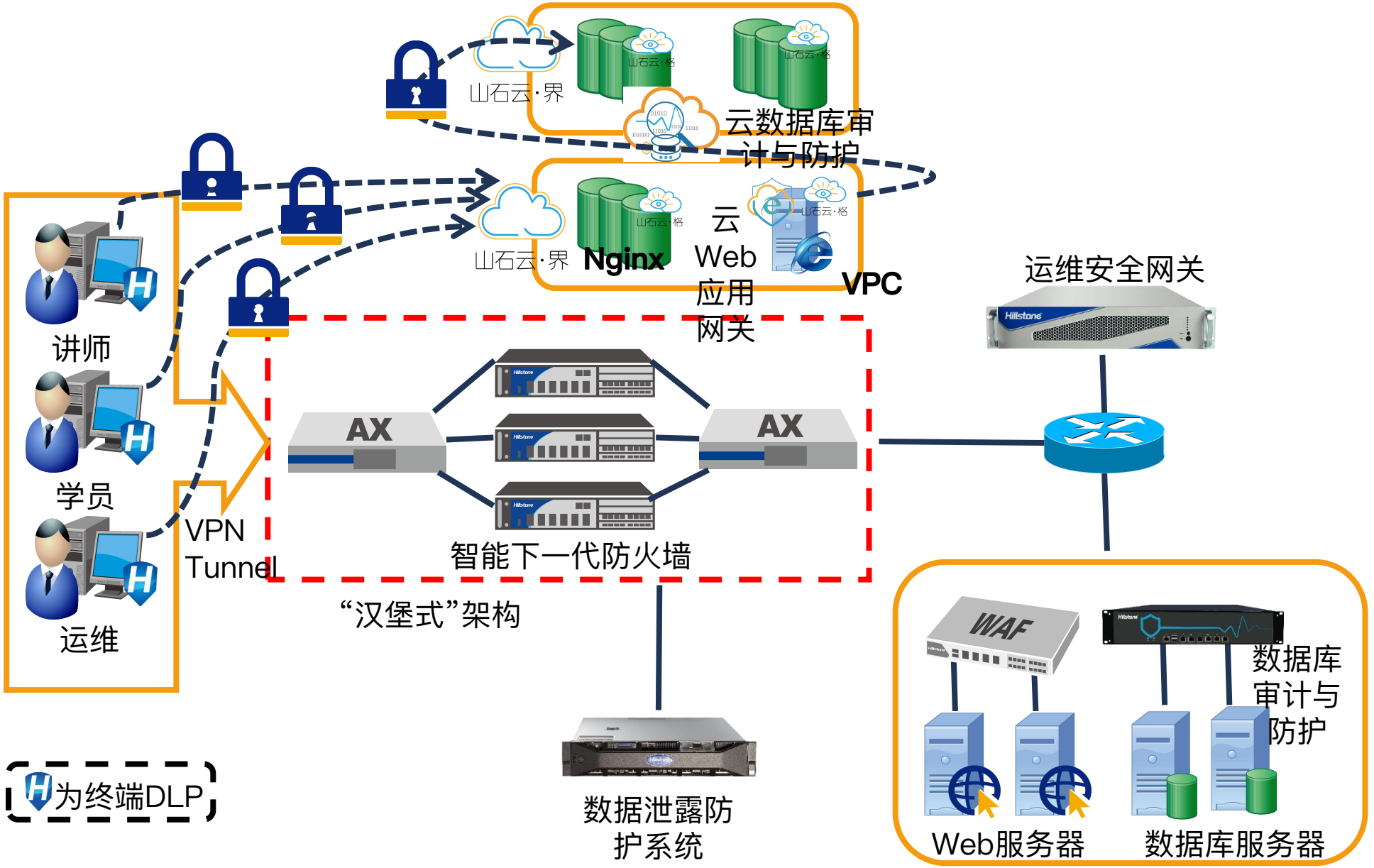


在线课堂应用场景和分析

应用场景	详细信息	应用场景需求分析
在线教育	• 疫情期间要求“停课不停教、停课不停学”；根据艾瑞咨询数据，预计在2022年中国在线教育市场规模将达5433.5亿元。 • 用户对在线教育的接受度不断提升、付费意识的觉醒以及线上学习丰富度的完善等是在线教育市场规模持续增长的主要原因； • 在线教育市场结构可能发生变化，疫情之前，我国在线教育的市场主体是高等学历教育及职业培训，约占整个在线教育市场规模的80%左右，成人是在线教育的主要用户群体，疫情之后，中小学学生使用在线教育的比例有望上升。	互联网在线教育企业扩容及安全需求 云上业务弹性扩展需要安全防护 个人信息和教育资源保护
在线课堂、远程毕业设计、远程访问图文资源	• 疫情期间，学校需要组织教学，因此会产生视频教学的需求，视频教学如果在学校进行流量会占用学校出口带宽，有可能会产生学校出口扩容的需求，已有学校联系； • 疫情期间，学生需要准备毕业设计，毕业设计需要使用学校资源，因此需要VPN的接入，已有学校联系并确定要购买500个vpn。	学校/教育局/电教馆/广电/运营商新建或扩容在线课堂 学生远程在线完成毕业设计 学生远程访问学校图书馆及中国知网等教育资源 Web网站和APP安全 服务器扩容涉及服务器负载均衡 链路负载满足不同运营商用户接入选路

