

GoPlus研报：打造模块化安全新生态

ZeY SevenUp DAO 2024年05月30日 16:01 广东



作者 | ZeY

TL;DR

1. 用户安全问题已经成为Web3 mass adoption的一个巨大障碍。零时科技的数据显示，2023年共发生安全事件506起，累计损失达110亿美元。对于个人用户来说，频繁的钓鱼和诈骗活动是最常见的威胁。
2. GoPlus 每日API调用量高达2100万次，并已经与超20个一二层区块链以及多个RPCs，RaaS(Rollup-as-a-Service)项目达成合作伙伴关系，获得如Binance Labs和7UPDAO等众多知名投资机构的青睐。旗下安全产品SecWareX自2024年3月份上线以来总链接地址数突破 1000 万，付费订阅高级安全服务地址数超过 5.7 万。
3. GoPlus是模块化的用户安全层。模块化主要体现在两点：一是GoPlus网络架构中的分层设计，二是用户安全模块USM的能够很容易集成到各类Web3基础设施上，为用户提供全方位的保护。
4. GoPlus 网络自底向上可以划分为基础层（Fundamental Layer）、安全软件生态系统层（SecWare Ecosystem）以及网络服务入口/用户安全模块层（User Security Module, USM）。
5. GoPlus创始人Mike曾是360安全浏览器的主要产品负责人，GoPlus模块化的特点也契合他打造SecWare生态，打通2B2C双向商业逻辑闭环的战略意图，GoPlus有望成为引领“Web3综合安防体系”的先锋力量。

一、前情提要

用户安全问题已经成为Web3 mass adoption的一个巨大障碍。根据零时科技发布的《2023年全球Web3行业安全研究报告》，2023年共发生安全事件506起，累计损失达110亿美元。相比2022年，今年Web3安全事件新增110起，同比增长65.3%。2023年，全球Web3安全事件攻击类型多样，从安全事件数量看，典型攻击类型Top5为：黑客攻击、安全漏洞、资产被盗、钓鱼、错误权限。从损失金额看，典型攻击类型Top5为：黑客攻击、安全漏洞、资产被盗、闪电贷攻击、诈骗。

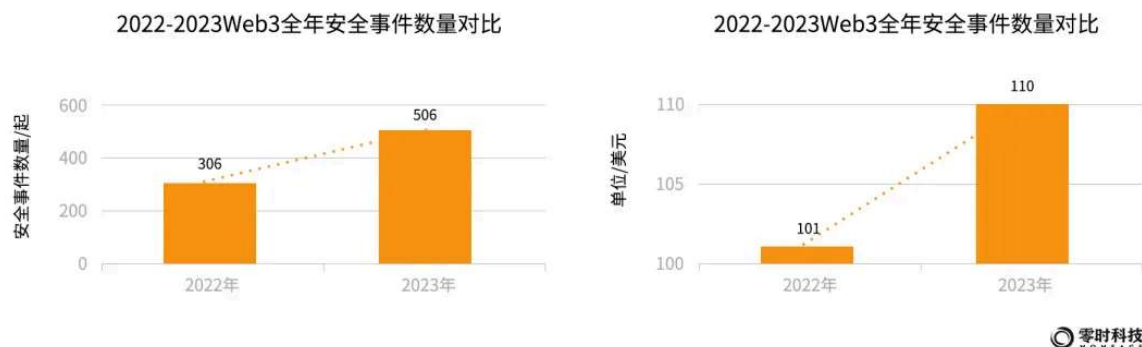


图 1 2022-2023Web3全年安全事件数量对比 来源: <https://mp.weixin.qq.com/s/G09px9q6yKiaqJV9p224LQ>

对于个人用户来说，频繁的钓鱼和诈骗活动是最常见的威胁。与针对协议的攻击不同，针对用户的攻击影响范围更广，显著降低了Web3的用户体验，特别是对于缺乏基本Web3安全知识的新手，使他们在复杂的链上操作环境中容易受到诈骗。

此外，自2022年以来，越来越多的组织开始设法“榨干用户的钱包”（Wallet Drainer），他们发布的恶意软件，诱骗用户签署有害交易，从而窃取用户钱包中的资产。这些钓鱼活动以各种形式持续侵害Web3用户，导致许多不知情的用户签署了恶意交易，造成重大财产损失。

以Arbitrum为例，Dune的数据显示，Arbitrum上曾参与安全性堪忧的合约代币交易的用户数量自2023年八月份以来就保持波动上升，而2024年5月这一数字更是达到了近4百万。

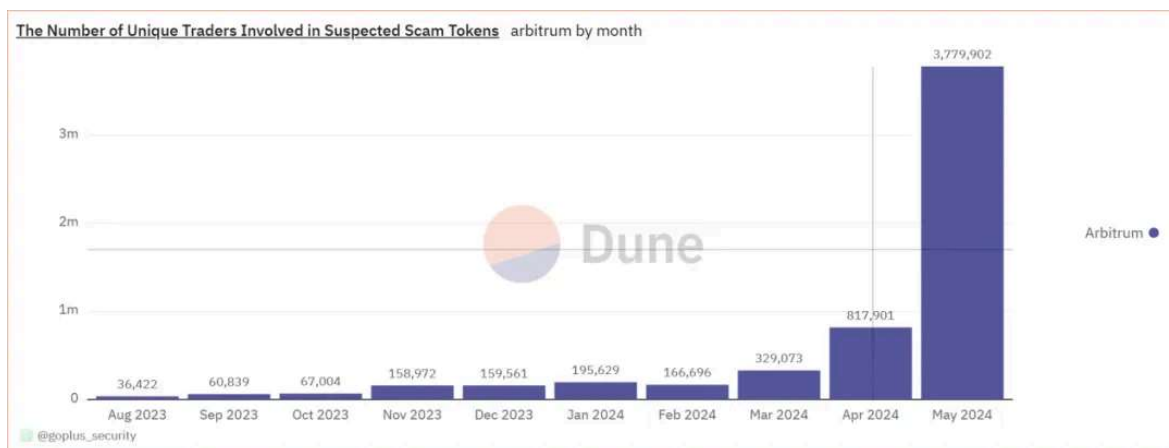


图 2 The Number of Unique Traders Involved in Suspected Scam Tokens 来源: https://dune.com/goplus_security/totaladdressbymonth

