2015 年会是基于风险的安全之年吗？

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Will 2015 be the year of risk-based security?		
原文作者	Bret Hartman	**原文发布日期**	2014 年 12 月 22 日
作者简介	Bret Hartman 是思科系统公司安全业务组的副总裁兼首席技术官，其研究方向包括信息安全、云计算、面向服务的体系结构、身份管理等。http://www.linkedin.com/pub/bret-hartman/0/3a/631		
原文发布单位	思科系统公司		
原文出处	http://www.net-security.org/article.php?id=2188&p=1		
译者	安天技术公益翻译组	**校对者**	安天技术公益分析组
免责声明	本译文为安天实验室针对网络资料翻译而成，并未取得原作者授权，仅供内部学习和交流使用，安天实验室不对任何可能因此导致的版权问题承担责任。		

2015 年会是基于风险的安全之年吗？

Bret Hartman

2014 年 12 月 22 日

随着 2014 年进入尾声，很多人都在预测来年的安全趋势。网络安全人员站在防御日益动态的威胁全景和网络犯罪的最前沿，预测 2015 年的安全趋势并予以公布已经成为一项传统。

在当前的世界中，攻击日益复杂、受利益驱动，而且由资金雄厚的有组织犯罪和国家控制。因此认为新的一年中会出现很多无法预见的复杂攻击类型是合理的。

在研究未来安全趋势的过程中，我回顾了 Gartner 的《2015 年的前 10 个战略技术趋势》。非常有意思的是，Gartner 认为这些趋势是未来 3 年的重大干扰因素，而安全是确保适应这些趋势的基础。

Gartner 所列出的其中一个趋势“基于风险的安全和自我保护”引起了我的注意。我将 Gartner 总结的几个重点列举如下：

- 在数字化的商业世界，安全不能成为终止所有进步的障碍。
- 企业将越来越深刻地认识到，不可能实现 100%的安全环境。
- 边界和防火墙是远远不够的；每一个应用程序都需要自我保护。

断言我们正在迈向完全自动化的网络可能还有一点早，但是 Gartner 公司以前总结的很多趋势已被证明是正确的，也促使了企业高管层关注网络安全。

很长一段时间中，我都鼓励安全从业者接受以下现实：问题不在于企业是否会遭到攻击，而是何时会遭到攻击。攻击者的动机和持续性都有所增加，而且对传统安全技术和应用的理解也进一步加深。攻击者冷酷无情，经常使用专门开发的工具来绕过目标的基础设施。

随着越来越多的企业采用了与物联网和万联网相关的新型商业模式，他们面临的挑战也更加严重。现在有 100 亿个互联的设备，预计这一数字将呈现指数式增长，到 2020 年，将会有超过 500 亿个传感器、对象以及其他连接的“物体”。思科估计，在未来十年，万联网将会在全球创造 19 万亿美元的股权价值（净利润）。采用适当的安全措施有助于个人和企业从万联网和物联网获得更大的价值。

了解在 2015 年将会面临的问题之后，您可能想知道企业应该采取什么样的战略来应对这些挑战并保持强大的安全姿态，以便从容应对下一个颠覆性技术的浪潮。

最好的起点是基于风险的安全运作方法，该方法或者关注威胁本身，或者只关注策略/控制措施。该方法必须涵盖所有潜在的攻击向量，迅速适应新的攻击方法，并在每次攻击后获取相应的情报。

此外，这种威胁为中心的安全策略也必须与业务风险相结合。需要注意的是，真正重要的威胁是那些严重影响应用数据的威胁。企业每天都面临众多的威胁，着重解决能够导致最严重损害的威胁可以提高安全控制措施的有效性，即利用自动化和动态的控制措施来阻止最严重的威胁。

采用包括上述属性的方法可以降低复杂性和碎片化，同时在整个攻击过程（攻击前、中、后）获得很好的可视性和连续控制。

Gartner 对 2015 年的预测是否正确呢？了解这一点只是时间问题。目前可以确定的是，不存在安全方面的“银子弹”，无论你采取什么样的战略，攻击和破坏都会发生。安全策略必须不断发展和改变，以便与动态的威胁全景保持同步，为企业提供必要的保护，使其保持适当的安全态势。

防御复杂攻击的必要技术已大大提高，我们可以采用可视化和广泛数据收集方法，通过相关性和背景来了解威胁情况，并动态地应用安全控制方法。

不知道您如何看待未来的安全趋势呢？我期待着看到这些大胆的预测如何在 2015 年及以后成为现实。