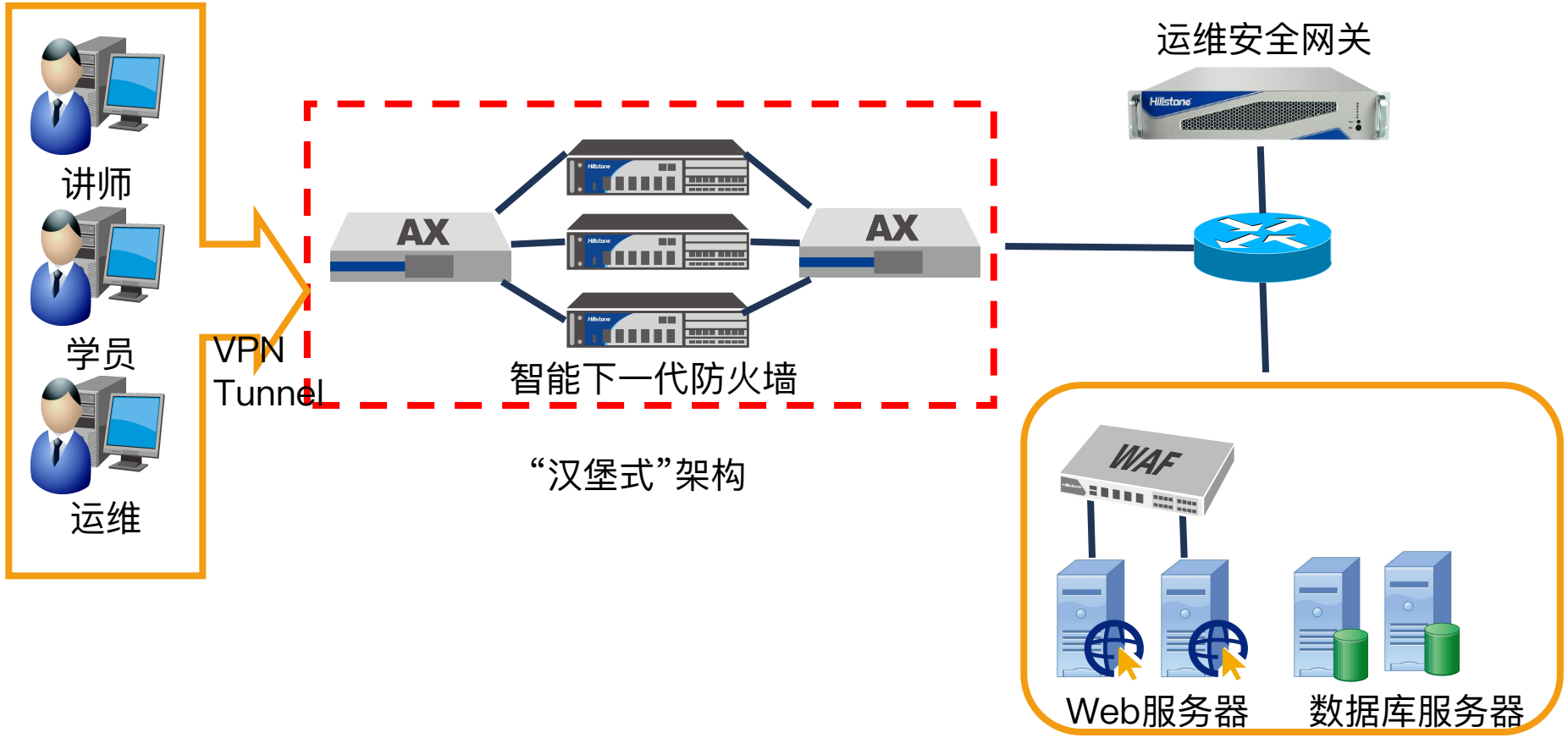
网安联抗“疫”公益系列活动之十五（二）·

山石网科远程教育安全解决方案

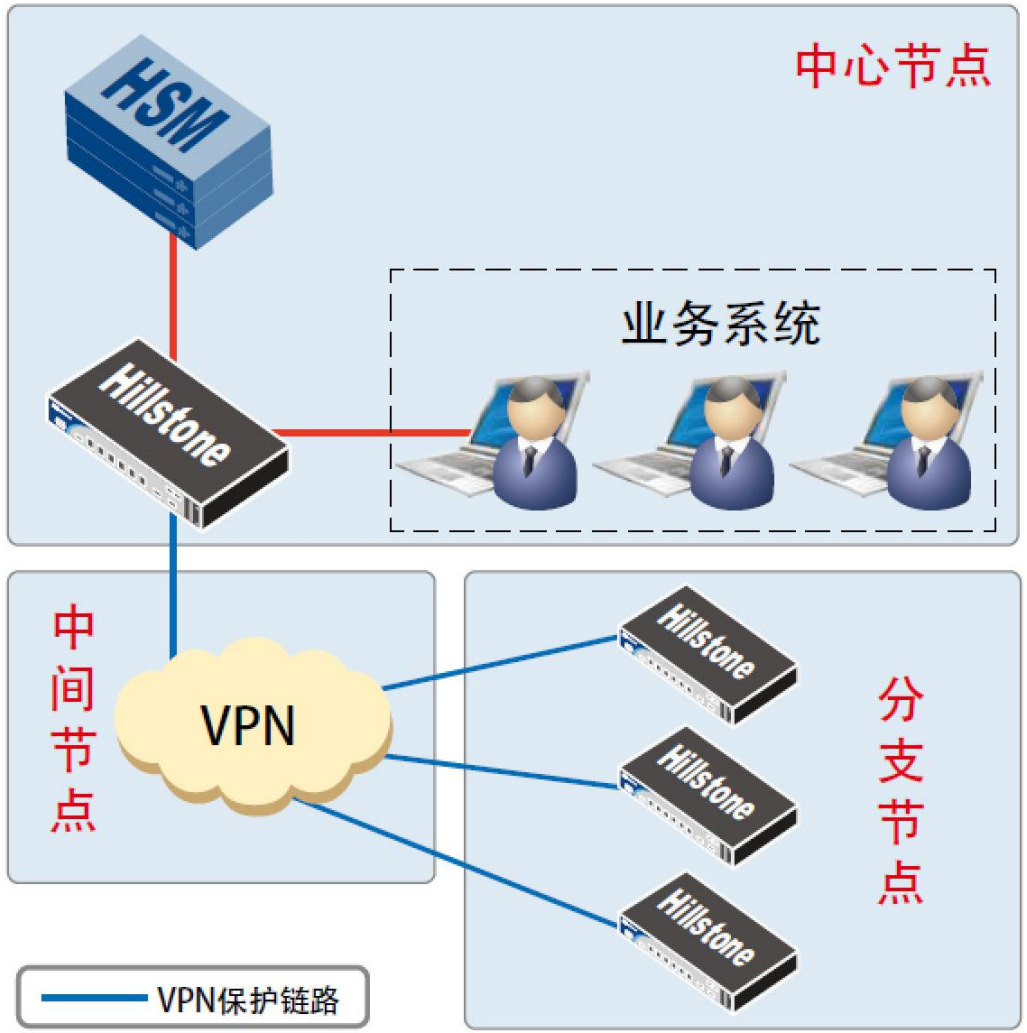


网络接入及安全防护

- 高级威胁检测加速网络攻击行为的检出
- 解决远程教育机构门户网站防篡改需求
- 双侧“汉堡式”组网解决远程教育机构VPN远程扩展需求
- 通过SLB、SSL硬件卸载、缓存加速、内容压缩等技术提高学员访问体验
- 实现对核心资产的统一认证、授权、审计，全方位提升运维风险控制能力



分支和高校总部IPSEC VPN互联应用场景



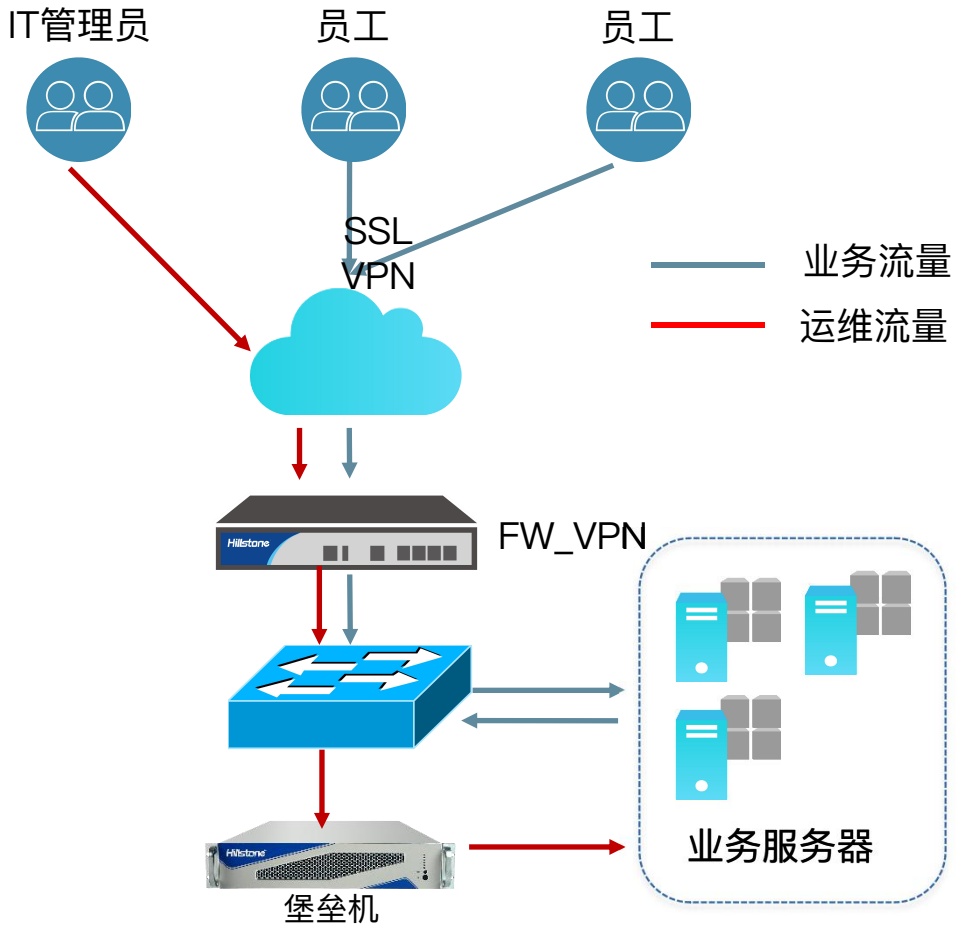
功能

- IPSEC VPN
- GRE VPN
- 安全防护
- 证书和预共享密钥

价值

- 兼容标准IPSecVPN厂商设备互联
- 提供端到端安全通道
- 提供数据传输机密性和完整性
- 实现混合云互联互通
- VPN链路实时监控和告警
- 日志查询审计