从2023年八月份开始，Arbitrum上涌现的新合约代币数量中，绝大部分都是此类疑似涉及诈骗用户的合约代币。

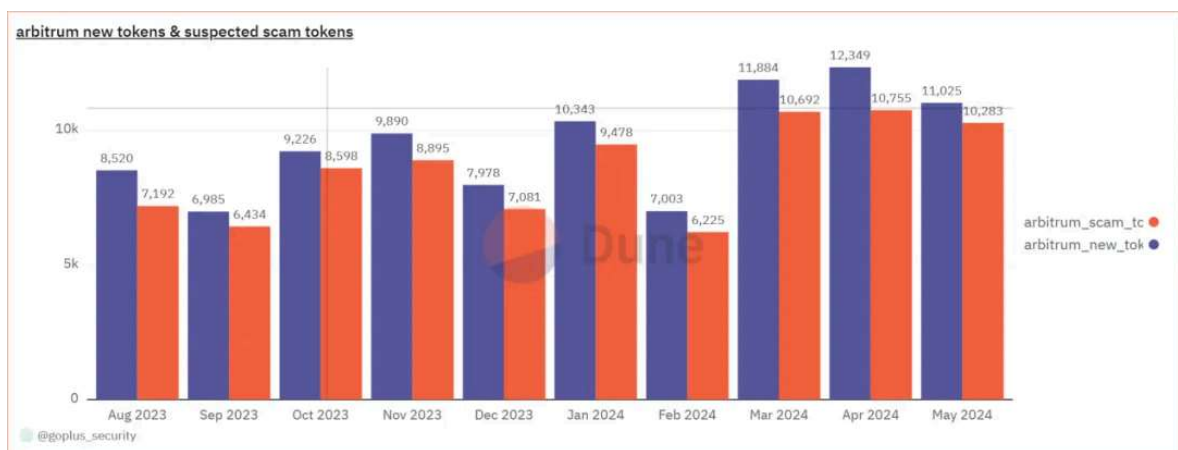


图 3 Arbitrum New Tokens & Suspected Scam Tokens 来源: https://dune.com/goplus_security/totaladdressbymonth

可以看出，随着大规模诈骗和钓鱼操作的出现，Web3用户的个人安全问题变得更加严峻，这表明Web3领域迫切需要全面而强大的安全解决方案。

二、GoPlus成立背景

GoPlus的创始人Mike曾于2010年加盟奇虎360，或许是因为Mike这段工作经历，GoPlus被冠以“Web3中的360安全卫士”之称。

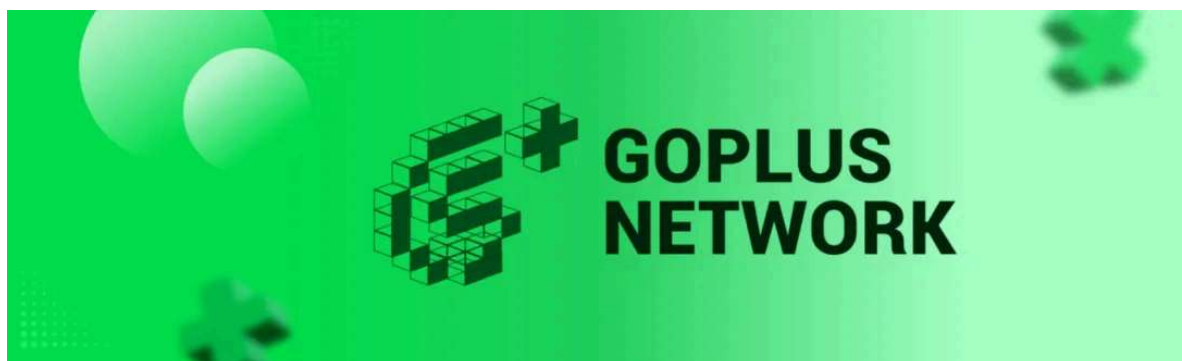


图 4 GoPlus网络 来源: <https://whitepaper.gopluslabs.io/goplus-network>

GoPlus的愿景是Navigating billions of users to Web3 with safety，即引领亿万用户安全地探索Web3世界。正是基于Mike的深厚Web2安全工作经验和GoPlus团队的共同努力，GoPlus网络得以成为一个创新的、用户驱动的Web3模块化安全层。其开放性和无权限特性使得用户能够拥有极高的自主权，而GoPlus的适应性也让它能够无缝集成至任何区块链系统，轻松增强用户安全性，为用户提供全方位的保护。

在整个用户交易的生命周期中，GoPlus始终扮演着守护者的角色，持续提供全面的保护机制。通过构建一个分散的用户安全网络，并结合尖端的人工智能安全解决方案，GoPlus能够深入执行风险分析，为用户提供智能且高效的安全服务。

GoPlus的目标不仅仅是提供安全，更是致力于填补当前区块链架构在用户安全层方面的不足，为用户带来更为有效、更具吸引力的链上安全体验，从而打造一个更为安全、人性化的Web3链上交互环境。

在过去的几年里，GoPlus经历了飞速的发展，用户安全数据的使用量较2022年增长了超过5000倍，每日API调用量更是高达2100万次。2024年3月，SecWareX的发布标志着GoPlus取得了显著成就，彰显了用户对其的高度信任和积极参与。



图 5 Grok认为GoPlus提供了最佳的区块链安全API 来源： <https://x.com/GoPlusSecurity/status/17910856681871773>

GoPlus已支持包括Optimism, Base, Avalanche, Solana等超过20个区块链一二层网络，并与RPCs、Rollups和RaaS(Roll-up-as-a-service)项目建立了合作伙伴关系。

GoPlus的产品逻辑和市场前景从一开始就赢得了众多投资机构的青睐。自2021年8月获得SevenX Ventures领投的2000万美元估值天使轮融资以来，GoPlus的发展势头更是势不可挡。到了2022年8月，更是成功获得了Binance Labs领投的1.5亿美元估值的战略融资。

Fundraising

InvestorsRounds

Round	Amount	Valuation	Date	Investors
--	\$ 4 M	--	Mar 08	Redpoint China Ventures*, Klaytn, Skyland Ventures, Gate.io Labs, KudasaiJP, Emirates Consulting, Crypto Times
Strategic	--	\$ 150 M	Dec 08, 2022	Binance Labs*
Private	\$ Millions	\$ 60 M	Apr, 2022	Arweave, SevenX Ventures, GSR, Crypto.com Capital, Kucoin Ventures, Harmony, Neo, CatcherVC, GeekCartel, Huobi Incubator, Avatar Ventures
Angel	--	\$ 20 M	Aug, 2021	SevenX Ventures*, Mask Network, Youbi Capital, Incuba Alpha, Puzzle Ventures, LucidBlue Ventures, InsurAce, Richard Ma, DeltaBC

图 6 GoPlus融资情况 来源： <https://www.rootdata.com/Projects/detail/GoPlus%20Security?k=MzgxNw%3D%3D>

