内部发行 免费赠阅

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

# 网安26号院

奇安信网络安全通讯 · 安全快一步

# 云原生安全出发！

P10



第23期
2022 年 11 月

奇安信
新一代网络安全领军者

# 打造新一代中国特色的安全托管服务

## 时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

**两种模式**
模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

**多种形态**
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

**两化融合**
帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享


### 首创“云地结合”模式

打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

### 7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

### 安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

### 安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

### 专家“一对一”指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

# 消除云原生安全混乱，你需要一位大厨

云原生应用、容器、Kubernetes 和敏捷开发实践加速了软件发布频率。根据云原生计算基金会 (CNCF) 调查，55% 的受访者每周或甚至更频繁地发布软件代码。

与此同时，安全主管们却在开发与运营过程面临大量云安全挑战。98% 的企业在过去 18 个月中经历过某种与云相关的网络攻击事件。

为应对这一挑战，企业尝试各种防护工具来应对不同的问题。 我们看到，喜欢创造新词汇的安全行业发布了应对云原生安全的各类产品：CWPP（云工作负载保护平台）、CSPM（云安全态势管理）、RASP（运行时应用自防护）等。面对众多的工具选项，用户可能会不知所措。更麻烦的是，这些分散孤立的安全产品，就像挤满后厨的厨师，炒出来的未必是道大餐。这些工具带来的并不是高效，而是耗时和支出的增加。拼接一起的安全工具，还会因错误配置带来漏洞，增加网络攻击面。正是由于防护产品自身的限制，客户无法成功实现云原生安全。

安全主管显然需要单一工具来集成多项云原生安全能力，以降低风险、开销和运营成本。看到这一需求与趋势，2021 年在云安全技术成熟度曲线中，Gartner 新加了 CNAPP（云原生应用保护平台）。

通过将基础设施即代码（IaC）扫描、容器扫描、云工作负载保护（CWPP）、云安全态势管理（CSPM）等能力工具集成在统一平台，CNAPP 可为云原生客户真正提供端到端的云原生应用保护。

正如云原生极大程度上改变云的使用方式与效果一样，云原生应用保护平台（CNAPP）及相关云原生安全能力，也将从根本上重构未来云安全的市场格局。

奇安信研究了国内外 CNAPP 各种安全框架，设计了适合国内云原生安全场景的 CNAPP 安全框架。整个框架以应用为中心，安全能力覆盖整个云原生架构及云原生应用的全生命周期。奇安信通过打造一系列全部云原生化的研发平台，支撑安全产品和安全服务的云原生化，为客户业务云原生转型提供全套完整的云原生安全解决方案。

本期专题重点介绍奇安信在云原生安全的思考与探索，看看这个大厨是否做出了合乎你口味的那道菜?

总编辑

李建平

2022 年 11 月 1 日

CONTEN

目录

## 安全态势



月度专题

# 云原生安全出发！ P10

云原生安全是云安全的下一个角力场。云原生应用保护平台（CNAPP）及相关云原生安全能力，则将从根本上重构未来云安全的市场格局。

TS






《网安 26 号院》编辑部
**主办** 奇安信集团

**总　　编　　辑**：李建平
**安全态势主编**：王　彪
**月度专题主编**：李建平
**攻防一线主编**：魏开元
**安全之道主编**：张少波
**奇安信人主编**：孙丽芳
**安全叨客主编**：王梦琪
**奇安资讯主编**：陈　冲
**研究报告主编**：包世玉


奇安信集团　虎符智库　安全内参


索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2122- L0058 号
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2022 年 11 月 26 日
发行对象：奇安信集团内部

## 事件篇

数据泄露仍是当前全球最主要网络威胁之一。法国军工巨头泰雷兹内部敏感数据遭勒索软件公开，俄乌网络战导致俄罗斯央行、乌克兰战场指挥系统数据泄露，我国台湾地区数千万公民信息遭暗网售卖。

### 勒索软件团伙公布法国军工巨头泰雷兹内部敏感数据

据 SecurityWeek 11 月 14 日消息，法国航空航天、国防与安全巨头泰雷兹集团发布声明称，勒索软件团伙 LockBit 3.0 公布了与该公司有关的数 GB 数据，但集团自身并未发现 IT 系统遭受入侵的证据。该集团内部安全专家推测，这批数据的泄露来源可能是合作伙伴的协作门户。数天前 LockBit 团伙发布了一个 9.5 GB 的归档文件，声称已掌握涉及泰雷兹集团运营的高度敏感信息，以及“商业文件、会计文件、客户文件、客户结构图和软件。”

### 加拿大最大肉类生产商被黑：部分运营中断 食品供应受影响

据 BleepingComputer 11 月 7 日消息，加拿大肉类生产巨头枫叶食品（Maple Leaf Foods）证实，周末经历了一起网络安全事件，导致系统与运营中断。该公司称，中断已经造成部分运营和服务无法正常进行，预计全面解决中断仍然需要时间，且期间部分运营和服务将无法正常进行。枫叶食品表示将继续与客户及合作伙伴携手，尽量缓和加拿大市场上的食品供应中断。

### 乌克兰“网军”入侵俄罗斯央行，公布大量敏感数据

据 TheRecord 11 月 7 日消息，乌克兰 IT 军声称已成功入侵俄罗斯中央银行，窃取到大量内部文件。有媒体审查了公开发布的部分“被盗”文件，总计 2.6 GB，包含 27000 个文件。从内容上看，这些文件主要涉及银行运营、安全政策及部分前任 / 现任员工的个人数据。中央银行是俄罗斯最重要的金融机构之一，也是该国货币政策制定者和国家货币监管者。据俄罗斯媒体报道，央行方面否认其系统遭黑客入侵，并表示这些所谓外泄文件原本就存放在公开域内。

### 网络攻击迫使丹麦最大铁路公司火车全部停运

据 SecurityWeek 11 月 4 日消息，由于供应商遭受网络攻击后关闭了服务器，丹麦最大的铁路运营公司 DSB 旗下所有火车均陷入停运，连续数小时未能恢复。据悉，遭受攻击的供应商 Supeo 有一款移动应用，可供火车司机访问运行的各项关键运营信息，如限速指标和铁路运行信息。Supeo 关闭服务器的决定令该应用停止工作，司机们只能被迫停车。DSB 一名代表透露，这是一起“经济犯罪”。

## 波音子公司遭网络攻击，致使全球多家航司航班规划中断

据 TheRecord 11 月 3 日消息，美国航空航天巨头波音的子公司、航班规划工具商 Jeppesen 发生网络安全事件，部分系统中断服务，导致北美、中东等多家航空公司的部分航班规划被迫中断、航班延误。此次事件至少影响了当前及后续空中任务通知（NOTAM）的接收和处理。NOTAM 是指向航空当局提交的通知，用于提醒飞行员注意航线上的潜在危险。事件发生后，伊拉克航空、沙特 Flynas 航空、加拿大太阳之翼航空等均发布受影响公告。

## 美国新闻业遭遇大规模供应链攻击：数百家报纸网站被植入“后门”

据 BleepingComputer 11 月 2 日消息，美国安全厂商 Proofpoint 披露，有恶意黑客入侵并操纵某家未公开名字的媒体公司的基础设施，在美国数百家报纸的网站上部署了 SocGholish JavaScript 恶意软件框架。SocGholish 会在网站上显示虚假更新警告，再利用伪装成浏览器更新（如 Chrome.Update.zip）的恶意文件感染网站访问者。有 250 多家美国新闻媒体网站受影响，其中包括国家新闻机构在内的不少重量级新闻机构。被黑的媒体公司主要向美国新闻机构提供视频和广告内容服务。

## 乌军战场指挥系统遭匿名黑客入侵：战场数据泄露

据 SouthFront 11 月 1 日消息，匿名黑客组织“Joker DPR”（顿涅兹克小丑）在电报群宣称，已成功入侵乌克兰武装部队（AFU）使用的所有军事指挥和控制程序，包括可接入北约 ISR 系统的美国 Delta 数字地图战场指挥系统，该系统目前是乌克兰部队主要使用的战场指挥系统。Joker DPR 宣称已经用病毒感染了所有接入 Delta 系统的计算机，并且篡改了其中的数据。该团伙还发布了大量软件屏幕截图（包括俄乌双方的作战单元）和视频证明自己的说法。

## 黑客长期潜伏国内一外贸企业邮箱，骗走 200 余万美元货款

据浙江法制报 10 月 31 日消息，杭州钱塘一家外贸企业的电子邮箱遭不法分子入侵，导致企业险些被骗 200 余万美元货款。据当地警方调查，黑客通过木马程序侵入了这家企业的邮箱，并长期潜伏，发现双方交易后，篡改了企业发送给国外客户邮件中的收款人信息及收款账户，致使客户根据邮件信息，将货款打进了黑客的账户。警方介入时，这笔货款仍在银行中转流程中，警方通过及时申诉支付冻结，将全部货款顺利追回。

## 台湾全岛个人信息被放在网上兜售，经调查至少 20 万条真实

据海峡导报 10 月 30 日消息，有台媒报道，台湾地区户政系统传出遭黑客入侵，有网友在海外论坛 BreachForums 上贩售 20 万笔台湾民众户籍资料，并宣称手上有全台 2300 万民众资料。台湾“调查局”本月 25 日获报后即展开追查，初步调查确认目前释出的 20 万笔集中在宜兰地区，且资料都吻合，宜兰“县长”林姿妙、民进党“立委”陈欧珀等人的个人资料都在其中。台湾“内政部”初步研判，该论坛上贩售的资料，看似由多个数据库组合而成，资料真实性有相似度，已交由检警调调查，并强调户役政资讯系统资料并未流出。

## 漏洞篇

OpenSSL 又一次曝出远程代码执行漏洞（CVE-2022-3602），引发行业关注。经奇安信 CERT 研判，该漏洞利用条件较高，较难被广泛利用，用户不必过于惊慌，但仍建议尽快升级至安全版本。

