深信服安全产品技术总监 殷浩

《新安全 新理念 新实践》主题演讲

大家好，我是深信服的殷浩。
接下来我想结合刚才何朝曦分析的安全技术趋势，来和各位分享下我们对当前网络安全建设理念的思考，以及一些最新的实践经验。

2014 年时，国际咨询机构 Gartner 在一份名为"2020 年的信息安全"报告当中给出了一个全新的观点。他认为过去的安全投资中防御类的比重占到了 60%以上，但是到了 2020 年，这些防御投资将会变得无用，需要增加检测和快速响应的投资，而且要占到总比重 60%以上，才能有效防止黑客入侵产生的危害。

那么什么是防御，什么是检测呢？
我们过去采购的 IPS、IDS 属于检测类的投资吗？
根据 Gartner 的定义可以看到，所谓的防御能力，指的是针对黑客的漏洞、Web 攻击的防御产品，比如 FW、IPS、IDS 等都属于这个类别。
而检测，指得是针对那些已经绕过防御体系，进入了我们内网的黑客行为进行检测的产品和手段。

那为什么需要加强持续检测的投入呢？我们可以从黑客入侵的视角来看一看。
黑客的在入侵的第一阶段，会采用各种攻击方式，来获取内部主机的控制权限。过去我们所投资的大部分都是用于这些攻击的防御。但是随着 APT、0DAY 等新型攻击的出现，这些防御体系都是可以被绕过的，黑客是一定可进入内网的。
黑客进入内网后，为了达成他窃取数据的目的，还需要进行持续的渗透，在主机上安装远程控制工具，或者横向移动寻找更重要的目标。而我们针对这些黑客进入内网后的异常行为却极为缺乏有效的检测和发现手段。
这也就意味着，很可能我们系统已经被黑客控制了，但是我们还不知道。

成功入侵后，黑客往往需要潜伏下来，在内网搜索更高级的目标进行渗透。
根据权威机构的统计，从黑客入侵成功，到他真正发现有价值的信息，窃取成功并离开，平均潜伏时间是 225 天。
也就是说，即使黑客潜伏进来，但是只要我们及时发现这些渗透进来的黑客，并及时处置,减少他在内网的停留时间，还是可以有效防止损失的造成。
需要加强快速响应的原因还有一个，就是因为当前业务系统的漏洞层出不穷。

那么我们该如何实现持续检测和快速响应呢？
要想及时发现已经潜入内网的黑客，需要从黑客的视角来看清楚内网每台终端或者服务器是否有异常行为，这些异常行为往往都是看似再正常不过的事情，很容易被我们忽略。
比如说，访问网站时的 DNS 域名解析报文是一个正常的行为，但是如果是从服务器发起，并访问的是一个不规则的 DNS 域名，那 98%的可能性是这台服务器已经被黑客入侵，并且正在向他的控制服务器发起通信。
这还是只是黑客入侵后的第一步，还有像内网的横向移动、数据库异常操作、网站被篡改挂了黑链等等大量的异常行为需要我们去检测发现。

此外，要想精准的发现这些异常，检测手段的部署位置，也是很重要的。首先，互联网出口是黑客控制内网终端和服务器通信流量的必经之路，所以一定要有检测手段。此外，一旦黑客控制了某台低等级服务器，还会寻找更高级的服务器进行横向移动时，就需要我们能够针对数据中心内部的东西流量进行检测，尤其是在虚拟化数据中心这是个难题，后面我们会提到怎么解决。最后，我们的应急团队处理了数百起的安全事件后发现，由于分支结构的安全管理松散，人员安全意识薄弱，所以他们很喜欢从分支机构的终端入手来进行跳板攻击，然后再对总部的数据中心进行渗透。所以第三个部署检测技术的关键点就是广域网边界。

这样是不是意味着又要增加设备了？
的确，如果采用独立的异常行为检测设备的话，方案预算需要重新申请，部署周期更长！ 所以，国际上另一种方式是在下一代防火墙、虚拟化安全产品、数

