奇安信

https://www.qianxin.com

2023年网络安全十大趋势预警

THE REPORT

发布机构：

奇安信集团

研究背景

过去的 2022 年，网络安全继续成为全社会的关注焦点。网络战在俄乌冲突中风头尽出；勒索攻击给企业造成的损失触目惊心；数据泄露事件愈发频繁、甚至威胁社会安全；供应链攻击无处不在……网络安全已经成为发展的先决条件。

2023 年是贯彻党的二十大精神的开局之年,也是“十四五”规划承上启下之年。1 月 13 日，工信部、国家发改委等十六部门出台《关于促进数据安全产业发展的指导意见》，提出到 2025 年数据安全产业规模超过 1500 亿元。可以预见，2023 年随着国际环境愈加复杂，数字化转型不断深入，网络安全面临的形势将更加严峻，新场景、新威胁势必将驱动网络安全新技术、新产品和新模式的复合创新，进而推动整个行业迈上新的台阶。

作为网络安全的领军企业，奇安信对 2023 年网络安全行业进行了十大趋势预测，一起洞察行业未来的发展脉搏。

目　　录

趋势一：数据安全成焦点需求 特权账号管理、分级分类紧迫性提升

近年来，数据安全已上升到国家战略高度，《中华人民共和国数据安全法》、《个人信息保护法》颁布实施，配套的《数据出境安全评估办法》、《网络数据安全管理条例（征求意见稿）》接连发布；国家网信办连续发布了对多家互联网公司实施的数据安全相关审查公告；基础电信、政务、金融、工业等行业陆续制定数据安全管理办法和考核评估规范。

随着数字化转型加速，数据的流存节点和区域变得繁杂、流动量呈现指数级增长、使用方式也不断多样化，政企机构的数据安全防护面临应用场景变化、保护对象变化、管理体系变化的挑战，新环境下滞后的安全建设将造成巨大风险敞口。大量的数据资产攻击、泄漏等事件为政企机构敲醒警钟，波耐蒙研究所和 IBM Security 联合发布的《2022 年数据泄露成本报告》显示，2022 年全球数据泄露规模和平均成本均创下历史新高，数据泄露事件的平均成本高达 435 万美元。

在被动满足合规和自主安全防护双向驱动下，预计未来数据安全建设将持续作为政企机构安全方向的焦点需求。为将数据安全与大数据基础设施和业务应用深度融合，更多政企机构将按“先理后治、补短固底”-“系统治理、体系规划”-“有序建设、持续运营”分阶段开展体系化的数据安全建设，并在每一个阶段应用相应的产品技术为支撑。其中，特权账号管理技术方案将成为高紧迫、高收益性建设项目。而数据分类分级技术应用也将加速落地，为健全以“数据”为中心的安全保护体系打通“第一道关卡”。

趋势二：寻找中国云原生安全出路刻不容缓

云原生安全是近年来全球网安市场热点，随着我国东数西算战略的部署，国家与地方政务云和企业云建设加快，数字化业务往云上迁移的步伐也在加快，云原生安全需求正在快速增长。

中国信通院在其《云计算白皮书（2022 年）》提出，云原生正通过改进企业的 IT 技术和基础设施，持续加速企业 IT 要素的变革，成为企业用云的新范式。对云原生安全的担忧，正成为企业应用云原生技术的“拦路虎”。中国信通院《2022 中国云原生安全用户调查报告》显示，安全已连续三年成为企业对应用云原生技术的最大担忧。针对微服务、容器和镜像的攻击屡见不鲜。究其原因，近 6 成企业认为技术门槛过高、人才储备不足，仅不到 1 成企业有独立安全部门应对云原生安全事件。

云原生安全应用防护体系建设，需充分考虑制衡和内生。云原生安全是保护云原生应用的安全，涉及企业开发、运维、安全等多个部门。“责任共担”与“能力内生”是云原生安全的两大关键。责任共担不仅是企业内部，还有云服务商和安全厂商之间，这已成为正式行标和关键共识。能力内生则是数字化时代做到统筹发展与安全，做到安全与新技术应用实现“三同步”的基本保障。

预计 2022 年，包括**容器安全、云工作负载保护、云安全态势管理、API 安全等安全能力及云原生应用保护平台产品**，将为国内所有主流云服务商的云原生环境，提供稳定可靠的支持。