三、模块化的用户安全层

Goplus的模块化设计理念在其网络架构中可以窥见一斑：从底至上分别是基础层(Fundamental Layers)、安全软件生态系统层(SecWare Ecosystem，这里的SecWare是指Security Software)、网络服务入口(Network Service Entrance)/用户安全模块层(User Security Module, USM)。

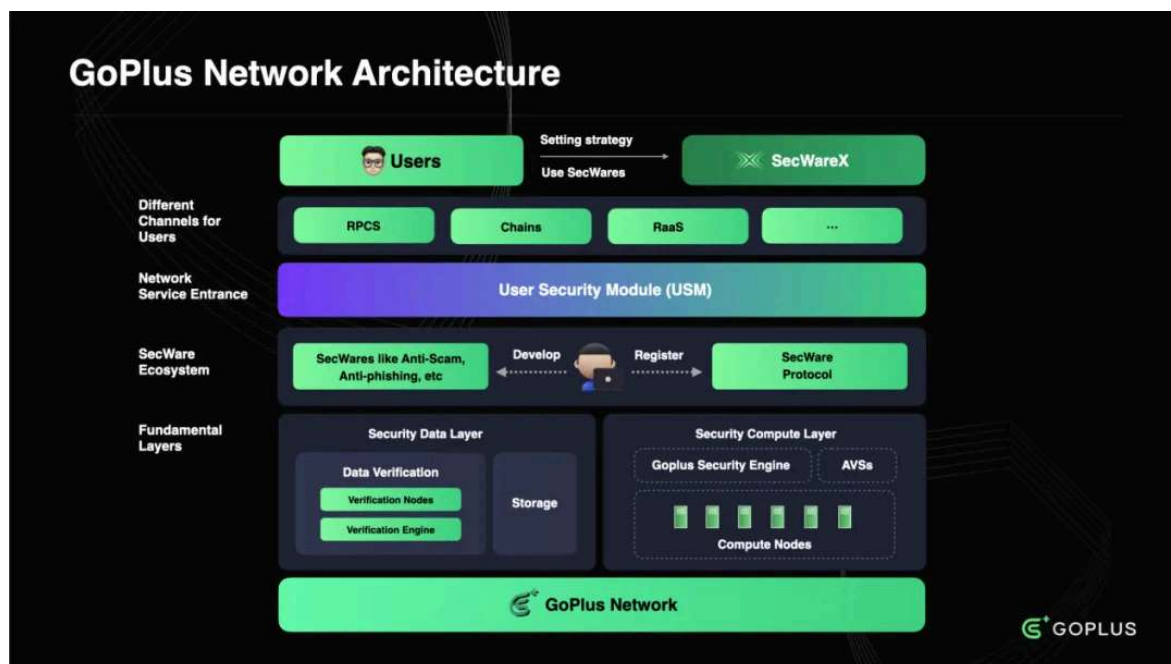


图 7 Goplus的网络架构 来源: <https://whitepaper.gopluslabs.io/goplus-network/goplus-network/architecture-overview>

每个层负责不同的任务，相互协调，提升了整个GoPlus网络的效率与灵活性。用户则可以在各种RPC、L1链以及RaaS等项目中使⤵GoPlus提供的安全服务。

1、基础层

基础层(Fundamental Layer)主要由安全数据层(Security Data Layer)和安全计算层(Security Compute Layer)组成。

安全数据层

安全数据层通过采用去中心化的方式收集、处理和存储与安全相关的数据，同时确保数据的完整性、真实性和可靠性。



图 8 安全数据层(Security Data Layer) 来源: <https://whitepaper.gopluslabs.io/goplus-network/goplus-network/security-data-layer>

GoPlus将安全数据分为7类，分别是代币安全数据、恶意地址数据、 NFT安全数据、授权风险数据、dApp安全数据、钓鱼网址数据等。

安全数据的提供者可以是任何人。例如，Web3应用程序的普通用户可以报告他们遇到的安全问题，例如可疑的诈骗活动、网络钓鱼或撤池跑路行为(Rug Pull)。专业的安全研究人员可以贡献他们在风险、安全分析和其他深入的用户安全见解方面的发现。

在收集到上述安全数据后，GoPlus网络会对其可信度以一种去中心化的方式进行两次验证。如果第一次验证出现争议，就会触发二次核查，由更加专业化的团队对此进行彻底彻查和裁决。

安全计算层

安全计算层允许任何开发人员根据用户在交易生命周期的不同阶段的安全需求加入并提供相应的安全解决方案。目前，GoPlus内置了SecScan自动安全检测、反诈骗、反钓鱼等多项安全检测引擎。



图 9 安全计算层 (Security Compute Layer) 来源: <https://whitepaper.gopluslabs.io/goplus-network/goplus-network/architecture-overview>

安全计算层由多个安全计算节点 (Security Compute Nodes, SCNs) 负责执行与安全相关的计算和验证工作, 如验证交易的安全分析结果、检测潜在的安全威胁和模拟交易等。在节点的准入机制方面, 采用了统一的质押机制和最小硬件规格标准, 有意加入网络的节点需要质押指定数量的代币, 并提供满足最低要求的计算资源。

同时, 为了进一步增强安全计算层计算结果的可信性, GoPlus计划在节点计算完成后, 将结果提交到EigenLayer提供的主动验证服务(Actively Validated Services, AVSs)来监督和验证计算过程。

2、安全软件生态系统层

GoPlus 针对用户交易生命周期的不同需求提供了不同的细分服务 (如反欺诈、反钓鱼和反 MEV), 这些细分服务被称作 SecWare (Security Software)。SecWare 生态系统层是基于基础层构建安全服务, 并将服务提供给上层用户的中间层。SecWare Protocol 是 SecWare 生态系统的核心, 该协议定义了用户、开发者和他们提供的安全服务之间的互动和关系。

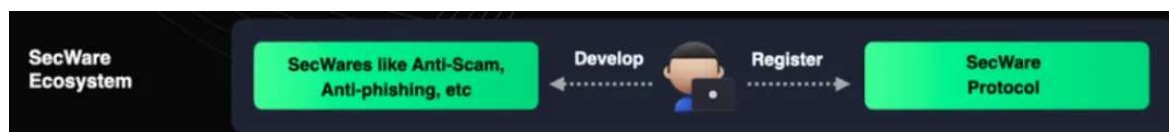


图 10 GoPlus安全软件生态系统SecWare Ecosystem 来源: <https://whitepaper.gopluslabs.io/goplus-network/goplus-network/architecture-overview>