据库审计产品上集成这些异常检测的功能模块，这样既降低了用户更新安全建设的整体拥有成本，让方案更可行，更容易落地，同时管理也更加简单。
更重要的是，对于那些已经采购了深信服安全产品的客户，只需要进行软件升级，就可以立即拥有这些领先的检测技术了。早一天部署，早一天看清内网的潜伏者！

接下来，我们再看看如何进行更快速的响应。
知己知彼，方能百战不殆，这句话同样适用于网络安全的对抗。
知己就是说，要能够清晰的掌握 IT 系统状态，有多少台终端、多少台服务器和网络设备，应用系统是什么版本等等都能一清二楚。
知彼指的是，能够从黑产、社工库、乌云等漏洞平台，充分掌握外部的威胁情报。
才能够在第一时间对比分析出，那些对我们系统真正能够造出危害的情报，我们才能进行更及时的处置。
所以，在 2016 的 RSA 大会上流行这样一句话：你永远不能保护看不见的资产！

大家可以看到，当前安全建设的一个重要基础就是可视。
过去我们安全建设只关注 IP、端口、特征，就足够用来分区好人、坏人了。
但是今天，还需要从用户、行为、业务资产者三个维度来收集更丰富的信息，才能帮助我们判断出一个用户、一个流量、一个业务系统的安全该状态。有了这些最基础的信息，我们才能够实现更准确的检测、更快速的响应。所以，我们认为当前安全建设的基础是可视化。

那如何更精准、更快速的实现风险的可视呢？
是采用人工分析还是自动化手段，是靠一己之力，还是众人拾柴火焰高高的方式？
毫无疑问，后者才能让我们更精准、更迅速！

所以早在两年前，我们就建立了能够自动分析未知威胁的云平台，它可以实时

收集每一台防火墙的恶意和可疑流量(当然这是在经过客户许可的情况下)，对可疑的流量，经过沙盒内虚拟执行后，会把确认的威胁特征，下发到所有在线的防火墙，提升对未知威胁的防护能力。
对于收到的恶意流量，会再加上外部威胁情报，在云端进行大数据分析，可以给出更全面、更精准的攻击者画像。

我们可以来看一个例子，这是从客户的防火墙上报过来的两个日志，一个是感染主机的木马恶意文件被拦截的日志，一个是内网 PC 链接僵尸网络控制服务器的异常 DNS。两条日志上报云端后，经过沙盒的执行，我们发现他们都是来自于同一个僵尸木马网络，而且找到了这个服务器的 IP 地址。

当我们的云平台加入了威胁情报和大数据分析，这个僵尸木马网络的整个画像就被清晰的勾勒出来了。围绕着这个控制服务器，一共有数百个 DNS 域名，十多个不断变种的恶意代码。所有的这些信息，我们都会下发到在线的防火墙设备中，帮助客户在第一时间有效应对这些变幻莫测的恶意威胁。

在此，我强烈的建议：
· 已经在互联网出口购买了深信服下一代防火墙的用户，尽快将你们的防火墙连入威胁感知云平台；
· 如果还是在使用传统防火墙的用户，也建议您尽快升级到具备威胁感知的下一代防火墙；
以帮助您更精准、更快速的抵御这些变化莫测的网络威胁。

也正是由于深信服在检测能力的突出表现，获得 Google 的认可，加入了 Google 主导的安全情报联盟 Virustotal。在这个联盟中，目前只有数十家在安全监测技术方面有突出成绩的厂商，大家每天都会共享各自最新的威胁情报数据、恶意代码数据。
国内也只有安天、金山、360 等少数病毒厂家能够加入这个联盟，而深信服是国内唯一一家以网络安全厂商身份加入的公司，这充分说明了我们在恶意代码检测方面的技术实力。