趋势三：零信任的全面落地将是2023年重点

无论是技术、产品实现，还是用户、资本市场表现，2022年都可以被看作是零信任高速发展的一年。

从国际视野来看，零信任架构演进已然进入全面落地推广阶段。美国国防、国土安全、情报机构、联邦政府等层面仅在2022年就先后出台十余项政策、规范、标准、参考指南等，全面拥抱零信任架构作为其网络安全战略。在商业层面，无论是全球知名科技公司如微软、谷歌、思科、IBM，还是国际第三方市场机构如Gartner、Forrester、CSA、Deloitte（德勤），也都在积极推出结合自身优势的零信任咨询、产品、解决方案、培训等相关服务。数据上也同样证明了这一点。根据IBM《2022年数据泄漏成本》报告显示，没有部署零信任的企业其数据泄漏的平均成本为510万美元，而部署了零信任的企业此项成本为415万美元。部署了零信任的企业数据泄漏成本平均降低近百万美元。

反观国内市场，零信任也持续热度高涨。一方面，以远程办公接入为主流场景的ZTNA（零信任网络访问）已然成为2022年国内最热的一个零信任细分赛道，技术、产品、市场、资本均快速入局；另一方面，还是可以看到一些大型政企组织不再满足于单点安全产品的采购，更倾向于选择一家能够真正了解其业务需求、安全痛点、方案适配性强的安全厂商作为其零信任落地合作伙伴，一同构建其自适用其自身的零信任。

2023年，零信任及其在多业务场景的全面落地仍将是每个组织企业的重点工作。零信任的价值毋庸置疑，但如何选择正确的工具、产品和供应商作为零信任战略合作伙伴，以实现预期的业务成果，成功打破安全与业务团队之间的孤岛，将显得愈发重要。仅能解决单点的远程办公安全问题从来不是零信任的初衷；

经历过大浪淘沙后，零信任也将逐渐回归其本源，即通过以数据资源保护为核心，遵循最小权限原则，基于身份进行细粒度的权限设置与判定，构建端到端的网络安全体系，旨在移除隐式信任，实现主体身份可信、行为操作合规、计算环境与数据实体有效防护。

趋势四：软件供应链安全的关注度依然炽热

数字化时代，软件无处不在。软件已经成为支撑社会正常运转的最基本元素之一，随着软件产业的快速发展，软件的供应关系也越发复杂多元，近年来，针对软件供应链的安全攻击事件一直呈快速增长态势，造成的危害也越来越严重，特别是由开源软件引发的安全问题更加突出。

奇安信代码安全实验室发布的《2022 中国软件供应链安全分析报告》显示，开源软件漏洞的增长速度、安全缺陷和高危安全缺陷的密度，以及典型缺陷的检出率均呈现出增长的趋势；国内企业开发的软件项目 100%使用了开源软件，存在已知开源软件漏洞的项目占比 86.4%，平均每个项目存在 69 个已知开源软件漏洞，十几年前的古老开源软件漏洞依然存在于多个项目中，并且也通过实例分析证实了“老漏洞”攻破最新主流产品的软件供应链攻击场景的存在；此外，报告还指出在开源生态系统中，Log4j2 之类的关键基础开源软件大量存在，它们一旦爆发漏洞，影响范围和危害可能会非常巨大。

因企业对第三方来源软件，特别是开源软件的检测、管控、治理的不足，可能会会带来多种多样的潜在威胁，包括漏洞、后门、恶意代码植入和欺骗、恶意依赖项、编译器破坏、依赖混淆、包完整性篡改、上游源代码删除、开源软件组件停止修复、未按时修复漏洞、包管理器恶意代码上传等，从造成的结果来看，包括数据泄露、勒索病毒、隐私泄露、恶意攻击、恶意挖矿等。

随着 2023 年我国《软件供应链安全要求(送审稿)》、《关键信息基础设施信息技术产品供应链安全要求(报批稿)》、《软件产品开源代码安全评价方法》等国家标准的编制或发布，国内企业对软件供应链安全的关注度将进一步提升，在这一方面的工作也

