助力
“双碳”战略目
标，针对政企用户对挖矿行为预
警难、定位难、防控难等特点，
亚信安全“挖矿”治理解决方案正式发布。
该方案以亚信安全XDR解决方案为基础，提供了挖矿失陷治理能力，通过针对黑产挖矿攻击链提供了全面覆盖“云管端关”的一体化防护技术，为贯彻落实虚拟货币“挖矿”整治工作提供了全面支撑。


图：比特币价格逐年增高

在巨大的利益驱使下，“挖矿”黑产在2018年逐步形成，近年来发展迅速，危害也越发严重。首先，“挖矿”造成了电力资源的大量消耗，极不利于实现国家的碳达峰、碳中和目标。其次，“挖矿”黑产非法占用系统资源、网络资源，影响办公效率和业务的正常开展，增加了网络攻击风险。此外，大量围绕“挖矿”的木马病毒开始盛行，目前全球共2700万的挖矿木马，且每周按照2万个增长。从亚信安全威胁情报团队收集到的样本数据分析来看，截止到2021年年底一共获取到的各个家族样本总数为12,477,248个，有些木马不但“挖矿”，还会造成机密数据泄露等严重的网络安全事件。

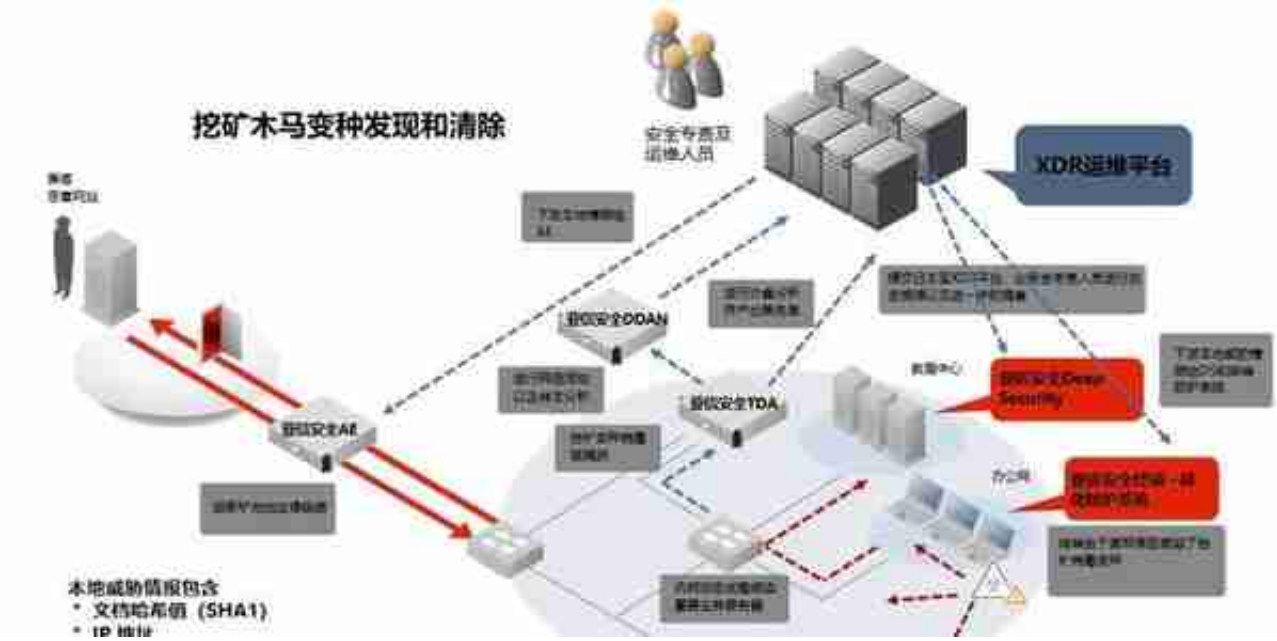
为此，自2021年9月，国家发展改革委等10部门联合发布通知，要求全面整治虚拟货币“挖矿”活动以来，能源、金融、制造、教育、运营商等多个行业，以及各个省市的“挖矿”整治行动都已经全面展开。

## 面对狡猾的“淘金客”
## 用户应当如何应对

有组织、有分工的“挖矿”团体在各路绞杀之下，已经变得更加狡猾：


图：挖矿病毒攻击杀伤链

挖矿病毒攻击杀伤链包括：弱点搜索、攻击武器构建、挖矿脚本及木马投递、漏洞利用、挖矿木马安装，黑产远程控制和挖矿获利七个步骤。因此，就应采用相对应的技术建立防护点，例如：资产风险梳理、威胁情报、补丁管理、病毒防护、行文检测，尤其是对“挖矿失陷”的治理。




图：亚信安全XDR方案，更有效的防御黑产挖矿

在防御方面，
亚信安全的XDR方案可以更有效的抵御挖
矿木马攻击。
亚信安全XDR是以设备联动威胁情报为核心，依据标准化运营流程，通过运营组件对资产的漏洞、威胁、APT攻击进行监控，从而构建防御、检测、分析、响应的安全运营闭环，不仅可以帮助用户更早的发现挖矿木马威胁、定位高危资产，并且通过根因和范围分析，确定是否被攻击，攻击受损程度，以及攻击是怎么发生。

图：亚信安全信池威胁感知运维中心(UAP)提供的挖矿行为情报

在安全运维工作中，用户可发挥亚信安全信池威胁感知运维中心(UAP)的联动机制，将信桅深度威胁发现设备(TDA)、信舱云主机安全(DeepSecurity)、信端病毒防护(O□ceScan)、信端端点安全管理系统(ESM)、信端终端检测与响应系统(EDR)、 网络检测与响应(TDA)、信舷防毒墙系统(AISEDGE)的协同工作，从而形成“感知识别、调查评估、遏制阻断、治愈加固”的全覆盖，让挖矿行为无处遁形。

## 挖矿治理“进行时”

目前，我国全面梳理、核查虚拟货币“挖矿”行为的整治工作已经全面启动。例如：6月13日，上海市政府官网就发布了《上海市经济信息化委、市发展改革委关于签署“不参与虚拟货币‘挖矿’行为信用承诺书”的通知》，对不履行承诺的数据中心运营企业将依法采取差别电价、信用惩戒等措施。

亚信安全将全力配合相关单位开展虚拟货币“挖矿”活动整治，助力企事业单位梳理网络资产、排查“挖矿”病毒风险，为下一步的整改工作提供可靠的技术支撑、数据来源和决策依据。