云计算基础与应用 第八章 云安全

原创

晴夏。 于 2020-06-29 14:51:24 发布 3137 收藏 14

分类专栏： 云计算基础与应用 文章标签： 云服务 云网络 云安全

本文链接：https://blog.csdn.net/weixin_43757333/article/details/107008739

以下为自己个人做的笔记，不带有商业性质，纯粹交流分享学习资料，如有侵权，请联系作者，作者看到会第一时间删除，如有侵权敬请见谅。

文章目录

- （很抱歉这一章开始没什么时间搞了…
  所以基本就是语音转文字加配图，也没有对语音转文字有比较大的修改，最近着实有点忙…以后什么时候有空再搞下这个吧）

8.1 互联网安全概述

我们先来看一下，我们也知道在互联网上我们经常会受到各类的威胁，或者说是有各类的安全攻击。这里边我们来看一下，在互联网上我们常见的威胁有哪些？我想呢是这样通过了解威胁，我们才能更好的去了解到我们在互联网上也好，在云上也好，会存在哪些哪些安全上的问题，这样的话我们也才做好更好的去做好各类的防御。我们这里主要列了主要的有一些威胁。首先第一个是病毒攻击，我们也知道黑客经常在互联网上传播各类病毒的代码，比如说这里边比如说我们硬盘也好，或者我们计算机里的系统也好，比方近年来出现了非常多的各类的病毒，对吧？比如说以前出现的熊猫烧香的病毒，他就把我们的文件文件给破坏了，对不对？这样造成我们的文件箱或者我们的系统要再去比如说熊猫烧香，等他去点开我们文件的时候就点不开了，这样的话对我们的系统或者文件造成了无法使用，这是一这一种很常见的攻击。

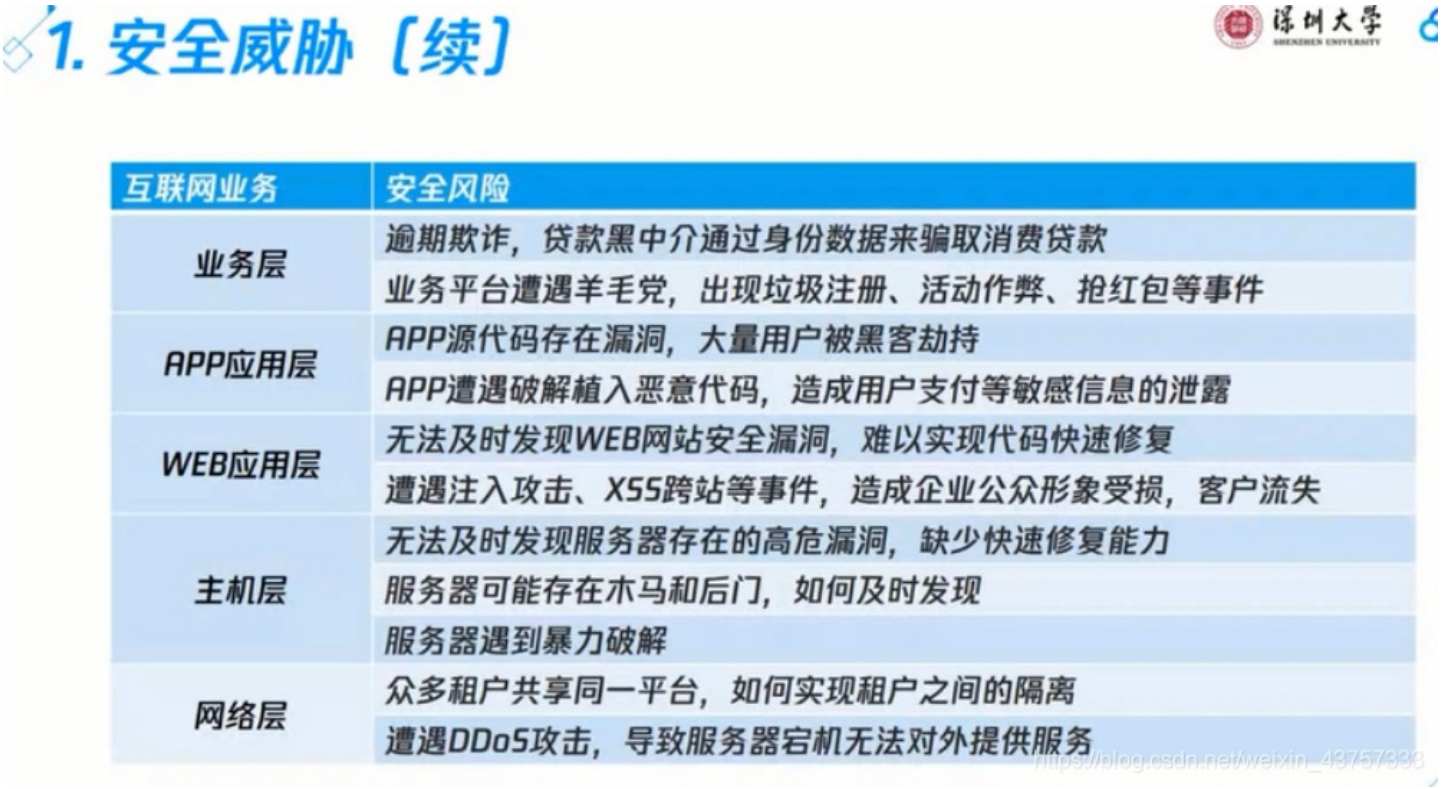
第二个就是木马攻击，木马攻击它是顾名思义它的黑客是通过我们的系统的漏洞，不存在我网站里边的在充在放，再放相应的后门的木马，这个就是像我们工程里面的木马一样把它放到里面去，然后再把我们的文件还有我们的信息进行上传下载，这样同时也可以对我们的系统进行破坏。这个就是像古代的木马工程一样。

第三个就是APP漏洞，这个里面的黑客主要就是利用我们开发者在我们设计APP的过程中，或者说我们一个是设计上的缺陷，还有一个编写代码里边的产生的漏洞，这里边应该来说这里还有在我们传输也好或者app本身也好，应该说很容易。如果我们写的不严谨的话，那里面会产生一些漏洞，当然话很容易一个它并且我们远程的一个控制。第二个就是我们的上传下，上传下载的数据里面它可以把我们盗取过去，还有我们的这里边如果它这里边的验证各方面的不严谨的话，这里也会利用我们自己的漏洞。

第4个，DDOS的网络攻击这个里边我们也知道原来是有个DOS的网络攻击，它更多的对我们的站点对我们的主机进行攻击，这里面要引起我们网络还有我们业务的瘫痪。第二个攻击它它和DOS攻击最大的区别是什么？它是通过分布式的主机更多的主机来攻击我们一个站点，这样的话它产生的应该来说是一个它的隐蔽性更高，因为它是通过大量的大量的攻击，所以它每一个攻击它的数据量，他的所带来的危险是比较小的，但是合起来也是很容易造成我们站点的瘫痪，这个也是会造成很大的一个威胁。

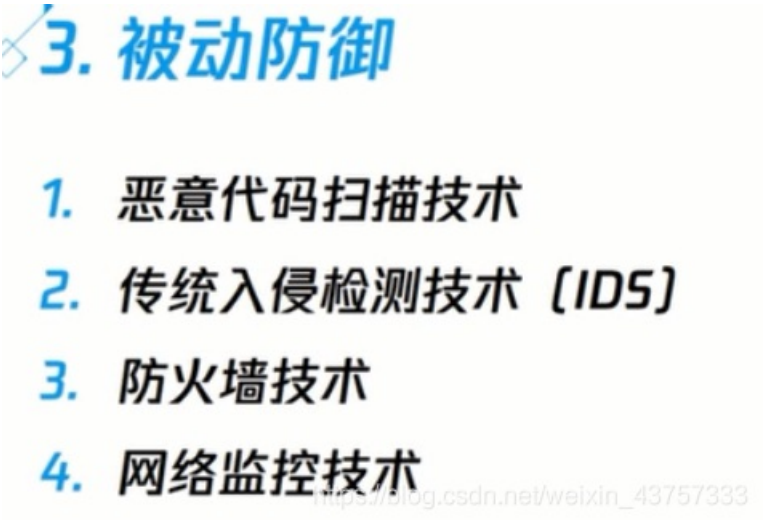
第5个渗透攻击数据的数据获取，这里面主要就是想通过这里面讲了有两个点，一个是渗透攻击，就是说他攻击的过程中他是相当于慢慢的渗透进去的，然后他要长期潜伏在潜伏在我们的系统里边，他他开始的时候我们就感觉不到它的存在，但是比如说他都是和我们的数据库，我们的隐身数据隐私的数据，当然比如说我们的，用户的密码，我们也知道比如说我们多个网站的密码应该说经常是一致的，我们获取了一个之后，其他的也就获取了，而且它这里面一直在里面潜伏着，可能我们发现的时候这叫渗透，我们发现的时候它开始的时候并不是一个很明显的工具，它慢慢的一步步的把我们的系统给侵蚀，这样的话发现的时候已经是这个数据已经大面积的，你可能已经是出现非常大的危险了。

第6个营销的撸羊毛，这里面我们也知道我们经常在各类的网站也好，还有好些系统也好，都会有各类的营销，这里面的营销这里比如说我们发红包也好或者各类的折扣，这里边肯定会有一些对。怎么说这里也可能会有折扣也好，还有营销这里面的一个优惠，这些优惠实际上都是有价值的东西，对吧？在这里边营销录音安保也就是说我们通过发现上面的漏洞，比如说我们的送优惠券，还有这里面的红包，他通过发现里面的漏洞直接就把这些给把这些优惠直接把它拿走了，这样的话应该说看看起来比较小，但你累计起来这里面也是一个很大的损失，这个就是我们目前的互联网网可能常见到的一些威胁。

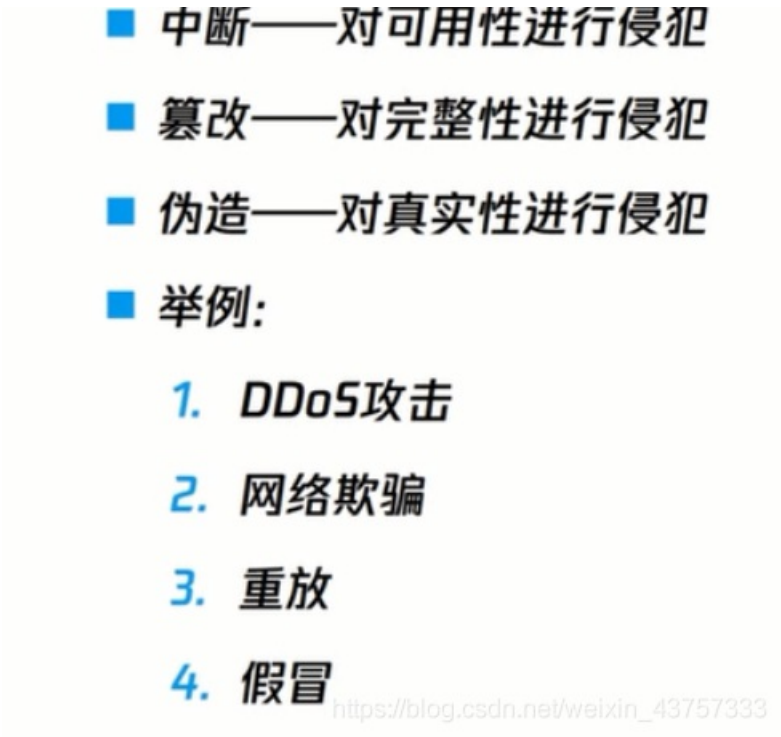


第二个我们再来看一下常见的威胁里边，其实它从不同的层面也得到了体现，这个我就简单过一下。他如果从互联网业务的层面来说，他可以从几个层面来划分，首先就从业务层面我们刚才讲到的，这里边一个就是他这里边讲到的是贷款，黑中介通过身份数据骗取消费贷款是吧？还有我们刚才讲到的如羊毛羊毛杂出现这些垃圾注册活动作弊还有抢红包这些事件，他就利用我们业务上的来进行的。第二个就是APP应用层，也就是说我们APP源代码它存在漏洞，这样的话其实上我们以前也发现有些案例，它比如说我们要注册APP的时候，它就不断的去 APP的时候，他不是要发一个微信的，短信的验证码，短信验证码里面如果她发现了触发这样的话，这也是一个很大漏洞，这样的话如果他不断的去触发这样的话，这个系统其实也是受不了的，因为他是发送短信它也是要支付费用，还有会造成我们的网络的堵塞，还有我们APP里面还有如果是受到破解了，这样的话我们用户敏感信息受到破破解之后有敏感信息的泄露，这个也是会对我们造成一个威胁。还有web应用层的我们web应用层里的安全漏洞对吧？还有各类的攻击，这里边我觉得这一块也是很容易受到威胁，而且这里边如果发现了之后没有及时修复的话，这个也是而且这里边要缺乏一个比较快速修复的能力，还有一个就是主机层的，就是我们的后台里边的这些主机层的，这里边也是比如木马后门这些我们也是要及时的关注的。还有一个是从网络层的网络层，也就是说这里边刚才讲到dDOS攻击，dDOS攻击也就是说如果他从网络层的角度，很多用户他这里边用在一个平台上，他但是如果受到攻击的情况下，特别是DNS攻击，大量的去攻击他，那样的话这个服务器肯定很低档机，这样的话就没办法再进一步的对外服务了，这个是常见的这些危险。

有了这些威胁之后，我想我们的系统肯定要对它进行防御，目前的防御有几块，一个是主动防御，还有一个是被动防御。这里边顾名思义主动防御和被动防御它是从不同的角度，也就是说主动防御是什么？它是从它的数据还有没有它的攻击有没有开始的时候，我们在防御措施有没有就开始已经部署了，或者说已经在起作用了？这个就是主动防御。
这里比如说数据加密，数据加密也是顾名思义我们的数据我们的无论是它存储也好还是传输也好，它还没有对我们发起攻击的时候，我们这些已经把这些已经把它进行加密了，这样的话其实做到了这个攻击之前对吧？
要访问控制，访问控制也是访问控制，也就是说我们的这些数据它在还没有我们不管他有没有攻击，我们对他的访问的控制的权限，我们都已经做好了设置，比如他的用户各方面的我们对他做好了做好了设置，这样的话也是做在攻击之前。
第三个就是权限设置，权限设置也就是说我们对我们的系统里边的这些和访问控制是类似的，我们设置了不同的权限对吧？这样的话它也是在攻击之前。
第4个是漏洞扫描，漏洞扫描也就是我们在我们不管它攻击有没有发生，我们去扫描它里边的我们的系统，还有我们的网络上面有什么一些漏洞，这样的话来有效的避免这个也是一个主动的措施。
第5个密罐技术应该说也是非常有意思的一个技术，蜜罐技术看这个名字好，蜜罐，它相当于一个放的蜂蜜的罐子，对吧？它这里面在网络上它是引用了这么一个概念，我们去设置违章的站点，然后违章他这里边比如说他让黑客让他攻击，只能感觉这个是一个很容易受攻击的，这样的话他引诱这些攻击者去攻击他攻击的过程中，我们同时可以获取这些工具，还有这些黑客他是怎么来工具的，从而我们再去采取这里边的防御的措施，这样的话应该说这个也是一个主动的错行为。我们主动的去设计一些引诱他们来攻击的，这样的话从而保护我们的系统。
第6个就是审计追踪，审计追踪这里面其实我们也知道我们进入各大网站的时候，其实我们都是有各类的登陆的日日志的，这里面也就说我们这也是一种主动的去跟踪我们用户在上面的轨迹，这样的话如果真有问题的时候，我们能够主动的去发现它。
第7个就是入侵防护，这里边这里面它是一个布防的新型的入侵检测技术，它这里面和入侵检测最大的区别，它这里面也是他主动的去完成一些比如说它这里边我们能够主动的去分析它这里边的我们的各类的数据，还有流量来主动的发现这里面有没有问题，入侵检测我们后面接着下来会介绍的。被动防御它这里边有比较大的区别，它是主动的去分析它这里面的数据，还有各方面的它的特征，来有效的发现这里边的攻击。
好，第8个就是防火墙入侵检测的联动，防火墙我们进行相对静态的对吧？他这块联动起来发挥这两个主动的一个发挥这两个的优势，这个就主动的防御，但这里面我们也要说一下，实际上主动的防御好还是被动的防御好，这是我们把它划分出来的，其实应该说现在的各类的技术更多地融合在一块了，有时候它既体现主动也会提，有时也会体现被动。



就下来要介绍的被动防御。背后翻译的从它的名字我们也看可以看到它相当于是在入侵，也就是说入侵发生或者说攻击发生了之后，我们更多的去做的措施。比如恶意代码就是攻击方式的时候，我们去发现它里边哪些是恶意的代码对吧？恶意扫描还有传统的入侵检测，我们去扫描的，我们去检测它哪个做了什么攻击对吧？还有现在的防火墙的技术，还有网络的监控技术，我们来去监控它的流量对吧？还有监控它流量的特征，这里面有效的来发现它我们这里面受到了什么样的一个攻击，我想这些都是被动防御里面经常出现的这些技术。