在SecWare 生态系统层, 开发者可以打造独一无二的安全服务软件, 供用户购买与使用, 由此产生的所有利润都被收集在一个收入池中。开发者有权根据他们安全软件的使用和性能提取他们的利润份额。开发者在提供服务之前, 需要质押一定数量的代币。如果一个 SecWare 未能满足特定的服务级别协议 (SLA) 或被发现具有恶意性, 可以削减一部分质押的代币作为惩罚。

截至本文完稿时, SecWare 生态系统层尚未正式启用, 并且GoPlus的代币经济学模型也并未公布, 但SecWare 生态系统层却有望成为GoPlus未来竞争格局中的一大优势, 原因会在下文详细讲解。

3、网络服务入口/用户安全模块层

用户安全模块(User Security Module, USM)是GoPlus网络架构中的一个关键组件。如下图所示, USM定位在网络的核心, 作为链和GoPlus网络之间的桥梁。

USM被设计为一个软件开发工具包(SDK), 可以无缝集成到各种Web3场景, 如钱包、dApps、RPC, 甚至L2 sequencers。这种模块化的方法允许USM轻松适应不同的区块链环境, 提供了跨多个网络的一致和稳健的安全层。

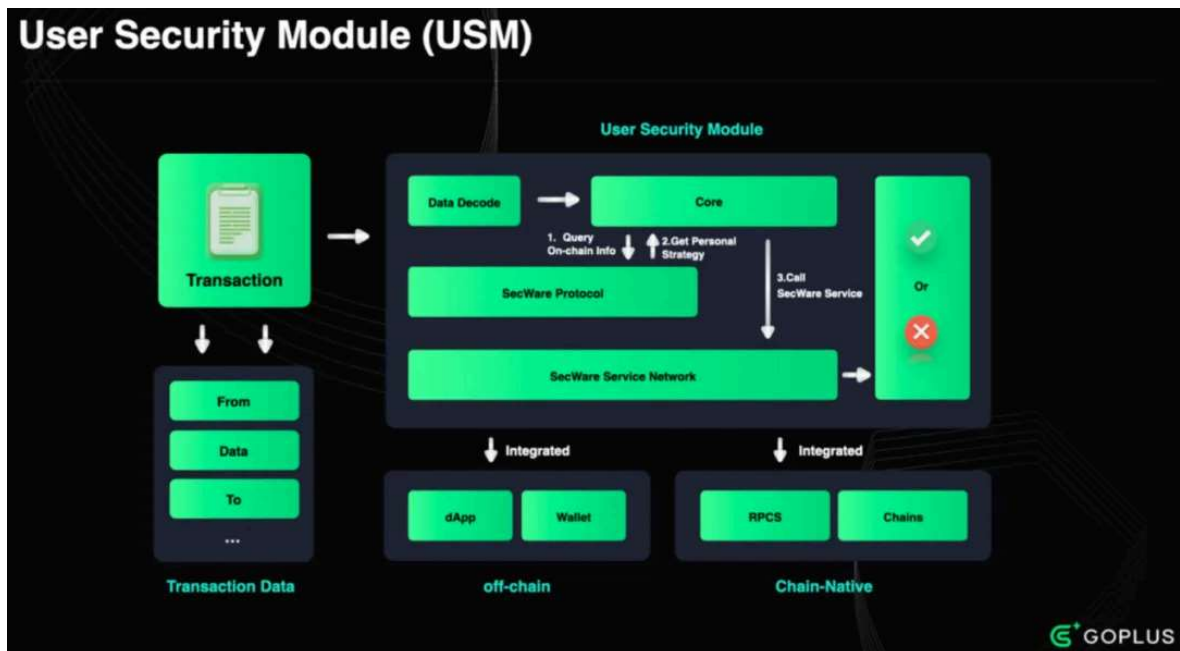


图 11 用户安全模块(USM) 来源: <https://whitepaper.gopluslabs.io/goplus-network/user-security-module/architecture-overview>

USM的主要功能是促进用户发起的事务和GoPlus的安全服务之间的交互。当一个交易被触发时，USM拦截交易数据并将其转发给安全软件SecWare。该软件利用GoPlus的安全数据层和安全计算层，使用先进的人工智能算法对交易进行实时风险评估。

然后，风险分析的结果被转发给USM，USM可以根据安全建议采取适当的行动。这可能包括在交易被认为安全的情况下继续进行交易，或拒绝恶意交易。

USM又被称为GoPlus的“网络服务入口”（Network Service Entrance），因为USM作为用户和区块链之间的接口，能够为Web3用户提供全面的端到端安全解决方案。USM的架构确保了安全层可以很容易地集成和适应不同的区块链，也可以成为模块化区块链和RaaS中的一个重要模块。

4、SecWareX

基于前文所述的SecWare Protocol和USM架构，GoPlus还推出了针对C端Web3用户的安全产品SecWareX。目前，SecWareX中有四个主要的功能：多链钱包扫描器、个人SecHub、安全任务中心、SecWare市场（尚未正式启用）。



图 12 SecWareX主页 来源: <https://secwarex.io/>

基于安全软件系统层SecWare Ecosystem的安全检测引擎，多链钱包扫描器SecScan可以为用户提供全面的钱包安全健康检查服务。通过多链钱包扫描，用户可以随时了解钱包的安全状况，及时发现和应对各种潜在风险。多链登录方式和自动化扫描过程显著降低了用户的操作门槛，增强了安全服务的可访问性和实时性。



图 13 SecScan检测用户钱包安全示例 来源: <https://secwarex.io/>

安全任务中心为用户提供了一个互动学习的平台，使用户能够在此学习、实践和掌握基础的安全技能，并在过程中赚取SecWareX的积分——能量块（Energy Block）奖励。

