AhnLab

安全月刊

2022.07 Vol.116

2022 年 RSAC 和 Gartner 峰会

RSAC 和 Gartner 峰会重返线下，揭示行业最新动向

2022年6月的第一周，分别举行了全球安全会议RSA Conference 2022以及Gartner Security & Risk Management Summit。这是2020年新冠状病毒大流行以来首次从线上会议恢复线下活动。AhnLab亲临会议现场，对过去2～3年间全球安全市场的主要热点及变化趋势进行了详尽的了解。

本文将分享这两场会议的主要内容及见解。

【图1】RSAC 2022 旧金山莫斯康展览中心（Moscone Center）全景

在RSAC 2022召开之际，由全球IT领域专业调查机构Gartner主办的“Gartner Security & Risk Management Summit 2022（以下简称Gartner峰会2022）”也在同一周举行。Gartner峰会2022自6月7日至10日于美国马里兰州国家海港举行，会议分别创下▲参会人员约4千人、▲参展企业224家、▲会议总数达350场的记录。在峰会中，Gartner分析员和安全领域的专家们通过演讲分享了最新安全情报。

【图2】Gartner峰会2022会议现场

两场活动都规模盛大，主要围绕网络安全这一主题进行了广泛且深入的探讨。下面就两场会议中主要涉及的▲人工智能（AI）、▲云安全、▲零信任（Zero Trust）和▲XDR ＆ MDR等内容进行了汇总。

人工智能在安全领域中的作用

网络安全的高度复杂性已不是新鲜话题。通过人力响应高级威胁、执行多种安全解决方案已达到极限，而这一趋势在未来将会愈演愈烈。能够处理庞大数据的人工智能被认为是这一问题的解决之策。

在Gartner峰会2022开幕式的主旨发言中，对10年之后的2032年，组织内利用人工智能响应网络威胁的合作模型进行了模拟。当组织遭受网络攻击时，商务专家将基于人工智能对商业影响的分析结果，集中于制定策略，而技术专家将通过人工智能取证服务，分析攻击方法和原因以找出响应方案。战略专家将依据响应结果，引导组织对运用人工智能加强安全的体系做出决策并予以投资。

【图3】Gartner峰会开幕式主旨发言（左侧：Katel Thielemann，Gartner VP Analyst，右侧：Andrew Walls，Gartner Distinguished VP Analyst，来源：Gartner）

Gartner通过该主旨发言提出了“AI Augmented”这一概念。直译过来时增强人工智能，其核心内容是强化人工智能并通过与人的协同效应，从组织的角度出发，将网络安全协作实现最大化。另外，演讲中还强调了人工智能会根据训练的数据发挥相应效果，因此需要人们在人工智能可解释性（AI-explainability）方面提高一个层面。