刚才我们介绍了防御方面，有两个方面，一个是主动防御，一个是被动防御，攻击方面同样也是存在两个方面，一个就是主动攻击，一个是被动攻击。它主要分为几个方面，一个就是中断，也就是说对我们系统引起中断，这里边相当于对我们的可用性，对我们平台也好，对我们的系统也好，当然会引起他的不可用了对吧？这里边就是我们刚才讲的，下面我们例子也提到了DDOS攻击，这里边就是攻击了之后让我们网络堵塞，让我们的系统用不起来。

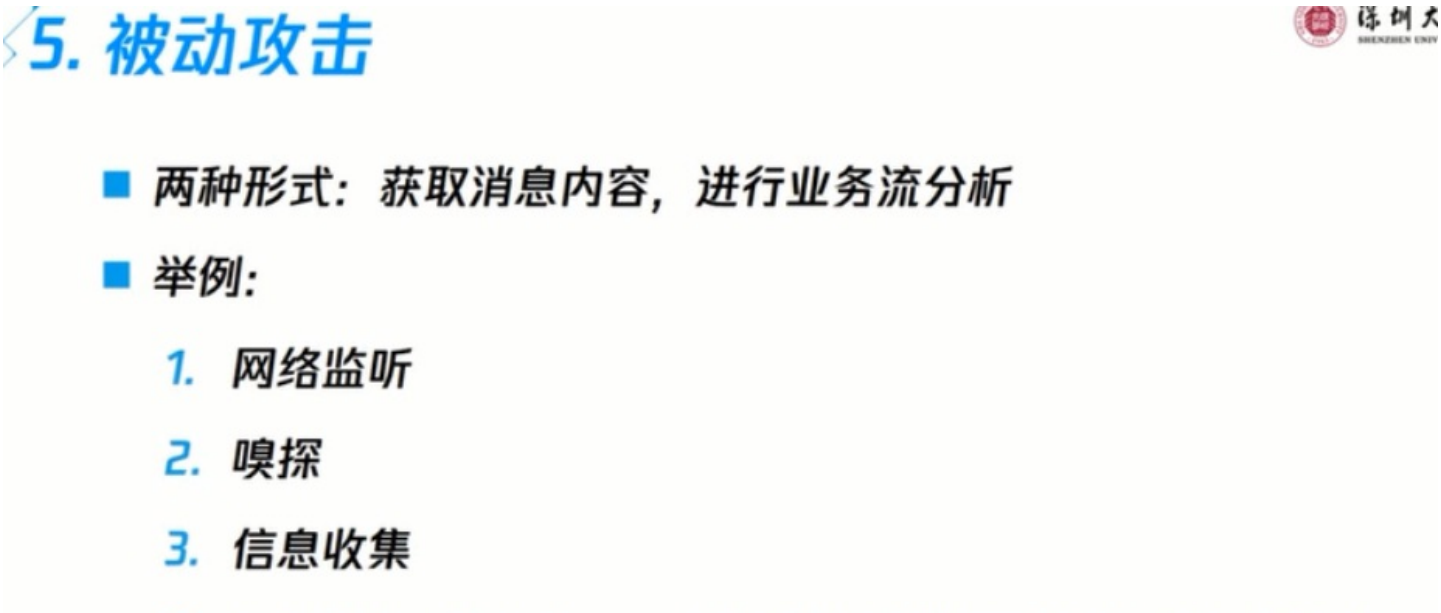
第二个就是篡改，也就是说对我们的数据对它的完整性，也就是把我们的数据进行篡改进行修改，这样的话对完整性进行了侵犯。

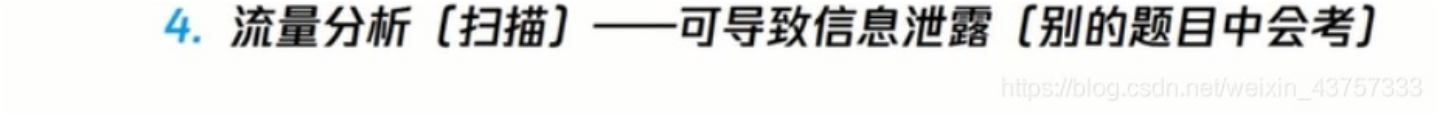
第三个方面就是伪造，这个也是类似对我们也是对真实性进行侵犯了，把我们的数据进行伪造。对吧？这里呢，比如说我们下面有一些例子，其实就是这三类类型，比如说ddos攻击它这里边就是对我们的系统进行攻击，然后还有ddos'攻击也是这里面对我们系统进行攻击之后，我们的系统就不可用了。

第二个就是网络欺骗，这里边就是篡改或者伪造，对吧？这里面也是一样，他利用一些假数据或者说把它的数据进行篡改了，进行是为进行一个欺骗的行为。

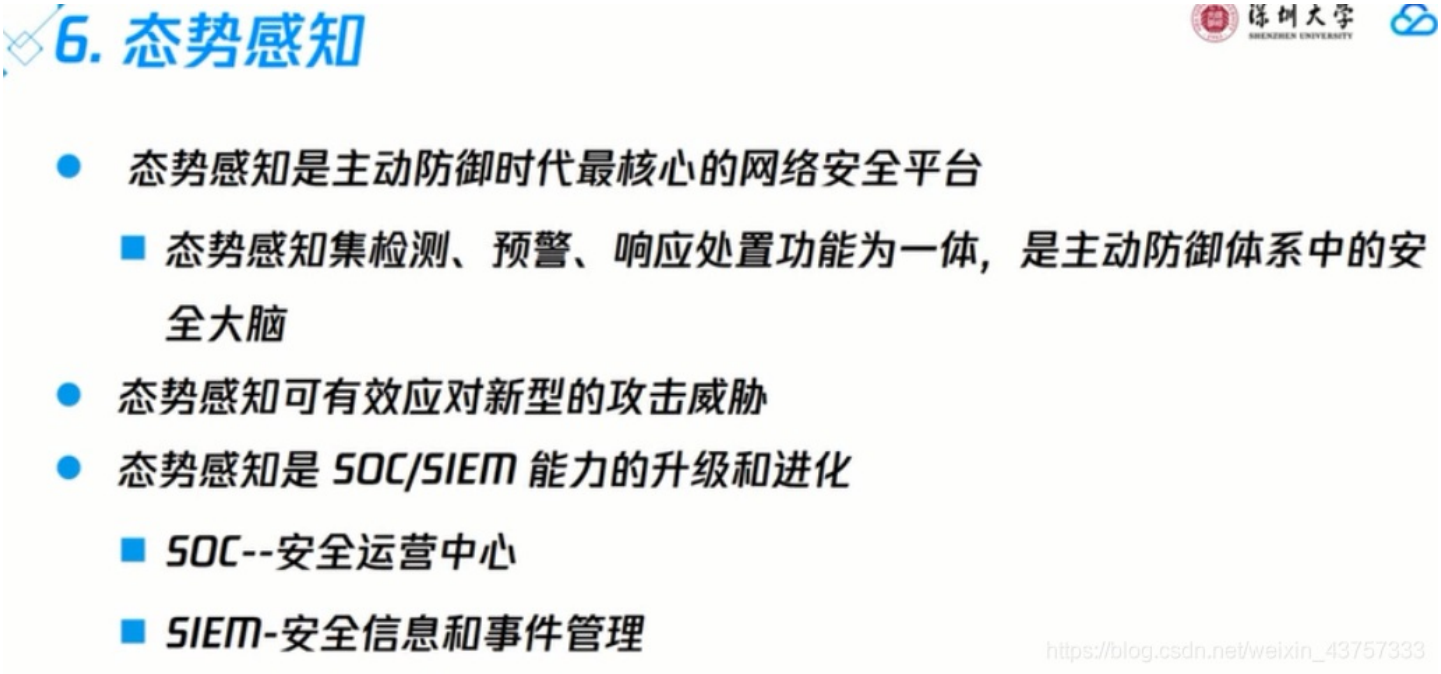
第三个就是从犯，重放它其实上更多的是比如说利用我们的密码信息它重新发送回去这里边或者说这里面更多的对我们这个系统的可用，还有当然是更严重一点的，他有些比如说他看我们去支持去取钱，在网络银行或者是一些支付行为的时候，它获取到这个信息，但它并不能把它破解，他只能是把他的信息再发回去，这里边也是会对我们的系统可用性对吧？也是会发生侵犯行为。

还有一个就是假冒假冒的更多，也就是我们刚才提到的伪造了对我们的真实性用一些假数据对吧？这个就是主动攻击，他主动的对我们的系统进行各类的攻击的行为。





我们还有一个被动攻击，顾名思义它的攻击它并不是主动的对我们的系统对我们的这些数据进行获取或者攻击，这里边它的这里边有两种信息，一个就是获取我们这个平台上或者我们系统里面的这些消息内容，还有一个对进行业务流来进行分析，比如说我们网络监听是吧？我们在网络是监听之类的数据，或许他有效的他想想获取的信息。
第二个嗅探这里边也就是说他相当于是去扫描或者说去扫描这里边的信息来获取到他想要的信息，当然这里边从防御的角度上是扫描，但是从攻击的角度他是去相当于或许他有效的信息，还是你讲的信息收集对吧？还有流量分析，流量的分析也是他就是类似于这里面去分析它这里面的流量也好，流量的数据还有流量的特征来有效地获取到我们系统上的信息。这里也是我们刚才所讲的他做的这些工作，后面比如嗅探他修看了之后，他获取了他这里面扫描到这里的漏洞之后，或者发现了这些漏洞，它后面就可以进一步的去就去发起他的这个行为，也就是说这里面的主动和被动也是可以相互的转换的。



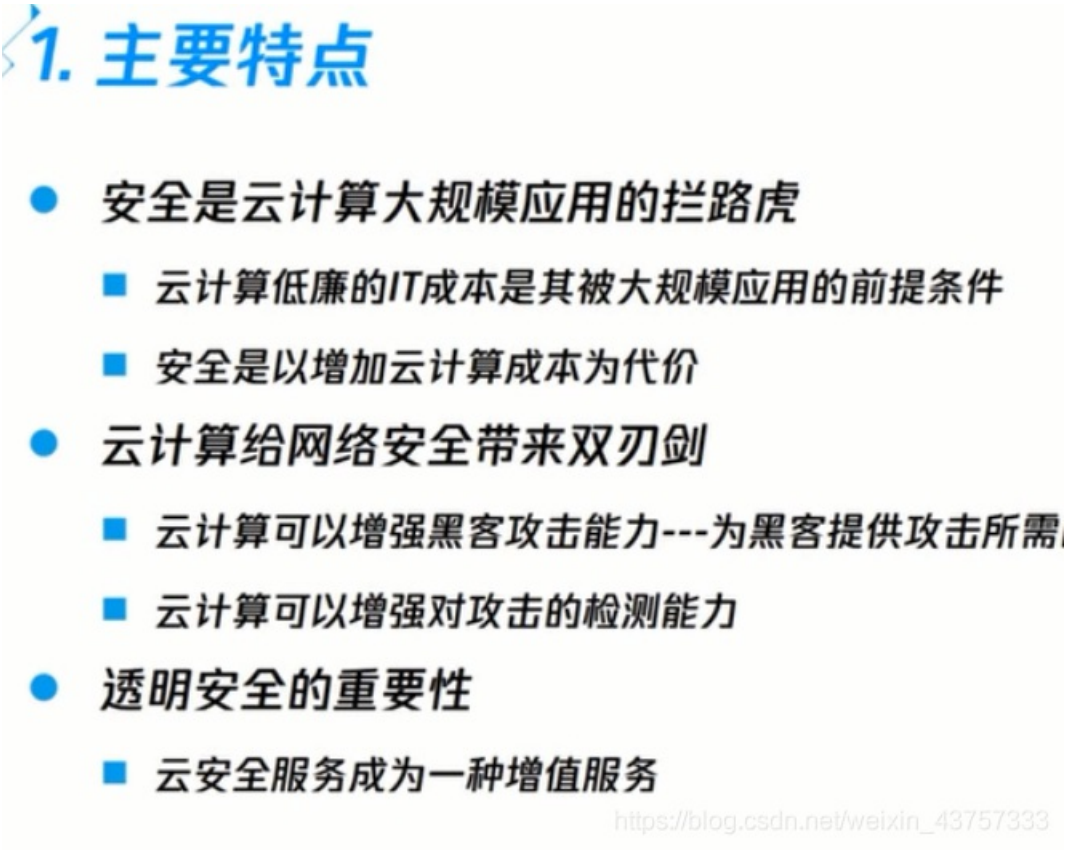
面对这些攻击，应该说目前也做了各类的防御，我们刚才讲到的主动防御，现在还有一个主要的现在一个非常核心的发展方向或者一个技术就是态势感知，态势感知它是一个主动防御，这个比较非常核心的一个网络安全平台，目前应该说在安全这一块很多都在做这一块的工作。态势感知应该说它是通过检测预警还有响应的为一体，它是主动防御体系中的相对于安全的大脑它是它利用现有的人工智能技术对吧？然后有效的去获取到他各类的信息过来。然后这里面提到态势感知更主要的还有一点就是说他获取到这个信息之后，去有效地预测它可能发生的危险，这个概念应该说最早是在军事领域里面提出的，它是覆盖了感知的理解，还有预测这三个层次。但是随着网络的兴起，这里面就放在我们网络上就开始感知了，它的主要的目的什么，是在大规模的网络环境中能够对对引起网络态势发生变化的安全要素进行获取，也就获取到哪些因素可能会引起安全的变化或者引起威胁，对吧？同时他还要理解，同时利用现在人工智能技术，同时他这里边还要去显示这里边可能还必须是他的发展趋势，这样的话在镜头的去进行一个决策，还有行动再做起它有效的防御，也就是说目前应该说它是综合的应用，这里面检测到的各类的技术相当于是一个一个集成起来，然后再进行一个综合的分析，比如现在的人工智能技术是吧？有效的趋势可能发生的攻击，应该说现在是更有效的进行对现在新型的各类的攻击。应该说现在他是感知应该来说也是一个安全运营，还有安全信息的事件的管理，他进一步的提高，还有一个进化。应该说是目前在一个非常核心的技术，现在也是在发展的技术。从几个方面来介绍了我们的云安全，还有互联网上的这些安全知识。