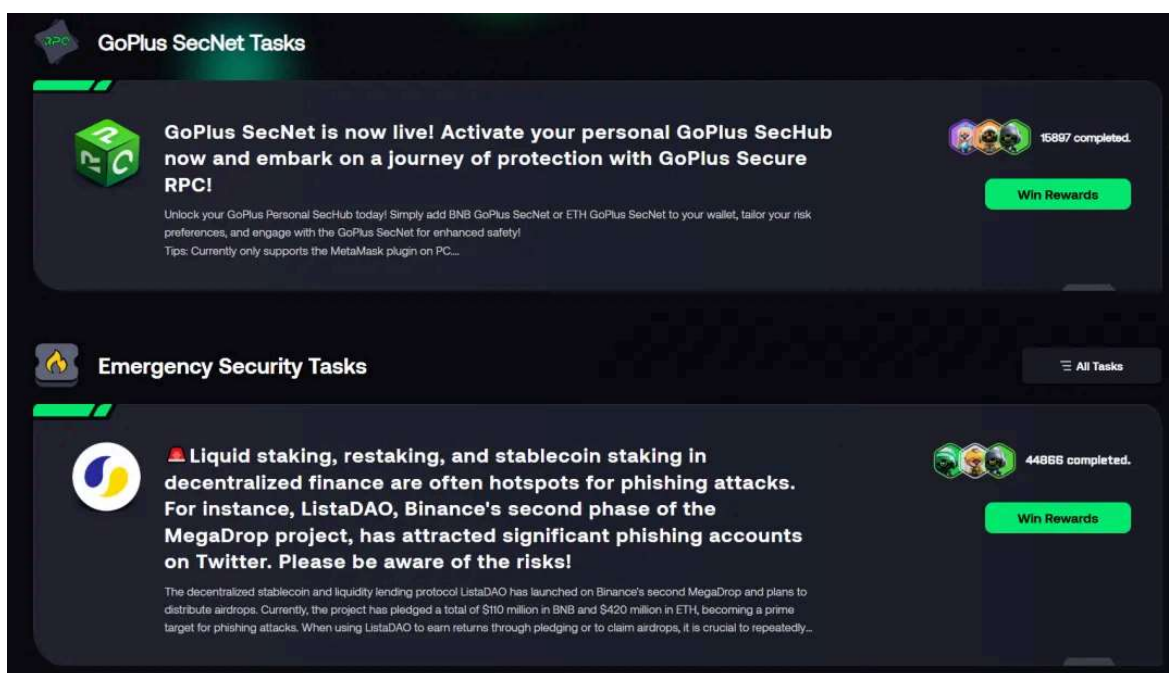


图 14 SecWareX的安全任务中心 来源: <https://secwarex.io/#hot-task>

个人SecHub是一个用户个人安全管理中心。实际上它更像一个游戏的登录界面，用户可以在这里看到安全等级、目前的积分、选择的安全策略以及可以完成的任务等信息。

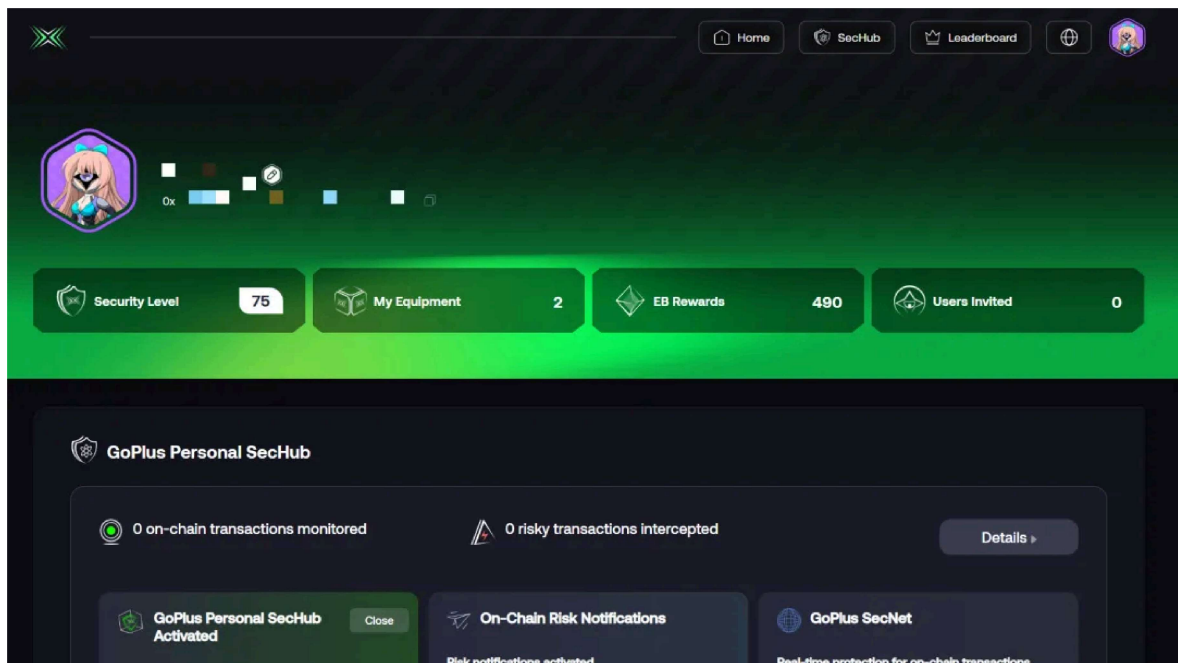


图 15 个人SecHub 来源: <https://secwarex.io/user>

据ChainCatcher消息，全场景安全服务平台SecWareX自3月7日产品上线至5月8日仅2个月便已取得亮眼的成绩：

- 总链接地址数突破 885 万；
- 日活跃有效地址数达到 262 万；
- 月活独立 IP 用户数超过 180 万；
- 付费订阅高级安全服务地址数超过 5万；
- 平台用户完成 4500 万次钱包安全扫描任务和 82 期热点项目的钓鱼网站识别、风险授权检测并撤销、签名和授权的安全识别、钱包的安全使用等任务。

四、构建SecWare生态系统型

打造生态这一想法源自于GoPlus创始人Mike Lee对Web2安全公司商业模式的反思。**2022年，在与7UPDAO的一次对话中，他认为Web 2的安全公司大家都在造轮子，比如各种安全服务的类别里面，每个公司是高度重合的，都在做同一个业务。安全资源的使用效率也是比较低的。**

想在Web3里面做得更好，Mike认为需要在整个市场需求匹配这一层有更好的解决方式，一方面是供需的有效匹配，另一方面是安全服务本身的组织效率问题，也就是供给侧能不能改变。像原来Web2一样，大家就会变得很卷，不停地重复造轮子，然后把一个可以做得很好的市场变成一个市场结构非常差的市场，在这里面可能有人活得还不错，但是大量的人其实活得都不好，导致整个安全市场的供给低效。



图 16 GoPlus宣传图Accelerate Security For Web3 with GoPlus 来源: <https://x.com/GoPlusSecurity/status/1788895612584464439>

他对Web3安全服务的形态的构想集中于两点：一是生态主导，而不是公司垄断；二是建立底层合作框架，每个从业者能找到自己合适的位置，在一个框架里面能够根据他的输入得到有效的激励。

附上对话链接: <https://mp.weixin.qq.com/s/bEnIRxPnjznFBcFkkl1kQ>

GoPlus最重要的产品设计理念可以总结为两点：模块化与生态。这里的模块化前文也有提及，这里稍作总结，主要表现为两点：一是GoPlus网络架构中的分层设计，二是用户安全模块USM的能够很容易集成到各类Web3基础设施上。