### F5 BIG-IP 安全漏洞通报

11 月 18 日，国家信息安全漏洞库（CNNVD）收到关于 F5 BIG-IP 安全漏洞（CVE-2022-41622）情况的报送。攻击者可以发送特制的 HTTP 请求以执行未经授权的操作。F5 BIG-IP 13.1.0，13.1.5，14.1.0，14.1.5，15.1.0，F5 BIG-IP 15.1.8，16.1.0，16.1.3，17.0.0，F5 BIG-IQ Centralized Management 7.1.0，F5 BIG-IQ Centralized Management 8.0.0，F5 BIG-IQ Centralized Management 8.2.0 等多个版本均受此漏洞影响。目前，F5 官方已经发布了修复漏洞的升级版本，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

### YApi 命令执行漏洞安全风险通告

11 月 11 日，奇安信 CERT 监测到 YApi 命令执行漏洞，远程未授权的攻击者可通过注入漏洞获取有效用户 token，进而利用自动化测试接口绕过沙箱限制，最终在目标系统上执行任意命令。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。YApi 是一款高效、易用、功能强大的 API 管理平台，旨在为开发、产品、测试人员提供接口管理服务。帮助开发者轻松创建、发布、维护 API。

### 微软多个安全漏洞通报

11 月 10 日，国家信息安全漏洞库（CNNVD）发布预警，微软官方发布了多个安全漏洞的公告，其中微软产品本身漏洞 78 个，影响到微软产品的其他厂商漏洞 3 个。包括 Microsoft Windows Kerberos 安全漏洞（CVE-2022-37966）、Microsoft Windows Kerberos 安全漏洞（CVE-2022-37967）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据、提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布了漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

### Citrix Gateway 和 Citrix ADC 身份认证绕过漏洞安全风险通告

11 月 10 日，奇安信 CERT 监测到 Citrix 官方发布安全公告，经研判，Citrix Gateway 和 Citrix ADC 身份认证绕过漏洞 (CVE-2022-27510) 影响较大。当 Citrix Gateway 或 Citrix ADC 作为网关运行时（使用 SSL VPN 功能或部署为启用身份验证的 ICA 代理），未经授权的远程攻击者可利用此漏洞绕过目标设备的身份认证，进而访问敏感服务。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

## OpenSSL 多个高危漏洞安全风险通告

11 月 2 日，奇安信 CERT 监测到 OpenSSL 官方发布了漏洞安全更新，包括 OpenSSL 拒绝服务漏洞 (CVE-2022-3786) 和 OpenSSL 远程代码执行漏洞 (CVE-2022-3602)。

攻击者可利用 CVE-2022-3786 漏洞，制作包含恶意电子邮件地址的证书，以溢出包含 "." 的任意字节数，此缓冲区溢出可能导致服务崩溃。CVE-2022-3602 漏洞存在于 ossl_punycode_decode 函数，当客户端或服务器配置为验证 X.509 证书时调用此函数，攻击者可以通过在电子邮件地址字段的域中创建包含 punycode 的特制证书来利用该漏洞，可能导致服务崩溃或潜在的远程代码执行。

此前业内有多篇文章将 CVE-2022-3602 与 2014 年的 HeartBleed 相提并论，引起大量安全人员的关注。经研判，此漏洞利用前提条件是必须配置客户端或服务器，以验证证书中恶意电子邮件地址，同时仅影响 OpenSSL 3.x，进一步限制了漏洞的利用范围，此次更新的漏洞可能不像 HeartBleed 那样容易被广泛利用，用户不必过于惊慌，但仍建议尽快升级到安全版本。

## Spring Security 身份认证绕过漏洞安全风险通告

11 月 2 日，奇安信 CERT 监测到 Spring 官方发布 Spring Security 身份认证绕过漏洞 (CVE-2022-31692) 通告，当 Spring Security 处理 forward 或 include 转发的请求时，可能存在漏洞，攻击者可利用此漏洞绕过授权规则。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。Spring Security 是一款为基于 Spring 的企业应用系统提供声明式安全访问控制解决方案的安全框架。

## SQLite 拒绝服务漏洞风险通告

10 月 28 日，奇安信 CERT 监测到 SQLite 存在拒绝服务漏洞 (CVE-2022-35737)。攻击者可以将大字符串传递给 SQLite 的某些函数，触发数组越界导致拒绝服务，消耗系统内存和 CPU 资源。目前，此漏洞技术细节与 PoC 已公开。鉴于此漏洞影响范围极大，建议客户尽快做好自查，及时更新至最新版本。SQLite 是使用广泛的开源数据库引擎，默认包含在 Android、iOS、Windows 和 macOS 及主流 Web 浏览器中。

## 苹果 iOS 和 iPadOS 任意代码执行漏洞安全风险通告

10 月 26 日，奇安信 CERT 监测到苹果 iOS 和 iPadOS 存在任意代码执行漏洞 (CVE-2022-42827)。苹果 iOS 和 iPadOS 系统内核边界检查不当，会导致越界写入问题，可允许恶意程序以内核权限执行任意代码。iOS 16.1 及以前版本、iPadOS 16 及以前版本均受影响。目前，此漏洞已发现在野利用，鉴于此漏洞影响范围极大，建议客户尽快做好自查，及时更新至最新版本。

## Oracle 多个安全漏洞通报

10 月 20 日，国家信息安全漏洞库（CNNVD）发布预警，Oracle 官方发布了多个安全漏洞的公告，其中 Oracle 产品本身漏洞 85 个，影响到 Oracle 产品的其他厂商漏洞 221 个。包括 Oracle E-Business Suite 安全漏洞（CVE-2022-21587）、Oracle E-Business Suite 安全漏洞（CVE-2022-39428）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据、提升权限等。Oracle 多个产品和系统受漏洞影响。目前，Oracle 官方已经发布了漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

## 政策篇

国内，我国首项关键信息基础设施安全保护的国家标准发布，关基保护工作迎来实施指南；

国际上，美国持续推进关基安全改善计划，继运输管道、地面交通、太空系统等领域后，又发布《加强铁路网络安全》指令修订版。


### 市场监管总局、网信办发布《个人信息保护认证实施规则》

11 月 18 日，市场监管总局、网信办宣布实施个人信息保护认证工作，并发布《个人信息保护认证实施规则》以下简称《实施规则》。《实施规则》以《信息安全技术 个人信息安全规范》《个人信息跨境处理活动安全认证规范》为认证依据，规定了对个人信息处理者开展个人信息收集、存储、使用、加工、传输、提供、公开、删除及跨境等处理活动进行认证的基本原则和要求。《实施规则》明确认证模式为“技术验证 + 现场审核 + 获证后监督“。认证证书有效期为 3 年。

### 国家标准《信息安全技术 关键信息基础设施安全保护要求》发布

11 月 7 日，市场监管总局标准技术司、中央网信办网络安全协调局、公安部网络安全保卫局在京联合召开《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204-2022）国家标准发布宣贯会。本标准是第一项关键信息基础设施安全保护的国家标准，将于 2023 年 5 月 1 日正式实施。标准提出了以关键业务为核心的整体防控、以风险管理为导向的动态防护、以信息共享为基础的协同联防的关键信息基础设施安全保护 3 项基本原则，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等 6 个方面提出了 111 条安全要求，为运营者开展关键信息基础设施保护工作需求提供了强有力的标准保障。

### 工业和信息化部发布《关于促进网络安全保险规范健康发展的意见（征求意见稿）》

11 月 7 日，工业和信息化部发布《关于促进网络安全保险规范健康发展的意见（征求意见稿）》，公开征集意见。《征求意见稿》提出，在建立健全网络安全保险政策标准体系、加强网络安全保险产品服务创新、强化网络安全技术赋能保险发展、促进网络安全产业需求释放、培育网络安全保险发展生态 5 个方面加强网络安全保险规范健康发展。

### 国务院办公厅印发《全国一体化政务大数据体系建设指南》

10 月 28 日，国务院办公厅印发《全国一体化政务

大数据体系建设指南》（以下简称《指南》），要求整合构建标准统一、布局合理、管理协同、安全可靠的全国一体化政务大数据体系。在安全保障方面，《指南》提出健全数据安全制度规范、提升平台技术防护能力、强化数据安全运行管理，包括开展内部数据安全检测与外部评估认证、建设数据安全态势感知平台、建立健全数据安全运行监管机制等。

## 工业和信息化部印发《网络产品安全漏洞收集平台备案管理办法》

10 月 25 日，工业和信息化部印发《网络产品安全漏洞收集平台备案管理办法》（以下简称《办法》），自 2023 年 1 月 1 日起施行。《办法》规定，我国境内的网络产品安全漏洞收集平台，应通过工业和信息化部网络安全威胁和漏洞信息共享平台如实填报网络产品安全漏洞收集平台备案登记信息，包括漏洞收集的范围和方式、漏洞验证评估规则、通知相关责任主体修补漏洞规则、漏洞发布规定等。已上线运行的漏洞收集平台应在本《办法》施行之日起 10 个工作日内进行备案。

国际

## 欧盟制定网络防御政策，以应对俄乌网络战

11 月 10 日，欧盟委员会和高级代表提出一份关于欧盟网络防御政策和军事机动性 2.0 行动计划的联合公报，以应对俄乌战争后不断恶化的安全环境，并提高欧盟保护其公民和基础设施的能力。通过网络防御政策，欧盟将加强网络防御方面的合作和投资，以更好地保护、检测、阻止和防御日益增多的网络攻击。网络防御政策包括 4 个支柱，分别为共同行动与协作、确保欧盟国防生态系统的安全、加强投资军事网络防御能力、建立网络防御合作伙伴关系。欧盟数字事务主管玛格丽特 · 维斯塔格在发布会上表示，“没有网络防御，就没有欧洲防务。”