会有更多的依据，特别是**第三方软件的安全分析和开源软件治理将成为企业保障软件供应链安全的重要任务**。

趋势五：合规之后，多云安全防护与托管运营是云安全建设重点

云安全资源池是中国云安全发展当前阶段，符合国情及市场需求的必然产物。这一产品形态的价值也开始被全球咨询机构重视。Gartner 在其首个《中国云安全资源池创新洞察》报告中提出，随着数字化和上云用云进程的不断深入，政企寻求以更灵活、敏捷的方式在云上部署安全能力。无论是私有云还是公有云，云服务商往往不会提供企业所需的全部安全能力。云安全资源池支持多云的统一管理、监测和自动化编排，可较好满足“等保”等合规性要求。这一集成型产品可较好的帮助政企，缓解其责任之内的云上安全风险。

这点在中国政务云云安全市场，表现尤为明显。IDC 在《中国政务云云安全市场分析》报告中提出，政务云作为关键信息基础设施，当前云安全建设仍以合规驱动为主；基于云安全资源池构建服务化安全能力，是租户安全建设的重要方面。多云安全的统一管理和托管安全运营服务，特别是对信创云的支持，是未来政务云云安全建设要考虑的重点。

云安全管理平台（CSMP）、云安全运营中心（CSC）和云安全托管运营服务（CMSS）的组合方案，将是契合这一发展方向的最佳选择之一。此外，Gartner 融合网络和安全即服务能力的 **SASE（安全访问服务边缘）架构**，是从访问场景切入，云安全的另一种发展思路。Gartner 在《2022 中国 ICT 技术成熟度曲线》报告中提出，SASE 是数字化转型的关键赋能者，能够有效提升整体的敏捷性、可见性、韧性和安全性。

趋势六：工业关基保护成为工业安全防护重点

工业领域的关键信息基础设施主要包括能源、交通、水利、石油石化和国防科技工业等重要行业，据统计，在关基领域占比超 70%。近年来，对工业领域的关键信息基础设施的网络攻击在全球各地不断出现。仅 2022 年就有欧洲近 6000 台风力发电机组遭网络攻击失去远程控制服务、伊朗国有钢铁公司遭受网络攻击后被迫停止生产、意大利铁路系统遭黑客攻击致多地车站受影响，越来越多的网络安全事件突显了工业关基网络威胁的严重性。

随着技术的进步，5G、云计算、大数据和人工智能的赋能，使得工业关基的数字化转型提速，其工业控制网络也向着分布式、智能化的方向迅速发展，在提升生产效率的同时，也打破了原本相对封闭可信的环境，网络攻击面随之扩大，网络安全面临严峻挑战。

尤其是《关键信息基础设施安全保护条例》、《关键信息基础设施安全保护要求》实施力度和工业关基的内控与合规要求的不断增强，在做好分析识别、安全防护、检测评估、监测预警、主动防御和事件处置 6 个方面的安全建设的同时，也对工业关基安全衍生了更多需求，如**工业资产分级分类管理需求、风险可视化需求、能力聚合需求、运营能力提升和攻防实战演习**的需求，这些都成为了工业关基安全建设接下来的重点。基于此，工业关基保护将成为 2023 年工业安全防护重点。

趋势七：攻击检测类产品走向服务化

近年来，中国作为世界第二大经济体稳步崛起，随之而来的境外势力针对我国大型企业、政府等所属相关系统发动愈演愈烈的网络攻击。这其中工具化、有组织的 APT 攻击更有抬头的趋势，为应对新形势下攻击手段更加隐蔽的特点，弥补传统的基于特征检测的安全设备检测能力的不足，基于威胁情报且可精准实时发现隐藏行为的攻击检测类设备应运而生。

攻击检测类设备通常需收集流量、主机、终端、系统日志数据进行分析，并提供可供分析的告警数据和攻击源，大部分客户在面对这些价值极高但技术门槛也较高的数据时会有无能为力的感觉，为将检测数据的效用最大化，基于攻击检测产品开发（NDR、EDR、CWPP）的服务产品应运而生，并被证明在实战攻防类场景中可发挥巨大的作用，绝大部分企事业单位对这种服务模式普遍认可并在安全建设中持续投入资源。

业界基于攻击检测产品的服务化能力均在普遍提升，在达成业界共识的基础上，预估 2023 年**融合产品检测能力和服务人员专业能力的产品会更多的以服务运营模式推向市场**。在此基础上也会进一步推进攻击检测类产品的精耕细作，检测平台之间逐步实现技术融合，从单一检测产品的威胁分析服务升级至多产品跨平台的综合性威胁检测服务。

