# 2022 年网络安全预测

简译版

**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** | Supply chains, ransomware, zero trust and other security predictions for 2022 | | |
| **原文作者** | 托马斯·塞古拉（Thomas Segura） | **原文发布日期** | 2021 年 12 月 31 日 |
| **作者简介** | 托马斯·塞古拉是 GitGuardian 技术内容作家。 | | |
| **原文发布单位** | Help Net Security | | |
| **原文出处** | https://www.helpnetsecurity.com/2021/12/31/security-predictions-2022/ | | |
| **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 | | |
| **摘要** | 网络犯罪正变得更加专业化、组织化、系统化和多样化。因此，更好的网络安全对国家和企业都至关重要。本文对 2022 年的网络安全情况进行了预测。 | | |
| **免责声明** | 本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。 | | |

# 2022 年网络安全预测

托马斯·塞古拉

2021 年 12 月 31 日

网络犯罪正变得更加专业化、组织化、系统化和多样化。因此，更好的网络安全对国家和企业都至关重要。

接下来，我将对 2022 年的网络安全情况进行预测。

## 1. 供应链问题继续让人夜不能寐

2021 年，IT 服务提供商 SolarWinds 遭到了供应链攻击，这是近年来最大的网络安全事件之一。该公司承认，攻击者将恶意代码被注入了一种产品中，该产品有数万用户，其中包括军事和公共政府部门等用户。供应链攻击者可以通过各种途径，将恶意代码或组件注入受信任的软件或硬件中。

在另一起攻击事件中，开源社区中非常流行的代码覆盖工具 Codecov 遭到感染。近年来，开源组件越来越多地用于企业环境中，但它们在安全标准方面仍然存在不足。因此，开源组件受到攻击者的青睐，被用作攻击向量。

一旦感染了诸如 Codecov 这样的工具，攻击者就可以从成百上千的下游用户那里获取敏感数据。代码库通常包含机密信息，攻击者可以利用这些信息来访问有价值的系统，因此这些代码库成为攻击者的高价值目标。

2021 年，供应链攻击不断发生，这种趋势还将继续下去。我们甚至会看到规模较小的供应链攻击针对开发者环境，尤其是在开发者环境变得越来越复杂和相互依赖的情况下。

## 2. 中小企业将成为勒索软件的目标

2021 年的勒索软件攻击主要涉及政府、制造业和银行业等大型企业。攻击者正在寻找高价值的攻击目标，而这一策略已被证明是有利可图的：美国财政部表示，52 亿美元的比特币交易与勒索软件攻击相关。

然而，随着小型企业迁移到网上，勒索软件逐渐成为一种网络犯罪商品，经济格局正在发生变化。中小型企业将成为勒索软件攻击的目标。

### 3. 勒索软件培训将成为主流

为了与这种新常态作斗争，许多关于勒索软件培训的公共和私人计划横空出世。当发生攻击时，危机管理的准备水平会影响结果，因此培训员工的应急响应很有意义。

### 4. 应用程序安全（AppSec）将成为企业的首要任务

2022 年，企业将 AppSec 问题。原因有三个：（1）随着供应链变得越来越复杂，DevOps 管道攻击面也在扩大，风险管理本质上是确保这些管道的安全。（2）开发人员及其特权访问仍然是黑客青睐的目标，黑客总是试图利用人为错误。（3）虽然安全肯定是重中之重，但没有人愿意因此而减慢开发周期。安全工具需要关注开发人员的生产力，因此在这两个目标之间找到完美的平衡将成为 AppSec 策略的核心。

### 5. 零信任架构将更加成熟

零信任已成为主流。高级攻击、云采用和远程办公的增加使企业意识到，他们迫切需要从“实施零信任策略”开始改进其数字安全态势。2022 年，企业会在这个方向上取得持续进展，尤其是在人和机器的身份验证方面。

### 6. “安全即服务”将使最佳工具民主化

从云安全态势管理到事件管理，通过软件组合分析或秘密检测……最近出现了许多专门的工具，即使对于大公司来说，安装和维护这么多不同的工具和产品也很快变得非常困难。幸运的是，通过友好的仪表板、基于角色的访问控制和 API 来提供灵活性，将这些工具集成到现有工作流中变得越来越容易。

### 7. 实时数据可观察性将成为网络安全的重点

2022 年，网络安全战略将侧重于实时数据的可见性和可观察性。获取公司正在使用的所有硬件和软件的完整 IT 资产清单或所有第三方供应商清单已经是一个巨大的挑战，更不用说与它们相关的网络威胁的完整概述。但是，随着企业朝着更好的检测和修复能力迈进，他们需要更好地监控威胁。

## 结论

未来几年，网络犯罪（尤其是国家支持的威胁）越来越多地针对公共和私营部门中最脆

弱的部分，因此，网络安全部门面临巨大的挑战。不幸的是，即使是一些防御最好的基础设施也遭受了破坏，这清楚地表明网络防御还有很长的路要走。

2022 年，网络威胁不会缓和；相反，它们的复杂性和广度都会扩大。

好消息是，利害关系无疑将公众舆论和政府推向了正确的方向，大多数实体将受益于明年实施、执行或审查安全最佳实践的加速计划。企业也渴望采用量身定制的网络安全解决方案，更好地管理未来网络供应链的复杂性。

# 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，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、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的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

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企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

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（如 APT 组织）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，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

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