## 乌克兰公布《个人数据保护法（草案）》，推进数据安全立法进程

10 月 25 日，乌克兰议会公布了《个人数据保护法（草案）》。根据议会发布的“草案解释”，近年来，包括乌克兰在内的全球互联网数据处理活动显著增加，特别是在大数据和社交媒体领域。鉴于国际上个人数据保护领域规则的发展，乌克兰国内外的立法状态并不能完全保障乌克兰个人数据的安全，需要对立法及其应用进行全面更新，遂制定此法。乌克兰企业也正在更新其隐私流程和个人数据处理的部门和规则，以期与乌克兰《个人数据保护法》及欧盟政策标准相符合，使个人数据保护规则与新标准接轨。

## 美国运输安全管理局发布《加强铁路网络安全》指令

10 月 18 日，美国运输安全管理局发布一项题为《加强铁路网络安全 -SD1580/82-2022-01》的指令文件，要求对指定的客运和货运铁路运营商实施监管，通过基于绩效指标的要求增强网络安全弹性。该指令的关键安全目标包括：网络分段和控制策略、针对关键系统实施访问控制、持续监控和检测、基于风险的安全方法，将进一步加强国家铁路运营的网络安全预防与弹性水平。该指令自 2022 年 10 月 24 日起生效，有效期为 1 年。 安

# 云原生安全出发！

云原生安全是云安全的下一个角力场。云原生应用保护平台（CNAPP）及相关云原生安全能力，则将从根本上重构未来云安全的市场格局。

# 云原生时代：安全该何去何从？

**作者** 奇安信云安全管理事业部负责人 孙立鹏

2022 云技术峰会上，某业界大佬在演讲中表示，云原生正成为企业上云的首选，全面云原生的时代正在来临。

容器、微服务等技术的应用，不仅重新定义了云上的开发运营体系、加快了业务上线和变更的速度，云的使用变得比以往更加便捷、高效。

云原生在给企业带来敏捷的同时，也引入了全新的安全风险和挑战。与传统的安全防护能力不同，云原生安全需要安全能力和云原生平台紧密结合，安全必须集成到持续集成和持续开发流程中，真正成为内生安全。

现在很多人将云原生安全称为云安全的下半场、云安全的未来，足见其重要程度。云原生时代，安全究竟该怎么做呢?

作为国内云安全领域，市场占有率多年领先的安全厂商（根据赛迪顾问相关报告数据），奇安信同样在积极寻求变化，以满足云安全合规之后客户对云原生安全的迫切需求。

## 现实：两成用户无云原生安全能力

2022 年 7 月，作为工信部直属科研事业单位的中国信息通信研究院，发布了《云计算白皮书（2002 年）》。白皮书显示，中国云计算市场在 2021 年仍保持高速增长，市场规模达 3,299 亿元，较 2020 年增长了 54.4%。《“十四五”数字经济发展规划》的发布、工信部《企业上云用云实施指南（2022）》编纂工作的启动等对政企深度上云用云的政策性指引，形成了 2021 年中国特色云计算产业发展的大背景。

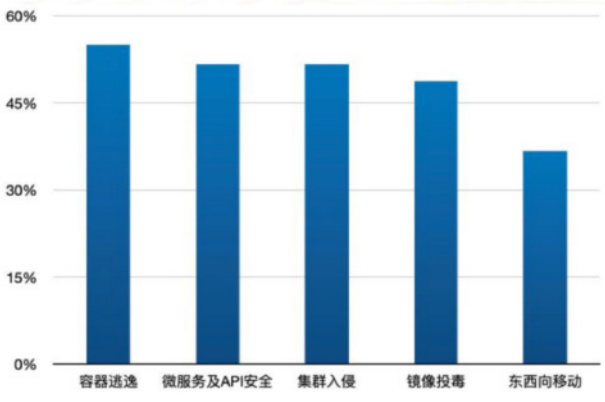
技术方面，白皮书认为，2021 年的突出特点，在于云原生正通过改进企业的 IT 技术和基础设施，持续加速企业 IT 要素的变革，成为企业用云的新范式。具体来看，表现在云原生生态的日趋完善、能力模型的日渐丰富、与企业 IT 建设目标和要素深度融合三大方面。

中国云原生技术的实际应用情况，中国信通院云原生产业联盟（CNIA），也连续多年以问卷、访谈结合的形式对多行业用户进行了统计。管中窥豹，从最新的《中国云原生用户调查报告（2021 年）》中，我们能够看到以下四个云原生应用的重要趋势：

- 混合云部署增长明显。仅 15.74% 的用户没有使用多云 / 混合云的计划。
- 容器用户生产环境中的采纳率再创新高。接近七成用户在生产环境中使用了容器技术，45.48% 的用户已将容器用于核心生产环境。
- 微服务架构获得用户普遍认可。已经使用及计划使用微服务架构的用户超过八成，54.81% 的用户已经使用微服务架构进行应用开发。
- 无服务器技术持续升温。近四成用户已在生产环境中应用无服务器，18.11% 的用户已将 Serverless 技术用于核心业务的生产环境。

或许是因为有云安全等级保护等合规基础，云原生技术在中国市场大放异彩的同时，云原生安全并没有被忽视。报告显示，近七成用户对云原生技术在大规模应用时的安全性、可靠性、性能、连续性心存顾虑。容器逃逸、微服务和 API 的安全是企业最关心的云原生安全问题。近六成的企业表示，容器及其编排系统自身的安全已成为最突出的云原生安全隐患。

中国用户普遍已经开始对云原生安全产生担忧，但从安全投入和能力建设角度来看，现状又仍显不足，甚




企业最关心的云原生安全问题

至可以说尚在起步阶段。报告显示，仍有约两成用户目前无任何针对云原生技术的防护能力。仅有四成用户具备对镜像的漏洞扫描能力和容器运行时入侵检测能力，具备对云原生集群的安全监控与审计能力的用户不到五成。企业人员架构层面，仅有 12.04% 的受访者表示，所在企业有单独的信息安全部门来处理云原生安全问题。

这就是 2021 年，中国云原生和云原生安全，不容乐观的大致现状。这也给了云服务商、传统和初创安全厂商在云原生安全这个角力场施展拳脚的空间。

## 云原生的安全，还是安全的云原生化

网络安全产业的某一细分领域，如果在领域定义、市场需求、产品类型等方面都不够明确、统一的情况下，哪方能有更大的话语影响力，哪方就能更多的占据主动权，影响甚至教育市场。近 10 年前的工控安全，目前的云原生安全，都是处于这样一个形势下。

观察当前云原生安全市场情况，更多是互联网公司起家的云服务商和安全厂商两方的市场角力。安全厂商又可以分为传统安全厂商和专注云原生安全赛道的初创企业两类。

两方的观点和优势也是非常鲜明。

云服务商的积累优势在于自身全栈的云服务技术架构、丰富的云服务产品及广泛的客户基础，更强调安全与云原生基础设施的深度融合。通过将安全能力与自家技术架构、服务产品的深度绑定，强调云原生安全不再外挂，随云而动，更灵活、更细粒度的安全能力和更好的安全体验。

无疑，这是将安全云原生化，进而让安全像空气一样，在自家的云服务体系中无处不在。对于云服务商而言，云是大局，安全的云是核心。

安全厂商则不然。云原生技术当前的应用推广不是迭代式，相对的，云原生安全未来数年大概率还只是会作为云安全市场的重要补充。同时，有一定体量、规模的安全厂商，业务一般会涉及云安全之外其他领域。所以，安全厂商的核心优势，在于安全能力、专业人员、服务流程的积累，更强调安全的目标和保护对象。

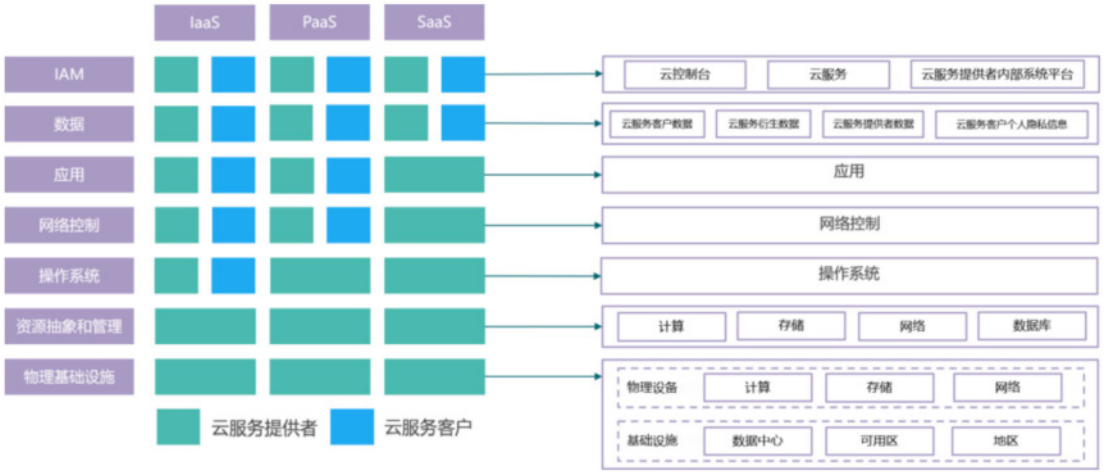
因此，对于安全厂商而言，云原生安全当前更多是面向云原生环境和应用的安全。

此外，云原生安全与当前的云安全，有着明显的区别和必然的联系。无论是因为安全的特殊属性，还是为了规范市场、拉齐能力底线，进入合规也是云原生安全必然的发展方向。换言之，合规的缺位也是当前制约云原生安全市场快速发展的重要因素。

研究 2019 年发布的等保 2.0 系列标准中针对云计算的安全扩展要求，不难发现，虚拟化环境是当时主要考虑的。从安全角度做好对云原生环境中容器、微服务等技术，以及贯穿云原生应用全生命周期的 DevSecOps 的支持，而不局限于某个特定云服务商的技术与产品体系，以更加合理地应对客户越来越多的混合云（不同云服务商参与）的部署场景，是安全厂商在理解云原生安全时更多考虑的。

## 制衡与内生：奇安信云原生安全关键词

作为成功实现 2022 年北京冬奥及冬残奥会网络安全“零事故”的全线安全厂商，奇安信对云原生安全理念，可以归结为两个关键词：制衡、内生。他们都不是新词，但是在云原生时代，有了新的安全内涵。