此外，加入了这个联盟后，我们每天还可以获得 20G 的威胁情报数据，从而帮助我们更加精准帮助用户发现内网的未知威胁。

这样看来，好像安全建设的工作，要分析的内容翻了数倍，要掌握的技术多了很多。但深信服认为：面对这么多的新技术、新应用，安全的交付需要简单易用。具体可以分成三个层级：
首先，产品需要简单易用。
为了避免复杂的安全策略配置，造成错配漏配等低级错误，我们认为可以通过向导式部署，来优化产品的配置管理功能。
比如说，下一代防火墙经常部署在数据中心,只要用户根据向导，选择好部署方式、保护的目标对象，保护业务系统所必须的功能和安全策略都会自动生成，从而在数据中心场景下近万条的安全策略都不再需要管理员手工一条一条去配置了。

第二个层级，需要做的就是方案架构的精简。
在同一个场景下，能用一台设备解决，就尽量用一台设备解决，比如我们把 2-7 层防御、检测都集成进入了下一代防火墙 NGAF。
在这个方式下，首先方案会更加实用，由于设备数量的精简，方案成本会得到降低。在 IT 预算有限的情况下，我们的用户让应用系统的建设和安全建设同步推进，从而避免安全事件发生造成了损失后，才开始加大安全投资的情况。
此外，从技术上来说，安全建设效果也会更好。过去，要想实现威胁检测和快速响应式，需要在 4、5 种设备之间进行分析和联动。但是集成以后，这些工作都可以在一台设备内部完成， 更加高效、更加精准。
最后，精简的架构，也就意味着减少了串行的设备，减少了单点故障，系统的可靠性也会更高。

第三个层级就是交付方式的创新。过去，即使买了设备，安全建设也仅仅完成了一半，还需要找第三方的厂家安全服务专家进行运维服务。但是这些专家一般都是定期服务，每周或者每月来进行定期巡检，难以满足当前快速响应的需求。

所以，深信服认为通过产品加云端安全服务的方式，把过去安全运维所需要的知识、能力、经验、技能、情报等变为云端的在线服务，配合不同场景下的安全产品，让用户在现有的人力资源情况下就可以做好安全建设和应急响应，实现安全的自动化、智能化交付，减少对人的依赖。

这种创新的交付方式，已经有了很多的合作案例。
比如与广东省公安厅网安大队合作的"护城河"项目，通过我们的网站安全风险扫描云服务，对 5000 多个政府、国企、教育的网站安全风险检查，一共发现 2000 多个网站存在的安全漏洞，并发现了 60 多起网络安全事件，涉及近百万用户信息的泄露风险。与此同时，我们也在帮助这些用户积极做好网站的安全加固。
这样的一种合作方式，可以开放给不同部位、行业的监管单位，共同提升看到我们行业互联网业务的风险可视能力。

随着 IT 环境的开放化、虚拟化，深信服认为当前的安全建设理念概况起来是三点：可视是整个安全的基础，我们需要加大持续检测和快速响应的投资，并且选择能够简单易用的实现交付的安全产品和方案。从而让我们的安全建设更富成效。

那接下来，我们就从如下四个主要的业务场景，来看看，基于新理念的安全建设方案和传统的方案有什么不同，深信服的这些创新能够给各位带来什么价值。

首先是，自建云数据中心的场景。当前数据中心已经开始大量使用虚拟化技术，虚拟机之间的流量大部分都在虚拟化内部实现了交换，数据中心内的安全边界也就消失了，从而内部是否存在跳板攻击等异常行为都很难发现。此外，要想把传统 IPS、WAF、AV 等安全技术部署进入虚拟化环境，需要开启多台虚拟机来运行，比较消耗性能。此外，当前业务的开放化，数据共享、数据交换越来越多，数据中心不再是封闭的。高明的黑客要想进来，还是会找到办法的。但是现有的安全体系难以让我们发现这些隐藏在眼皮底下的黑客。