以下不属于主动防御技术的是？A.数据加密B.蜜罐技术C.访问控制D.防火墙技术
D

以下不属于被动防御技术的是？A.网络监控技术B.审计追踪技术C.传统入侵检测技术（IDS）D.恶意代码扫描技术
B

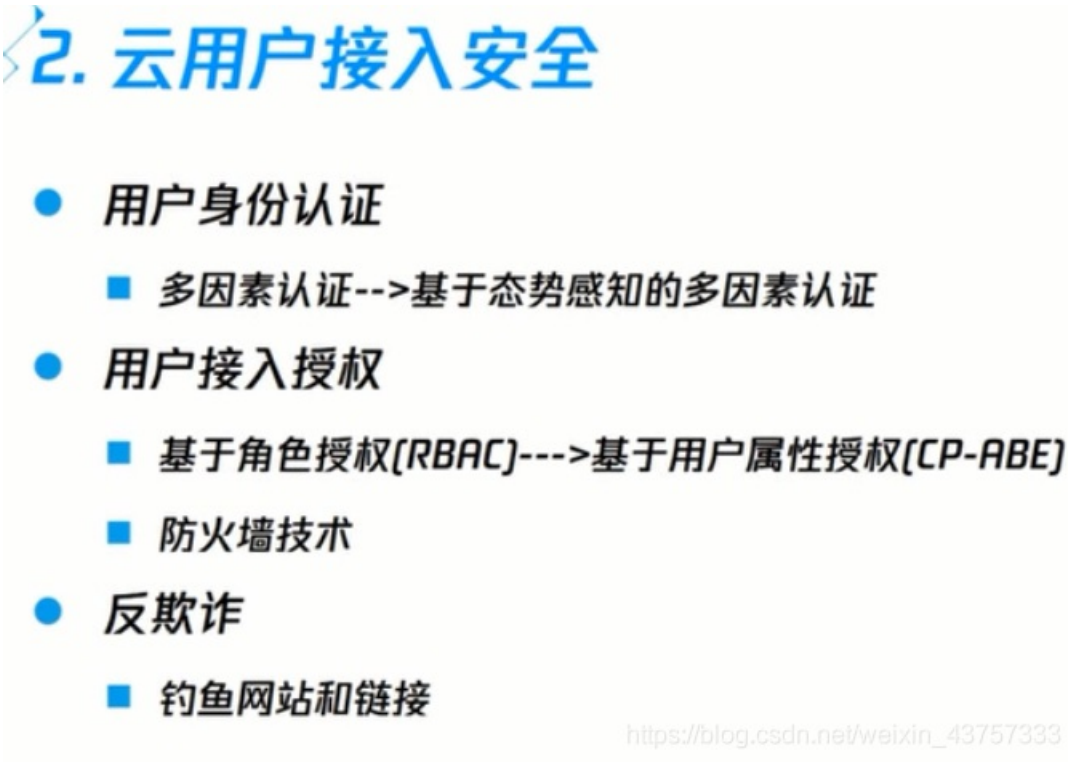
以下哪项属于被动攻击？A.嗅探B.中断C.篡改D.伪造
A

8.2 云安全工作原理



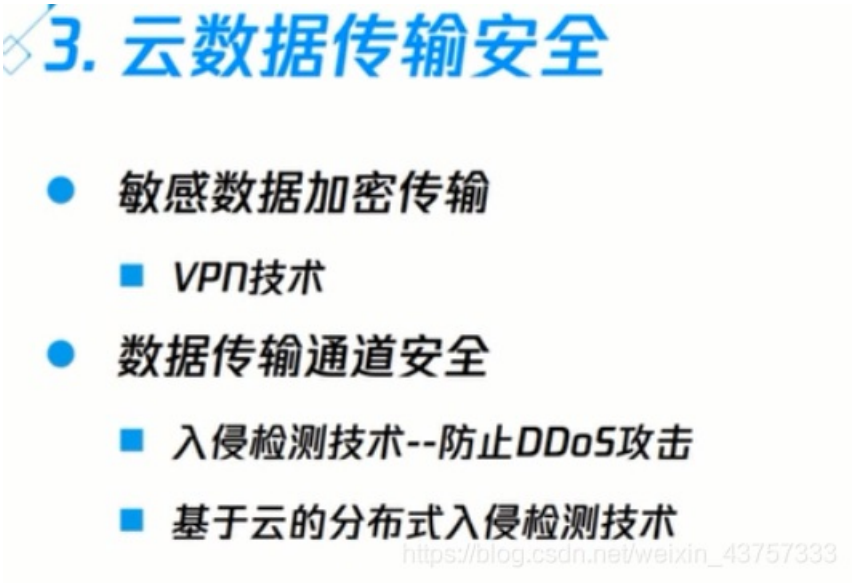
首先我们也知道云计算现在应该说在已经深入到我们的工作，还有各类的生活和应用中，应该说云计算已经深入到我们各个领域和各个行业里边了，这里边云计算应该来说给我们带来了非常大非常方便的使用，对吧？但是这里边应该说我们很多部署很多工作也部署到了云上，但是这里边应该说在云计算大规模的使用的过程中，比如说我们把好多数据都部署在云端上，那这里边呢也会存在一个问题，如果要把这些应用真正的用好，其实安全是非常重要的。其实我们可以想，如果我们部署在任何一家的云上，如果我们部署上面的一个应用，比如 APP应用也好，或者某一个方面的应用，如果老出现安全问题，那的话我实际上首先我们作为我们来说，我们部署的人不敢在上面部署，而对用户来说他也不敢去用部署在云上的东西，对吧？当然这里边所以这里边也提到，首先安全是云计算大规模运用的一个拦路虎，对吧？这里边首先应该说我们现在目前的云计算应该说大规模使用，它是带

来了非常好的非常多的一些好处，比如说我们以前要做一个应用，我们给自己建机房，还有自己去做这个方面的安全防御，这里面其实上对于来说，特别是现在的创新创业来说，小规模的创业者这个难度是很大的对吧？但是我们现在因为有了这些各类的公有云，我们可以在比如说我们腾讯也好，还有其他的公司也好，它各类的云我们直接就可以在上面去租各类的服务器，还有在上面进行部署，这样的话应该说这个是提供了非常便利的，所以这里边而且成本非常低。如果不是的话，比如假如说我们要做一些特别是我们有时候要做一些短期的工作，我们做了大量的服务器，这样的话我们不可能去买大量的服务器回来。但是我们可以做比如说我们做一个很短时间，这里面就大约减少成本，对吧？这个应该说是目前的大规模应用，或者应该说它相对比较方便，而且低廉的成本相对来说是大规模应用的一个前提条件，非常方便使用。但是这里边也存在一个问题，什么问题？我们要真正的把云计算推好，其实安全是非常重要的，但安全应该说它是要我们也知道安全这东西相当于是我们要做保卫工作，保卫工作肯定是要增加成本的，但这里面也就是会增加云计算的成本，在这里面应该说我觉得是一个相辅相成的，你只有把保障好了才会更多人的使用，而且才可能把成本逐渐的降下来，对吧？所以这里面提到安全是增加云计算成本的作为代价的，就是我们向你请保镖来保护，请保镖来我们肯定付出一定的代价。这里边和这里的云计算也给我们网络安全带来了应该说提的是一个双刃剑，应该说有两个方面，一个方面就是云计算可以增强黑客的攻击能力。我们刚才提到了云计算可以提供大规模的计算能力，对吧？这里边应该说对于黑客攻击来说它也是一样，这个相当于是矛与盾的问题了，你我们可以要利用云计算的能力，但是云计算能力也存在一个问题，他也会给他一个可以利用它本来他要去做一些计算或者做一些攻击的时候，它本来是需要这些部署，它有更多的这些计算能力，但是现在用它也是可以通过方便的云计算来得到这个能力，这是一个方面，但同时云计算还是也可以增强我们对工具的抗体检测能力，应该说相当于是一个武器，既可以给好人使用，也可以给坏人使用对吧？给我们我们自己所用的时候，我们还有同时又可以增强对抗的攻击，对吧？因为我们的计算能力增强了，我们的检测能力增强了，同样我们的云安全能力也是会得到提高的，也就说相当于是有两个有两面性对吧？尽可能带来更高的一些威胁，但是对我们的防御来说也会带来更高的一个检测能力。但同时我们在云计算的安全的使用的过程中，我们可能也要注意一点就是透明安全的重要性，也就是说云安全我们希望是看成为一种政治的服务，就像我们刚才所讲到的，所以对安全来说，经常我们所提到的安全的平时我们是感觉不到的，为什么感觉不到？就是说我们在使用的过程中，我们更多的是说出了问题的时候，我发现有安全问题，但是安全这里边也会对于很多用户来说，他可能会觉得特别云上的安全服务来说，他可能会觉得啥？就是我用的过程中我没我觉得我们没有受到攻击对吧？但是其实没有受到攻击有两方面，一个方面可能的确它的安全防护做得很好。另外一个方面就是说他可能刚好那一小段时间，其实上这里边也是小概率事件，网络上的攻击是非常多的，是做多做少的问题，对吧？这里边还有一种工期相对没有引起太大的关注。这里边也就是说这里云服务里面的安全，如果要真正的用户成为一种增值服务的话，是让用户体会到我们这里的安全，而且让他确实感觉到这里边他受到了安全的保护的工作，让他真正成为不是觉得这个相当于是个基本的，而是它这里边相当于是叫像这些人情保镖一样，他觉得这里边是绝对物有所值的。这个也是我们要我觉得云计算的，特别是我们云安全上面需要注意的一个特点。

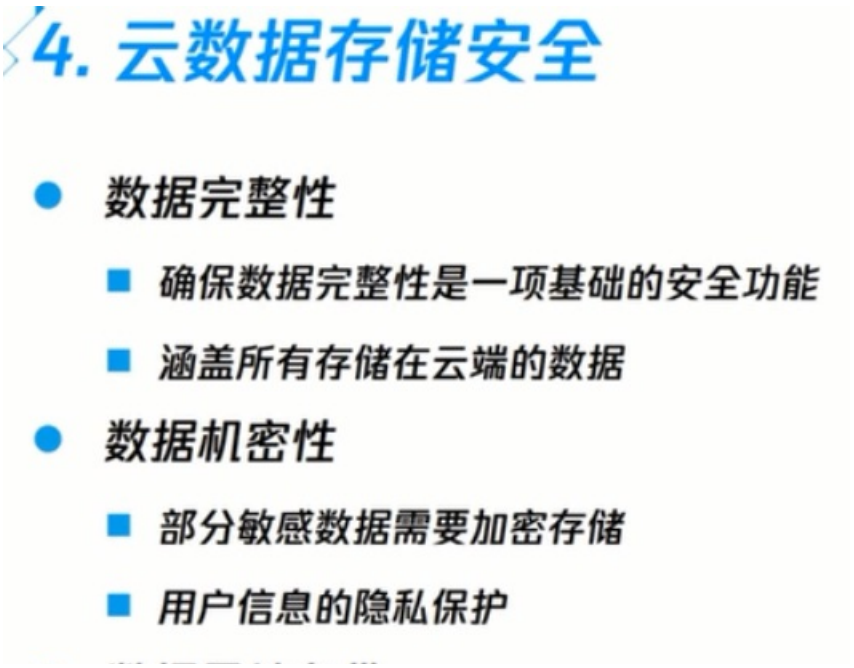


目前我们在云安全方面有涉及到几个方面，首先的一个要云端用户接入的安全，也就是说我们的用户首先要接入到我们云上来的时候，我们第一块要做的你说首先要做的就是用户的身份的认证，也就是我们在他登录之后，我们要对他的用户的身份进行认证，目前的认证应该来说是基于多因素的认证，特别是基于我们目前的态势感知的多因素的认证，这里边就像我们平时说的，为

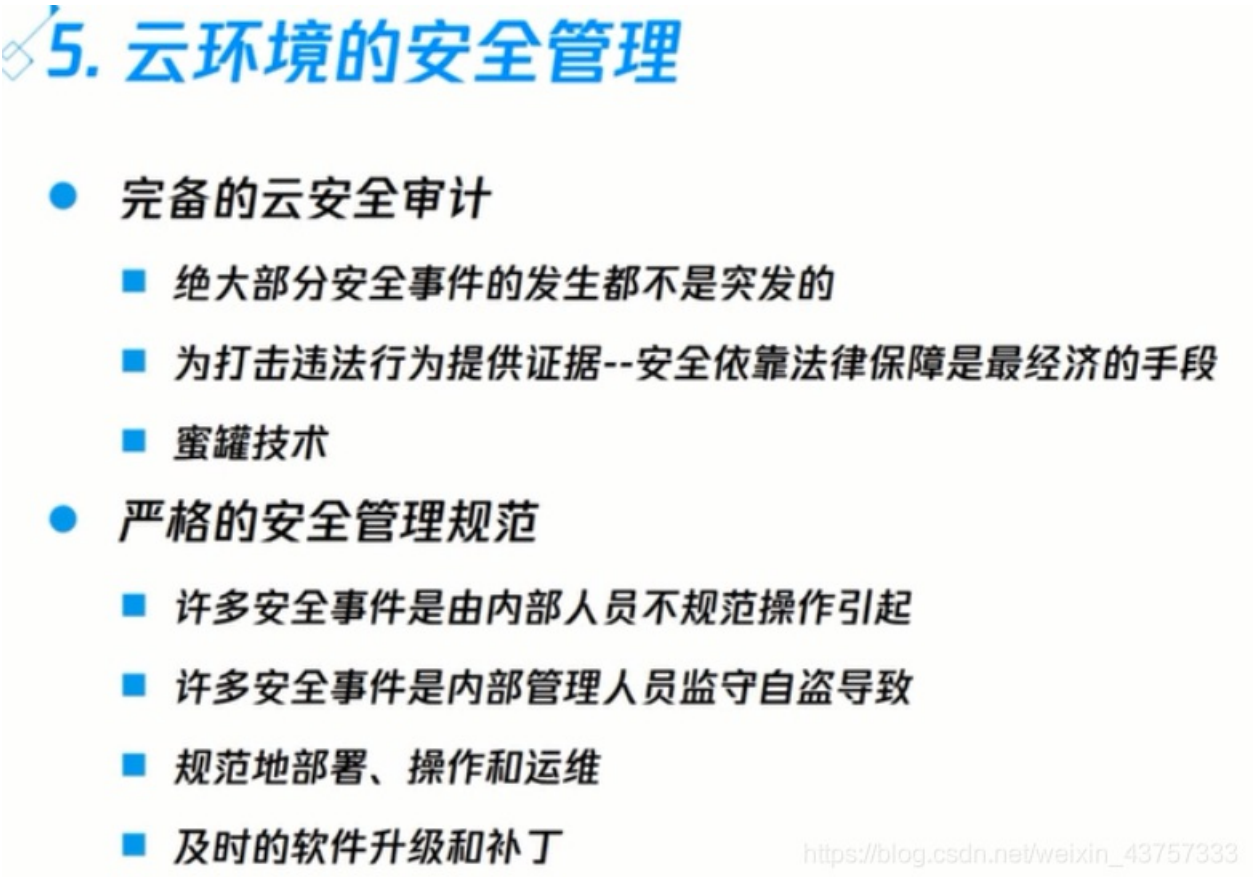
什么说叫多因素的认证，这里又同时发展到基于态势感知的多因素认证。
我们举个例子，比如说我们经常在登录网站的账账户的时候，或者我们登录一些系统的时候，我们是不是经常说我们要收完，账户密码，同时特别我们收银行的时候，我们是不是更加发现从他有个短信验证，对吧？这里边也就是说他有多个因素来保障他用户登录的接入的安全，但是有时候他比如说我们如果是在酒店里面登录的时候，比如我们经常在家里或者到陌生之后，他肯定是要多方验证的。但是如果比如说我们天天的在家里登录，这里边他分析到你地方还是比较还是比较安全的，比较稳定的，它这样的话它应该说它接入的过程中，它就不一定要完全的按照多个因素去验证了，因为他觉得你这个车也就是我们他分析到你说他听说态势感知到我们这里面的地方是安全的，对吧？这个就是基于态势感知，我们发现它环境变化的时候，这里边应该说有很多的感知，其实我们经常用的时候也会发现我们的账户在一个地方，然后到另外一个城市，他可能会提醒小心你的账户是不是被盗了，对不对？
这个也是一个问题。第一个首先有了认证之后，我们这里边还有一个接入的，接触了之后要进行授权，授权里面也就说我们这里面我们的在对里面的使用也好，它有一个授权的过程，授权现在有之前应该说比较传统，还有一个是基于角色的授权，角色的授权也就是说ｒｂａｃ这里边举一个简单的例子，比如说我们在一个公司里边，它不是有各类的级别，比如说有总经理也好，还有各类的级别对不对？这里边也就是说我们在给他授权的时候，我们就要给它设置好什么级别的，它能够有什么样的一个权限，对吧？这个应该说按照角色来进行授权。但是在我们云端的话，它里面还存在一个问题，什么问题？它这里面是要有一个新的技术就叫属性的授权，它为什么要用基于属性的授权，他应该说这个是更加细粒度的，而且可控性更加强。对吧？这里边我们刚才讲到基于角色的授权，它是由运营商来设置，就说他现在系统里面直接给你设置好了，谁是基于什么样的一个属性角色，它就具有什么样的一个一个角色来做，对吧？但是但是在云端里面我们的数据其实更多的时候应该说它是我们作为用户我们就要去受授权他，但是云的运营商是没有办法管理我们用户的资源的，比如说我们上传到云端的数据，应该是我们来授权他，我们的数据应该是有谁来谁可以获得我们这个数据，哪一级的权限。要不的话如果是直接用运营商来授权的话，我们就不大愿意把这个数据放到云端去了，对吧？这个权限应该是我们来定义的。这里边比如说我们现在经常用到的我们学校里边的这些各类的我们登录服务器，我们是老师学生，他的权限都给我们设置好了，但是我们真正放数据的时候，实际上是我们用户的数据，我们是让用户来掌握，这里边比如说我们在我们作为现在医疗这边也是一个非常污热的方向，比如说我们各类的医疗数据，我们的云我们现在在放到云端的话，我们是希望谁能看，比如说各类医疗系统上面，比如说我们是给医生看还是给研究人员看，这个可以由我们来定义我们从我们，用户的角度我们去定义好我们这里边我们这个用户可以给哪些人看，这个就是里边的一个技术。基于用户他接入之后，他的授权中我们经常还授权还会做一个什么，还有防火墙的控制，防火墙应该说是一个非常经典的技术了，这里面防火墙她一个安全一个非常主要的工作，他就要建立比如说IP地址等这一系列的这些白名单，也就是说他哪些基于白名单，哪些可以连接过去，就让它过去，如果是在我黑名单里面的那些地址是我们觉得是非法的，我们就让它过去。这个应该说是也是一种授权，我们这里边我们应该说再把认证了之后，这里面的我们的数据也好，还有我们上面的各类的使用也好，我们要再进一步的给它进行授权，就在认证之后。第三个经常我们现在要做的一个反欺诈，反欺诈制里边也就是说我们用户接入到里边，比如说我们经常在网上也可以经常看到的，我们在网上也会看到有一些有些钓鱼网站，它的一个是利用我们用户一不小心或者说用户的态度小便宜，我们用户到了一个伪装的网站里面，我们敲入我们账户密码，这里面我们就可以就给别人获取或者点着了，他说你中奖了什么之类的对吧？把我们的关键信息给链接过去，所以这里面我们同时还需要一个在我们用户接入端，我们这里面还是需要有一个防的欺诈的一些技术，对，这个是在接入端我们需要这里面做的一块的工作。