云计算安全责任共担模型

先说“制衡”。网络安全工作的制衡，无论是通过技术手段还是管理手段，核心都不是制约而是平衡，目的是要保障网络安全实现零事故目标，即业务不中断、数据不出事、合规不踩线。

云安全的制衡，主要体现在云服务商、云上租户与安全厂商三者之间。业界耳熟能详的“云计算安全责任共担模型”，最能恰如其分的体现云安全三方制衡的理念。该模型对 IaaS、PaaS、SaaS 三种服务模式剖析云服务参与主体需要承担的安全责任，对应行业标准（YD/T 4060—2022）由中国信通院牵头制定，并已于 2022 年 7 月正式发布施行。

发生勒索、挖矿、数据泄露等安全事件，最终蒙受财务和声誉损失的只有云服务客户。所以对于云服务客户而言，明确自身责任内云安全能力真实建设情况与实际运营效果，应该成为合规外的重要驱动力。这不仅有助于真正降低云安全事件发生的概率，更有助于产生经济损失后的定责。

要实现此目标，客户自然可以根据自身需求和实际市场情况，自由选择云安全能力提供方进行采购。但是，既然责任整体一分为二，那么承担另一部分责任的云服务商理应避嫌。一是出于让责任边界更清晰，方便客户对供应商进行管理的考量；二是不能让“共担”这一业界共识名不副实，无法实现共担背后的重要意义。

我们看到的市场现状是，部分云服务商在部分项目上对安全的大包大揽。云原生安全亦是如此。设想，如果云服务客户的安全责任，也全部由云服务商或与其有利益关系的安全厂商承担，一旦出现安全事件，客户能否第一时间得知真实详情？事后如何定性、追责？

当然，这不是说云服务商不要和安全厂商合作。恰恰相反，一个开放的生态，云服务商、安全厂商、客户的三方的积极参与和务实合作，才能让客户云安全工作的管理有抓手，云上安全事件的应对底线有保障，对关键业务系统、核心生产环境的上云用云真正放心。

再说“内生”。如果说信息化时代，安全处在伴生的位置。在数字化时代，安全应保持与新技术应用的“同步”，并做到内生。

中国信通院《中国数字经济发展报告（2022 年）》显示，2021 年产业数字化规模达到 37.18 万亿元，占数字经济比重 81.7%，占 GDP 比重 32.5%。可以说，产业数字化已经成为数字经济发展主引擎。

实体经济的数字化转型，数字化基础设施是关键底座。云计算的发展进程，已经成为我国数字基建的晴雨表。

统筹发展与安全，是发展数字经济的核心指导思想。安全与业务系统同步规划、同步建设、同步运营的目标，

便是要实现安全与数字技术、与数字业务的深层次融合。云原生技术作为云计算的“新人”“红人”，更应在推广应用的早期，就围绕云原生技术和其支撑的业务系统，建立起自适应、自主、自生长的云原生安全能力，助力客户实现“保护云原生应用安全”这一目标。

奇安信是内生安全理念的提出者和坚定践行者。2021 年，奇安信与咨询公司 Gartner 联合发布了《数字化转型需要内生的安全框架》报告。报告提出，基于中国网络安全建设现状，需要一种更具中国特色、切实有效的网络安全建设体系。

内生安全框架以系统工程方法论结合“内生安全”理念形成，包括网络安全能力体系、规划方法论与工具体系、能力化组件模型、建设实施项目库（即“十工五任”）、网络安全部署和运行体系参考架构等多个组件，目的是引导政企机构规划和建设网络安全，使其从“外挂”走向“内生”、从“走形式”转向“实战化”，适应数字经济的发展。2022 年北京冬奥会和冬残奥会网络安全保障任务的圆满完成，“零事故”目标的成功实现，便是内生安全框架一次在奥运场景下的最佳实践。

要实现安全在云原生环境的内生，奇安信认为云原生安全的设计规划需秉承以下三个原则：

一是安全左移。安全从开发阶段介入，尽早暴露容器等云原生技术在应用过程中的风险，降低在运行时阶段再进行修复的代价。

二是全生命周期覆盖。云原生安全应以保护云原生应用为中心，安全能力覆盖云原生应用的全生命周期，真正让 Sec 贯穿 DevOps 全流程。

三是原生融合。云原生安全体系与架构应能够与云原生技术环境融合，从外挂式的割裂走向内生。

在云原生安全建设思路与内容上，奇安信认为，云原生安全主要应从云原生制品安全、云原生基础设施安全和云原生运行时安全三个维度入手。云原生安全能力，当前应覆盖云原生基础设施安全、制品安全、容器安全、微服务安全等。

奇安信基于多年云安全市场的积累与深耕，目前能够提供包括容器安全、软件供应链安全、CWPP、CSPM、API 安全、RASP（运行时应用自防护）等面向云原生技术的安全能力及 CNAPP 平台产品，稳定可靠的支持国内所有主流云服务商云原生环境。其专业、高成熟度的云原生安全能力，已获得中国信通院“云原生能力成熟度 – 云原生基础架构安全域 L4”的权威认定。

针对云原生应用的安全防护，Gartner 发布的《CNAPP 创新洞察》报告认为，云原生应用保护平台（CNAPP）解决方案涉及基础设施即代码（IaC）扫描、容器扫描、云工作负载保护（CWPP）、云基础设施授权管理（CIEM）、云安全态势管理（CSPM）等跨越开发和生产环境的关键能力。

通过将这些能力工具集成在统一平台，CNAPP 可为云原生客户真正提供端到端的云原生应用保护。

CNAPP 平台可以提高云原生应用的安全可见性、改进兼容性、加快风险识别能力、实现风险和合规检测自动化。

正如云原生极大程度上改变云的使用方式与效果一样，云原生应用保护平台（CNAPP）及相关云原生相关能力，也将从根本上重构未来云安全的市场格局。

## 结语

云原生安全的建设，应以云原生应用为中心，覆盖云原生应用全生命周期，贯穿一体系（DevOps）、两方向（安全左移与安全右移）、 三环节（构建、部署、运行）和四目标（面向开发、面向云原生基础设施、软件定义、全流程一体化安全运营）。

当前，国内云原生安全市场的主要玩家各有所长，相较于帮助云服务客户构筑能力成熟完备、责任边界明确、服务灵活高效的云原生安全体系这一目标，仍有距离。

随着客户对云原生技术的理解和应用不断深入，对云原生安全服务能力的需求与评价愈加明确，第三调研机构和科研单位在该领域的深度参与投入，以及相关报告、标准的出台，云原生安全成为中国云安全市场高速发展核心引擎之时，指日可待。

# 一体式云原生安全防护体系的建设路径

作者 中国信息通信研究院 栗蔚 刘如明 杜岚 李永欣

本文提出业内首个云原生应用保护平台模型，对模型中的安全能力进行了分层介绍，为行业用户深入实践云原生技术、构筑完善的云原生安全能力提供参考。

## 引言

云原生以其高效稳定、快速响应的特点极大地释放了云计算效能，成为企业数字业务应用创新的原动力。在改变云端应用的设计、开发、部署和运行模式的同时，也带来了新的安全需求和挑战。传统基于边界的防护模型已不能完全满足云原生的安全需求，需要设计全新的云原生安全防护模式，基于动态工作负载，实现云原生技术架构和规模应用的全面防护。

## 背景与形势分析

**云原生技术在生产环境采纳率急速升高**

云原生的理念经过几年的发展，不断丰富、落地、实践，云原生已经渡过了概念普及阶段，进入了快速发展期。过去几年中，以容器、微服务、DevOps、Serverless 为代表的云原生技术正在被广泛采纳，2020 年 43.9% 的国内用户已在生产环境中采纳容器技术，超过七成的国内用户已经或计划使用微服务架构进行业务开发部署等，这使得用户对云原生技术的认知和使用进入了新的阶段，技术生态也在快速的更迭。

**颠覆性技术架构变革带来全新安全隐患**

云原生技术架构充分利用了云计算弹性、敏捷、资源池和服务化特性，在改变云端应用的设计、开发、部署和运行模式的同时，也带来了新的安全要求和挑战。以容器、Serverless 为载体的云原生应用实例极大地缩短了应用生命周期；微服务化拆分带来应用间交互式端口的指数级增长及组件间组合设计复杂度的陡升；多服务实例共享操作系统带来了单个漏洞的集群化扩散；独立的研发运营流程增加了软件全生命周期各个环节的潜在风险。云原生的特有属性带来了架构防护、访问控制、供应链、研发运营等领域全新的安全隐患和安全防护需求。

**传统的边界防护模型难以应对云原生安全风险**

云原生关注快速开发和部署，这种特性要求进行防护模式的转变，从基于边界的防护模式迁移到更接近基于资源属性和元数据的动态工作负载的防护模式，从而有效识别并保护工作负载，以满足云原生技术架构的独特属性和应用程序的规模需求，同时适应不断变化的新型安全风险。安全防护模型的转变要求在应用程序生命周期中采用更高的自动化程度，并通过架构设计（如零信任架构）来确保安全方案实施落地；在云原生系统建设初期，需要进行安全左移设计，将安全投资更多地放到开发安全，包括安全编码、供应链（软件库、开源软件等）安全、镜像及镜像仓库安全等。进入云原生时代，物理安全边界逐渐模糊，并变成了无处不在的云原生安全体系，从外到内，无论可视化、运维和安全管理，还是南北向和东西向网络、容器基础架构、微服务应用模式、身份安全、数据安全等，都给安全市场带来了更丰富的产品维度，衍生出更多元的发展机遇。