在RSAC 2022中，微软公司安全、合规、身份和管理部门副总裁，Vasu Jakkal通过发表强调了运用人工智能进行安全创新的重要性。

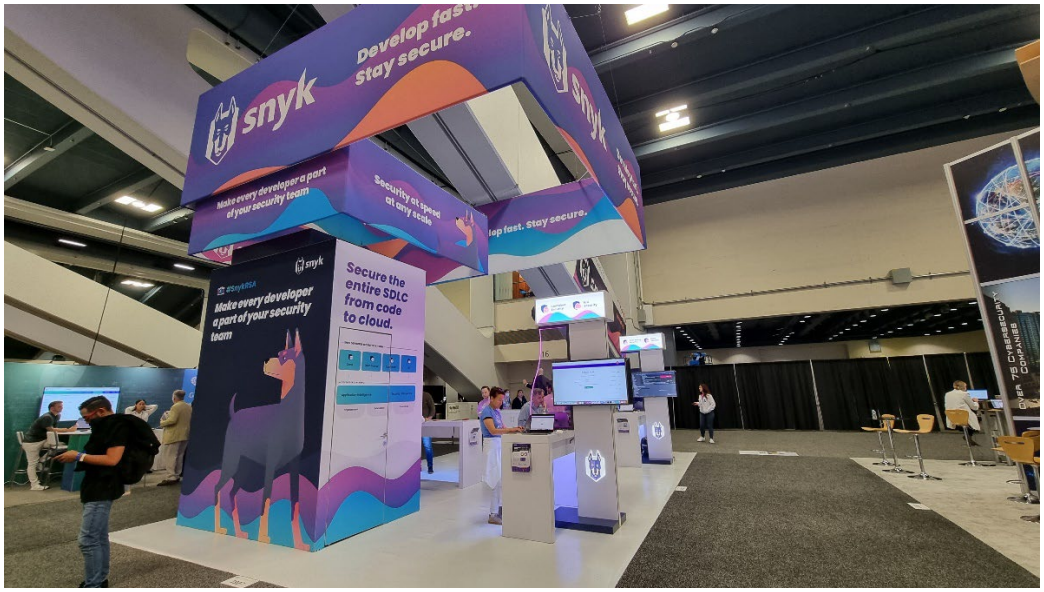
【图4】Vasu Jakkal，微软副总裁进行发表（来源：RSAC）

Vasu Jakkal副总裁强调，目前每秒发生921次网络攻击，攻击者行动如此之快，必须提高相应的响应速度。在

这一背景下，可以快速处理大量数据的人工智能脱颖而出，特别是在检测领域对威胁进行分类。基于这一点，可以根据业务情况和形势进行定制响应。此外，为促进人工智能技术在安全领域的发展，敦促在积极的数据共享的基础上，最大限度地发挥人工智能的潜力。

云原生安全的核心是?

在过去几年里，云安全一直是安全行业的主要话题，在RSAC 2022及Gartner峰会2022上依旧受到了广泛关注。在两场活动中，进行了多场会议，从多角度审视云安全。众多安全企业通过展览展示了自己的解决方案和新的安全功能。



【图5】RSAC 2022 DevSecOps供应商Snyk展位

最近云安全的前提是“云原生服务的生命周期越来越短”这一事实。因此，需要一种能够快速响应变化并提高运营效率的新的安全方法。

最具代表性的方法是“DevSecOps”。DevSecOps是“开发、安全和运营”的缩写，在软件初始阶段起在整个集成开发和运营的“DevOps”流程中应用安全性。通过这一方式，缩短了开发和运营时间，并在DevOps基础上增加了安全性，既能确保安全的开发结果，又能加强相关部门之间的合作。

Gartner建议将“云原生应用程序安全平台（Cloud Native Application Protection Platform: CNAPP）”作为DevSecOps在管道中的安全措施。CNAPP集成了云工作负载安全平台（Cloud Workload Protection Platform: CWPP）和云安全态势管理（Cloud Security Posture Management: CSPM），并且添加了其他附加功能。

Gartner高级总监分析师Charlie Winckless在2022年Gartner峰会上进行了“Outlook for Cloud Security”会议发表。他解释，作为CNAPP对DevSecOps安全的基本组件，CWPP负责运行时保护、CSPM负责云安全态势管理、AST（Application Security Testing）负责扫描Artifact。

同时还强调了作为云原生安全运营核心元素的自动化的重要性。核心是基础架构即代码（Infrastructure as Code: IaC)以及策略即代码（Policy as Code）。其目的是利用代码来构建构成DevSecOps管道的基础架构以及应用的策略，自动化分发、控制和管理，从而实现快速采取措施和更改。

零信任（Zero Trust）成为大势所趋

在RSAC 2022和Gartner峰会2022中，不难发现不少展位都将“零信任（Zero Trust）”放在最前面。Palo Alto Networks、Illumio、iboss等多家企业展位的标语上都引用了零信任这一词语。随着网络威胁的不断进化，零信任已成为安全领域的新趋势。