趋势八：云上实战化安全运营迎来持续关注

新的行业生态不断涌现，企业 IT 系统已经变得愈发复杂。应用和数据已经从核心 IT 环境延伸到了云（包括公有云、行业云、边缘云、私有云），并正在加速延伸到包括物联网、移动设备在内的边缘环境。在边缘创造和处理的数据量正在呈指数级增长。当下及未来的 IT 环境中，办公网、数据中心、多云环境、远程办公等场景将交织在一起。面对愈发复杂的 IT 系统，企业应对数据安全问题需要有体系化的建设思路，不能头痛医头脚痛医脚，必须要依据企业业务发展状况，统筹规划、分布实施。

然而，多数用户在后期运维过程中，还是难以有效应对安全产品的策略调优、网络攻击等工作。在数字经济的今天及未来，安全托管服务（MSS）是弥补客户安全人才短缺无法高效应对网络安全相关问题的首要选择。正如再高档的汽车都离不开 4S 店的维修保养服务一样，网络安全建设后的运维工作同样离不开托管安全服务。在中国，网络安全市场有着自身的特殊性，相当一部分企业的复杂的 IT 系统仍采用本地化或混合 IT 架构方式部署，缺少基础的安全能力，与公有云架构相比，安全建设需要从头做起。因此，很多企业还是希望能够进一步获得技术层面耦合度更高的安全服务，高效地获得更新的安全能力，及专业安全人才及时的支持。

随着国际形势的恶化与护网的发展，客户对安全的要求不止合规，逐渐向攻防实战化演进。基于云上的实战化会迎来企业的持续关注。

趋势九：安全运行受到更多重视

长期的网络安全建设投入了大量的设备和人力，各类网络安全产品自身能力发挥不足，安全策略有效性不够。网络安全运行管理和 IT 运行、业务运行管理不融合，各类安全产品产生大量的日志无法及时有效分析，快速准确发现网络攻击事件，事件处置不及时，事件处理效率低下，同时新业务、新技术不断发展，网络攻击隐蔽、多变且持续不断，整体来看网络安全建设投资难以发挥真正的效能。

随着网络安全的发展，安全运营中心已逐渐成为网络安全建设的标配，但运营中心成熟度普遍不高，报告显示，88.6%的受访企业已经建立了专门的安全运营中心，但总体来看，处于一、二较低成熟度级别的受访单位占比仍然高达 65.5%，大多数单位的安全运营中心的成熟度还比较低。网络安全建设投资是否发挥能效，安全运行是否能切实保障业务，是否具备“能对抗”的实战化安全能力，逐渐成为客户关心的重点。而**实战化、常态化、体系化的网络安全运行，将成为安全运行未来的发展趋势**。

趋势十：XDR 渐入主流，ASM、BAS 初露锋芒

随着网络攻击日益隐蔽和复杂，攻防对抗从原来的技术之争逐步演变为速度之争。传统的单点安全防护设备无法有效应对安全运营的问题。而 XDR(拓展检测&响应)通过集成威胁检测、分析，响应中不同的产品&工具,通过关联分析、事件聚合、威胁情报、自动响应等技术手段形成整体检测和响应策略，从而看见威胁,消除孤岛，提升效率。**XDR 的落地价值也正在被主流所客户认可。Gartner 预测到 2027 年 XDR 的渗透率将会达到 40%。**

由于数字化转型的深入，疫情催生下的远程办公，复杂的数字供应链等导致企业的数字资产暴露面隐患日益增长。而 ASM(攻击面管理) 通过客户的资漏配补数据的融合分析，从攻击者视角帮助安全团队掌握资产安全姿态、收敛资产暴露面、防护网络攻击路径。全面资产可视提升客户安全运营以及 IT 运维能力，也是多数客户评估攻击面管理的起始点。

安全防护系统、安全设备的有效性评估一直是困扰着安全主管和安全团队的问题。而 BAS 也是试图解决这个问题。BAS（入侵和攻击模拟）通过非侵入性的模拟攻击，评估安全设备的检测有效性，验证安全产品的配置，从而进一步评估安全体系和架构。**近两年 BAS 的能力边界也在拓展，覆盖渗透、暴露面验证、红蓝对抗等攻防场景。成为安全团队喜爱的“瑞士军刀”。**

安全产品的平台化、集约化是大势所趋，即不同的安全能力组件在统一的平台架构下彼此协同和打通。我们也看到越来越多的 XDR、 ASM、BAS 彼此集成整合的应用场景。而这些最终给平台最终使用者——安全分析团队带来收益。