用户接入了之后，我们接着下来呢，也就是刚才提到的用户接入之后接着下来，我们就是一个云数据方面的安全了，没数据方面的安全这里边应该说涉及到一些比如说我们的一些敏感的数据，还有一些高价值的数据，这里边比如说我们公司里边它的一些商业的商业高比较机密的一些数据，我们肯定不希望我们的数据被竞争对手知道，对吧？这里边我们要进行一个数据的传输，所以数据传输这里边我们就要保障数据传输的安全。在这里我们比如说基于里面我们经常用到的加密传输，我们就会用到一个技术是一个加密传输里面的一种协议。第二个就是我们这里边的传输通道的安全，这里面也就是说实际上我们的云计算，他的接入就是要接受云盘云平台里面，但是这个云平台里面它这里面它围绕着外围，我们目前比如说有使用的sda的这些路，由我们来进行它的路径的规划，对吧？对它的比如说有一些比较敏感的链接，我们可以把它指定它要用哪些路径，还有哪些路径的连接，来有效的保障他传统传输的安全。这里边我们可以用sdm对路径的安全进行规划来进行实施，对吧？同时我们还要考虑到一个问题，我们之前也提到了防盗别人对我们的攻击，也就是说比如说我们dDOS的攻击，它这里面对我们的服务器进行攻击，而且从分布式的过来，这我觉得我们这里面很需要注意的一点就是我们的数据传输过来之后，我们怎么来防止，因为他一共下来我们可能就中断了，对不对？这里面我们要防止这种传输的终端，也就是说他如果他这里面工具过来，我们有效地需要的传输传不过来了，而且是给他这种攻击的，不断地对我们服务器传之类的数据对吧？这样的话产生各类的攻击，这里我们就要做一个入侵的检测技术，对吧？这样的话可以防止比如说我们DOS的攻击，还有dDOS的工具，我们还同时我们还是要充分的利用这里边的云平台的特点，然后我们这里面也提到了云的分布式的入侵检测技术，也就是说我们可以 GPS也好，还有其他的技术，我们发展分布式的，通过这样的话通过分布式的就是说因为我们的工具不是有一个它也是dds也是分布式的进行攻击，我们同时也是充分的利用好云的特点来建立分布式的陆生节检测技术，这样的话非常应该说这种也是非常适合我们云平台防御，我们平云平台受到 dDOS的攻击或者DOS的攻击，对吧？这个就是在传输层面，首先我们在接入层面，在数据传输层面我们要保障安全。



接下来我们再来看一下我们的数据，传到了云上之后，我们是不是也要保障它的安全？这个就是我们的数据传到云平台之后，这个时候传到之后，我们是不是要把它存储起来，对吧？这个里边也会涉及到我们云数据存储的安全。也就是说我们首先它用户能够接入进来，然后再接着下来，它有效的能够传输，就相当于是我们去举个简单例子，我们去存钱什么的是吧？你首先得这是合法的用户，然后你还能够安全的送到一个地方，送到了之后你还得把这些钱得保存好，对不对？这里面对于我们原来说就是要把这个数据保存好，这个数据保存好的应该说这里面首先我们要保存好的数据，这里面首先一点，我们数据首先一个很基本的一点就在保障数据的完整性，这里面也就像我们的钱传过来之后，你要变成一大堆产品产超是吧？这个钱可能就没办法使用了，也就是说这里面我们存到云上的数据，我们觉得从这里边不管它是有价值还是没有价值的，只要在我们云上存储了的，我们必须就要保障数据的完整性，不要受到破坏，这个也是我们这里提到的完整性是一项基础的安全功能，我们的数据的完整性在我们平台上是要保障的，而且要涵盖到所有的存储在我们云端的数据都要能够保障对吧？而且这些数据在保持上把它完整性之后，这里面我们要进一步的比如说数据的机密性，也就是说我们这里边如果比如说我们有一些比较具有商业价值的数据，或者商业价值比较高的数据，我们就要进行加密的存储，进行一个保密的存储，对吧？这里面也提到比如说哪些是要的，我们这里边有一些是商业价值非常高的数据，对吧？我们如果给人获取那是一个那是一个很大的损失。第二个比如说一些敏感的数据，隐私的数据，我们涉及到个人隐私，还有一些用户的，他还有有个人有比如说单位的对吧？那些因素如果给获取过去了，还有比如我们现在讲的健康数据，我觉得这个都是要受到隐私的保护的，我们这里面就要对它进行一个加密的存储。最后一个就是数据的异地备份，数据异地备份这里面也是涉及到这里边也是应该说是非常重要的一块了，其实不仅在云上之前，我们做各类的线下的各类的服务器的时候，我们也要做各个异地备份，你是为了防止这个数据出现灾难的时候，我们能够有效的备份，比如说出现海啸地震，但这个相对比较少了，它的服务器异地备份是非常重要的，你要不的话一个服务器上面如果只有单一的话出现问题了，后面就会出现灾难性的结果，对吧？这个也是出现一个我们需要做的一定备份的工作。好，这里面我们是从这三个方面分析了，最后我们再来同时我们从技术的层面去保障了接入传输对吧？还有存储方面的安全。



还有一点也非常重要，就是云环境的安全的管理，也就是说我们这个数据我们的放到了云端之后，实际上这里边我们还要注意管理工作，安全的管理工作，整个环境的安全管理工作，这里边一个就是完备的云安全的审计，其实上我们也知道，其实现在也会有一些安全的事件，但是很多安全的事件，它真正发生的时候，它并不是说是突然冒出来的，接上了很多的一些事件，比如说我们经常提到的现在出现的各个我们经常说的很多事情，比如说真正发生的时候，他并不是说突然间就会有一个是平时积累下来的，也就平时的可能你哪个地方不注意，这里面就会发生这个事，比如说有一些有一些人喜欢喝酒后开车，当然现在法律已经严

禁了，但这里面他迟早这个人很容易就出事故。对吧？因为这个是很他平时养成了这么一个行为，那是很容易发生。所以我们觉得这里边还是要做好语音安全的审计工作。这里主要的就是说我们要注意整个机制的建立。还有一点，我们的还要打击违法行为提供证据，就是我们的安全要依靠法律来保障，是对经济的手段，实际上也是其实我们在社会上其实上很重要的就是我们之所以每个人按照自己的遵纪守法，也就是我们能够按照自己的轨道去做事情，是因为我们有法律的保障，哪些能做哪些不能做，法律已经规定了。大家的话在安全上同样是一样，我们要严厉的去打击各类的危害者云安全的行为，对吧？这里边也是如果比如说我们这里边如果出了问题的话，比如说我们现在在街上，像现在我们现在的相对来说，特别在一些大城市里面，它的安全措施做得非常各类的监控，世界很多地方的这些人也说中国是最安全的地方，因为各类有各类的监控，监控做好了有什么好的，就是你任何一个在违法犯罪行为很容易就可以捕捉到同时能够跟踪到很快就可以把你给抓到谁做犯罪的，这样的话正式作用是非常大的。好，第三个就是蜜罐技术，另外我们在上一节也提到了，就说我们可以有效的去，也就是我们平时要把它做好平时的云安全的工作，就是我们要把把这些措施做好，同时我们要也可以去看看我们平时会有受到哪些攻击，对吧？比如说我们可以设一些伪造的这种攻击点出来，然后去有效的去获取它这些攻击的手段来保障我们的云安全，对。这个是我们应该说要建立的是完备的，要有制度，我们有相应的机制，还有相应的方法，我们之前所讲到的各类的防御手段，还有法律的保障，还有我们去主动地去获取一些可能受到的攻击。这是从完备性来上就与安全审计上来做。还有一个就是严格的安全的管理规范，这个也非常重要，其实上应该说目前我曾经有个有一个统计，就是说我们现在的很多安全的问题，它有很多时候并不一定完完全全的受到外面的一个，而且有些可能是我们内部人员不规范引起的，特别还有一点就是我们内部管理员的坚守指导导致的更加严重了。所以我们这里要建立相应的安全管理规范，曾经我们知道有些医院他医院的信息我们知道非常宝贵，但是后面发现真正因为他其实在医院里面他也做了各类的防火墙，相应的各类的安全防御措施都有，但是有曾经出现过有些医院的数据泄露，后面发现他是真正的数据系统，并不是说真正的他别人给别人攻破了，它的系统它是怎么样的，它里面的工作人员，比如说里面的工作人员，他他是保安人员或者其他人员，他是趁着系统打开的时候，他就把这数据把它拍下来了。所以这里边应该来说我们也是非常要注意的，就是内部人员的培训管理，还有我们这一代要做的一个规范的部署操作，还有它的运维，同时我们要及时地进行软件的升级，还有补丁，因为我们也知道这里面的各类的安全也好，个也是在不断的在发展的。我们要不断的进对这个软件也好，还有各类的补贴不断的建立这个升级，同时打上相应的各类的补丁，因为病毒也好，各类的攻击实际上都是不断的在发展的，对吧？应该说我们通过这几个方面，一个接入、传输、存储，还有在做好规范的管理，有效的把我们云安全这方面的管理的有效的建立起来。好，给各位同学介绍了这几个方面。

以下说法不正确的是？A.云计算服务不存在安全隐患B.安全是云计算大规模应用的拦路虎C.云计算给网络安全带来双刃剑D.安全是以增加云计算成本为代价
A

以下属于云用户接入安全技术的是？A.基于云的分布式入侵检测技术B.用户接入授权技术C. VPN技术D.入侵检测技术
B

云数据存储安全不包括下列哪项？A.数据开放性B.数据完整性C.数据机密性D.数据异地备份
A

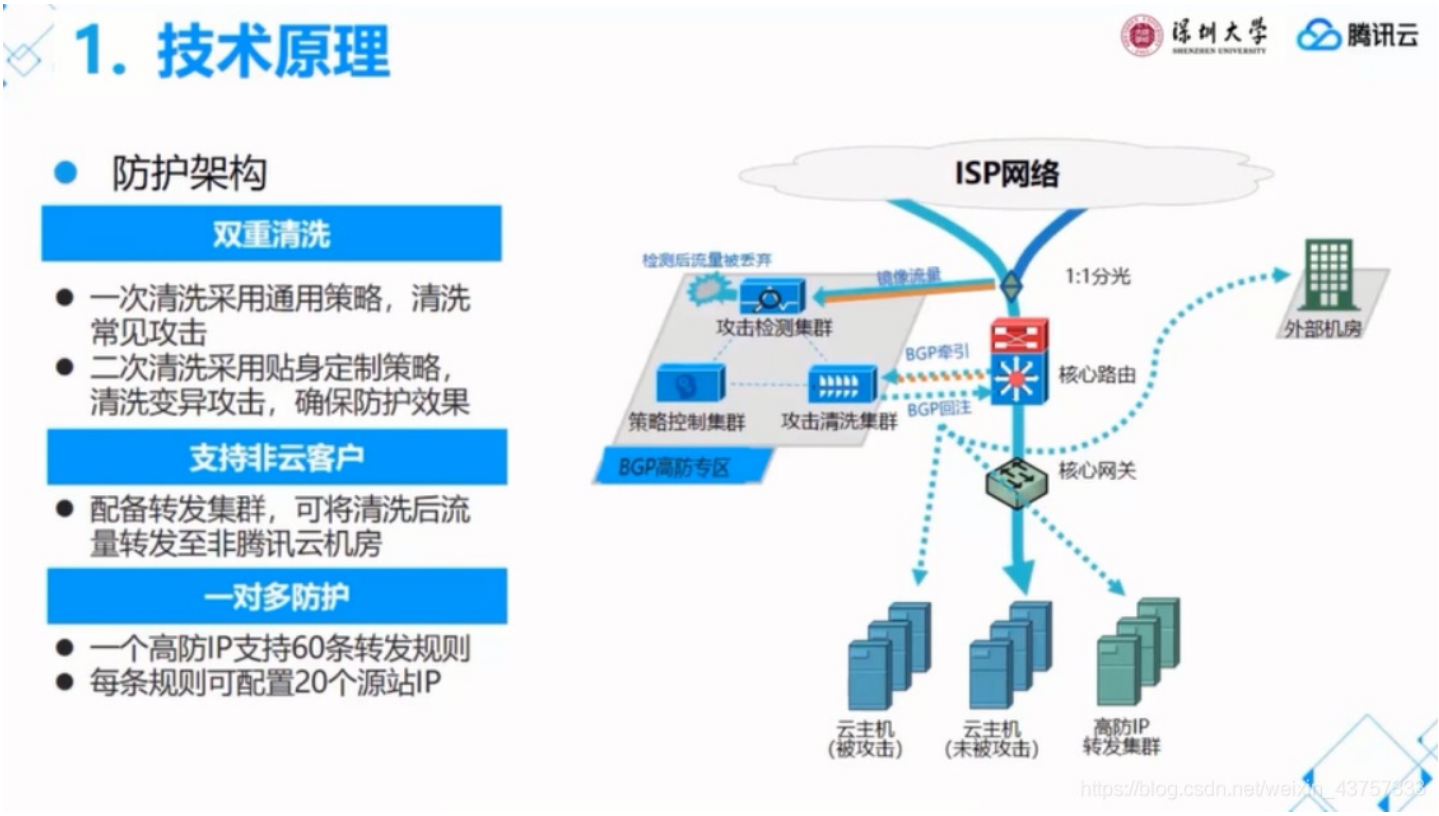
8.3 云安全技术

提供的产品叫大禹系统。大禹的话它主要是做什么？然后他是怎么网络这块提供的产品叫大禹系统，大禹的话它主要是做什么？它是怎么实现的？用它的一些优势和它用在什么地方，这是我们本次要讨论的内容。

在这里插入图片描述

那么首先我们看这样一个图，然后左侧这是一个勒索的邮件，如果你不在规定的时限内向我们支付比特币，你的服务就会受到严重的ddos攻击。其实非常无奈，因为说我们随随时随地都可能会受到DOS攻击，并且不需要什么漏洞，它只需要以海量的流量来访问你即可。
像在这里的话，它攻击的一个低廉的成本，100GB以下的攻击流量，用户只需要去付费，200就能攻击一次，600就能包一天。那么经过这么多年的发展，其实DOS的产业链条已经发展的十分的成熟了，各个团伙之间分工也非常明确，合作非常紧密，俨然的形成了一个井然有序，不断扩张的地下市场，而各个链条的获益的模式也不尽相同。比如说有出售工具的，像这地方是全面蔓延的今天许多DOS工具在网络上可以直接免费下载，但是一些质量好的有特殊定制服务的软件，还是需要通过专业的制作团伙去购买。那么软件的作者一般会根据攻击团伙的需求，编写这种定制化的软件，并收取费用，这样的话出售这种攻击流量，莫说我们除了说有攻击工具之外，我们发起的这种ddos攻击还需要配合一定的流量。一般而言这种通过抓肉鸡去构建咱们僵尸网络，来获取流量，他耗时耗力，并且不够稳当。所以当我们一些攻击的时候，我们会选择向流量平台去租用流量。
那么据说我们的安平情报团队调查，流量的供应商会把所掌握的流量的管理权限有偿的提供给攻击者去实施我们的网络攻击，一般是按量付费的。那么再就是说接单的中介抽水，顶多是的。黑产的他已经高度成熟，并且催生出了产业链条中的中介服务。也就是说接单中介最基础的模式就是接单人员说收到客户的基于不同需求的第一单是一单，包括填单等这种订单之后，再把单子分发给具体相用攻击的人。那么这样的话根据目前对黑市的调查，完成各地单他这个报酬根据攻击难度跟攻击市场从上百到上千都不等，那么中介再去按照协商好的比例去那么再就是攻击者的直接获利，像在黑产中介中，或者说我们整个产业中，ddos攻击者不再是这种单纯去发泄不满的年轻人，也不再是组织攻击的主角，他们更多的是客户所雇佣的打手，通过接单中介或者说通过自己直接接活，然后黑场人员他这个月收入可以达到15万元人民币，巨大的一个潜在的利润，去驱使说攻击者不断的去铤而走险，也使得说攻击成为互联网企业中他挥之不去的梦里。
像在这里我们会谈到你其实没有办法，你如果说不想付这10比特币，你应该怎么做呢？你就申请更高的带宽部署更多资源的服务器，这个成本会更高。那么要不然我们去购买这种非常昂贵的这样一些设备，我们说首先管理起来很困难，而且那种设备也是价格非常高的。那么现在有没有什么好的办法呢？