所以，结合新安全理念，深信服认为自建数据中心的安全建设应该涵盖四类产品、一类服务：

· 在物理网络边界部署下一代防火墙、数据库审计、VPN 等安全硬件设备，实现从用户接入访问到数据库的多重防御，提升了黑客仿冒用户身份，正面突破，越权访问的攻击成本；

· 在虚拟化环境部署云经和云纬安全组件，实现对虚机之间资产和流量的可视、可控。然后再配合深信服的安全服务云，从而可以形成从物理到虚拟化的纵深安全体系，并且具备了从防御，到检测+响应的安全管理闭环。

在整个方案中，虚拟化的安全，是很多朋友都比较关注的。

云安全组件这个方案的特点在于，每台物理服务器上只需部署一个安全组件，就可以实现防御和检测功能，这极大的减轻了服务器虚拟化的性能消耗。

在部署了组件以后，我们就可以直观的看到了所有虚机资产的状态，还可以根据业务属性进行安全域的划分。而且，这些组件可以实现虚拟机间东西流量的可视、可控，通过 L2-L7 防御和检测功能，实现各种横向攻击的异常检测，确保堡垒不会从内部被攻破。

更重要的是，这些安全组件的部署都十分简单，我们的组件已经实现了和 Vmware 平台的自动化对接，您只需要在管理界面上轻松点击 4 个步骤，整个虚拟化环境就可以实现安全的可视、可控了。

总之，我们希望通过构建起从数据中心物理边界到虚拟化内部，从身份认证到数据库访问的多重防御和检测体系。

更重要的是，发现了这些异常之后，这些异常的分析和处置都不再需要大量人力的堆积，通过自动化的云服务，您就可以获得专家团队的 7*24 在线帮助，只需要在我们提供的微信应急管理界面上轻松点击几下，威胁就可以被轻松解决掉。

更出色的网络安全能够带来更出色的业务成果。

我们再来看看第二个场景，有多租户的行业云。
一直以来，关于政务云、行业云，大家讨论的一个重要话题就是，业务迁移到了云上以后，系统的安全到底该谁负责呢？
先以最成熟的公有云 AWS 为例，他们认为安全责任应该是租户和云平台公担的。租户负责自身业务在云中的安全性、合规性。平台方负责云平台自身的安全性和合规要求。
此外，公安部三所正在制定的云计算等保标准中，也明确提出了需要针对租户、平台方划分清楚各自安全责任的要求。

但是我们看到，对于很多已经把业务迁移到了云上的用户来说，处在了一个两难境地。前几天，一位政务云客户表示，已经近百个的政务网站迁移到了上面。但是他们却被说成该省的最大养马场，养的是木马。
虽然，云平台该买的安全设备都买了，但是黑客还是成功入侵了很多网站，挂了木马、改了黑链。而且租户缺乏手段来及时发现业务系统的异常，往往是被挂马了半年，被用户访问投诉了才发现。
所以，这就是当前很多租户的两难境地：一面是严格的安全责任，做不好要挨板子；另一面，很多云平台却没有提供充足的安全技术手段，来帮助租户实现从防御到检测和响应的闭环安全管理。

所以，针对这些租户，我们提供一种和云平台无关，一站式 Web 业务安全服务方案。只要在 VPC 的虚机上安装一个我们的插件，在再链接到我们的安全服务云，就可以为 Web 业务提供从风险评估到安全防护，从安全运营监测到应急响应的全生命周期安全管理服务。

当然防护是最基础的要求，我们把下一代防火墙 2-7 层的防护功能都集成到了这个插件上。

大家都知道，Web 业务更新迭代快，代码一更新，难免存在一些漏洞，所以我们需要在业务上线的同时，对服务器进行漏洞扫描。不但要进行通用漏洞的扫描，还要实时通报乌云等漏洞平台发布的漏洞。