## 云原生架构下的典型安全风险及解决方案

云原生架构的安全风险包含云原生基础设施自身的安

全风险，以及上层应用云原生化改造后新增和扩大的安全风险，其中最突出的是云原生计算环境的安全风险，包括了容器网络安全、组件安全、容器镜像安全及镜像仓库安全等。

**容器化部署成为云原生计算环境风险输入源**

网络管控层面，网络的细粒度划分增加了访问控制和分离管控难度，访问控制粒度过粗引入了权限放大的风险导致越权攻击。网络分离管控不合理增加了横向攻击的风险导致威胁扩展；编排组件层面，云原生编排组件存在漏洞及管控风险增加入侵概率，工具自身漏洞导致非法提权和逃逸攻击。编排组件不安全配置引起账户管理问题导致系统入侵，编排工具组件众多、各组件配置复杂，配置复杂度的提升增加了不安全配置的概率；容器镜像层面，镜像构建部署过程不规范引入自身风险。容器化环境的常见风险之一就是用于创建容器的镜像版本存在漏洞，从而导致所部署的容器存在漏洞。同时，镜像来源不可信也可能引发恶意镜像注入，攻击者可将含有恶意程序的镜像上传至公共镜像库，诱导用户下载并在生产环境中部署运行，产生安全问题。运行时层面，容器特性增加云原生运行时逃逸风险和威胁范围。逃逸风险对于容器化的云原生场景是一个不可避免的风险面，特别是在多业务系统、多租户环境下，风险更高，直接危害了底层宿主机和整个云计算系统的安全。造成容器逃逸的因素主要有容器环境配置不当、危险挂载、程序漏洞、宿主机内核漏洞等。

**开源社区提供了基础的单点防护工具**

云原生计算基金会（CNCF）托管的安全项目中已初步具备了对容器镜像、身份认证、基线扫描等风险的单点防护能力，典型的工具如下：

· Clair

Clair 的目标是能够从一个更加透明的维度去看待基于容器化的基础框架的安全性。通过对镜像的分层文件系统进行扫描，发现漏洞并进行预警，使用数据是基于 Common Vulnerabilities and Exposures 数据库（简称 CVE），各 Linux 发行版一般都有自己的 CVE 源，而 Clair 则是与其进行匹配以判断漏洞的存在与否。

· dex

dex 是一个基于 OpenID Connect 的身份服务组件，用来进行用户认证和授权，并提供基于多种标准的身份服务和认证解决方案。dex 的设计采用了安全和加密的最佳实践来最小化攻击者获得系统访问权限的风险，dex 的架构划分也可以减轻任何单个攻击可能带来的损害。例如，dex 缺省使用 token 生命周期管理，并自动轮换签名密钥。由于密钥本身是加密的，攻击者需要在短时间内同时侵入数据库和一个 dex 工作节点才能得到 token。

· kube-bench

kube-bench 是针对 Kubernetes 的安全检测工具，根据 CIS 的安全性最佳实践检查 Kubernetes 是否安全。kube-bench 可以运行在本地或 Kubernetes 集群环境中，根据执行的测试结果推荐一些可用于 master 或 worker 节点的安全配置。kube-bench 通过运行符合 CIS Benchmark 的测试来实现，并获得总结性的信息及相关的修正建议。例如，如果 kube-apiserver 上关闭了身份认证，给出的建议中会解释如何启用身份认证，进行相关修正操作之后，可以再次运行这个工具进行检测，直到完全符合安全标准。

· Falco

Falco 是一个云原生运行时安全系统，可与容器和原始 Linux 主机一起使用。它由 Sysdig 开发，是 CNCF 的一个沙箱项目。Falco 的工作方式是查看文件更改、网络活动、进程表和其他数据是否存在可疑行为，然后通过可插拔后端服务发送警报。通过内核模块或扩展的 BPF 探测器在主机的系统调用级别检查事件。Falco 包含一组丰富的规则，编辑这些规则以标记特定的异常行为，并为正常的计算机操作创建白名单规则。

· Open Policy Agent

在应用开发中，应用程序往往需要根据特定策略的决策结果来判断后续执行何种操作。比如，权限校验就是策略决策的一种典型场景，它需要判断哪些用户对哪些资源能够执行哪些操作。这些策略可能随着时间需要不断的动态更新。当前策略决策的逻辑往往硬编码实现，在软件的业务逻辑中，当需要更新策略规则集时，还需要修改应用代码、重新部署应用，非常不灵活。Open Policy

Agent，简称 OPA, 为这类策略决策需求提供了统一的框架与服务，将策略决策从软件业务逻辑中解耦剥离，将策略定义、决策过程抽象为通用模型，实现为一个通用策略引擎，以便适用于广泛的业务场景。

## 全生命周期全要素覆盖，构建云原生安全一体式防护体系

云原生技术栈的延展突破了传统的安全防护框架，初期的云原生安全产品大多从云原生安全的一个维度切入，导致云环境下安全孤岛和整体复杂性增加，缺乏端到端的可观测性，云原生安全保护需要一种从开发到运行时全生命周期的一体化防护方案。

Gartner 提出了云原生应用保护平台（CNAPP）模型，模型包含制品安全、云基础设施安全和运行时安全等内容，旨在整合工具和安全平台，将安全性和合规性视为跨运营和安全团队的连续统一体，从而提高云原生的安全性和工作负载可见性。

中国信息通信研究院也牵头编制了《云原生应用保护平台（CNAPP）能力要求》标准，标准中定义了制品安全、运行时安全和基础设施安全领域的多种云原生安全功能，同时具备研发与运营阶段全流程的信息双向反馈和一体化管控能力，实现价值流动，助力企业构架高效便捷的云原生安全防护体系。

**融合应用云安全防护模型夯实基础设施安全**

云基础设施安全主要从基础设施及代码（IaC）安全、权限管理（CIEM）、云安全态势管理（CSPM）和云原生安全态势管理（KSPM）四个层面进行安全能力的构建。基础设施及代码（IaC）安全层面，通过将虚拟机、网络、负载均衡、数据库等应用转化机器可读的定义文件，实现基础设施管理与持续集成持续交付（CI/CD）工作流的融合，能够解决原有 IT 基础设施管理的成本过高、可扩展性和可用性不足、监控和性能可见性不够及配置不一致等问题，IaC 安全应具备多种常见类型的 IaC 文件安全检测、风险扫描、可视化展示，并提供风险描述及安全加固建议等能力；权限管理层面，由于云原生应用的短暂性，用户身份凭证需要具备频繁轮换的能力和限制受损凭证影响范围的能力，以适应对高速云原生应用的需求。为了进一步有效地保护环境，以及驻留在其中的数据，需要具备对用户、设备、应用服务的联合身份管理技术，对应用和工作负载做到相互认证彼此通信，实现在多云环境中最小特权原则，以减少过多的权限、访问权限和云基础架构权利；云安全态势管理（CSPM）层面，现代 IaaS 和 PaaS 工作负载的复杂性和规模继续呈指数级增长，为了防止配置错误导致整体工作负载风险，应具备对云资产的安全管理能力，如云资产管理、安全基线检测、云主机风险评估、安全策略管理；云原生安全态势管理（KSPM）层面，KSPM 是一套用于自动化地强化 K8s 集群的安全性和合规性的工具，KSPM 相较于云安全姿态管理（CSPM），CSPM 处置企业的所有云基础设施，而 KSPM 则关注 K8s 的

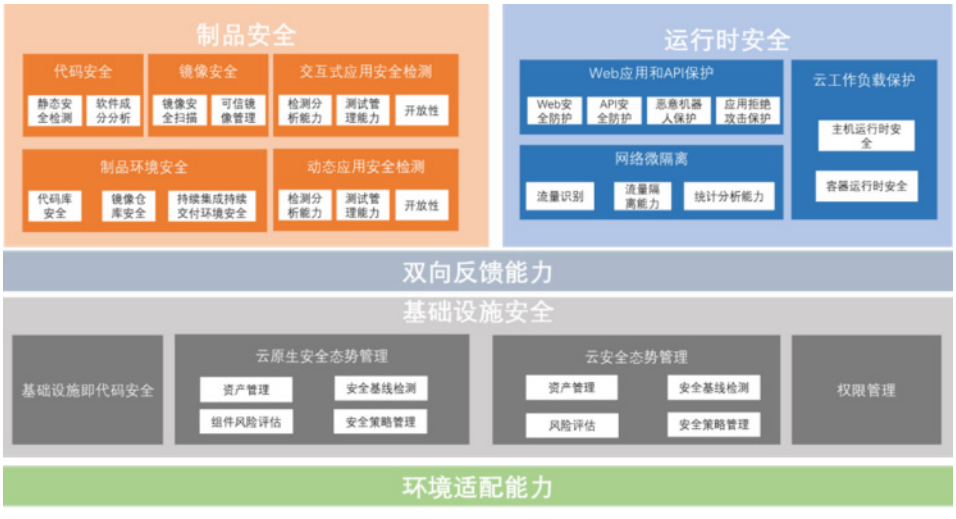



图 1 云原生应用保护平台（CNAPP）能力架构图

安全性。完整的 KSPM 应具备资产管理、安全基线检测、组件风险评估及安全策略管理等方面的能力。

**全流程安全左移打造云原生制品安全**

云原生制品安全主要从代码安全、镜像安全、安全检测（包括交互式应用安全检测和动态应用安全检测）和制品环境安全四个层面进行安全能力构建。代码安全方面，重点考虑静态安全测试和软件成分分析，通过分析应用程序代码进行安全漏洞的检测并管理导入或使用的开源组件，在开发阶段对应用程序的安全性进行全面检测，从而发现安全漏洞，确定应用程序是否易受攻击；镜像安全方面，需具备镜像安全扫描能力和可信镜像管理能力，帮助用户提前发现容器镜像中存在的漏洞、恶意代码、敏感文件等所面临的威胁及其存在的脆弱性，并进一步开展修复工作，从而有效降低生产环境的安全风险；安全测试方面，需尽可能构建多样化互补的安全自动化测试能力，让应用中存在的安全漏洞、不安全方案尽可能在上线前暴露出来并及时修复，以显著降低应用研发迭代过程中的安全问题、修复成本以及线上安全风险，重点能力包括动态应用安全测试、交互式应用安全测试；制品环境安全方面，重点围绕镜像仓库、代码库及持续集成持续交付环境等环境的安全能力建设展开。镜像仓安全应具备仓库自身安全、镜像拉取安全及镜像安全扫描等方面的能力，代码仓库安全应具备仓库自身安全及源代码扫描等方面的能力，并具备持续集成持续交付环境及制品安全加固的能力。