图 17 GoPlus宣传图GoPlus The Modular User Security Layer 来源: <https://x.com/GoPlusSecurity/status/1791051077665607905>

上述模块化的特点也契合GoPlus打造SecWare生态的野心。在安全软件生态系统层SecWare Ecosystem中，GoPlus就计划允许开发者以质押代币的形式加入，并能够在GoPlus安全产品SecWareX中计划开发的安全软件市场中出售，获取收益。在基础层中的安全数据层的设计中，GoPlus允许第三方提供安全相关的数据；安全计算层中，GoPlus除了提供算力的节点外，也引入了主动验证服务AVS作为第三方参与。USM架构也使得GoPlus的安全服务能够很轻易地与RPCs，各类L1链或是L2 Rollup等项目达成合作。

五、打造2B2C双向商业链条

常见的2C安全服务有模拟交易的浏览器安全插件（如Pocket Universe, Kekkai，其中Kekkai是日语中“结界”的意思，该项目获得了GoPlus的投资）、合约/地址风控监测（如Quickintel, AegisWeb3）、高风险地址交易链条追索（MistTrack）、合约授权管理（Revoke.Cash）等。而2B的项目有已融资超2亿8千万的智能合约审计公司Certik。

Securing Web3: How GoPlus Security is Changing the Game with User-Centric Solutions | HackerNoon

与上述项目针对目标客户提供单一产品的项目不同，GoPlus的目标是通过构建SecWare生态，打造2B2C双向商业逻辑闭环的安全产品。



图 18 GoPlus产品生态 来源：<https://whitepaper.gopluslabs.io/goplus-network>

从一开始，GoPlus就坚持开放、无需授权和用户驱动的承诺，努力解决困扰许多现有安全服务的中心化问题。你会发现GoPlus的发展路线中从来不是只有自家产品，而是巧妙地通过激励机制引入了各种各样的利益相关者共建共赢。

2024 Q2-Q3：

- 推出安全RPC服务GoPlus SecNet：首期覆盖以太坊和BNB链，让SecWareX用户大规模访问并体验实时的链上风险控制。

- SecWare协议开放：打造GoPlus网络开发者生态系统，让更多的服务通过SecWare服务用户。此外，GoPlus计划广泛开放生态系统，允许大量有兴趣的安全服务公司和开发人员进入。

2024 Q4:

- 启用安全数据层：允许安全数据贡献者通过代币成为数据贡献节点。
- 正式发布USM，能够开放集成到各种RPC以及跨不同链的序列，扩展安全服务的规模和范围。这将促进模块化公链和RaaS集成伙伴关系。
- 支持更多区块链，增强GoPlus网络在多链环境下的适应性和兼容性。

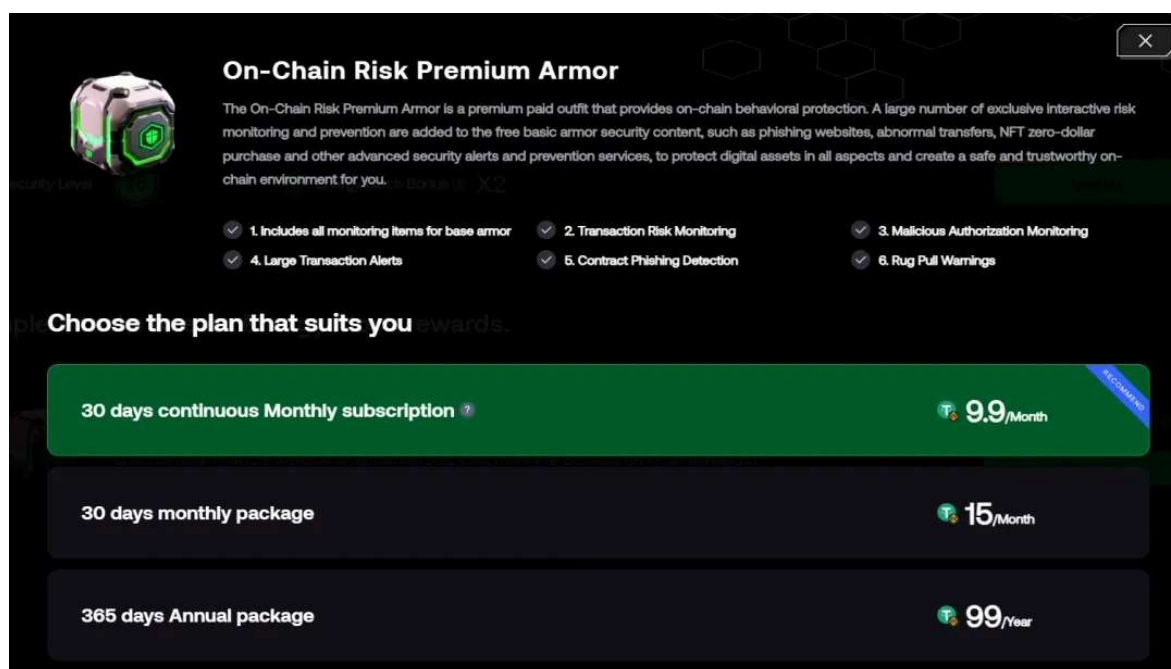
2025 Q1:

- 启用安全计算层：使GoPlus网络生态系统中的更多开发人员能够在该网络上部署他们的服务，同时还将引入计算层节点的激励计划。
- 开源部分安全引擎代码：开放开发者平台和试验场。
- 推出SecWare开发者平台：允许开发人员自由开发、部署和发布他们自己的软件。

而GoPlus打造2B2C的双向商业链条，也使得构造了拥有多样化的收入来源，能够捕获到的商业价值较竞争对手要更多，成为GoPlus重要的护城河。据GoPlus联合创始人Yufeng (Eskil) Xu介绍，目前GoPlus的收入方式主要包括：

- SecWareX的用户安全服务订阅费（目前主要收入来源）；
- USM与区块链集成的gas费；
- 提供给第三方的高级API/SDK付费服务（计划在未来市场地位巩固后继续拓展）

SecWareX的用户安全服务订阅费是目前GoPlus主要的收入来源。目前根据链上数据，已经有超过57k用户订阅了安全服务，SecWareX目前已经创造了超过1.6M USDT的现金流收入，足见GoPlus安全产品恐怖的吸金能力。



On-Chain Risk Premium Armor

The On-Chain Risk Premium Armor is a premium paid outfit that provides on-chain behavioral protection. A large number of exclusive interactive risk monitoring and prevention are added to the free basic armor security content, such as phishing websites, abnormal transfers, NFT zero-dollar purchase and other advanced security alerts and prevention services, to protect digital assets in all aspects and create a safe and trustworthy on-chain environment for you.