移动用户SSL VPN接入应用场景



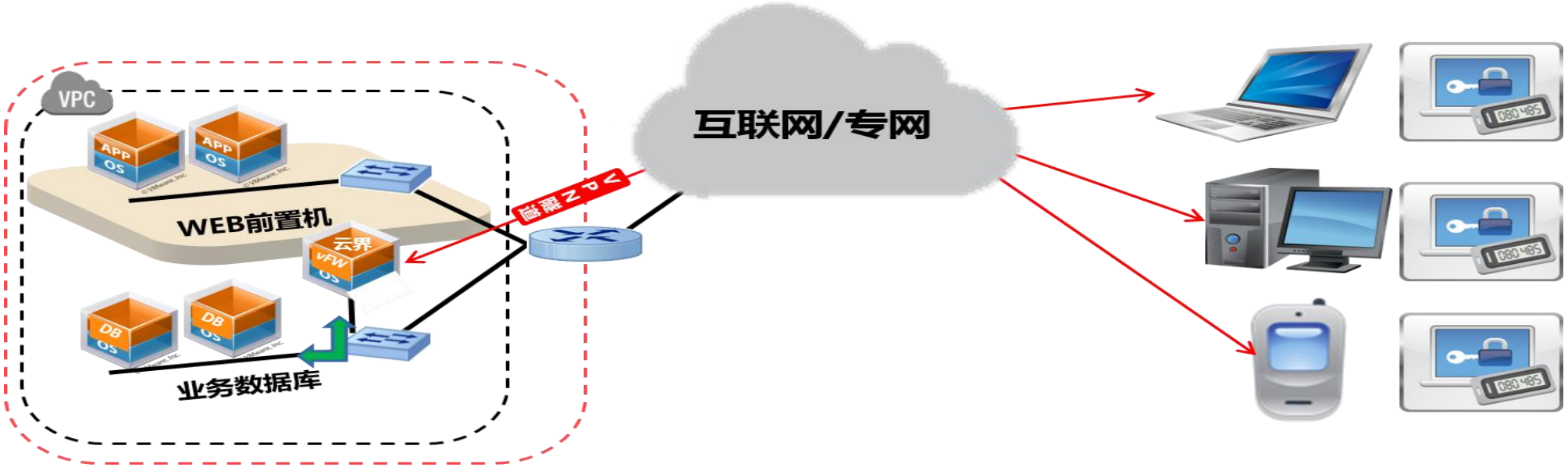
功能

- SSL VPN
- 身份认证
- 数据加密
- 安全防护

价值

- PC主机、安卓苹果移动终端安全接入
- 基于U-key、软证书、用户名/口令认证、短信认证
- 支持和AD域控对接，实现SSO登录并设置访问规则
- 基于角色控制，实现私有应用访问控制
- 基于接入终端的安全性准入控制（注册表、文件、杀毒软件、系统漏洞等）
- 控制审计运维人员远程管理权限和指令

云界vSSLVPN应用场景



功能

- SSL VPN
- 身份认证
- 数据加密
- 安全防护

价值

- PC主机、安卓苹果移动终端安全接入
- 基于U-key、软证书、用户名/口令认证、短信认证
- 基于角色控制，实现私有应用访问控制

山石网科VPN优势

Gartner

2019年全球网络防火墙魔力象限：山石VPN功能的配置和管理的易用性，收到客户广泛好评

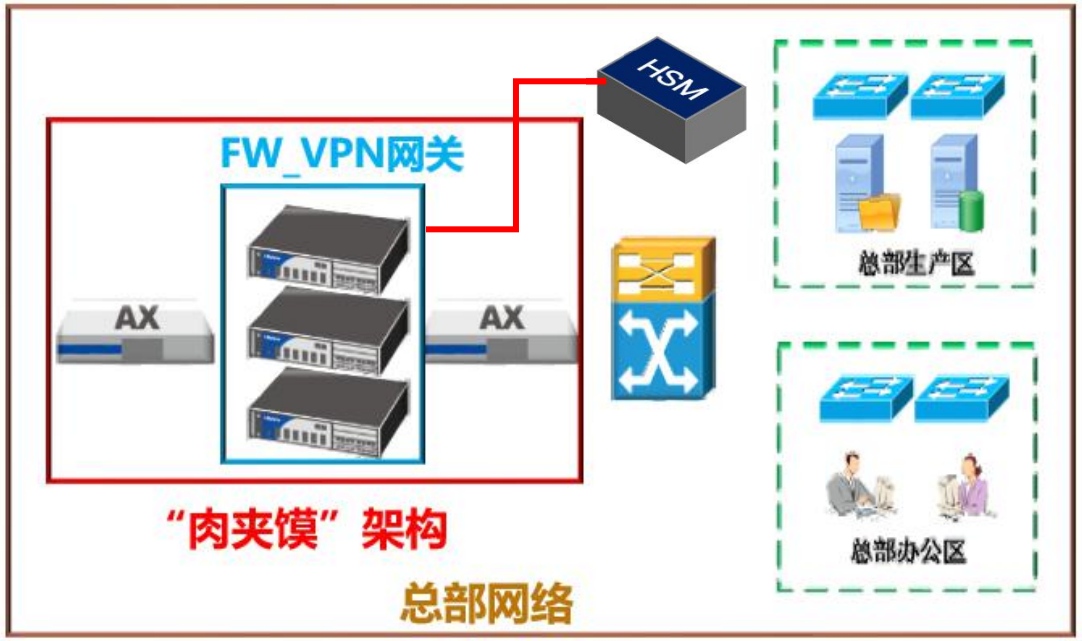
高性能

山石网科产品内置VPN硬件加解密引擎，相较其他厂家基于软件的 SSL 加密方式性能提高 了1 到 2 个数量级。

国密算法

山石网科硬件加解密加速支持所有国际通用的加密认证算法，包括 DES、3DES、AES128/192/256 位、MD-5、SHA-1 以及中国国密算法 SM-2、SM-3和SM-4等。

智能VPN扩展应用场景（ADC+NGFW）



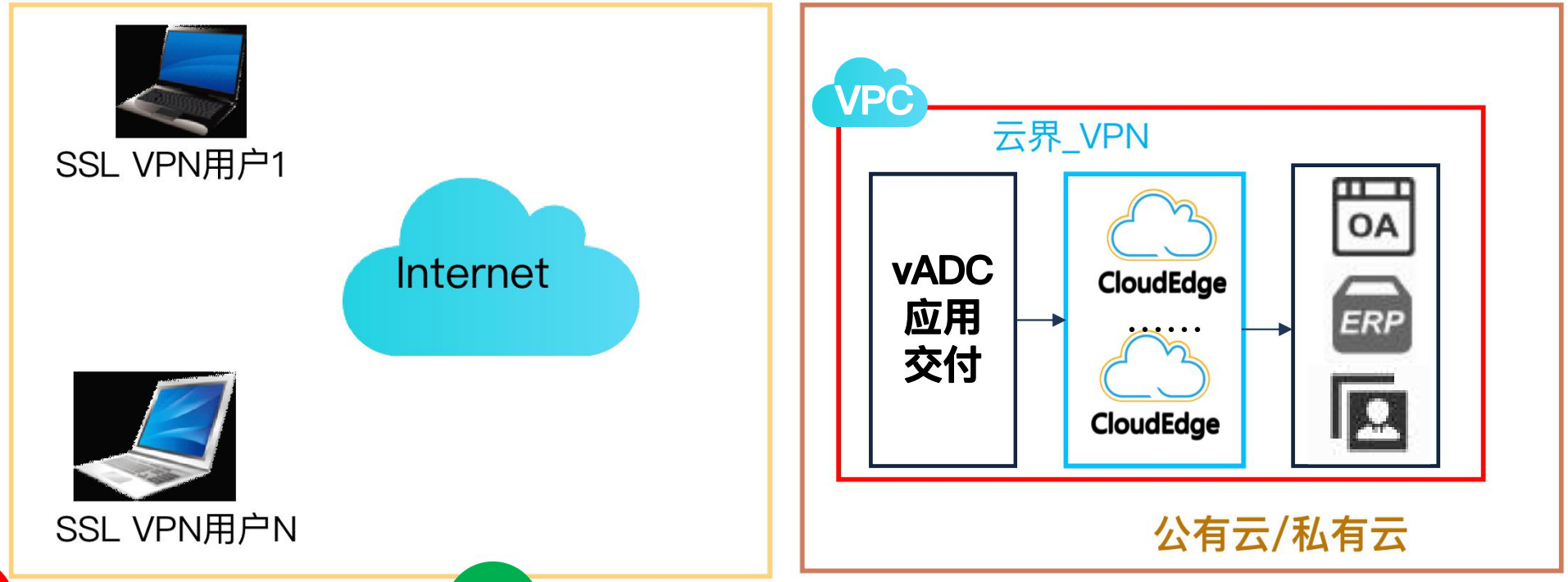
功能

- SSL VPN
- 负载均衡
- 高可靠

价值

- FW_VPN部分弹性扩展、弹性扩展不影响现有业务，确保业务永续
- “肉夹馍”架构解决TCP状态不一致导致VPN连接闪断，提升业务稳定性
- 独特的会话保持与调度技术、为用户业务的高效性保驾护航
- HSM根据SSL VPN用户查询快速定位到所属设备并记录日志（开发中）