**关注应用全生命周期防护打造云原生运行时安全**

云原生运行时安全主要从 Web 应用和 API 保护（WAAP）、网络微隔离和云工作负载保护（CWPP）三个层面进行安全能力的构建。云原生应用大多通过 Web 和 API 方式对外提供服务，随着云原生架构下微服务的增多，API 数量激增，微服务间的网络流量多为东西向流量，无法通过传统边界防御的方式检测。Web 应用和 API 保护（WAAP）层面，核心安全能力应包括 Web 应用防火墙、API 保护、Bot 防护和 DDoS 攻击防护，多角度全方位地扩展云上应用安全防护范围和安全深度；网络微隔离层面，需要具备流量识别、流量隔离和统计分析能力，能够识别云原生网络流量基本信息及异常行为，对不同的流量特征进行精准隔离，对不同维度的流量日志的统计分析与可视化，以及自动化产生隔离策略实现对网络流量的闭环管理；云工作负载保护（CWPP）层面，主要围绕主机运行时安全和容器运行时安全展开。主机运行时应具备资产清点、风险发现、入侵检测与响应处置等方面的能力，为物理计算机、虚拟机（VM）、容器和无服务器工作负载提供统一的可见性和控制力。在运行时 CWPP 应该保护工作负载免受攻击，通常包括系统完整性保护、应用程序控制防护、内存保护、行为监视、基于主机的入侵预防、可选的反恶意软件保护和容器运行时的入侵检测与响应、处置等方面的能力。

**建立双向反馈通道强化云原生安全体系**

云原生应用保护平台应具备双向反馈能力和环境适配能力。双向反馈层面，具备与 DevOps 工作流中各阶段的安全检查工具进行集成的能力，实现检查结果统一管理，并能够将检查结果与开发构建、测试运行和生产运行各阶段的数据进行关联分析，如问题镜像是否在运行、运行容器中有漏洞软件包是否为在组件库中的位置。同时应具备在 DevOps 工作流中提供控制能力、安全风险分析能力和控制策略设置能力，也应具备安全问题修复全流程的跟踪管理能力，能够分发修复任务并跟踪问题修复的全流程，实现应用开发与运营全生命周期的安全管理；环境适配层面，云原生应用保护平台应具备一定的环境适配能力，包括边缘、多云、混合云等云环境适配、CICD 环境适配和异构兼容、信创兼容的物理节点适配。

## 结束语

云原生安全作为云原生技术与安全融合的新兴领域，正在成为企业和用户关注的焦点。中国信息通信研究院发布的云原生应用保护平台模型，作为业内首个系统性的云原生安全防护体系模型，将为服务商安全产品演进和用户能力建设提供重要参考。未来，中国信通院还将深耕云原生安全技术领域，深化云原生安全平台建设，为用户提供安全自检和攻防演练等公共服务能力，帮助企业定位云原生系统安全问题，验证安全防护能力。

# 云原生应用保护平台（CNAPP）：落地云原生安全的核心抓手

作者 奇安信云安全研发总监 鲍坤夫

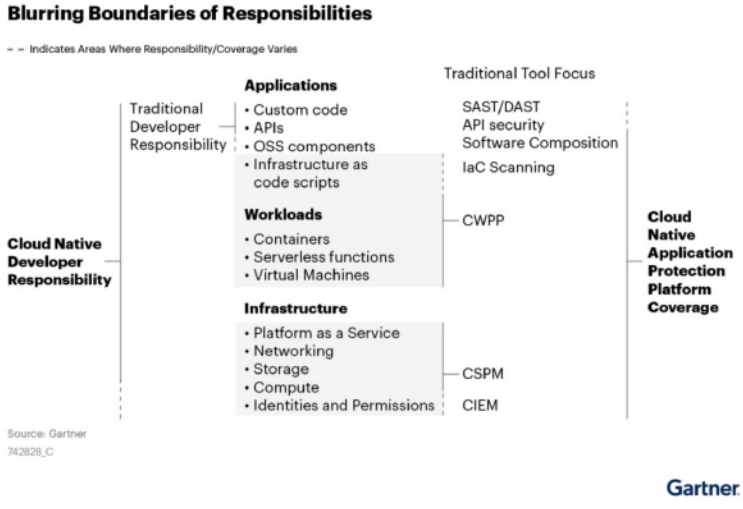
随着云原生技术在国内外的广泛应用，企业数字化转型的进程也不断加快，但安全维度能力缺失明显。一是现有合规要求无法全面覆盖云原生场景，二是现有安全防护手段无法有效针对云原生架构进行安全防护。于是 DevSecOps 及安全左移相关的理念相继提出，狭义的理解是要在开发阶段引入必备的安全能力，广义的理解和三同步相呼应。具体到云原生场景，就是要在云原生应用的规划阶段就做好安全设计，并要求云原生安全的整体方案能够覆盖到运营阶段。

基于此，作为整体解决方案的云原生应用保护平台（CNAPP）应运而生。

## 什么是云原生应用保护平台（CNAPP）

2020 年 Gartner 发布了云原生应用保护平台创新洞察报告，使 CNAPP 成为时下流行的安全语。然而，CNAPP 不仅仅是一种炒作的新安全工具。CNAPP 是一个平台，旨在为具有云原生工作负载的现代企业用单一的整体安全解决方案替换多个独立工具。Gartner 定义了 CNAPP：云原生应用程序的最佳安全体系需要一种集成性的平台，这种平台从开发阶段开始，延伸到运行时保护。企业管理者应该评估新兴的云原生应用保护平台，这些平台为云原生应用的安全提供了一个全生命周期的防护。

Gartner 定义的 CNAPP 强调企业需要专注于云原生安全解决方案，这些解决方案提供完整的生命周期方法来实现应用程序安全，而不是简单的拼凑安全工具。随着云原生技术在国内的快速和大量普及，2022 年信通院牵头发起了 CNAPP 标准框架的定义和能力要求，包括制品安全、基础设施安全和运行时安全三大能力域，覆盖云原生应用研发运营全生命周期，同时兼顾平台的双向反馈和环境适配能力，共计 15 个功能模块，包含 500+ 个能力项，全面详细地评估了云原生应用的安全防护能力。总之，CNAPP 不是一个单一的工具，它是以应用为中心，覆盖云原生整体技术架构和云原生应用全生命周期的整体安全解决方案。



## 为什么需要 CNAPP


为了解决云原生应用的基础设施和全生命周期过程中的风险，出现了 CWPP、CSPM 等云原生安全工具或者产品，但是这些工具或者产品只是为了解决单一的安全问题，也只聚焦在生命周期的某个阶段。DevOps 改变了传统应用的开发模式，将开发和运维过程连接起来，保持云原生应用从开发到运维的一致性，并强调可观测性，如果安全的运营流程不能打通应用开发到运维的过程，会导致没有办法观察应用全生命周期安全风险，也没有办法制定覆盖从开发和运行时的一致安全策略，给云原生应用的安全运营过程造成巨大困扰。

这些困扰包括：

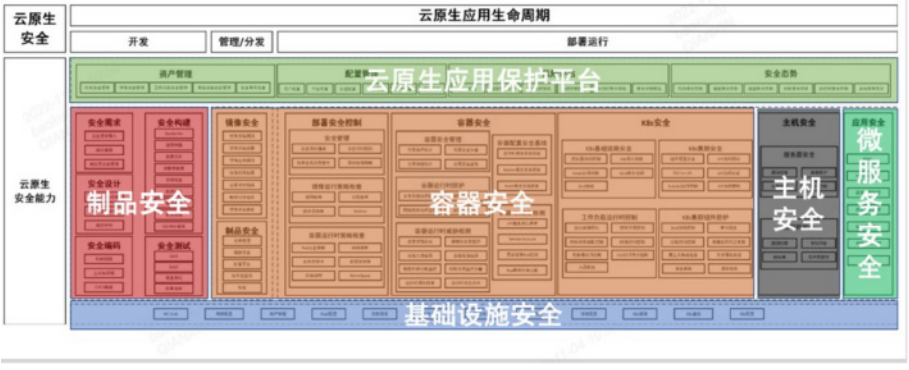
第一，在云原生供应链安全管理场景中，如果只在开发阶段关注供应链安全问题并不能解决云原生应用全生命周期供应链安全问题，例如，代码违规提交，镜像违规分发和部署导致供应链监控盲点，我们应该怎么发现和监控到这些问题？另外，在日常漏洞运营过程中，如果通过威胁情报等渠道发现新的供应链安全漏洞后，我们应该怎么快速评估和定位哪些业务或者应用正在受影响？

第二，在云原生安全风险评估场景中，我们通过各种安全工具或者平台发现了大量安全漏洞后，怎么评估哪些漏洞应该被高优先级修复？漏洞修复前还有业务在开发、在部署、在上线怎么办？另外，怎么评估漏洞是在生命周期哪个阶段、哪个时间引入的，以及谁引入的？还有没有其他应用正在受影响？应该采取哪些措施防止风险进一步漫延或者缓解风险？

第三，在云原生安全治理场景中，我们怎么评估企业里面哪些应用风险最高？哪个业务部门风险最多？哪个容器镜像的风险影响面最大？另外，在云原生应用开发流程里面哪个阶段引入或者发现的风险最多？我们应该优先改进哪个流程？从上面这些问题可以看出，多个、脱节的解决方案在可见性和集成复杂性方面天然地存在隔阂和间隙。这意味着 DevSecOps 团队需要做更多的工作，来降低跨企业工作负载的可观察性。而通过使用 CNAPP，企业可以解决这些问题并改善其整体安全状况。

## 如何实现 CNAPP？

奇安信研究了国内外 CNAPP 各种安全框架，包括 Gartner 云原生安全技术体系和 CNAPP 平台定义，以及国内信通院 CNAPP 能力要求，并结合奇安信内生安全理念，设计了适合国内云原生安全场景的 CNAPP 安