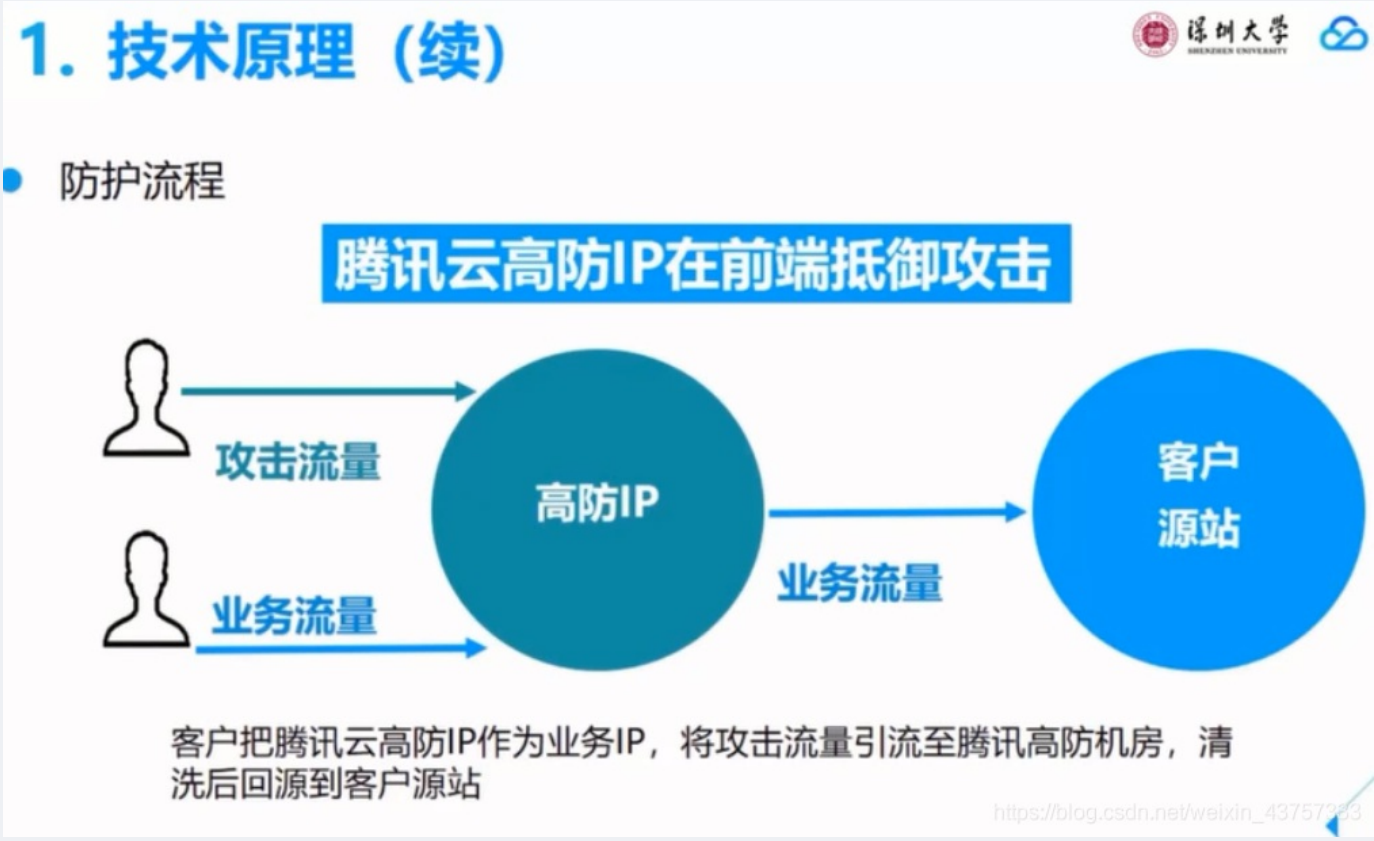
其实就是我们现在要讲的大禹的系统，大鱼的系统它提供一些产品的功能，比如说有哪些呢？首先我们说所有的腾讯云主机都可以免费的去享受两GB防护峰值的一个ddos攻击。原来你在企业里边你外网的带宽是100兆，200兆，那么别人拿500兆攻击，你肯定就当机了。而现在我们在腾讯上可以免费的去获得两GB这样的一些防护的峰值。
那么这里的话就是说我们的高防包，我们的BGP的高仿包可以去提供高达310g的防护的峰值，并且我们说非常好的一点是，我们在购买好之后不需要去调整你的业务，也就是说如果说我们的业务是在腾讯上，你正在遭受ddos攻击，那么我们直接去购买bdp的高仿包，我们都不需要对业务做任何的调整，那么就可以去完成这样的一些防护。
再一个就是我们的bgp的高防IP，如果说我们现在不在腾讯云上，我在自己的机房现在正在遭受这种地道式攻击，我现在去腾讯上购买一个bgp的高仿IP，我将我的域名解析到高仿IP上，那么高仿一批把流量给我清洗，然后再把正常的流量回注到我，那么这个也是提供310g的一个防护的峰值。这样就是我们的DNS节水检测.
那么就是说指的是我们的local dns劫持，一般指的是通过改变指定的域名在运营商测的这种配置。比如说我们现在打开www.QQ.com，他怎么去跳到腾讯视频，那么这个就是一个劫持，我们会做这种检测。



那么实现的技术原理是什么？就是说我们的大禹的产品，BGP的高仿包，BGP的高发IP，他为什么能给你提供清洗？那么它的一个技术原理就是通过这样的一个双重清洗，首先我们如何做检测攻击呢？我们是采取风光1:1分光的方式，做流量的迹象，然后旁路检测镜像的流量，那么这样做的话它就不影响你的业务。那么检测原理主要是为基于我们流量行为去做建模，加上ai的智能引擎，去分析流量中是否存在攻击。我们说检测到了攻击如何去清洗呢？

如果说我们检测到某个IP正在被攻击，**那么我就通过bgp的路由牵引，那么把它牵引到咱们清洗攻击这样的一些集群的防护中**。那么清洗之后，我们干净的流量直接回注的方式，再回到咱们的核心路由，然后再走原来的路，走到你的云主机等等。那么这样去做，我们会有非常好的这种清洗的算法，主要基于我们的IP， tCP、Udp、 aPC、ps等等。那么用协议的规范以及人机识别来去过滤咱们的攻击流量，不涉及不查阅，不涉及咱们的一些业务的报文。

> 防御系统对数据是完全没有感知的，它只分析这个里边是不是存在攻击的行为。



那么它的一个技术原理的实现的一个防御的流程是什么？对于我们的高防，包括我们谈到其实不涉及什么流程，你直接买就行了。然后他不需要你去修改你的业务零变更，那么对高仿IP，首先我们说所有的流量都经过你的域名解析到我们购买好的高法的提升，然后我们把恶意的流量攻击的流量经过刚才的清晰流程，给他清洗掉，然后把正常的业务的流量给它导到咱们的客户的源站。

那么是这样的，也就是说我们是把高仿IP给它作为业务的发布IP，那么怎么做？就是我们的DNS解析到上面这个然后把正常的流量再转发到你一个网站上。

那么这么做的话，这个产品的优势首先在哪里？第一个我们说超大的防护带宽。平台对单点提供t级别的一个防护的带宽，并且说在这里他其实也是有这种多种业务场景的，比如说我们在这里能给你防御什么？像 cc攻击、 web入侵，那么通过这种高效动态的调度。那么有效组织起比如说咱们腾讯云上那么全网的各种冗余的带宽跟防御的能力，比如说我们在这其实就可以看到有单点是t级的带宽，

这就是说我们去集中动态调度。那么再有就是说我们在这里顶级防护上能够抵御像ddos、 cc入侵，然后避免说我们的IP避风带宽被打满的现象。

那么针对这种攻击的流量能够实现秒级的清洗，那么再就是平滑体验这一块，具备快速的去流量切换，那么在被这种大流量攻击的情况下，保持咱们业务的平滑，再就是隐藏我们的源站，隐藏我们的web服务器的地址，黑客去做入侵跟篡改，保护咱们的网站的信息。

那么再有就是定制策略，为了说最受影响的这些行业，比如说这些电商为这些行业他去做这种定制的专属的策略，针对特殊类型的攻击去实时抓包，并且制定这种特殊的策略。

那么再有就是说我们还有这种定制的专家服务，安全专家服务，那么它根据你的服务范围跟服务的级别以及驻场的次数价格不同，主要是由以下几类，第一个就是定制divorce的防护策略，那么再有就是渗透的测试，漏洞的修复，紧急安全突发事件的驻场，那么他就可以去帮你从全方位去解决咱们的网络的一些安全的风险。

那么在这除了说我们的超大的带宽更专业的服务之外，我们还会看到业界最全的28线的bgp那么我们就能够做到在任何的用户访问的时候延迟都是很小的，那么线路都是稳定可靠，都是走的是同。再一个就是说我们这是个ai的引擎，所以在这的话，因为它是在互联网中不断的进化，那么我们的成功率就是说我们清洗的成功率可以达到99.995%。

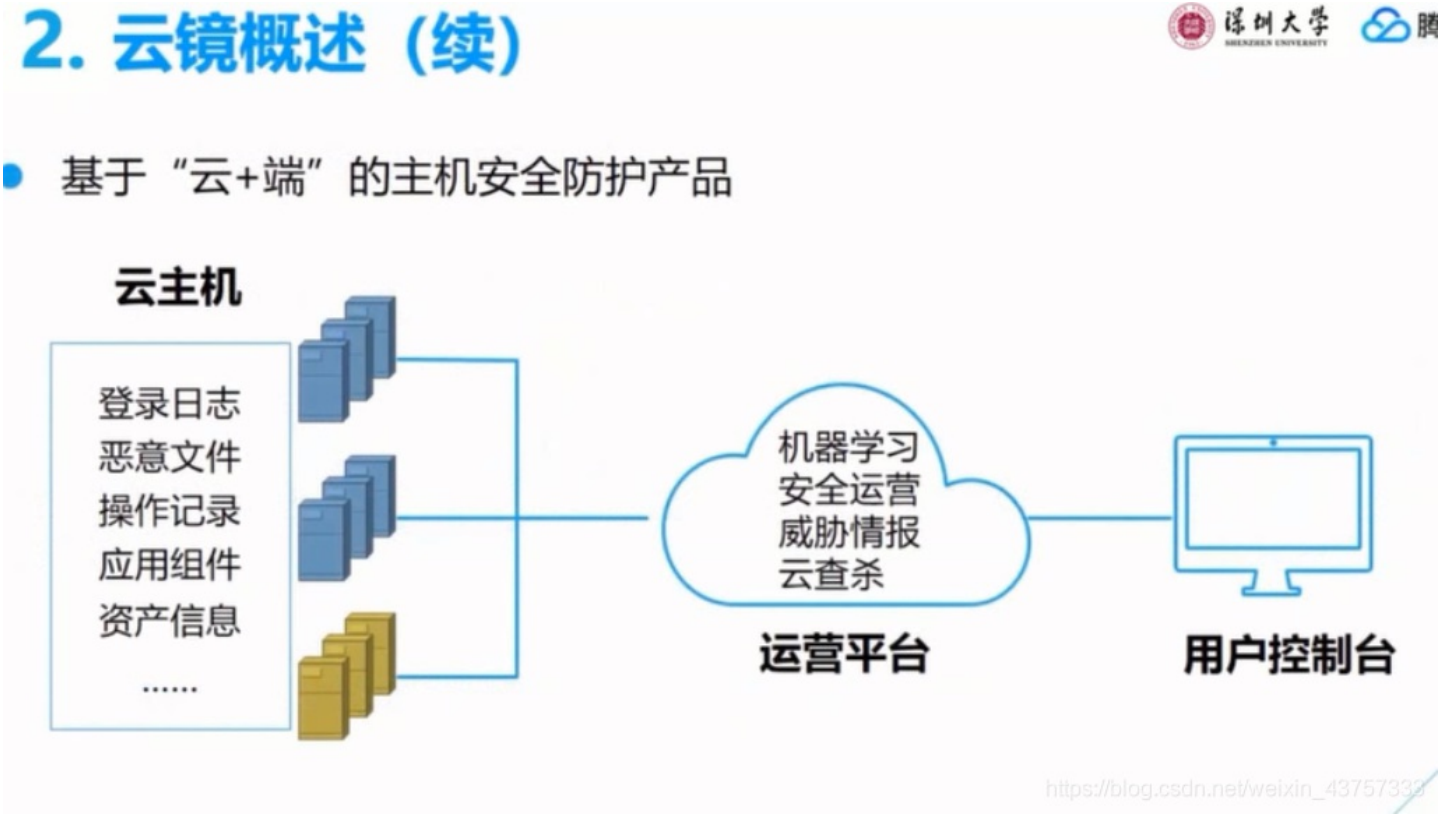
那么对于这样的一些产品来说，那么它可以应用到什么地方去？比如说刚才我们会看到谈到电商，其实他们是什么？就是一个网站对不对？所以在这的话我们提供游戏网站、金融等多种场景。那么游戏我们大家都玩过游戏，那么游戏你在玩的时候去有大量的外挂跟你一起玩，比如说直接爆头，那么这种情况的话其实有影响了我们的游戏的公平性，那么这个时候你心情就很差，就不再玩。那么对于游戏的运营者来说，那么这个就会导致咱们的用户的丢失、流失。

那么再有就是你攻击之后老是掉线，比如说他的平台正在受到攻击，那么你的一个访问就会很慢。那么再有说我们的网站，它的服务器的真实IP泄露之后，那么这种流量的攻击或者说我们的应用层的攻击，就会直接导致瘫痪。那么金融上我这就更不用说了，在各种金融领域，那么他ddos攻击真是高风险区，最终就会让你的APP网站什么的，没有办法把它打开，严重的影响投资者的信心。

那么这个过程的话就是说我们的应用场景我们可以应用到这些领域下，那么对于主机层面上来说，我们在这里主要去解释什么是云镜，我们在这里主要说的是就是主机级别的安全，包括说它的一个技术的原理，产品的优势跟应用场景。那么首先什么是云镜？

那么云境它是咱们在主机上部署的一套软件，去帮助你去实现入侵检测，然后再去做到咱们的暴力密码破解拦截，漏洞的一个扫描等等。那么我们为什么会需要这样的一些产品？首先说服务器一旦被黑客入侵，企业将面临比如说业务被中断，比如说他把你的服务器可视化了，那么数据被窃取，你想想我们的核心的数据被人拿走之后，这存在多大的风险？再有就是说被加密勒索，我们在17年刚经历过的，你不掏钱，你这个比特币是吧？你就这个资料就被加密就打不开。

那么再就是服务不稳定了，你说他要在你的服务器上安装了各种病毒木马，比如说我们说挖比特币的程序，大量的消耗你的一个资源，那么对你来说就会造成这种服务的各种不稳定性，那么使用我们的云镜就可以有效的去预防跟防御以上的问题，保障咱们企业的网站和应用系统内一个安全性。



那么首先我们来看一下云境这一块，所以云静他们其实是一款针对我们云上的一些主机，它整体的安全防御的系统，为咱们的主题提供多种层次全方位的系统防护技术。

那么比如说我们在这里就融合了腾讯多年的这种海量的威胁情报的数据，那么漏洞的信息以及说通过机器学习那么为咱们的用户去提供黑客的入侵检测，漏洞风险的一个预警的这种全方位的服务。那么这里边主要包括你像在这里谈到的密码的暴力破解的拦截，异地的登录的检测，咱们的恶意文件的识别，然后高危漏洞的检测，应用组件、资产信息等等，那么给大家提供这种全方位的服务，去防止企业说这个数据被泄露的一个问题。

那么云镜它主要的功能有哪些？像在这里谈到木马查杀，木马查杀跟大家想的点击查杀，然后去杀木马它不太一样。这个是基于机器学习的对各类恶意的文件进行检测，像包括说各类的web shell这种后门和这种二进制的木马，那么对检测出来的恶意的文件进行访问控制跟操作，比如说隔离，防止恶意文件被再次。
那么再就是密码的破解，它就可以拦截，对这种密码的恶意破解类的行为进行检测和拦截和共享这种全网的恶意的IP库，自动化的去实施拦截的策略，这个是不需要咱们用户去做什么。再一个就是说我们的登录行为的审计，要根据你登录流水的数据，去识别常用地登陆区域，那么对可疑的登录的行为去提供这种实时告警的通知。那么再就是我们的漏洞管理这块，对主机上存在的高危漏洞风险进行实时的预警跟提供修复的方案。比如说我们就在网页上告诉你，你服务器中的操作系统或者说装的软件有漏洞，然后我再告诉你这个漏洞应该怎么修复。那么再有就是说我们的资产管理这块，我们支持对机器进行分组和标签管理，基于我们组件识别技术，快速的去掌握服务器中软件进程端口它整体分布的情况，那么这个技术的原理是什么？