智能VPN扩展应用场景（vADC+云界）



功能

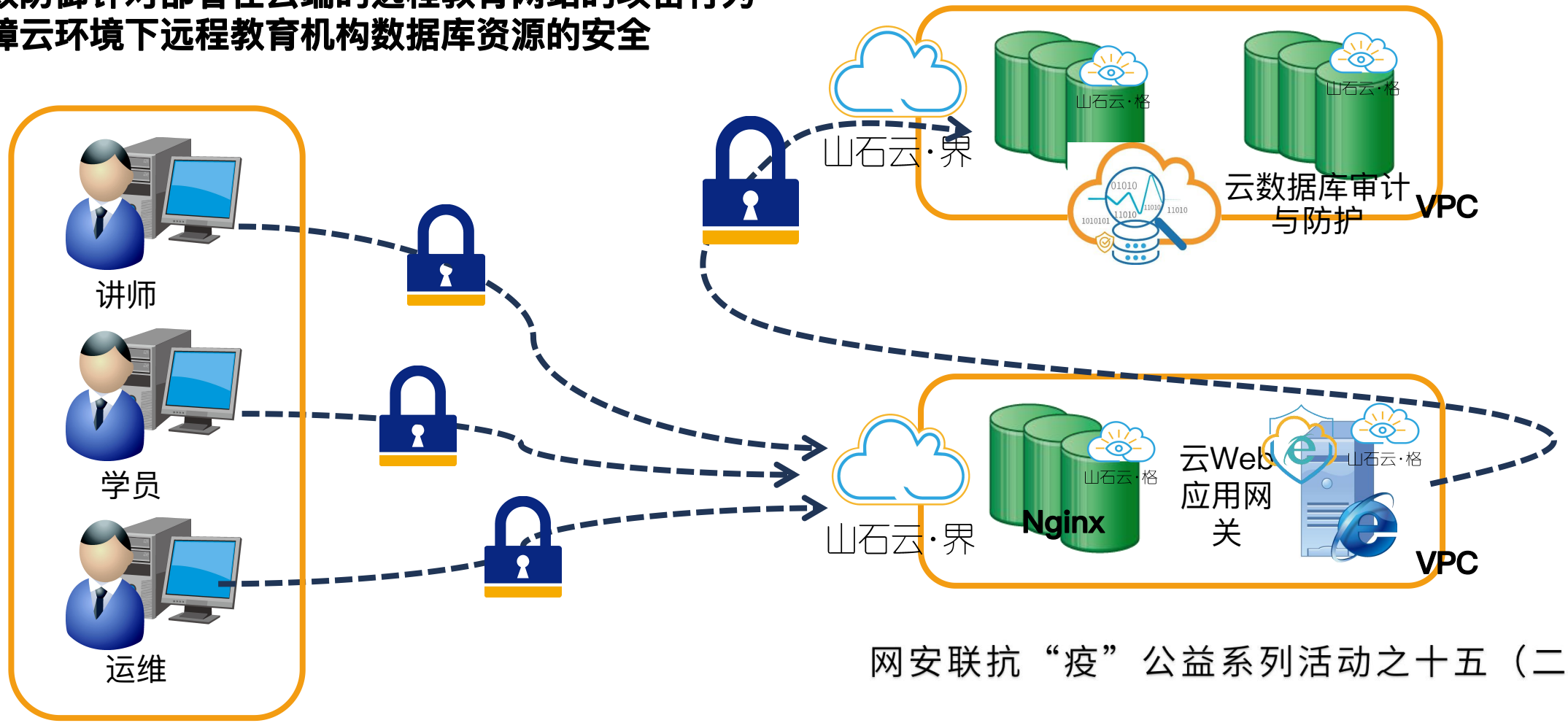
- SSL VPN
- 负载均衡
- 高可靠

价值

- 云界_VPN搭配vADC按需弹性扩展，满足流量和用户数量突增的需要
- 独特的会话保持与调度技术、为用户业务的高效性保驾护航
- vHSM根据SSL VPN用户查询快速定位到所属设备（开发中）

虚拟化接入及安全防护

- 解决虚拟化VPN远程接入及快速部署
- 使用微隔离最大程度上降低远程教育机构云端虚机间的威胁扩散
- 有效防御针对部署在云端的远程教育网站的攻击行为
- 保障云环境下远程教育机构数据库资源的安全