全框架，如下图所示。

不难看出，整个框架以应用为中心，安全能力覆盖整个云原生架构，以及云原生应用的全生命周期。其中纵向从下到上覆盖云原生应用运行的基础设施，包括 IaaS 平台、PaaS 平台、主机及容器工作负载，以及应用自身对应的微服务；横向从左到右覆盖云原生应用的整个生命周期，包括开发、部署和运行时。

值得注意的是，CNAPP 平台作为提供云原生安全防护与运营能力的平台，自身不需要具体实现从基础设施层到应用层的各种安全能力，而是通过对接这些能力来实现云原生全生命周期安全运营的效果，包括数据采集和分析、策略下发和告警响应处置等。

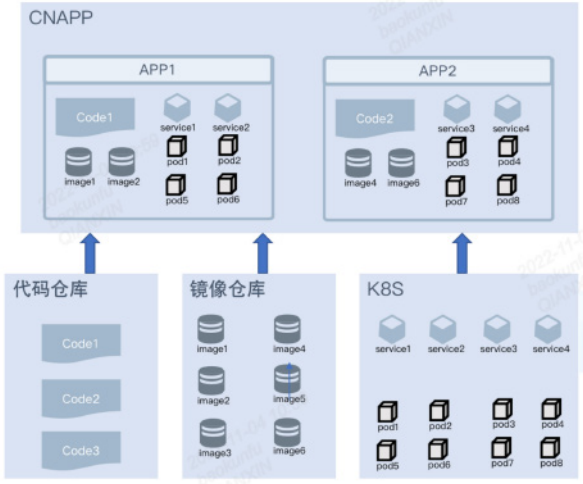
CNAPP 平台应包含四个核心能力模块，我们认为分别是资产管理、配置管理、风险评估和安全态势。企业依托平台的这些功能模块，可以实现云原生应用全生命周期安全运营。

**首先是云原生资产管理**

CNAPP 的资产管理模块包含云原生资产定义、云原生资产采集和云原生资产关联三个过程。其中，云原生资产的定义非常关键，传统环境或者云环境的资产定义比较简单，一般是以工作负载的 IP 为主，结合其他业务属性进行定义，并把资产等数据保存在 CMDB 等系统中。但是云原生技术出现后，因为容器 IP 的不固定，这种单纯以 IP 定义并管理资产的方式不再适用，同时传统环境或者云环境一般只关注应用运行时资产，没有覆盖应用的开发和部署阶段。

因此在云原生场景下，资产需要被重新定义，需要以应用为中心并覆盖应用的全生命周期。

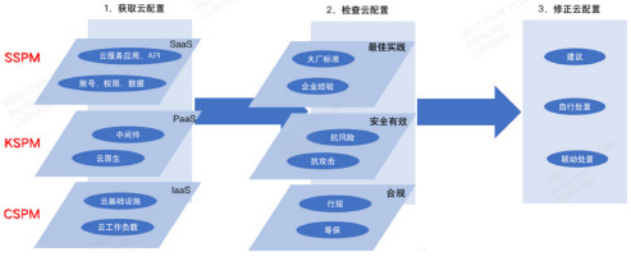
云原生应用在生命周期各个阶段的资产形态不一样，需要把它们都定义出来，包括代码、镜像、集群、nodes、namespace、service、pods、进程和端口等。云原生资产定义好后，就需要进行云原生资产的采集，需要从云原生应用生命周期的各个阶段进行采集，包括代码仓库、镜像仓库、k8s 集群和运行时容器等。最后资产采集回来以后，需要围绕应用将生命周期各个阶段的不同资产进行关联，为后面安全能力的关联、风险关联和态势分析打下基础。




**其次是云原生配置风险管理**

在业务向云原生技术架构转型过程中，云平台的配置风险和云原生平台的配置风险是最容易被忽略的，一方面是因为用户对云产品或者云服务的配置不熟悉，容易配错，另一方面是缺乏一些工具方便用户进行配置检查和问题修复。

CNAPP 的配置管理模块用于解决云原生应用整个运行环境的配置安全，包括云平台、容器编排平台、主机以及容器等工作负载，它通过从 CSPM、KSPM 及 CWPP 产品中采集配置数据并进行集中分析，按照优先级给出配置风险和修复建议，并且在应用整个生命周期

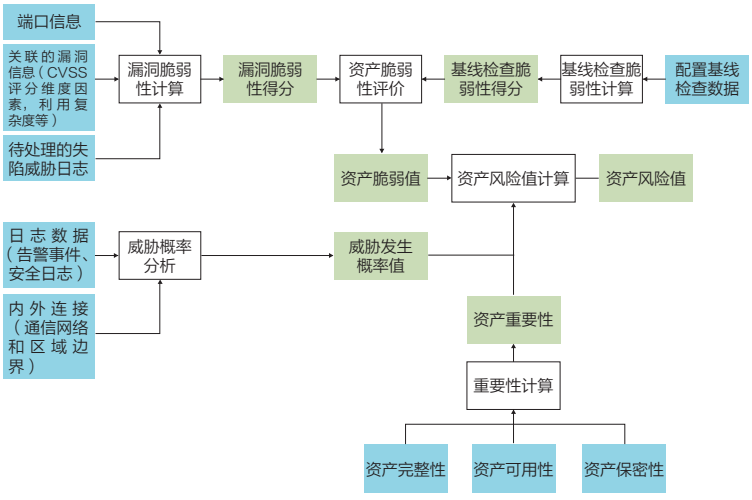


中持续进行监控，保证应用全生命周期配置安全。

**第三是云原生风险评估**

在日常安全运营过程中，漏洞的修复和告警处置是最重要的工作之一，但是面对大量漏洞和海量告警时，漏洞修复和告警处置的优先级就成了一个问题。

CNAPP 的风险评估模块通过多源数据汇总计算、叠加网络暴露面计算并结合资产重要性等业务属性对资产的风险进行整体评估，给出漏洞修复和告警处置的优先级。其中多源数据汇总计算除了结合云原生应用的漏洞、基线和弱口令等脆弱性数据，还结合了应用的流量及告警威胁数据，进行实时动态计算。叠加网络暴露面计算是指会根据云原生资产的网络拓扑及流量数据，计算云原生应用的南北向和东西向暴露面。最后根据资产的标签或者分类属性，结合资产的重要性等业务属性进行综合风险评估。




**第四是云原生安全态势**

CNAPP 的安全态势模块用于辅助企业从宏观角度了解企业所有业务的整体风险情况。其中，面向业务的态势分析，包括可视化展现应用态势、镜像态势和租户态势，指导需要重点改进的业务部门及应用，而面向 DevOps 流程的态势分析，包括可视化展现开发态势、部署态势和运行时态势，指导需要重点改进的流水线阶段。


## 结语

云原生时代，需要建设以云原生应用保护为核心的 CNAPP 平台，为云原生应用提供全生命周期的安全防护及可视化，同时具备云原生应用的风险评估和全流程管理能力，为云原生应用提供事前安全预警分析、事中攻击威胁实时检测、事后响应处置的云原生安全运营闭环，全方位保护云原生应用全生命周期安全并满足监管合规要求。奇安信通过打造一系列全部云原生化的研发平台，支撑安全产品和安全服务的云原生化，为客户业务云原生转型提供全套完整的云原生安全解决方案。

奇安信 CNAPP 能力基于云原生化的大禹平台，覆盖各种公有云、私有云、混合云及云原生环境，通过定义标准的资产、漏洞、基线、日志和告警等 LDM 模型，支持海量数据的采集、分析和存储，为客户业务数字化转型提供一体化的全生命周期安全解决方案。

随着云原生正式开启云计算的下半场，云原生安全也将是未来几年云安全的主要发展方向。CNAPP 作为云原生安全的整体解决方案，也将值得更多企业进行深入探索和实践。

# 云原生场景下的容器安全风险与实践

作者 容器安全资深专家 王亮

云原生安全是指云平台安全原生化和云安全产品原生化。作为一个全新的安全理念，云原生安全旨在将安全与云计算深度融合，推动云服务商提供更安全的云服务，帮助云计算客户更安全的上云。

安全原生化的云平台，一方面通过云计算特性帮助用户规避部分安全风险，另一方面能够将安全融入从设计到运营的整个过程中，向用户交付更安全的云服务；原生化的云安全产品能够内嵌融合于云平台，解决用户云计算环境和传统安全架构割裂的痛点。

作为云原生场景下的主要工作负载，容器的特点决定了它并不像过去虚拟机那样，不同机器之间有着强隔离机制，因此容器安全面临着更加严峻的挑战。

## 容器面临三大安全风险

具体而言，容器主要面临的风险包括以下三个方面。

首先是网络隔离风险。容器调度集群 kubernetes 的命名空间并没有网络隔离的效果，默认情况下 pod 之间能互相访问、pod 能访问宿主机，比如，可以访问宿主机上的服务、可以访问“宿主机所在网络”的服务，当然也可以访问集群 service 和其他 pod，并且不受“kubernetes namespace”限制。

需要注意的是，kubernetes namespace 不是内核的 namespace，而是“项目”的概念。一个项目属于一个 kubernetes namespace。

其次是容器逃逸风险。“容器逃逸”是指攻击者在获得容器的控制权限之后，利用容器内某些命令执行能力，进而获得该容器所在的直接宿主机上执行攻击命令的权限。与虚拟化技术类似的是，逃逸同样是容器最为严重的安全风险，直接危害了底层宿主机和整个云计算系统的安全。

通常情况下，容器逃逸攻击包括以下几个场景。

其一是在容器中就可以访问特殊网段的“元数据服务”，攻击者可通过 metadata 中的 etcd 凭证获取 k8s 集群权限，或者通过漏洞获取云 metadata 中的集群证书信息。