首先它是基于运行强大的一个策略库，漏洞风险管理，首先它这个是基于腾讯云安全团队的威胁、情报收集跟挖掘的能力，第一时间去感知互联网上新出现的各类的恶意攻击行为。然后再就是漏洞检测的范围，涵盖咱们整体的操作系统和它上面装的各种的业务服务器，上面那些应用软件，通过腾讯安全应急响应中心，它广泛的去收集互联网中的漏洞的情况。那么基于腾讯集团的一个漏洞收集响应的流程，提供腾讯安全团队自演的修复的布丁。
那么对常见的开源程序框架等外部应用进行漏洞的检测和修复。那么例如我们的 discuss water price是一个pHP reldis等等这样的一些产品，那么进行及时的修复。那么在就是说我们的弱口令漏洞的一个检测，以及我们说系统配置的漏洞，那么支持咱们系统级别的漏洞的检测和修复，包括比如说windows，他如果说存在高危的系统级别的漏洞，我们就会向云服务器去推送windows update的补丁包。那么Linux如果说官方的rpm语言更新没有高危的漏洞补丁，就会向用户去推送这种rpm的补丁。那么整个来说就是依托于腾讯云安全的运维的能力，和互联网的0的预警系统，我可以第一时间去获取到漏洞的细节。那么海量的云服务器的海量安全攻击事件的数据，可以去挖掘出最新的安全性的风险。那么基于腾讯安全运营团队的漏洞嫌疑流程，可以快速的去完成漏洞危害的判断修复，一定的制作等等。

2. 技术原理（续）

- 充分利用云的优势对密码破解行为进行拦截

那么我们来看一下它的一个技术原理，那么它就是通过咱们充分的利用腾讯云的优势，对密码暴力破解拦截。那么首先你正常跟恶意的登陆，都要经过一下咱们的云，那么云静根据你的一个常用的一些登录地跟咱们登录的行为，那么进行去判断你是不是恶意。

那么如果是匹配到了，比如说恶意的行为，那么我们就会直接把你拒绝掉，那么留下正常的一个登录的请求。再就是说我们基于ai的这种 web shell的检测，那么这个也是依托于腾讯云这种安全平台的全网恶意文件，样本收集能力，以及说基于机器学习的网站后门检测能力，可以实时的去检测和查杀咱们的各种木马，同时提供咱们的恶意文件检测跟一键清除。

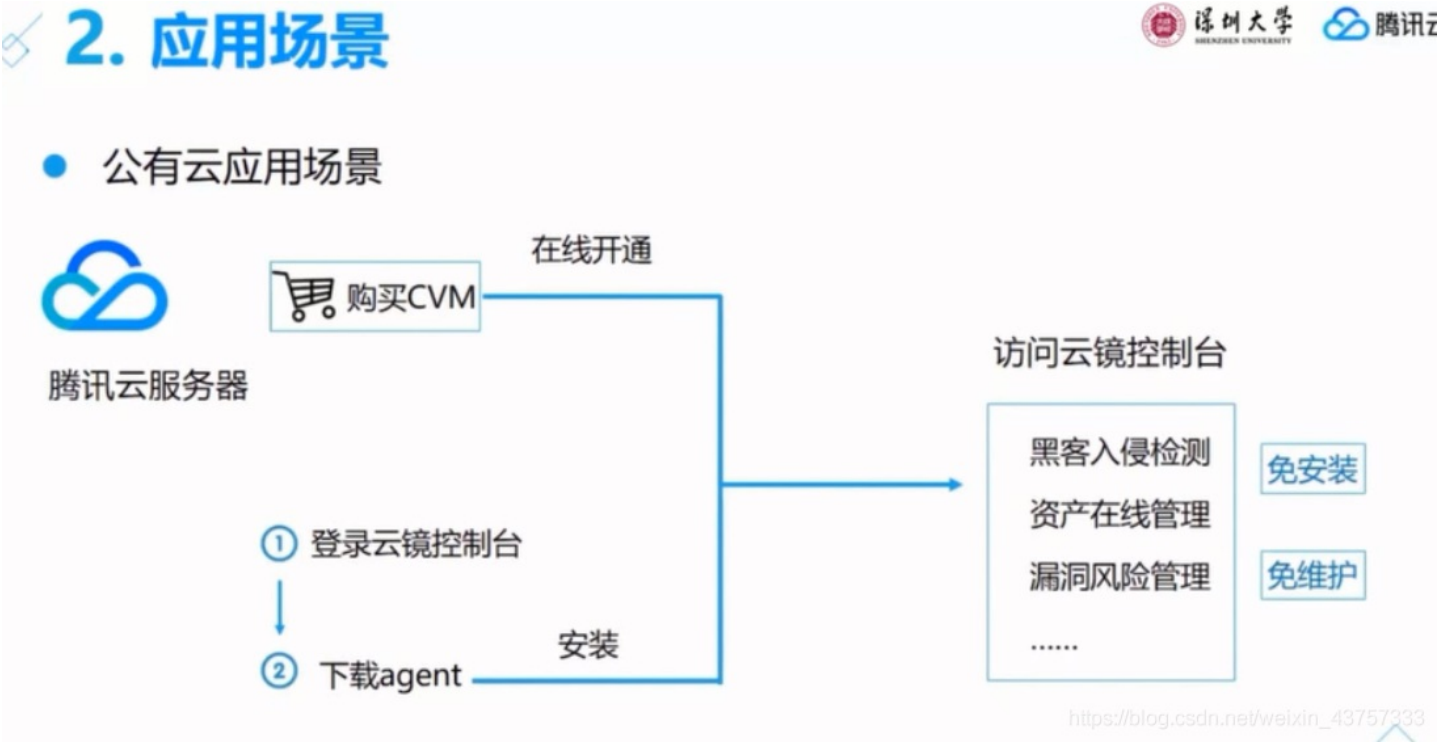
2. 技术原理（续）

- 基于腾讯电脑管家的恶意文件检测能力

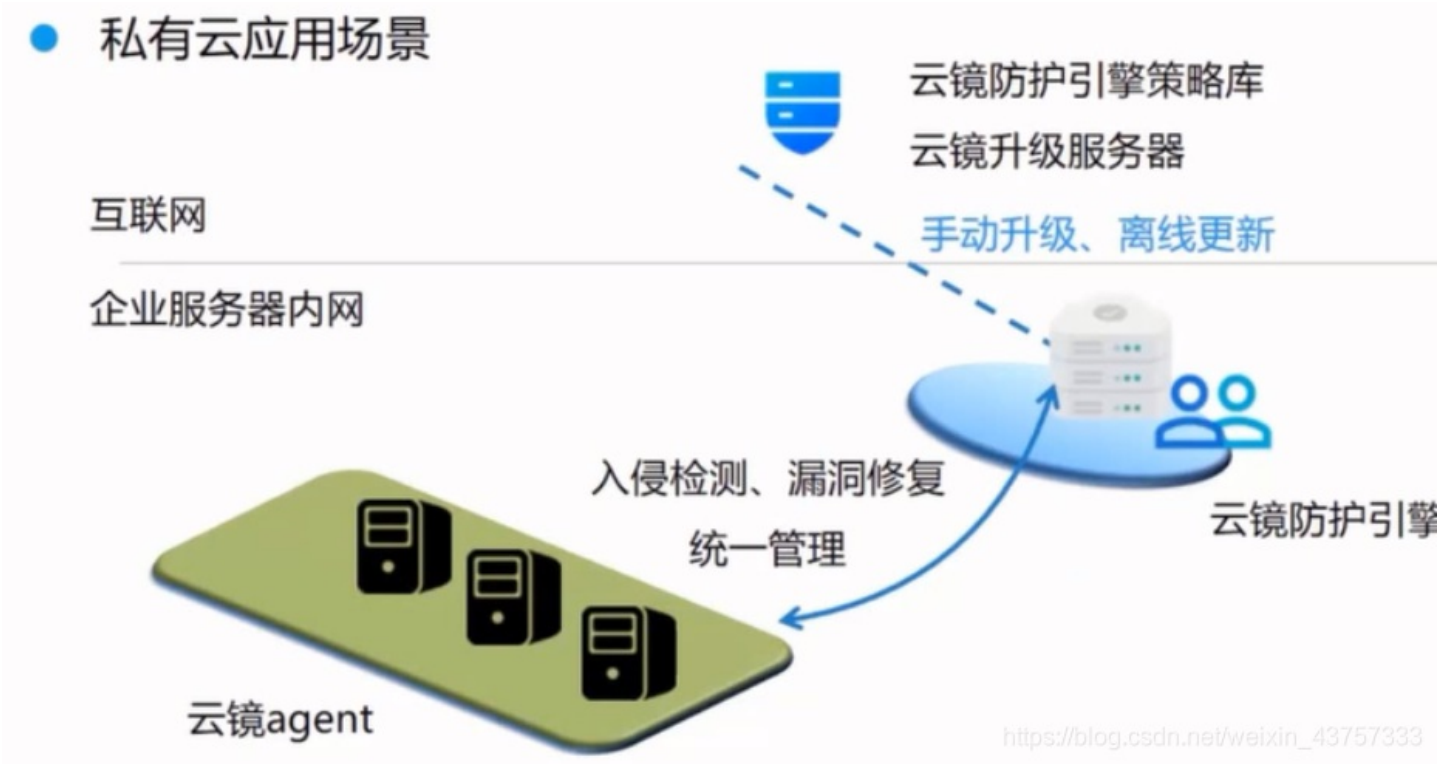
再有就是基于腾讯的电脑管家的恶意文件检测能力，那么在这里的话，它就可以结合上咱们腾讯的电脑安全管家，去实现咱们的病毒木马的更多的样本的检测能力。那么再有就是说我们的一些整体产品优势，我们可以总结一下，那么首先它提供全面的漏洞的监控。

2. 产品优势

那么在这里的话像基于腾讯的各种安全团队，这种动态的一些检测能力，那么能够对全网的这种威胁情报可以及时的收集。再就是领先的入侵检测，我们集成了各种的这样的一些引擎，去确保说咱们能够在被入侵的时候实时检测到，并且我们通过这样的一些集中化的控制台，可以去做到主机资产的集中性的管理，我们有多少台主机，有多少个进程，有多少个端口，那么他们分布的情况都可以快速的通过咱们的平台进行可视化的运营。那么再有就是说咱们的云境，这个系统占用率非常低，我们可以低到什么？我们在疯狂工作的时候， CPU它的利用率也会远远的小于2%，那么它的内存的占用率也会小于30兆，并且它完全不依赖我们的第三方，就是说我们对服务器的资源消耗的占比会非常的低，那么它可以应用到什么场景下，那么它什么时候去安装呢？



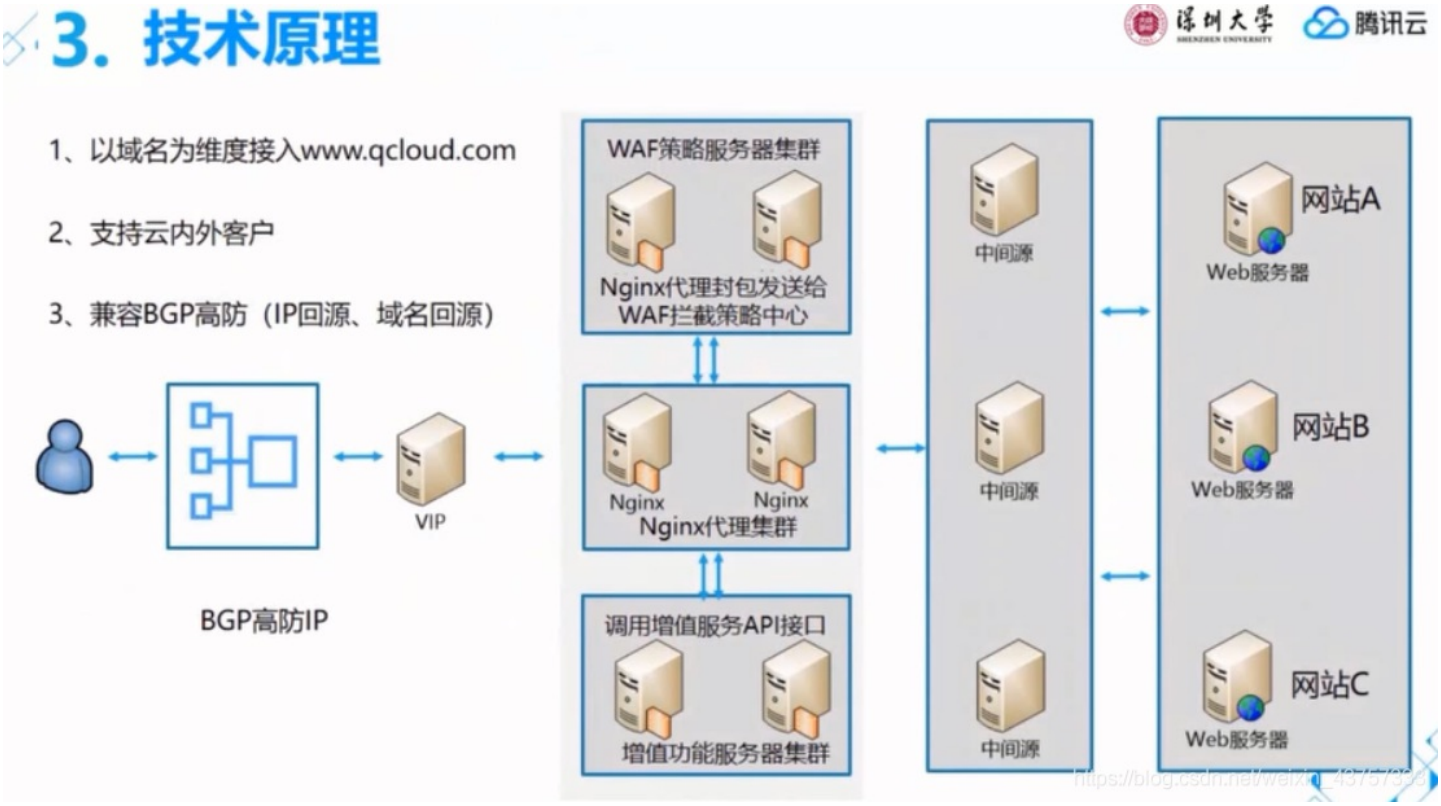
那么在这我们可以看一下，首先在公有云的应用场景，我们在购买咱们的cvm的过程中，如果说不会刻意的把它勾掉，那么默认情况下它就会安装。那么如果说我们留意的话，我们在购买云主机的过程中，那么在结算上面有两个免费开通，那么其中一个安全产品的加固指的就是我们的云计，那么如果说我们没有进行安装，后期我们需要我们可以登录咱们的云镜的控制台，去下载我们的代理，然后根据咱们的一个帮助的文档，去快速的完成下载代理跟安装代理的工作，我们就拥有了咱们的各种功能，像黑客的入侵检测都移动的管理，资产的在线管理等等。如果说我们没有把它勾掉，这个就是免安装，免维护，你就不需要知道这件事情，但是你就拥有了这样的一些能力。