网安联抗“疫”公益系列活动之十五（二）·

“云化”的远程在线教育系统

业务的变革

- 业务系统复杂
- 连续性、可靠性要求高
- 业务系统生命周期快速迭代
- 高并发、大流量

云化的便捷

- 资源共享，提高资源利用率，降低建设成本
- 业务快速部署&响应
- 高可扩展性、高可一致性、高可靠性
- 提高运维效率，降低运维成本

网安联抗“疫”公益系列活动之十五（二）·

便捷与威胁随行相伴

1st 外部网络威胁

黑客持续攻击
恶意入侵
勒索病毒植入
DDos攻击
网页篡改
……

2nd 内部威胁扩散

“内鬼”引发的内部威胁
内部威胁横向扩散
扫描、提权、渗透等动作畅通无阻

3rd 不可视难溯源

云内流量多而杂
互访关系不可视
威胁不可视
服务不可视

4th 云上数据库防护

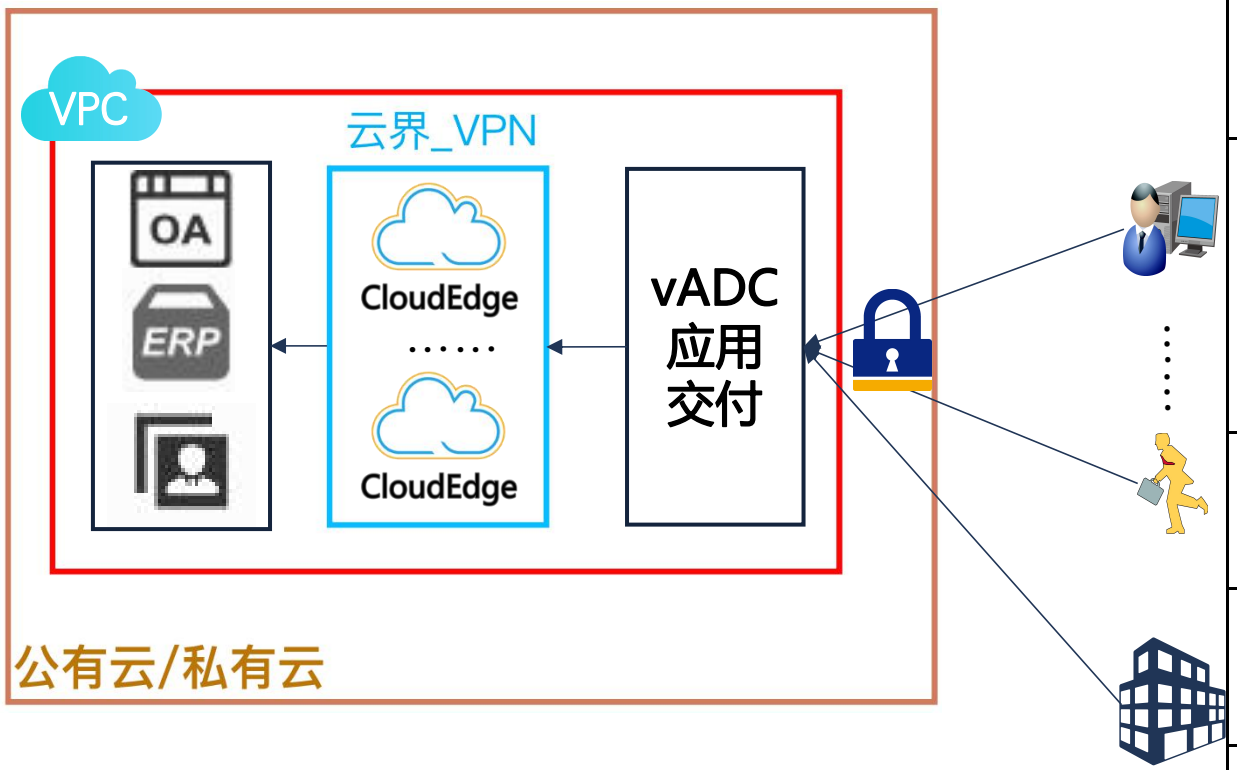
云内数据泄露
云数据库审计
云内数据库高危操作
……

网安联抗“疫”公益系列活动之十五（二）·

云上远程教育亟需解决的安全问题

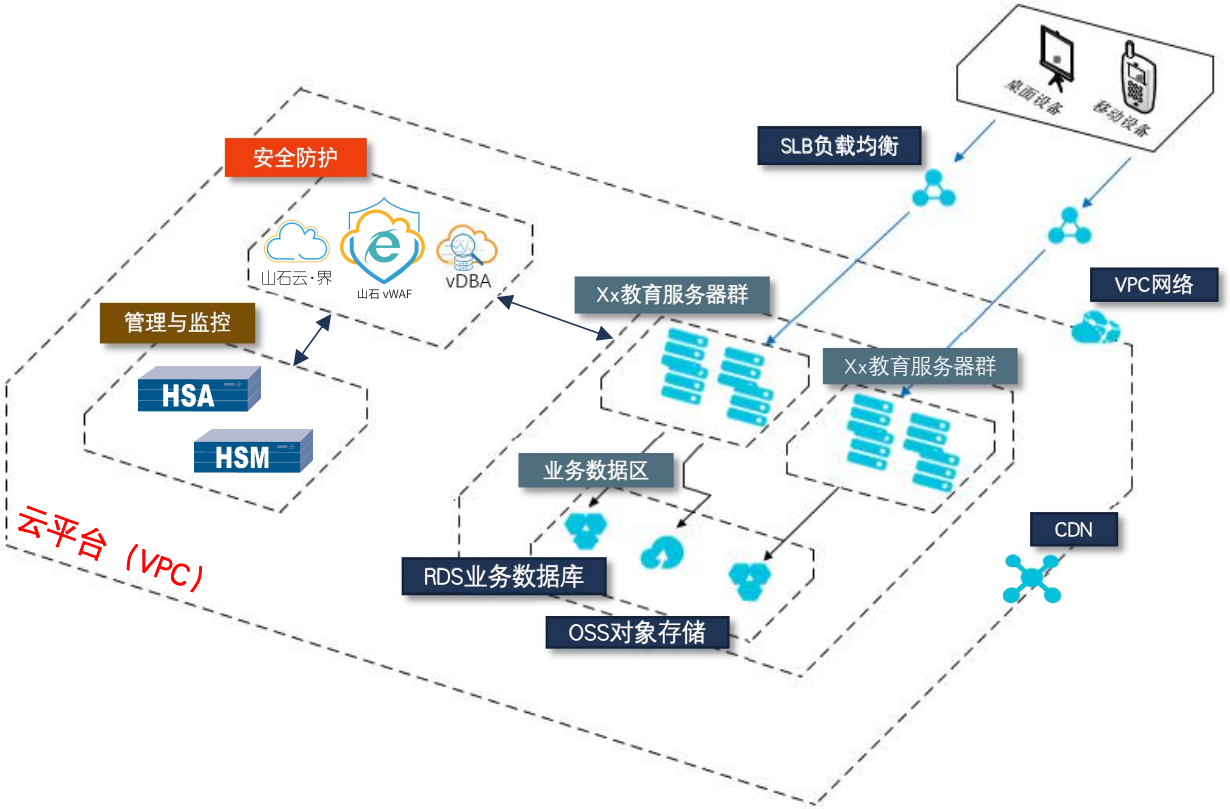
网安联抗“疫”公益系列活动之十五（二）·

应用场景——远程接入，访问云内教育资源



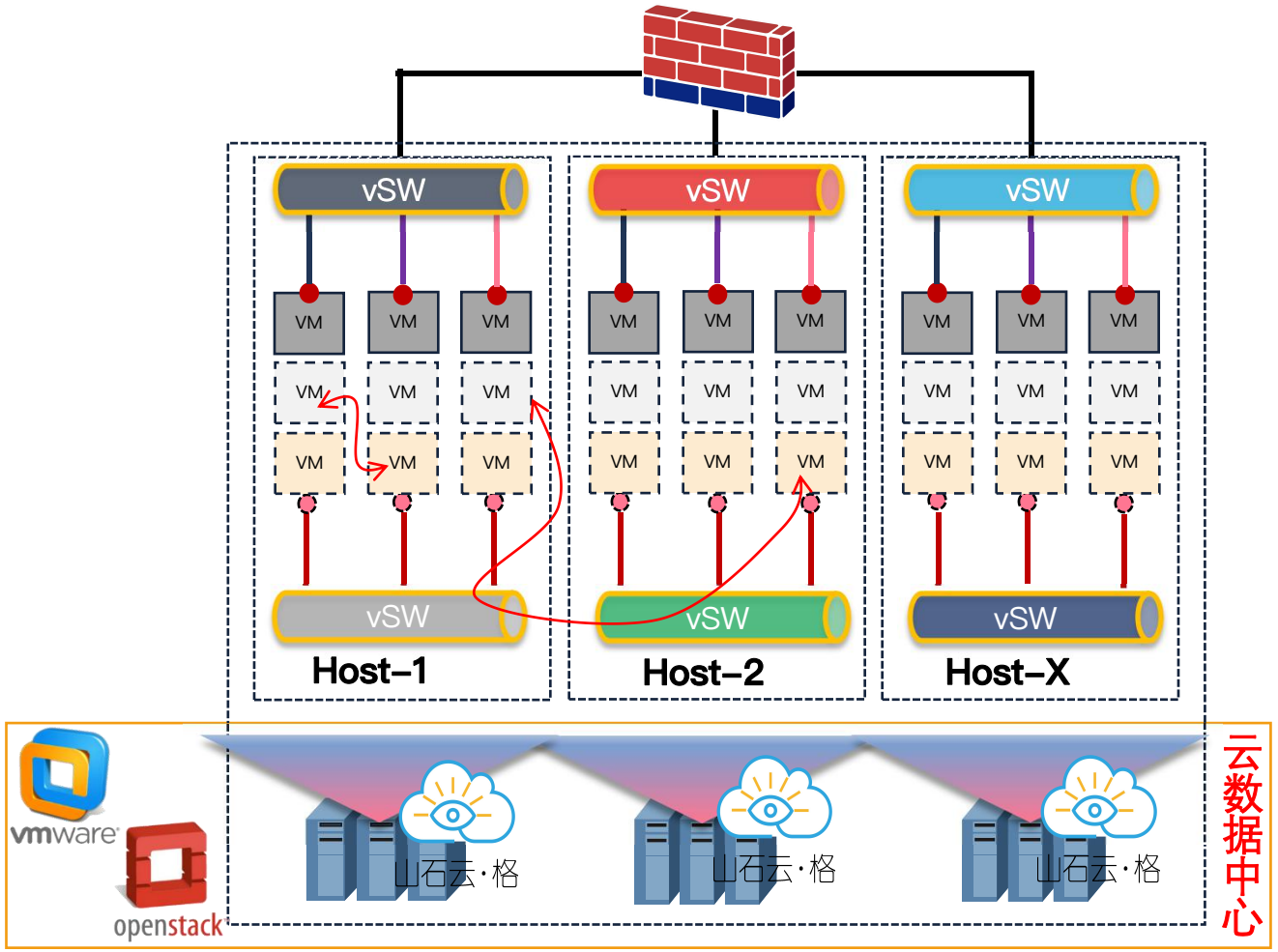
需求分析	• 学生/教师需访问学校内网资源/业务 • 本地数据中心与云端数据中心互联 • “疫情”期间流量激增，避免出现VPN频繁掉线、资源访问不了等问题，需保障持续性服务
方案说明	• 通过在云上VPC出口部署山石云界并配置SSL VPN，可满足教师/学生通过PC/手机等终端VPN拨入，从而达到访问学校云内资源/业务的需求 • 通过两端建立Ipsec VPN，可以实现本地与云端的互联 • 通过山石应用交付产品（ADC）的智能VPN扩展方案，解决由于学员数量激增而导致的VPN掉线、资源访问慢等问题
应用场景	• 远程接入，访问云内资源 • 接入终端激增 • 公有云/私有云
方案价值	此方案能够有效满足教师/学生访问云上内网资源、本地与云端互联的需求，同时通过ADC的智能VPN扩展方案，让运维人员快速完成VPN的扩展和升级，避免因流量激增而导致的VPN掉线、资源访问慢等问题
商机	针对学校、教育机构、在线教育平台的云上业务，主推云界解决远程接入问题，vADC可配合云界实现快速VPN扩展，应对突发情况
案例	广东省外语艺术职业学院、内蒙古机电职业技术学院、武汉电力职业技术学院、广东第二师范学院、……

应用场景二——云上教育业务需全面防护



需求分析	• 互联网测安全风险（如黑客Ddos攻击、入侵、篡改等攻击风险） • 数据安全风险 • 远程运维风险 • 安全网元配置管理&日志存储
方案说明	• 以VPC为维度，通过山石云·界、vWAF等安全网元为云上教育业务抵御外侧的恶意威胁攻击 • 通过vDBA对云上资产数据保驾护航，防止学生/教师信息、教学资产泄露 • 通过统一管理平台vHSM对多个多种网元进行统一管理 • 通过日志管理平台对多个多种的日志进行收集存储
应用场景	• **学校、教育机构、在线教育平台的云上业务** • **安全规划不完备or准备扩容** • **公有云/私有云**
方案价值	此方案能够持续有效地为在线教育的开展保驾护航，从事前检测、事中防护、事后运维审计等多个维度出发，为用户提供持续、可靠、完备、符合等保的安全解决方案
商机	针对学校、教育机构、在线教育平台等的云上业务，可通过**云·界、vWAF、vDBA、vHSA、vHSM**等产品组合的解决方案来满足安全防护、运维管理、审计溯源、等保的需求
案例	太原科技大学、江苏农牧科技职业学院、学盈通教育科技有限公司、桂林电子科技大学、广东第二师范学院、南方医科大学、宁波工程学院、深圳大学城图书馆、……

