为什么网络安全建设需要深信服下一代防火墙？

近几年来，越来越多的安全事故告诉我们，安全风险比以往更加难以察觉。随着网络安全形势逐渐恶化，网络攻击愈加频繁，客户对自己的网络安全建设变得越来越不自信。到底怎么加强安全建设？安全建设的核心问题是什么？采用什么安全防护手段更为合适？已成为困扰用户安全建设的关键问题。

安全建设的两个核心问题，您考虑的全面吗?

问题一：看不看得到真正的风险

1、攻击看得到么？： 只有看到 L2-7 层的攻击才能了解网络的整体安全状况，而基于组合方案（即部署了多种安全设备）的大多数用户没有办法进行统一分析，也就无法快速定位安全问题的根源，同时也加大了安全运维的工作量。

2、没有攻击就安全？： 没有攻击并不意味着业务就不存在漏洞，一旦漏洞被利用就为时已晚。最近几年，大家都在谈论 APT 攻击，而 APT 攻击最令人头疼的就是它可以安静地潜伏在网络中，伺机行动，在没有窃取到机密信息之前，它会想尽一切办法将自己隐藏起来。所以，好的解决方案应该能够及时发现业务漏洞，防患于未然。

3、攻击多就威胁大？：即使有大量的攻击也不意味着业务安全威胁很大，只有针对真实存在的业务漏洞进行的攻击才是有效的。看不到有效攻击的方案，就无法让您看到网络和业务的安全情况。

问题二：防不防得住潜藏的攻击

1、防护有没有短板？： 防护技术不能存在短板，存在短板必然会被绕过，原有设备就形同虚设。传统的防火墙设备或者 IPS 设备，只能针对网络层和传输层进行攻击防护，面对网络的第七层-应用层的各种攻击常常束手无策。

2、潜藏攻击怎么办？： 只针对外部黑客对内网终端和服务器的攻击进行防护，是远远不够的，如果终端和服务器主动向外发起的流量中存在攻击和泄密行为，也同样会带来很大危害。所以，流经网络的双向流量内容都需要进行检测，实时发现黑客针对内网的控制通道，阻断泄密的风险。

综上所述，真正能看到攻击与业务漏洞，及时查漏补缺，并能及时防住攻击才是最有效的解决方案。那么基于攻击特征防护的传统解决方案是否真的能够达到要求呢?

传统组合方案（FW+IPS+WAF）能否满足您的需求?

有几款设备就可以看到几种攻击，但是难以进行统一分析。在没有攻击的情况下，系统无法看到业务漏洞，但这并不意味着业务漏洞不存在，因而很难指导用户进行正确的安全建设；

有几种设备就可以防护几种攻击，大部分组织单位用户无法全部部署，所以存在短板；即使部署完整，这些设备也不对服务器和终端向外主动发起的业务流进行防护，在面对新的未知攻击时，缺乏有效措施，导致系统面临被绕过的风险。

其他品牌的下一代防火墙能否全面解决问题?

目前市场上的众多品牌，可以看到除 Web 攻击外的大部分攻击，但无法看到业务漏洞。由于攻击和漏洞无法关联，所以很难确定攻击的真实性；

防不住 Web 攻击，也不对防护服务器/终端主动向外发起的业务流进行防护，比如信息泄漏、僵尸网络等，应对未知攻击的方式比较单一，只通过简单的联动防护，仍有被绕过的风险。

深信服下一代防火墙可以完整覆盖组织单位网络建设的安全需求！

威胁看得到——可视

深信服下一代防火墙可以分析出网络中的应用类型、应用内容中的威胁和攻击、威胁带走的数据内容，并能实现报表呈现，实现真正的 L2-7 层统一的安全可视化；

通过主动或者被动流量检测，及时发现业务漏洞，即使没有攻击也能找到业务中潜在的风险；

通过攻击与业务漏洞的关联分析，可以帮助您准确地找到有效攻击，清楚网络和业务运行的安全状况。

攻击防得住——双向

深信服下一代防火墙具备 L2-7 层的攻击防护技术，不仅可以防护外部攻击，还能检查服务器/终端外发流量是否有风险，弥补了传统安全设备“只防外、不防内”的不足。

同时，可以检测服务器外发数据是否有泄密或篡改风险，以及内网的终端电脑是否被黑客控制、形成僵尸网络。