【图6】RSAC 2022 Palo Alto Networks、思科展位

首先，零信任并非解决方案，而是一种安全方法或愿景。美国白宫国家网络局长John Chris Inglis在RSAC 2022主题演讲中将零信任定义为“改变政府和企业的安全流程”。此外，Gartner高级研究总监Thomas Lintemuth将其定义为“持续验证非明文信任和上下文信任的愿景”。

那么，零信任具体是怎样构成的呢？在Gartner峰会2022的“5 Steps to Start the Zero Trust Journey”会议中，Thomas Lintemuth提出的零信任架构共包含七个阶段。下面简单介绍一下。第一阶段到第三阶段分别验证用户、设备和用户想要连接的应用程序。在第四阶段中，对用户、网络、工作负载和应用程序等进行监控。在第五阶段中，自动化威胁情报应用和应用程序管理。在最后的第六和第七阶段中，进行数据安全和分段（segmentation）。

综合RSAC 2022和Gartner峰会2022的各会议对零信任的讨论内容，得出的结论是，在身份验证完成并持续验证安全性之前，零信任不信任任何东西。

零信任的概念之所以备受关注，是因为在当前IT环境下需要管理的层级和对象多样化，仅靠现有网络边界安全已无法保证安全。尤其是对于动态的分布式云原生应用程序更是如此。对此，零信任架构将基于细化的访问控制加强了安全。

XDR & MDR，离我们还有多远?

可能有人质疑XDR是否仍然是一个与现实相去甚远的营销术语。然而，在本次RSAC 2022和Gartner峰会2022上，证实了XDR并非是一时的潮流，而是安全行业未来发展的方向。

【图7】RSAC 2022 XDR，MDR供应商展位

众多组织和企业已定义XDR，可以概括为“一个可集成、关联多个安全防御、检测与相应组件的数据与告警，并将其情景化的平台”。XDR的作用是，从多个单点安全产品获取的告警作为威胁事件导出，提供各种类型的检测选项，并基于自动化响应提升安全运营效率和生产力。

XDR还涵各种领域，例如端点和网络，以及电子邮件和云。所有区域都应得到安全保护是最为理想。但是，要保护的优先级通常根据采用XDR的组织或提供XDR的供应商的具体情况来确定。

在Gartner峰会2022的会议中， Gartner高级总监分析师Dave Messet建议， 如果需要在XDR组件之间设置优先级，应该先集成▲端点（EPP/EDR）、▲电子邮件（SEG）、▲身份（IAM）。因为最近的高级攻击场景中可以看出，端点通过终端用户点击钓鱼邮件的链接而遭到入侵，其后窃取ID和密码等凭据受到损害。

接下来介绍一下MDR。随着从EDR到XDR“检测和响应”的概念的兴起，MDR也备受关注。MDR可以定义为“一种基于快速检测、分析、调查和响应来缓解和控制威胁的安全运营服务”。它不受地点限制提供，其特点是基于专家分析和调查不仅是维护和威胁，而且还可以得出可实现的结果。

MDR服务的组成部分包括24小时监控、入侵检测、入侵调查、入侵控制和威胁捕获。此外，还增加了攻击面管理和入侵响应能力以完成MDR服务。

根据Gartner的调查结果，从2020年到2021年，全球MDR市场增长了48.9%。原因很简单。这是因为，尽管威胁在进化，需要保护的领域也在增加，但很少有组织能够运行24小时安全并检测和响应威胁。由此，可以预计未来对MDR服务的需求将继续扩大。

结语

在RSAC 2022和Gartner峰会2022上，可以亲眼目睹新冠状病毒大流行期间安全市场的急剧变化。两场大会共同揭示的代表趋势是“从单点解决方案转换为集成平台”。上面提到的CNAPP和XDR都是集成多个解决方案的平台概念，零信任也旨在实现这一目标。此外，为响应安全的高度复杂性，人工智能和自动化的应用范围的扩大也可以说是主要趋势。

预计从今年起暂停的线下活动将重新恢复生机。让我们拭目以待现有趋势将如何发展，明年又会出现哪些新趋势。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com
© 2022 AhnLab, Inc. All rights reserved.