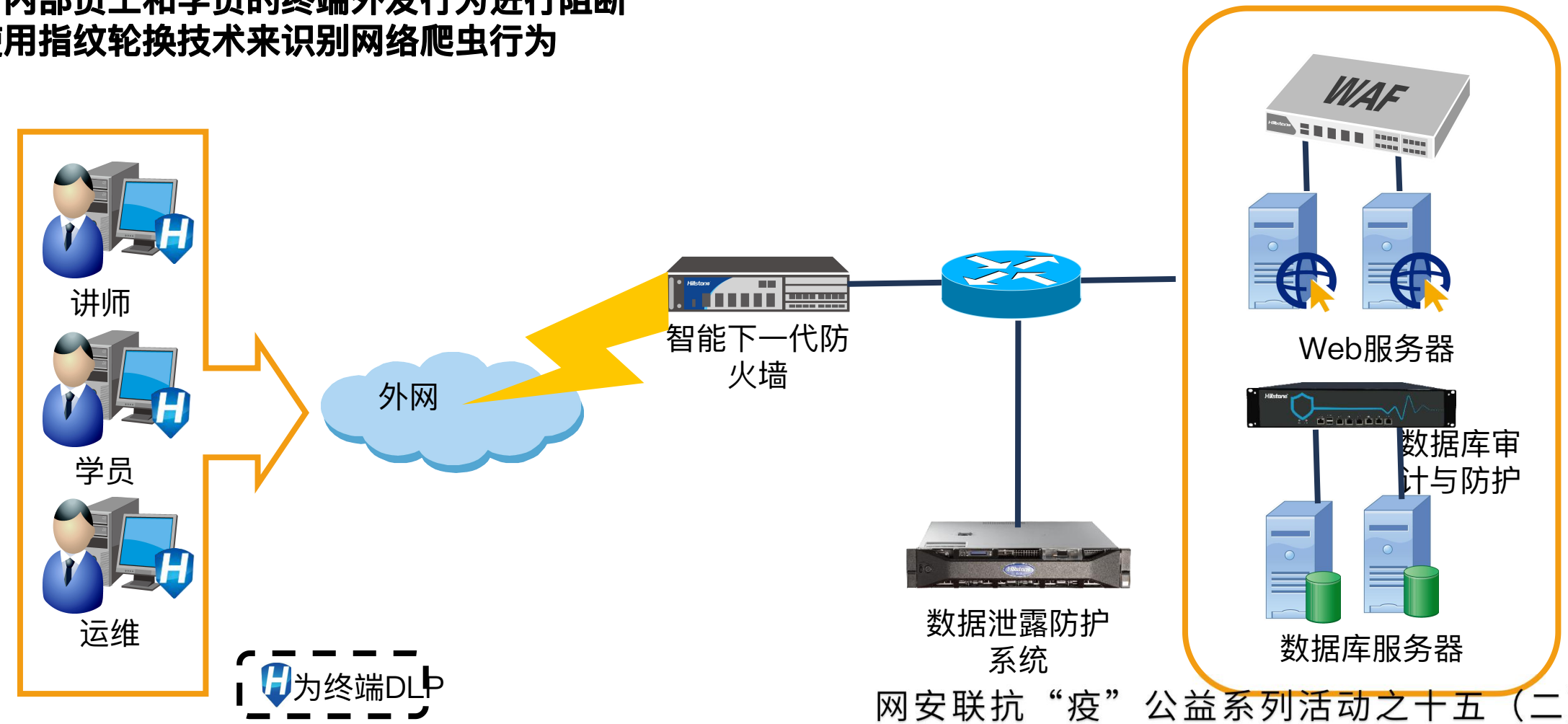
应用场景三——云内“微隔离”，威胁难扩散



需求分析	• 云内东西向流量安全防护与隔离，防止威胁扩散 • 云内流量可视化 • 云内资产业务链梳理 • 云内网络、服务质量监控
方案说明	• 山石云·格以“微隔离” “零信任”的理念，为云数据中心内每一虚机台提供贴身的安全防护，防止因内部威胁而导致的全面扩散 • 通过云·格全面的可视化技术，可清晰地掌握云数据中心内各教育资产的互访关系、业务类型、协议类型，帮助运维人员快速发现、定位威胁、溯源等 • 通过云·格独有的SPM功能，有效监控各教育资产的服务质量，帮助运维快速、有效地发现服务质量有问题的业务虚机，保障教育系统高质量地提供服务
应用场景	• **学校、教育机构、在线教育平台的本地云数据中心** • **私有云**
方案价值	此方案能够持续有效地为学校、在线教育平台等开展在线教育保驾护航，防止因运维不当导致的内部威胁在云环境内快速扩散而导致的业务瘫痪，同时能够帮助运维人员清晰明了地了解云内各业务的互访关系、协议、业务类型，通过持续地监控网络/服务质量，帮助运维人员预知问题、快速定位问题，保障在线教育的稳定开展
商机	针对学校、教育机构、在线教育平台等的本地云数据中心，可通过**山石云·格**解决其云内东西向流量的微隔离、可视化问题，并为远程教育系统提供持续的网络、服务质量监控
案例	东南大学、山西大学、大连大学、重庆理工大学、浙江中医药大学、……