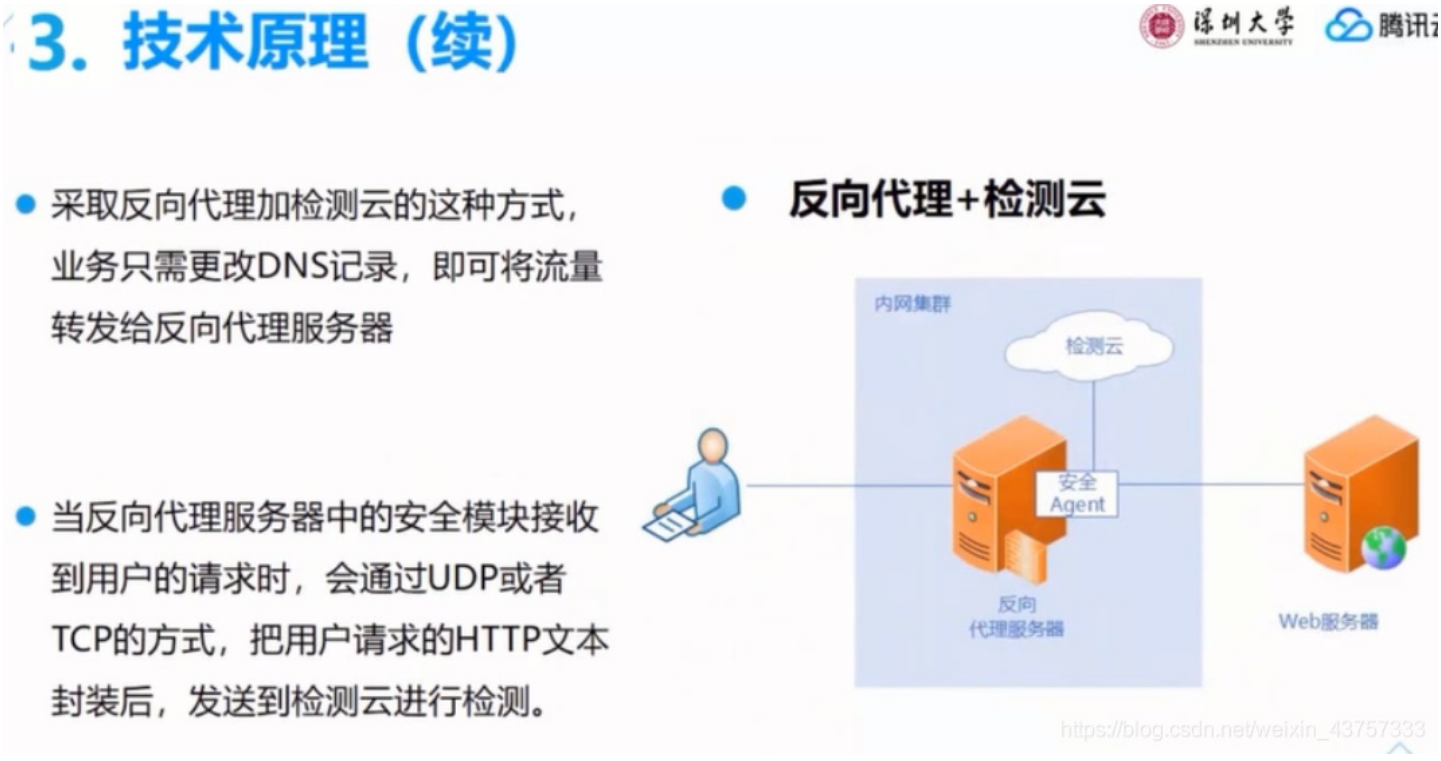
再一个就是说我们的私有云部署，私有云部署用户可以基于说企业本地服务器资源的构建，那么去完成本地的一些部署。这个的话首先用户需要去手动的去下载云计算的代理，并手动的在本地服务器上进行安装。那么对于说非腾讯云的这种服务器，我们需要去保障本地防火墙开通相应的端口，具体的端口的话是我们以产品文档为准，

这里主要介绍的是网站管家的概述，然后技术原理，产品优势以及应用场景等等。那么首先什么是网站管家？我们首先在这里看一下，那么在金融网购门户上都存在什么问题？金融上我们说金融的数据是非常涉密的，你一旦说数据被泄露，这个问题就很严重。那么在网购的时候，你的一个信息有没有被贩卖？有没有被泄露？那么我们的主业网页上的一些数据到底是不是被人篡改了呢？那么说我们是由于这些网站它都是有利可图的，并且是拥有海量的用户数据。所以说这一些它就是我们所谓的重点关注对象，他就可能会去爬你的数据，然后去篡改你的网页等等。那么我们为了去拒绝掉他，爬我们的数据去篡改我们的网页，我们在这里去提供了一个网站管家，它就能够去实现咱们的防御外部入侵。

互联网中发生这种零碎漏洞的时候，我们可以优先的去提供补丁。那么再有我们通过AI去做这种业务的防控，可以做到隔离恶意的访问，并且我们还对咱们的这种网页有保护网页内容的一个功能，做到防篡改，我们把你正常的网页去做一份云缓存，当你真的被篡改之后，我们的云缓存提供服务



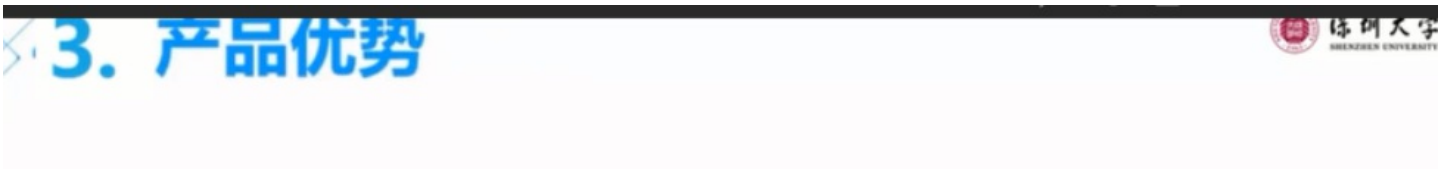
接下来我们来看一下它的一个技术原理是什么。我们首先是以域名为维度，我们把域名接入进去，用户在访问这个域名的时候，首先我们会过滤一个 b g p的一个高仿，然后经过了高仿之后，我们就可以进到咱们高可用的这样一些IP上。我们的virtual Ip那么进来之后我们的nginx那么它代理分包，然后发送给我们的waf，这也是我们的网站安全管家，把它发送给我们的万福之后，然后我们就可以去快速的去调用咱们的增值服务入口，去确定那么现在是不是有问题。如果是把它隔离掉，如果不是然后放行，那么这个的话就是存在我们的整个检测的机制。那么首先我会看到这里有一个代理的集群，代理分包，代理的服务代理本身就是一种安全的网关，我们可以基于会话去做双向的代理，中断了用户跟服务器之间的直接连接，适用于各种的加密的协议，这也是web的cache服务中常见的一些技术，那么对dota可以去做到有效的医治。那么再有的话就是说我们的整个过程代理它也防止了咱们的入侵，直接的去进到咱们的业务系统上。像我们的业务系统就是 a网站、b网站、c其实我们经过了代理还有中间员，那么这个对用户和对恶意的用户来说，其实并没有直接的接触到你的网站，对这种非预料的特别的行为也有所抑制。
那么这种web的常见的策略有哪些？首先就是特征识别这一块，去识别出入侵者，然后再去防御它，那么这是一个前提。那么怎么去识别这个特征？其实就是攻击者的指纹，比如说怎么缓冲区溢出的时候，这种 share code。然后再有就是我们的sql注入中最常见的真表达式。那么对这些来说，我们就可以正确的去识别出。那么再一个就是说我们的算法的识别，那么特征这种识别有一些缺陷，比如说真表达式，其实我们可以去换一些其他的算法，那么我们说现在在追求这种新的方式，更加精准的去识别，那么对这种攻击进行归类，那么相同类的特征进行模式化，而不再是单个特征的比较。算法的识别，有些类似于项目模式的识别，但是对攻击方式的依赖性很强。你比如说circle注入 ddos，xxs等都开发了相应的一些算法的识别，算法的识别其实就是进行语义的理解，而不是靠长相去识别的。那么在说模式匹配这一块，这个是ids中古老的一些技术，然后把攻击的行为归纳成一定的模式，匹配后就能够确定它是不是入侵的这种行为。

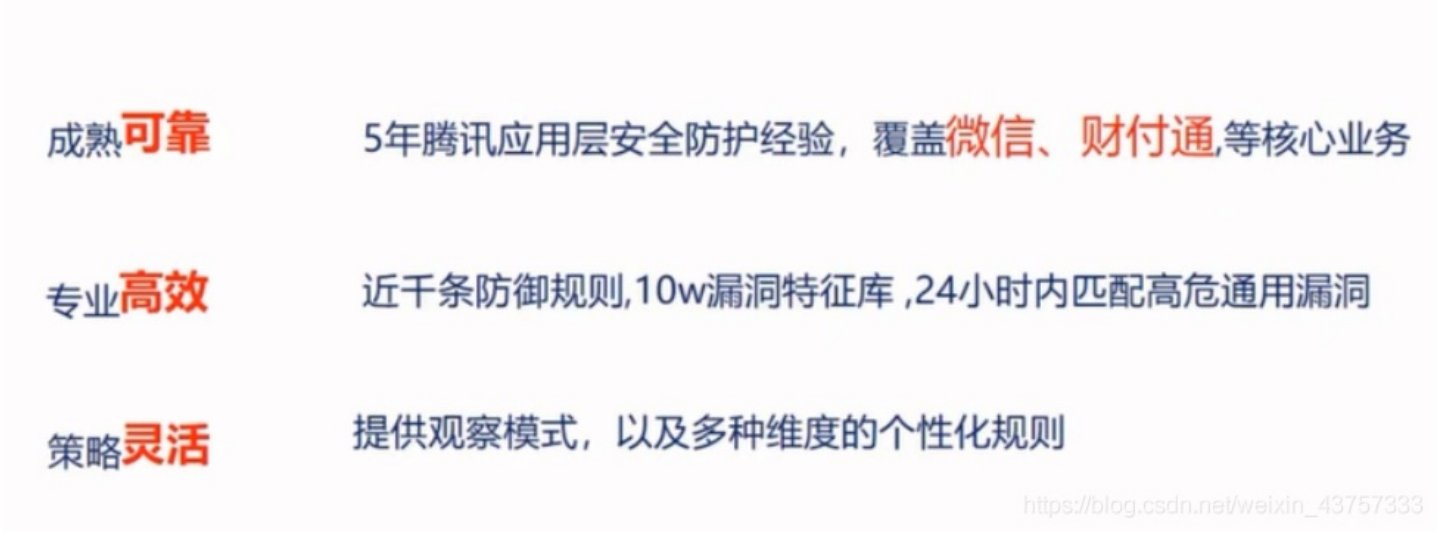


比如说我们现在在说代理的时候，我们说

> 采用咱们的反向代理，那么就可以去检测我们这个过程中是不是有攻击。

既然说我们有了反向代理，我们在代理这一层面上，我们就可以去加上咱们的各种的安全模块，所有的用户来访问的时候，我就会去决定，那么此次咱们现在是不是要把你的流量做清洗，或者说是不是有恶意的行为，是不是要拒绝掉，这个就可以在我们代理层就可以去解决掉一部分。





那么再就是我们来看一下，那么咱们的一些产品的优势在哪里？首先他已经应用于咱们成千上万的服务器上，成熟非常可靠。那么在这里的话，我们的微信财富通已经在使用了。
那么再就是我们的高效这一块，高校这块我们说近千条的防御的规则，10万的漏洞的特征库，24小时匹配咱们的高危通用的漏洞，这个的话都是比传统厂商反应要迅速很多。
那么再有就是我们的策略非常灵活，我们还提供这种观察模式，以及说多种维度的一个个性化的策略。比如说如果说咱们没有直接的证据证明了受到了入侵，但其实我们还有这种观察模式，去作为重点观察对象去检测，重点检测咱们的一些各种行为跟表现，去确定是不是当前受到了入侵。

再一个就是说本身它是一个高性能高可靠的 CEO系统，首先我们的waf它可用性可以达到99.9%，那么我们的正则的防护已经达到了1000多条，如果说我们现在使用的操作系统现在有零类的漏洞，那么对厂商来说通常需要30天到90天的一个修复的周期，而在这一块我们24小时就可以跟进你的一个热补丁，然后整个的网络延迟会小于咱们的5~10毫秒。
那么第一个我们说完之后，我们再看第二个，就是说个性化制定防护这块特别的有好处。那么首先我会进入到你的观察模式，然后我就看你现在的是不是存在异常，如果是我可以去自定义一些规则，去判断，那么它现在是不是具体是什么特征，然后我们还有一些url的一个白名单，这个白领就是说我们会去对自己的安全部门，然后去做一些放心。那么再有的话就是说我们的恶意IP的惩罚，那么对这种时常来攻击的这种黑产的IP，我们会直接的把它拉到我们的黑洞路由里边，它无法再返回到咱们的一些产品，

它可以运用到什么地方去，所以根据前面的描述，我们说网站安全管家它是什么东西，他就是防护咱们整个网站的一整套的系统，所以说它可以在哪里？比如说咱们的这种抢购、政府网站，然后咱们的金融等多种场景下都适合。所以我们会注意到这些其实就是网站应用，像这种高并发抢购的场景，我们可以智能地去过滤掉你这种恶意的攻击和垃圾的访问。那么对政府网站来说，保障他不篡改，就是说我们的网站信息是正确的。那么再一个就是金融上有效的去检测DNS链路劫持，防止这种流量被恶意执行到其他诈骗的这种网站上。那么再就是有效的去检测这种撞库的行为，保障咱们的用户的信息不泄露。那么再就是说数据泄露这一块直接提到避免说因为你注入的攻击导致说核心的数据被拖库。那么再有就是说我们在看这样的一个行为，企业是怎么去应用的？

我们会看到中间是有一个web应用防火墙，恶意的攻击垃圾的访问，再走到我们的防火墙，这就会直接的去被拦截并识别掉。那么正常的访问就会正常的放行，正常的放行之后访问的是我们云创云上防篡改的这样一些云备份，那么你访问成功没有问题，然后就访问到我们的企业的网站。那么这样的话其实你想想真的说你篡改我的网站，其实没有什么用，因为你访问的其实是一个防篡改的云备份，所以我们的漏洞的扫描的服务，在这块我们去监测你的网站是不是有漏洞，那么腾讯的外部web漏洞扫描是用于监测咱们网站漏洞的一个安全服务，为咱们企业提供这种7×24小时全面精准的这种漏洞检测跟专业的一个修复建议，去避免说漏洞被黑客利用，进而影响咱们网站的一些安全。

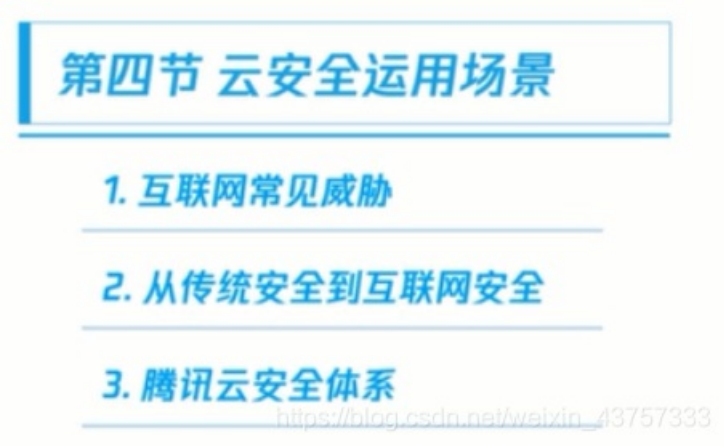
再就是漏洞扫描，这是一款纯SARS服务，用户是不需要去安装任何的软硬件，也不需要去改变目前的c网络部署的状况。那么强大的一个并发的扫描能力，可以给咱们企业去检测上千个网站，极大的去降低咱们安全运营的成本。

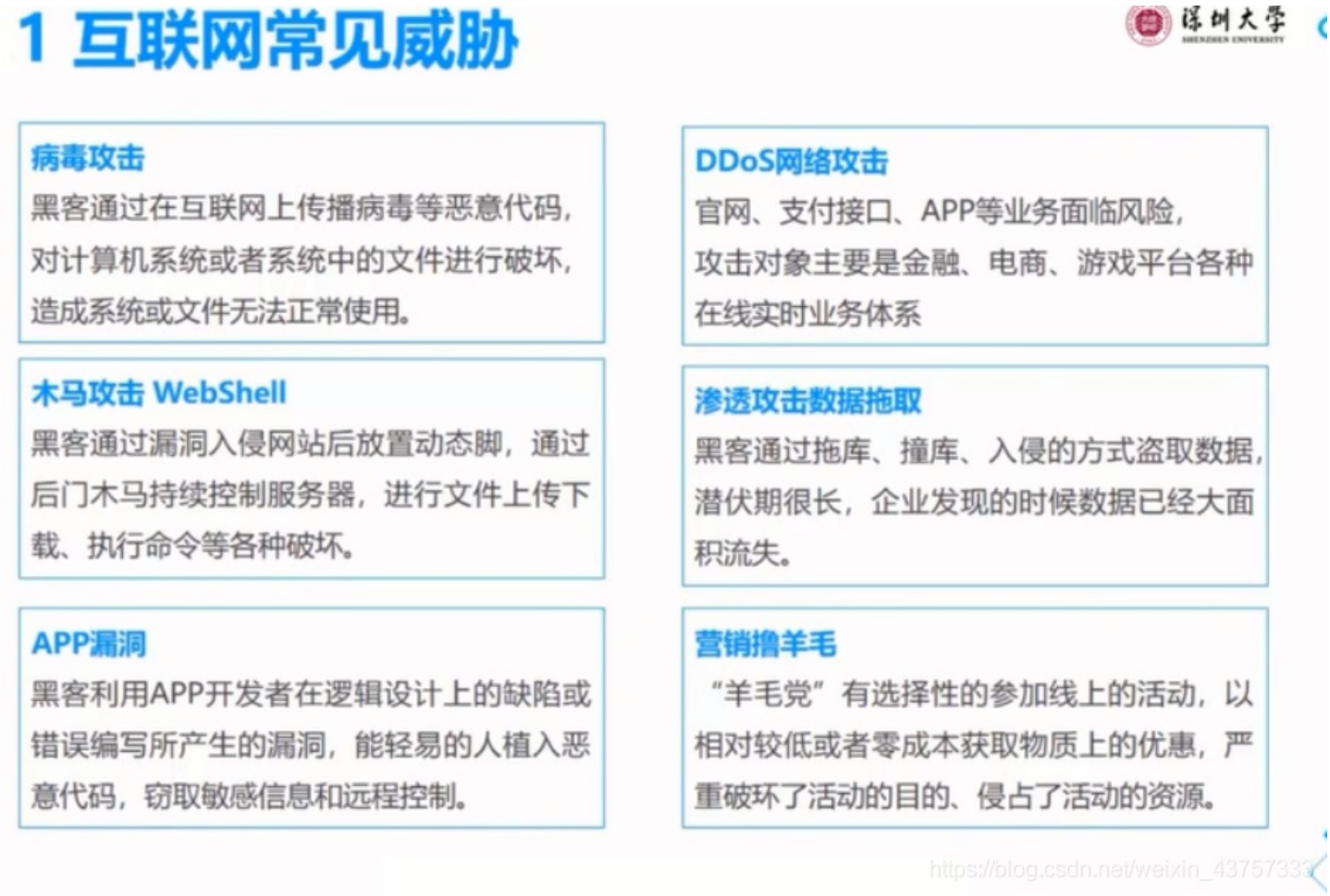
那么业务层面我们提供天域的业务安全防御系统。那么在这里我们会主要了解 什么是天域的防刷，那么天域的防欺诈这两个主要的功能，首先防刷，我们说刷其实就是刷奖品，刷优惠。那么在这儿我会谈到一个职业叫羊毛党，黑产的羊毛党。比如说我们现在企业为了要发展新的用户，在线上举办了一些活动，这个奖品非常的优厚， 我们原本想的是发展用户，但是举办活动的信息的被羊毛党发现了。那么这个时候我们在举办当天，所有的奖品一瞬间就被黑产的给他拿走，他们其实并没有发展任何一个用户，奖品却损失了花了很多的人力物力，最终没有达到效果。其实现在黑产业也越来越专业了，像他们也是分工协作的，黑产的上层它有这种软件开发，比如说我们说抢购的时候，你为什么总是抢不过机器？其实就是他们开发的软件就专门用来做抢购的。那么再有就是说中游他会大胆的去养一些号码，然后养一些账号，然后下游就是说他们所有的工作都完成了，奖品拿到手之后，下游就开始去比如说有很多的公众号，然后还有一些APP就专门去搞一些优惠券，然后去搞一些什么便宜的情况下就卖给你正品。那么这种情况下你要有意思知道你买的可能是。

