简译版

2018-2019 年六大安全趋势

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	6 Security Trends for 2018/2019		
原文作者	Curtis Franklin Jr.	原文发布日期	2018 年 10 月 15 日
作者简介	Curtis Franklin Jr.是 Dark Reading 的高级编辑。https://www.darkreading.com/author-bio.asp?author_id=512		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/cloud/6-security-trends-for-2018-2019/d/d-id/1333043		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

2018-2019 年六大安全趋势

Curtis Franklin Jr.

2018 年 10 月 15 日

在 Gartner IT 展览与研讨会（Gartner Symposium/ITxpo）上，分析师彼得•福斯特布鲁克（Peter Firstbrook）列出了 2018/2019 年的六大安全趋势。在未来一年，这些趋势很可能会成为公司高官们谈论的重点。

本周，Gartner Symposium/ITxpo 在美国奥兰多举行，来自世界各地的约 9000 名公司高管参加了会议，共同探讨计算机和网络行业的趋势、策略、最佳实践和技术发展。会上，Gartner 副总裁兼分析师彼得·福斯特布鲁克向与会者介绍了 2018/2019 年的六大安全趋势。他并未过多地谈论具体技术，而是侧重于策略问题。在未来一年，他列出的这六大趋势很可能会成为公司高管们谈论的重点。

在这六个趋势中，只有一个涉及到特定的技术领域。其余五个则涉及如何计划、购买和部署安全产品。

趋势 1 :公司高管将开始关注安全问题 ,安全专家必须做好准备。

根据已经生效的《通用数据保护条例》（GDPR），安全事件（如“魔窟”[WannaCry]等攻击事件）导致的数据泄露和破坏，将会带来高额罚款或者看得见的重大经济损失，这迫使公司高管和董事会开始关注安全问题。这意味着，他们将会使用业务语言提出有关安全的问题——安全专家必须做好准备，使用业务相关的语言回答他们的问题。

福斯特布鲁克说 ,安全专家必须能够从业务风险而非安全威胁的角度来讨论安全需求和响应。他还指出，采用多样性的方法将会提高 IT 安全团队的需求响应能力，有助于满足不断增长的人员需求。

趋势 2：有关数据保护的法律法规越来越严苛，IT 安全团队必须慎重响应。

无论是用声誉和业务损失，还是用立法和监管机构的直接罚款来衡量，数据泄露的责任成本都在不断增加。这在一定程度上改变了安全和数据保护成本的算法，不过它们最终都取

决于业务风险情况。

新一轮立法导致的一个结果是，客户对其个人数据的收集、存储和使用有了更直接的控制权。因此，许多成功的公司正在寻求通过一些方法（例如通过第三方进行信用卡交易，而非自己处理这些交易及交易产生的数据），来规避部分数据收集工作。

趋势 3 安全产品正在迁移到云端，并在此过程中变得更加敏捷。

福斯特布鲁克说，这一趋势的重要性在于其影响。他以普锐斯和特斯拉汽车为例进行了说明——前者是一款扎根于经典汽车的混合动力汽车；后者则在很多方面进行了重新设想，包括汽车的推进力和连接程度。他说，当其他汽车制造商还在努力将汽车的各部分连接起来时，特斯拉已经推出了汽车互联的思路。

他指出，云安全服务比传统的本地产品更加灵活和可扩展，而且它们还提供了另一个优势——人员扩充。他说，充分利用云服务的关键是：确保云服务有完整的应用程序编程接口（API），以便集成到更大的生态系统中。

趋势 4 部署机器学习，为简单任务和复杂分析提供真正的价值。

福斯特布鲁克说，将机器学习部署到安全领域，最大的阻碍是可能会出现大量的误报——对于分析师而言，获得的噪声（noise）可能比有用信号（signal）还多。而现在，机器学习能够对告警进行分类，以提高信噪比（ signal-to-noise ratio），最终提高分析师的工作效率。

福斯特布鲁克认为，这正是机器学习在安全领域的真正价值。不过，他也承认存在另一个阻碍——机器学习引擎的训练，其他专家也警告过这一点。

趋势 5：与技术和业务因素一样，地缘政治因素也会影响安全产品的购买。

公司都有自己的地理位置，这在现实世界中是不可避免的事实。这意味着，国家之间的关系可能会对公司之间的关系产生影响，特别是在安全产品的信任方面。

在安全领域，地缘政治因素已经影响了对一些公司（如卡巴斯基和华为等）产品的购买决策。在购买安全产品时，你是否信任这些公司的产品可能不是最重要的因素。

如果你的客户群包括政府机关或部门，而且他们有自己信任的公司，那么这就会限制你的购买方案——你只能从这些“受信”公司购买产品。随着网络战变得越来越激烈，这种趋势很可能会更加严重。

趋势 6：权力和能力的“中心化”最终将导致“去中心化”

安全行业正处于“中心化”时期。例如，目前基本上是两家公司垄断了全球的证书签发。对这种权力中心化的担忧开始导致去中心化。

福斯特布鲁克指出，去中心化最典型的例子是区块链技术。在安全领域，分布式账本技术仍处于早期阶段，但是现在许多公司都在寻求各种方法来使用该技术。

去中心化的另一个例子是向边缘计算的迁移。在边缘计算中，计算能力被分配到端点设备，而非局限于位于体系架构中心的云。

对于成功的公司，福斯特布鲁克建议他们探索不同的去中心化架构和提供商，从而避免拘泥于任何单一分布式模型。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com