数据安全防护

- 对高危的SQL访问语句与行为进行实时阻断
- 对内部员工和学员的终端外发行为进行阻断
- 使用指纹轮换技术来识别网络爬虫行为



网安联抗“疫”公益系列活动之十五（二）·

远程教育机构数据泄露隐患

远程教育机构数据资产泄露场景

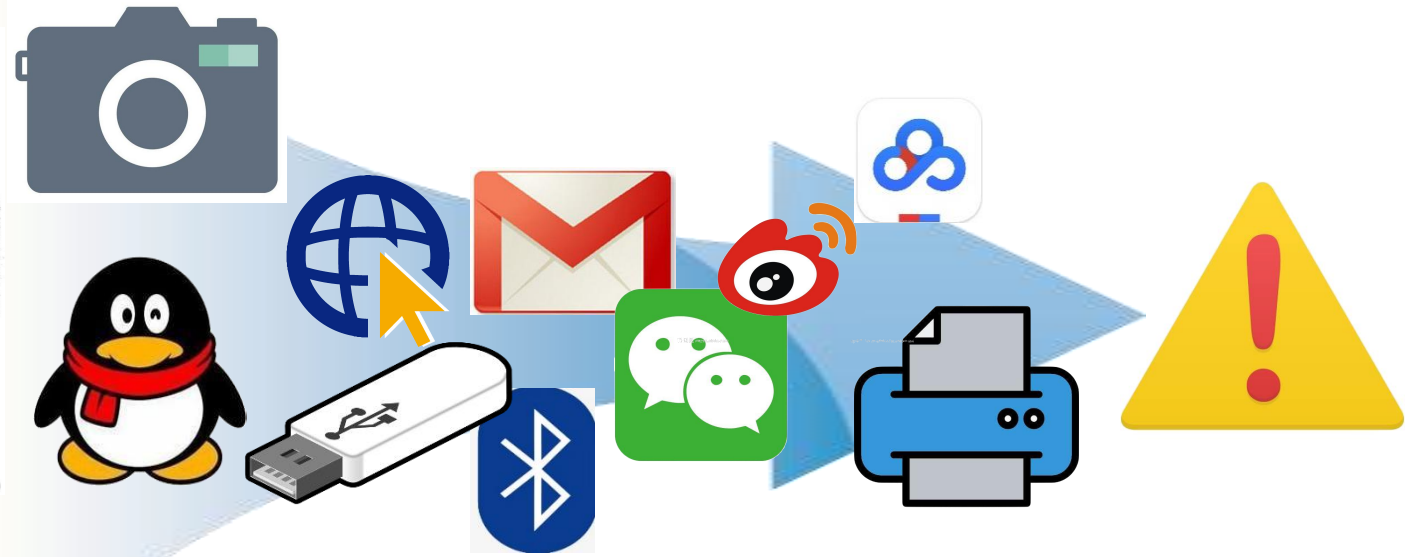
黑客
竞争对手
访客

老师

学生

内部员工
运维
第三方

数据资产

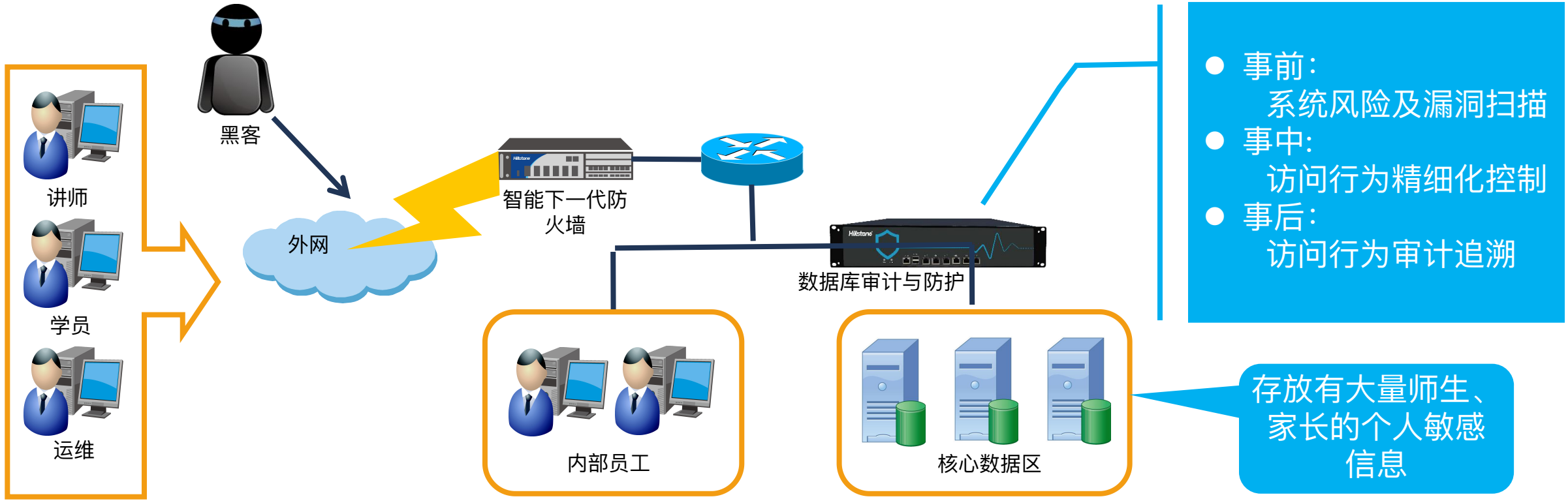


网络黑客攻击
网页爬虫行为
师生无意识式外泄
内部员工有意泄露

网安联抗“疫”公益系列活动之十五（二）·

个人敏感信息泄露防护策略

●外部黑客利用远程教育机构后台数据库漏洞进行攻击并爬取师生、家长个人隐私数据，此时可在事前对数据库进行漏洞扫描，及时检出可能存在的系统危险，防患于未然；
●部分在线教育属于临时业务，学员建立的初始口令多为弱密码，很容易被暴力破解或撞库攻击，此时可在数据库前串接一台DBA防火墙，阻断网络中异常流量的访问行为；
●讲师、运维人员登录高权限账号直接获取学员信息，此时可配置相关策略对账号登录权限进行精细化管理，并对用户访问行为进行审计溯源和控制。



教学资料、运营数据泄露防护策略

可强制要求在线教育学员、讲师、运维安装DLP客户端

- 账号
- 密码
- DLP唯一标识

讲师

学员

运维

VPN Tunnel

外网

智能下一代防火墙

业务服务器

数据库服务器

视频服务器

数据泄露防护系统

为终端DLP

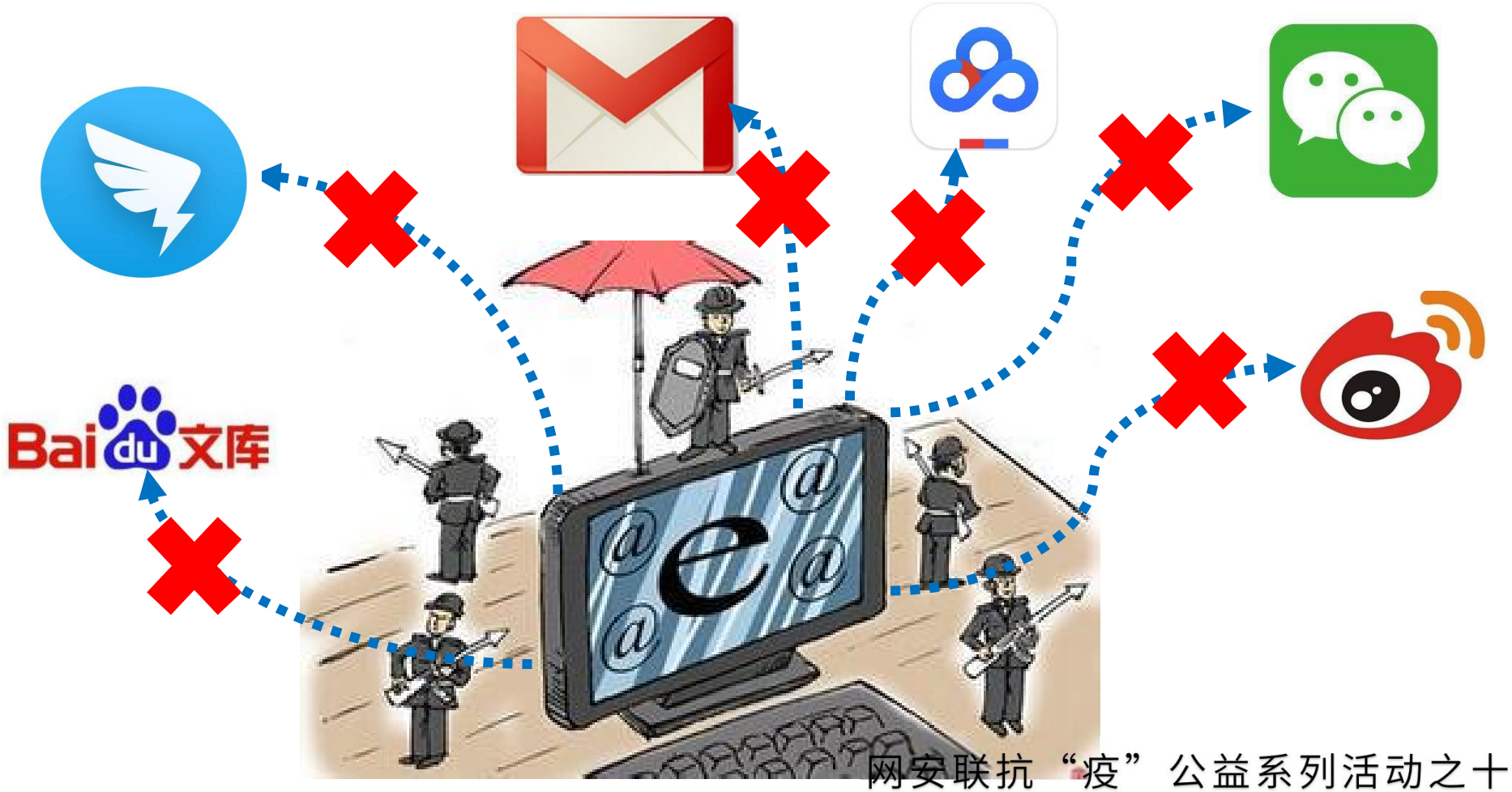
网安联抗“疫”公益系列活动之十五（二）·

应用场景—截屏

在线教育业务中，学员可使用自己的电脑设备访问教学视频、资料等资源，使用过程中存在数据有意或无意的泄露行为，比如有意录屏在线视频用于非学习用途，这种泄露途径就可以通过添加屏幕水印等方式进行标记，一旦发生泄露可以进行追责溯源。

应用场景—通过邮箱等网络渠道泄密

学员、讲师可能有意或无意间将已存在于自己电脑中的课件、讲课视频、押题试卷通过邮箱、网盘、钉钉等渠道泄露出去，为防范此类事件发生，可通过预置策略阻断相关核心教学资产的泄露行为。