关于腾讯云 WAF 产品，以下描述错误的是哪项？A.可以有效防御 SQL 注入、 XSS 跨站脚本B.是一款腾讯云针对网站安全推出的智能一站式智能专业防护平台C.可以有效过滤 DDoS 攻击、 提供 DNS 链路劫持检测D.可以预防木马上传、非授权访问等 OWASP 攻击
C

腾讯云针对主机安全提供了云镜产品，云镜提供的核心功能有哪些？A.木马查杀B.密码破解拦截C.漏洞管理D.登录行为审计
ABCD
以下哪项是腾讯云网络安全产品大禹提供的免费功能？A.基础防护，包含DDoS2Gbps防护峰值B.BGP高防包C.BGP高防IPD.DNS劫持检测
A

8.4云安全应用场景





那么第一个小章节我们就给大家去聊一聊，那么对于互联网来说，它常见的一些威胁有哪些？那么我们会讲到安全到互联网的安全，整个腾讯云的安全体系架构有哪些？我们最后展现的是咱们如何实现互联网安全的纵深防御体系。第一个小节，我们说互联网中常见的风险有哪些？到互联网中危险的层出不穷，各式各样的。我们说只有通过对各种威胁进行分析和梳理，与互联网的业务体系关联起来，这个它是建立一个有效的安全防御体系的第一步。那么第一个我们说案例这一块，我们说病毒攻击，黑客通过在互联网中去传播病毒，文件和计算机系统造成破坏。像在2017年5月份左右，像咱们都有经历过的，windows敲诈勒索病毒大规模在全球进行爆发。那么感染比如说咱们的企业高校甚至公安政务，那么这种内网的话，然后我们的操作系统的文档，甚至是整个操作系统就已经中招了，那么这些产品就无法打开，那么你除非交比特币进行赎回，这样的话就说木马像2018年的2月份，国家计算机病毒应急处理中心网络监测也发现，那么连续出现众多与天气有关的外部网站，被植入了恶意的木马的现象。那么这些外部网站通常会以高温预警为主题，但实际上是一个带有恶意插件的假冒的外贸网站。那么一旦说计算机的用户点击了这样一些网页，就可能会导致计算机操作系统自动去下载和捆绑其他的病毒木马的恶意程序，就导致你资料的被窃取。再就是我们的APP的流动，就是说我们在开发APP的过程中难免会存在这样那样的一些缺陷，像在2014年国内某知名在线旅行平台，这个APP就被爆出漏洞。那么由于说将用户的支付记录保存并被发现了存在这种目录遍历的漏洞，而导致敏感信息可以被黑客去读

取，涉及到像身份证银行卡的2.5千瓦，那么这种大量的信息漏洞就会导致用户的一些支付造成破坏。在金融行业腾讯云已经有这样的一些多年的经验，像腾讯本身有各种各样的一些支付的体系，那么在这的话，我们有很好的一些产品能够应对这样一些 a p p的漏洞。那么再就是我们的DOS的话，在互联网见的比较常见，那么主要是通过大量的一个网络流量去攻击去访问，那么导致你的带宽和资源被占用。那么这样的话我们就没有办法对外提供服务，我们也可能必须要交这样一些赎金。那么再就是说我们的渗透攻击，数据的拖库和撞库，像我们说前段时间某平台上就收到这种投诉，说大家的资料被泄露了，在另外一个网站上也有同样的数据，会用同样的账号密码也能够登录，但是我们却从来没有注册过，那么就说明原网站已经被脱库了。那么再一个的话就是说我们的撞库，那么我们的账户我们可以想象自己平时在互联网中使用的账号密码，我们在这个网站上使用的账号密码是不是也在那个网站上也使用？如果是的话，那么如果是其中的一个网站，它存在比如说数据泄露，把你的账号密码身份证等等这些泄露干净了，那么这个时候我们的其他的所有使用同类凭证的就存在这样的一些风险。那么这个的话一个托库，我们说你的资料会被泄露，那么这样的话我们对企业来说资产损失。那么第二个的话就是说你如果说启动同样的密码发生了撞库，那么你所有使用同样口令的网站都会存在安全性风险。那么再就说撸羊毛这件事情，比如说我们说在鲁阳门我们企业做活动有各种优惠，那么这个其实是我们希望去通过这样的一些活动去增加我们的活跃的用户。它其实说羊毛党他就天天去参加这些线上的活动，以较低的成本甚至是零成本去获得你的一些优惠和奖品，严重的去破坏了你举办活动的目的，把你的奖品都拿走。那么这样的话其实你举办这个活动钱损失了，但是并没有达到你预期的效果。

在这里插入图片描述

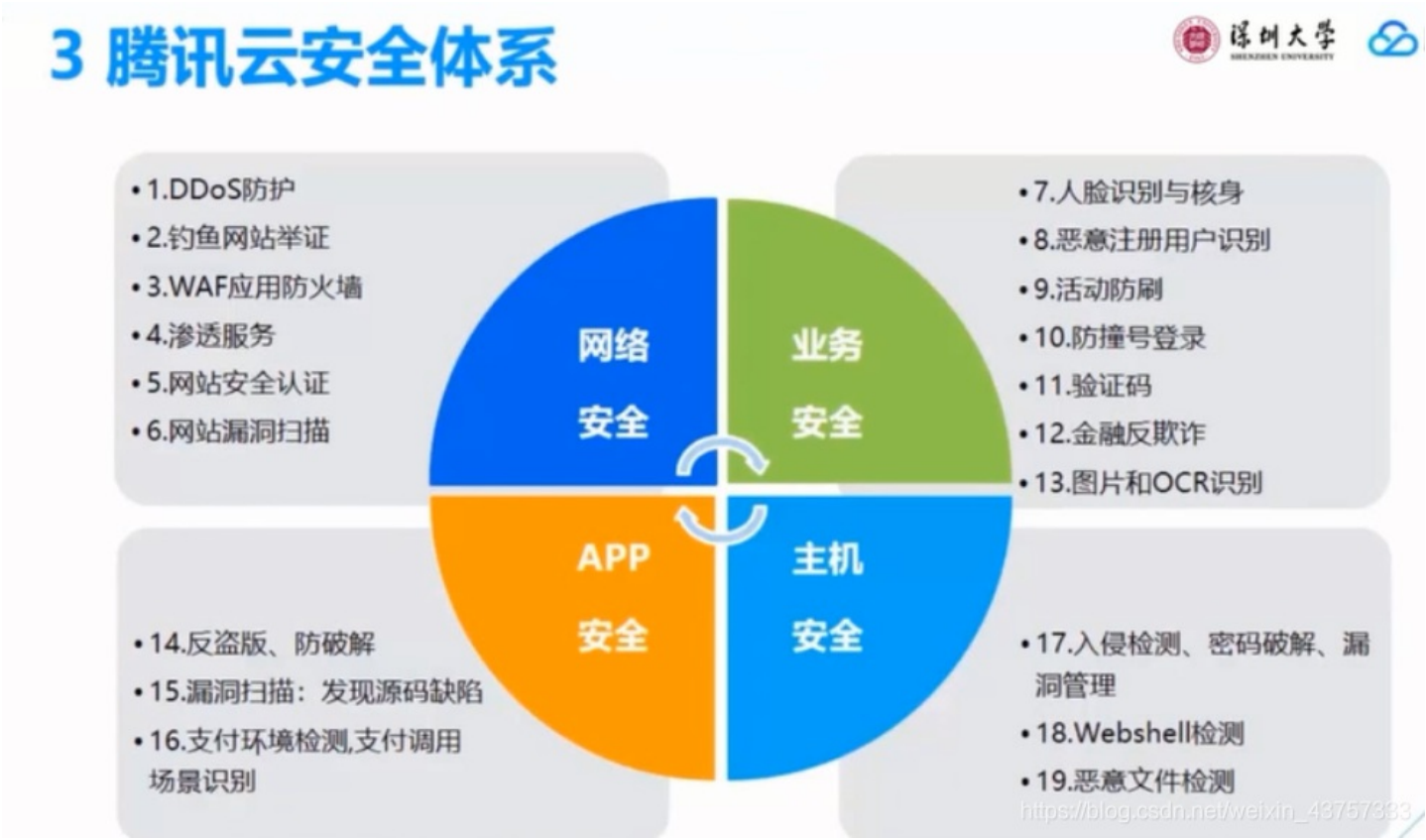
所以说我们可以总结一下，那么对于互联网的这样一些风险来说，我们在每一个互联网业务的层面都存在什么样的风险？简单分析一下，像基于对互联网常见的一些危险的分析，比如说我们在这里将业务安全层上，那么在这个可能就会有这种欺诈预期，这是我们在金融行业下欺诈预期指的是什么？我从你的贷款平台借钱，然后就没有然后了，那我就不还钱了，那么这种情况的话他就存在这种恶意的欺诈，那么这个钱就预期了。那么再有的话就是贷款的黑中介，通过伪装身份或者说包装你的资料来完成这种骗取消费的贷款，那么对咱们平台的业务层面，这是一个极其致命的问题。那么如果说这种数据多的话，咱们的平台可能就会资不抵债。那么再一个就是APP的应用层，你在开发的过程中存在的缺陷漏洞可能就会被泄露，可能造成这种后果。比如说你如果说做的是一个手游，那么如果你的代码存在漏洞，那么我们说任何需要去买的装备，我们都可以去通过破解去实现，不需要买。那么这个的话对公司的语音就会有各种各样的一些伤害。那么这样的话就是说我们的外部应用层，那么外部应用层主要指的是咱们的网站的入侵检测和咱们的一些防御以及外部安全漏洞的一些扫描。那么如果说咱们的外部网站有漏洞，那么这个可能就会以外部为入口，那么去遭到破坏，然后入侵服务器的那么对服务器来说主基层那么我们的操作系统是不是有漏洞呢？好的，我们现在使用的是应用软件是不是有漏洞？那么这个时候谁去帮我们去发现，我们怎么样快速去修复？这些是你面临的问题。那么这就是网络层的租户共享同一个平台，我们怎么去实现租户之间的隔离？那么当我们真的说受到了D DOS攻击的时候，我们导致服务器宕机，没有办法对外提供服务，那么这个时候我们应该怎么办？所以其实我们可以总结一下，其实安全它是一个过程，不能够依赖于一种类型的安全，为企业的信息去提供保护，也不能够依赖于一种产品去提供我们所需要的所有的安全性。那么安全的防护就是一个木桶的理论，那么整体的网络和业务层的一些安全取决于防护最暴露的环节。那么像在这个过程中，如果说我们要头疼，一头脚疼就一脚，那么这种方式其实并不能够完整的去解决你所有的安全性的问题。在企业中我们习惯于去安装一些企业的防病毒软件，我们认为就解决了问题，其实不然我们是需要去配置一些比如说业务一上线就配套完整的安全性的解决方案，而不是一个软件那么简单。那么我们一整套就要涵盖咱们在这里谈到的业务层，卖不成、主题层、网络层等众生的这种防御的体系，这才可以。

2 从传统安全到互联网安全

信息安全体系		传统数据中心
安全审计与风险控制	安全评估	渗透测试服务
	事件管理	SIEM系统
	入侵检测	IDS、IPS设备
	漏洞检测	漏洞扫描系统
APP应用层防护		MDM系统

Web应用层防护		WAF设备
主机层防护		安全防护软件
网络层防护	DDoS防护	DDoS防护设备
	网络隔离	硬件防火墙

那么我们说从传统的咱们的互联网的已经发展了很多年了，那么针对说互联网业务的纵深防御体系的安全的需求，那么基于说你自建的数据中心传统安全解决方案是不能够高效和高质量完成的，那么我们现在主要来聊一下你为什么不能够完成。首先说传统的安全体系主要存在像缺失业务层的安全解决方案，那么更多的是在传统的架构体系中进行一些防御，大量的依赖于各个厂商的硬件盒子，它的交付成本高周期长，并且说部署了之后扩展难度非常高，并且说各个厂商之间都是各自为战，他们缺乏合作跟联动，造成了单点防御的严重的缺陷，容易给黑客可乘之机。再就是说他们复杂的一些产品，众多的这种产品架构，那么对于it部门的运营跟管理是一个很大的挑战。再就是说你要去招聘一些互联网安全人才，这个的话就是耗费大量的人力物力财力，现在我们其实是就可以通过咱们那些更好的互联网的法律体系去做。比如说我们的ｌｄｓｌｐｓ设备，那么我们的入侵检测系统，那么再加上我们的MBA，就是移动设备的管理的系统，我们的wap设备所反映的设备，我们就要从多个层面去考虑这个问题，但是我们去管理这些设备就又回到了一个问题，那么对我们的it部门的运营造成了很大的困扰，我们其实就可以不用买这些设备。



我们直接来看，那么对腾讯云上来说，它就提供了你各种各样全方位的一些安全防御体系，那么安全是腾讯的基因，腾讯云实现服务价值最基本的保障就是安全性，那么安全性稳定性、海量服务、大数据能力和贴心服务，是咱们企业去选择云计算最关键的几点因素。其中的话我们说安全性它也是最关键的。腾讯云的安全生态的实现得益于说腾讯在安全领域积累了多年的丰富经验，并且拥有非常深厚的互联网的安全基因，因为说腾讯本身就生活在互联网中，为用户的基数的庞大，比如说 QQ跟微信在诞生之初就跟安全两个字联系在一起，比如说你们要刷Q币要到号，那么这个时候腾讯就要去阻止这种行为，那么对抗的行为已经有了19年有20年，所以说腾讯在安全这一块的经验是非常充足的。那么在就是说我们提供这种可信可靠保障体系，那么这是咱们的核心的服务理念。我们从这可以看到我们覆盖了从物理层到网络层到应用层，主机层APP层每个上面都会有咱们的产品。对于我们来说，像在网络层我们提供这种DOS的防护，瓦符的应用，渗透的服务，网站漏洞扫描等等都会有。那么在业务层面我们提供人脸识别恶意用户的识别活动防刷防撞号，那么验证码保护进入的反欺诈，那么在APP这一块我们有防盗版防破解，防漏洞，有问题，比如发现你的源码的一个缺陷，那么再就是主基层做入侵保护，然后咱们的密码保护，以及我们的漏洞管理，多个层面去解决你的一些安全性的问题。

互联网业务层面临的风险有哪些？A.撞号登录B.羊毛党活动作弊C.逾期欺诈D.系统漏洞
ABCD

腾讯云安全体系包含以下哪些内容？A.网络安全B.业务安全C.主机安全D.应用安全
ABCD

服务器遭遇暴击破击时，可以通过腾讯云的哪个安全产品进行防护？A.腾讯云大禹B.腾讯云WAFC.应用管家D.腾讯云云镜
D