- ✓ 1. Includes all monitoring items for base armor
- ✓ 2. Transaction Risk Monitoring
- ✓ 3. Malicious Authorization Monitoring
- ✓ 4. Large Transaction Alerts
- ✓ 5. Contract Phishing Detection
- ✓ 6. Rug Pull Warnings

Choose the plan that suits you

Subscription Plan	Price
30 days continuous Monthly subscription	9.9 / Month
30 days monthly package	15 / Month
365 days Annual package	99 / Year

图 19 GoPlus提供的链上风险高级防御服务付费模式 来源: <https://secwarex.io/task-detail/18>

与其他的2C安全产品创造的现金流相比，GoPlus可谓遥遥领先。以推特/X上关注量达7.46万的Pocket Universe为例，Pocket Universe是一个保护用户免受诈骗的浏览器扩展程序，目前已经成功保护14万多用户和4亿美元以上的资产。而且它承诺如果用户使用其浏览器拓展后，在没有受到警告的情况下丢失了资产，用户将获得达2万美金的保险赔付。

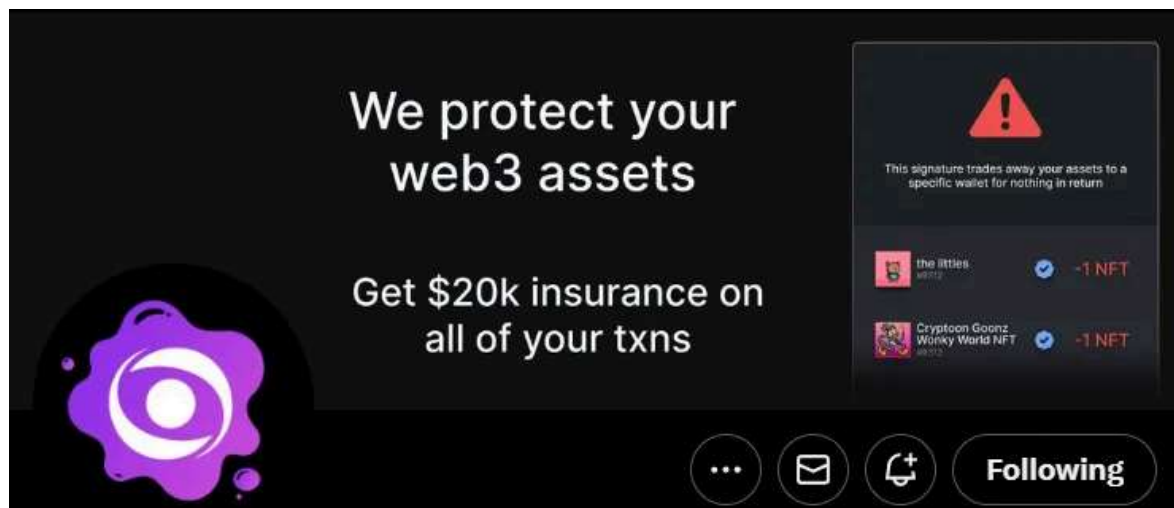


图 20 Pocket Universe推特/X主页 来源: <https://x.com/PocketUniverseZ>

尽管Pocket Universe已经取得了以上成绩，但它的收入模式却并不成熟：在Pocket Universe的官网可以发现，用户安装其拓展程序是免费的，甚至还需要给损失的用户单笔赔付2万美金。也就是目前Pocket Universe除了与项目方合作可能获取一定的收入之外，大部分时间Pocket Universe是亏本运营的。