网安联抗“疫”公益系列活动之十五（二）·

应用场景—通过U盘等外设装置泄密

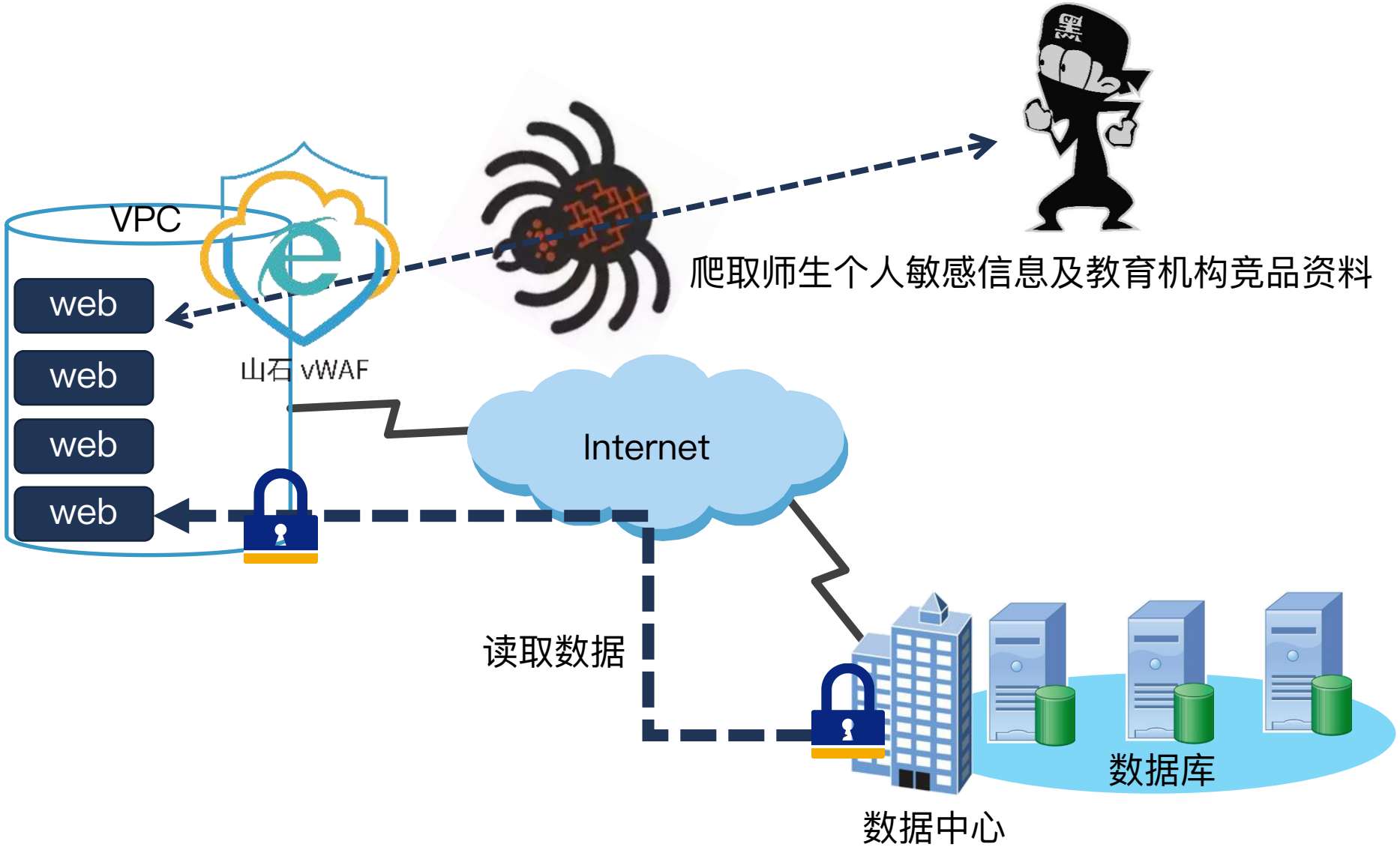
处于商业利益目的，远程教育机构内部员工可能有意将企业运营数据通过U盘、打印、蓝牙等方式泄露出去，为防范此类事件发生，可通过预置策略及时阻断相关外泄行为，并做好详细的审计记录，如此员工电脑的IP、MAC地址、具体时间、欲外泄数据具体内容等信息。

防御远程教育门户网站爬虫行为

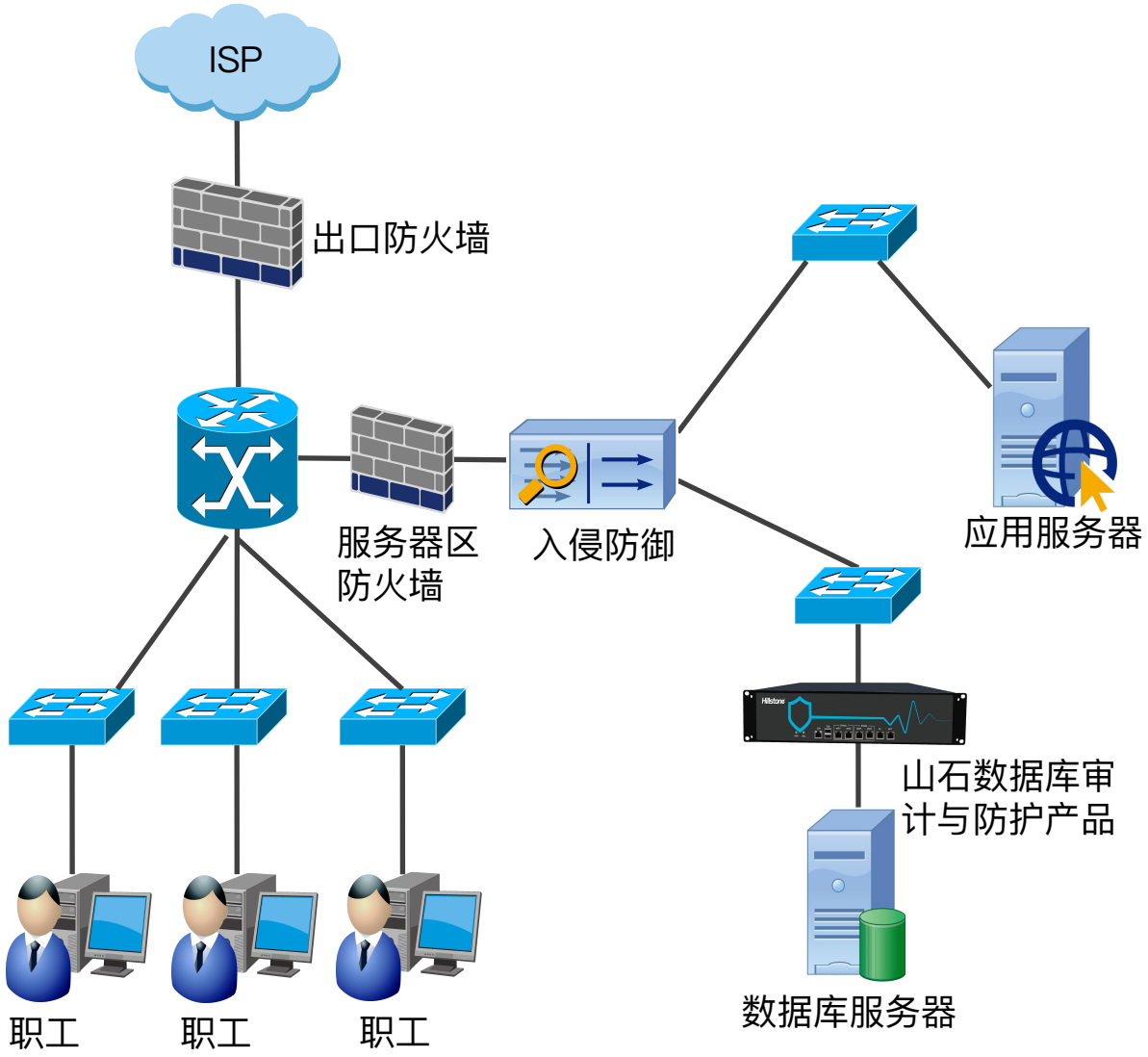
- 黑产可能利用工具扫描&爬取到Excel, Word, HTML等可能包含师生、家长的个人敏感信息的文件
- 某些远程教育友商可能为了取得不正当竞争优势而爬取远程教育机构课程的价格信息

此时可使用使用指纹轮换技术准确分析出恶意机器流量及高级爬虫，做到快速、准确的对黑产行为进行检测和阻断

防御远程教育门户网站爬虫行为



典型案例——某教委“三通两平台”网络安全改造项目



- 某教委“三通两平台”，为其所属的中小学提供教学课件共享、网上精品课等服务
- 用户面临的问题：
  1. 用户业务系统曾遭受恶意攻击，导致精品课程视频数据丢失；
  2. 用户网络安全现状不符合等保规范；
- 用户需求：
  - 对数据库操作日志进行记录，当有安全事件发生后，可以做到有据可查；
  - 满足等保合规性要求（二级）；
- 用户数据库种类：Oracle、MYSQL两种
- 产品方案：DBA2230

网安联抗“疫”公益系列活动之十五（二）·

客户价值

- 网络接入及安全防护
- 虚拟化接入及安全防护
- 数据安全防护

- **实现了在本地和云端的VPN远程安全接入、快速部署、扩展，解决了师生无法登录VPN、业务访问慢及网络闪断的问题；**
- **减轻了Web和应用服务器的负载，提高了远程教育平台运行效率和学员的访问体验；**
- **防止因运维不当导致的内部威胁在远程教育机构的云环境内快速扩散而造成业务瘫痪，同时能够帮助运维人员清晰明了地了解远程教育机构云内各业务的互访关系、协议、业务类型；**
- **从自然人、数据、渠道角度提供全面的安全管理，及时防范对师生、家长个人隐私信息、机构教学资产的泄漏事件的发生。**

网安联抗“疫”公益系列活动之十五（二）·

方案价值

- 在最短时间内检测出复杂的安全违规事件，为IT部门提供多种机会来跟踪和阻止网络攻击行为；
- 实现了在本地和云端的VPN远程安全接入、快速部署、扩展，解决了师生无法登录VPN、业务访问慢及网络闪断的问题；
- 减轻了Web和应用服务器的负载，提高了远程教育平台运行效率和学员的访问体验；
- 为远程教育机构构建一个统一的IT核心资源运维管理与安全审计平台，实现对各种IT资源的帐号管理、认证授权、行为审计的集中管理和控制；
- 从自然人、数据、渠道角度提供全面的安全管理，及时防范对师生、家长个人隐私信息、机构教学资产的泄漏事件的发生。

网安联抗“疫”公益系列活动之十五（二）·

谢 谢

地址

广州市天河区珠江新城华夏路28号富力盈信大厦3805-06室

网站

www.hillstonenet.com.cn

E-mail:

wjzhong@hillstonenet.com

服务热线

400-828-6655