目的只有一个，就是当您的 Web 一旦上线，或者进行了更新，我们就能够让您看到系统存在的风险，从而避免漏洞风口器过长，给黑客提供了入侵的便利。防止漏洞长期暴露在互联网上，让黑客有可乘之机。
此外，我们还能帮助您实时监控网站的安全状态，什么时间被谁攻击了，攻击是否成功，内部主机是否被黑客控制了，网页是否被篡改、挂了黑链，等等这些安全事件都可以精准地被发现。
而且这些安全事件报告，还可以通过微信及时的发送到您的手上，让您 7*24 小时掌握云上业务的安全状态。而且一旦出现重大问题，还可以请求我们的云端安全专家帮助您进行应急响应和业务修复。

那么针对正在开始规划、建设云平台的建设方来说，选择一个能够帮助自己和租户满足合规要求、真正具有安全成效的云安全解决方案也是十分重要的，要不然云平台建好了，但是没人愿意往上面迁移也是个问题。

所以，我们提供了安全资源池解决方案，将等保合规所需要的安全设备以 NFV 的方式，运行在我们的超融合平台上。而且安全资源池可以通过 Rest API 实现和云平台的管理对接。让租户可以根据自己的业务需求选择不同性能、功能、时间周期的虚拟安全服务设备，满足不同的合规要求。
更重要的是，这个平台极具伸缩扩展性，前期买上两三台服务器，就可以实现完整的合规方案，等到租户增多了，只要增加硬件服务器就可以实现安全资源的平滑扩展。

总之，我们在私有云、政务云等不同数据中心场景做了很多的安全方案创新，目的只有一个，就是今后，无论您的业务是在哪里，选择的什么云平台，在云上或者在云下，我们都可以让您的业务同样安全、合规，可以有效抵御威胁，保护数据资产。

看完了数据中心的两个场景，我们再来看看网络安全空间中的一个兵家必争之地，互联网出口。原因之一前面已经提到了，这是黑客控制内网服务器和终端进行数据窃取的重要通道。

此外，互联网出口还是内网用户上网的必经之路，在这些看似正常的上网行为中，实际上还隐藏着巨大的"看不见管不住"风险。比如说当前 60%以上的互联网应用都是采用了 Https 加密流量，越是非法网站，越会采用加密方式隐藏其内容。

所以，互联网出口的安全管理方案有两个关键要求，一个是让上网行为可视可控，满足合规要求，防止敏感信息外泄；另一个就是在实现安全上网的基础上，能够实现针对发现 ATP 攻击、发现被黑主机的异常检测，防止黑客破坏行为真正造成损失。用一句话来概括我们的方案的价值就是：让非法行为尽收眼底，被控主机一网打尽，敏感数据走出不去。

最后，我们再来看看移动业务安全。移动业务就像风筝，在天上飞着，看起来很美但是危机四伏，只要线一断，就会坠落。移动业务由于是在外部不可控的环境下进行操作，访问内部系统和数据，所以一旦出现身份被盗用、终端丢失、被恶意软件控制、权限管理松散等问题，就会严重影响我们内部的数据保护。看到很多安全事件，都是从移动接入开始的。

所以，移动安全不仅仅是 VPN，还要把安全风险的可视化能力、控制能力延伸到终端上。为此根据不用业务场景的需求我们的 EMM 终端管理软件提供了数百种安全功能。但是，我们建议客户一定要基于业务场景来使用。

没有意识到风险是最大的风险。
网络安全具有很强的隐蔽性，
一个技术漏洞、安全风险可能隐藏几年都发现不了。
结果是"谁进来了不知道、是敌是友不知道、干了什么不知道"，长期"潜伏"在里面，一旦有事就发作了。

——习近平主席的 419 网络安全讲话

所以大家可以看到，在党和国家的领导下，我们的安全理念是顺应国家网络安

全建设的大方向的。我们认为，在今后的安全建设中：

可视是安全建设基础，

需要加大持续检测和快速响应的投资，

并选择更简单易用的方式，实现安全的交付。

最终，希望通过我们的创新，让 IT 更简单、更安全、更有价值。