同样一款针对C端用户的浏览器拓展项目Fire已经正式停止运营。从对比中可以看出GoPlus已然拥有的不俗盈利能力。

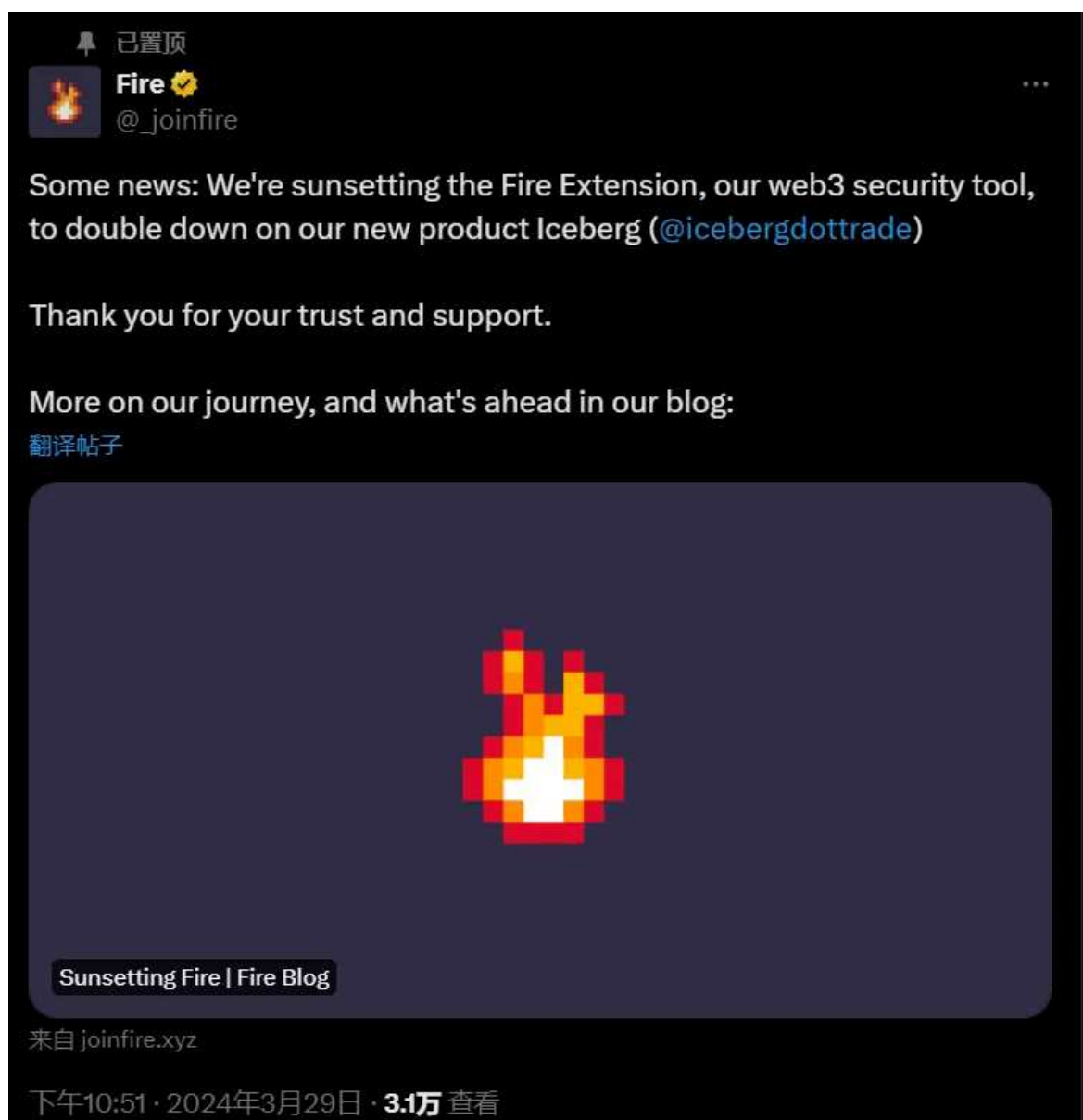


图 21 Fire宣布停止支持Fire Extension 来源: https://x.com/_joinfire/status/1773724738470428926

六、行业前景

一项关于 2022 年智能合约审计的值得注意的统计数据告诉我们, 被黑客攻击的已审计协议数量与未审计协议数量大致相同。虽然这并不意味着智能合约审计不起作用, 而是仅凭它们不足以作为防止黑客攻击的安全措施。

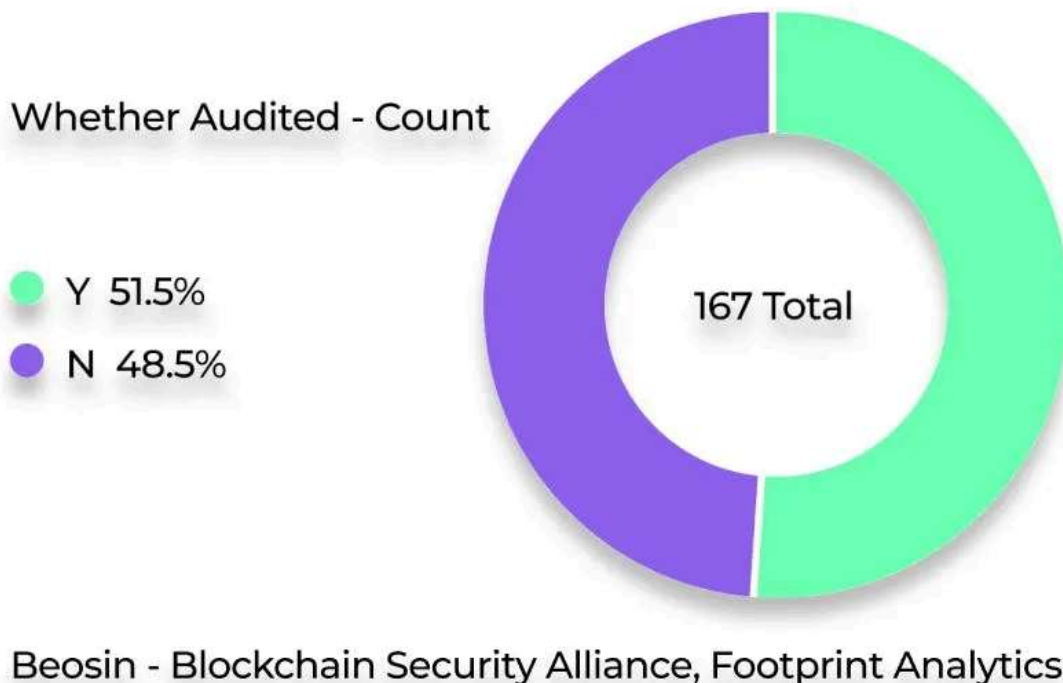


图 24 2022年被黑客攻击的已审计协议数量与未审计协议数量对比 来源: <https://hackernoon.com/zh/2023-%E5%B9%B4-web3-%E5%AE%89%E5%85%A8%E9%97%AE%E9%A2%98-%E5%8D%81%E4%BA%BF%E7%BE%8E%E5%85%83>

有观点认为, Web3用户安全需要全方位多角度的考量, 不能只依赖于事前安全机构审计或是浏览器安全插件。构建全面的安全服务体系时, 需要统筹B端和C端, 建立一个以用户为中心、事前多方风险控制、以预防为主而非事后追责为主的“Web3综合安防体系”。

GoPlus的解决方案精准地回应了这一需求, 其方案涵盖了SecWareX、Personal SecHub、USM等产品模块, 为用户提供了一个坚固的安全屏障。展望未来, GoPlus将不断向“平台化”和“中介化”方向发展, 有潜力成为引领“Web3综合安防体系”的先锋力量。

七、结论

GoPlus是模块化用户安全层, 具有专业的区块链安全检测能力。模块化的设计理念更是使得GoPlus在构建SecWare生态系统以及打造2B2C双向逻辑链条方面脱颖而出, 有潜力成为引领“Web3综合安防体系”的先锋力量。

参考资料

- <https://whitepaper.gopluslabs.io/goplus-network>
- <https://www.rootdata.com/Projects/detail/GoPlus%20Security?k=MzgxNw%3D%3D>
- <https://new.qq.com/rain/a/20240520A07G0X00>
- <https://www.chaincatcher.com/article/2123375>
- https://dune.com/goplus_security/totaladdressbymonth
- <https://mp.weixin.qq.com/s/J7Pbu5E6h9VqzvnNTmbwfw>
- <https://mp.weixin.qq.com/s/bEnIRxPnjzxnFBcFkkl1kQ>
- <https://t-www.panewslab.com/zh/articledetails/6938a7ycz723.html>
- <https://hackernoon.com/securing-web3-how-goplus-security-is-changing-the-game-with-user-centric-solutions>
- <https://docs.gopluslabs.io/reference/api-overview>

免责声明

市场有风险，投资需谨慎。本文不构成任何形式的投资建议，读者应考虑本文中的任何意见、观点或结论是否符合其特定状况。据此投资，责任自负。



交流群（备注公司及岗位）

7UPDAO

声明：请读者严格遵守所在地法律法规，本文不代表任何投资建议。

7up DAO 关于我们



7UpDAO是一个投研驱动的Web3投资机构，致力于投资Web3方向具备高创新性、高成长性的一级和二级项目。

微信群：加微信chenchen202277备注公司及岗位入群

Twitter: @7upDAO

Discord: <https://discord.gg/7updao>