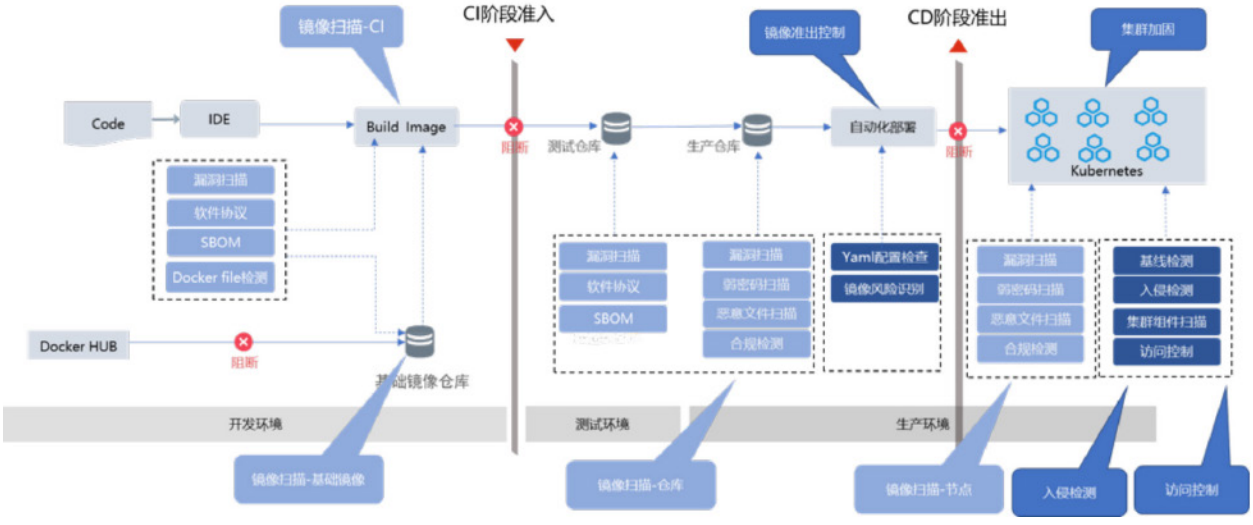
其二是通过容器中挂载宿主机根目录到容器后写入 ssh key，然后在容器中连接宿主机 ssh 可逃逸到宿主机。挂载宿主机目录后，也可以用 static pod、cron 服务来做攻击。

其三是利用内核漏洞做容器逃逸，修改容器进程 task_struct 数据结构的 nsproxy、cred 字段，修改命名空间和 capability。

最后是容器镜像风险。镜像中的基础镜像、安装的软件有可能版本比较低，存在历史漏洞。尽管这种漏洞不一定能够被攻击者直接利用，但提供镜像的服务商依然需要重视这类风险。

风险更大的场景是镜像中存在研发运维留在镜像中的敏感信息，比如，pod 中的应用想要和云服务通信时需要有 ak/sk 来签名或者 sts，所以反编译应用或者查看环境变量后能看到 ak/sk 或者 sts。

当然，除容器本身所面临的的安全风险外，云原生




安全的 4 个 C，包括云（Cloud）、集群（Cluster）、容器（Container）和代码（Code），每个层面的安全风险，也都有可能直接或间接威胁到容器的运行。

## 全生命周期的容器安全最佳实践

针对容器面临的安全风险，奇安信提出了贯穿云原生全生命周期的安全理念，分别在开发、运行的不同阶段部署进行检测，包括在 CI/CD 阶段进行镜像使用控制，运行时阶段进行入侵检测、访问控制、集群加固等安全能力。

在镜像安全方面，镜像可裁剪到只留下必要的可执行文件，再加上面的运行时监控，就能削减很大的攻击面，容易发现威胁。启动镜像扫描任务后，首先会从镜像仓库下载镜像，解压镜像，启动镜像文件分析，CVE 漏洞扫描、恶意文件扫描等。

在运行时访问控制方面，应当采用如下隔离访问控制策略，包括 pod 不能主动访问“宿主机所在的内网”、pod 不能主动访问宿主机、pod 不能主动访问虚机 metadata、pod 能主动访问外网、同一个“k8s namespace”下 pod 网络可以互通，但不同“k8s namespace”下 pod 网络不通，以及不限制宿主机网络（node 可以自有访问 master 和外网）等。

不过需要注意的是，集群的网络策略并不能完全实现上面要求的网络隔离效果，因为它的默认策略是拒绝，用户只能加白。所以用户还需要借助其他的手段来做网络隔离，如 iptables 等工具。

在运行时入侵检测方面，首要步骤是安装安全监控进行容器信息数据采集，入侵检测技术的可靠与否很大程度上取决于采集的前期数据是否准确。现有的容器安全监控主要分为两类，第一类方案借鉴传统主机在系统中添加安全服务的方式，通过在容器中添加监视代理监控其异常行为；第二类方案采用无代理监控方式在容器外部对容器进行监控。进行容器入侵检测方法会采用这些检测工具帮助完成获取容器信息。

根据检测源的不同，容器入侵检测技术可分为基于主机的异常检测技术和基于网络的入侵检测技术。

在传统主机领域下基于系统调用的入侵检测方案，往往针对单一特权进程的运行行为进行监控，而在容器环境下引入了更多的安全风险。对异常识别来说，重要的表征是特征选取的是否合适。系统调用作为应用程序访问操作系统服务的接口，容器的攻击行为通常可以通

过系统调用来表现。

基于主机的容器安全入侵检测还可以对特定行为进行异常检测。针对 docker 面临的被恶意用户利用内核漏洞进行攻击的行为，基于进程所属命名空间状态的检测方法检测容器逃逸，这种方式也可看作为基于容器安全机制的异常检测方法。由于 docker 容器的本质是进程，容器内的进程相当于守护进程的子进程，通过获取当前进程的状态标识与初始化进程（宿主进程）的状态标识进行对比，如果相同则判定异常。这种方法能够有效检测出容器逃逸攻击行为。

| Kubernetes 基础架构关注领域 | 建议 |
| --- | --- |
| 通过网络访问 API 服务（控制平面） | 所有对 Kubernetes 控制平面的访问不允许在 Internet 上公开，同时应由网络访问控制列表控制，该列表包含管理集群所需的 IP 地址集 |
| 通过网络访问 Node（节点） | 节点应配置为仅能从控制平面上通过指定端口来接受（通过网络访问控制列表）连接，以及接受 NodePort 和 LoadBalancer 类型的 Kubernetes 服务连接。如果可能的话，这些节点不应完全暴露在公共互联网上 |
| Kubernetes 访问云提供商的 API | 每个云提供商都需要向 Kubernetes 控制平面和节点授予不同的权限集。为集群提供云提供商访问权限时，遵循对需要管理的资源的最小特权原则 |
| 访问 etcd | 对 etcd（Kubernetes 的数据存储）的访问应仅限于控制平面。根据配置情况，应该尝试通过 TLS 来使用 etcd |
| etcd 加密 | 在所有可能的情况下，最好对所有存储进行静态数据加密，并且由于 etcd 拥有整个集群的状态（包括机密信息），因此其磁盘更应该进行静态数据加密 |

与此同时，随着网络流量的增加及攻击变得更加广泛复杂，基于网络的容器异常入侵检测也成为了容器运行时的重要检测手段。该技术能够基于容器集群内流量获取并对流量中的数据进行还原，根据攻击特征分析发现来自网络的攻击。

在运行时集群安全方面，用户需要根据应用程序的受攻击面，关注安全性的特定面。集群安全包括集群组件漏洞、集群配置错误。其中集群配置错误风险在近几年频繁出现重大安全事故。下表列出了安全性关注的领域和建议，用以保护 Kubernetes 中运行的工作负载。

## 六大优势筑牢容器安全防线

基于上述实践，奇安信容器安全产品具备以下六大优势：

第一，功能全面。产品同时具备主机与容器多种云工作负载安全防护能力，其中容器安全防护覆盖了容器构建、分发、运行全生命周期安全需求。

第二，安全左移。产品可检测镜像所包含的开源组件许可证，可基于开源许可证类型阻断 CI 阶段构建流程。

第三，全面兼容。产品支持主流的 Docker Registry、Harbor、Jfrog、AWS 等 12 种镜像仓库对接；支持 k8s、华为 CCE、AWS、Openshif、阿里云、腾讯云、灵雀云等混合云环境。

第四，支持多种防护阻断能力。产品支持集群计算节点文件防篡改、集群容器网络 L3-7 层访问控制、集群容器中的进程阻断及风险镜像启动阻断。

第五，强大的安全运维能力。产品支持任务进度可视化，实时查看相关检测流程任务执行过程，提高安全运维效率。

第六，强大的多维度可视化展示镜像、pod、Node、命名空间、service、controller 等的访问关系、漏洞信息。可进行实时流量采集下载，提供离线网络分析数据。

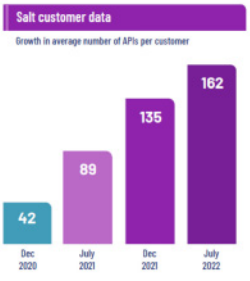
# 云原生时代 API 安全防护漫谈

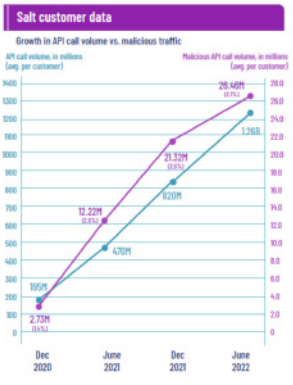
作者 奇安信网络探针事业部研发总监 姚翼雄

## API：云原生时代核心资产

数字化转型、发展数字经济是“十四五”期间的主旋律，数据、连接和智能是数字化转型的三个核心。数字化转型加速了业务系统向云原生信息基础设施的迁移。同时，随着数字化进程的不断深入，数字化、云化、微服务化的相互促进，API 作为连接数据的重要通道、连接数字系统的神经元，其数量正在呈爆炸式增长。

API 已经在物联网、云原生等场景中广泛应用，“API+云服务”的模式已经成为企业对外提供服务的主流模式。


据以色列安全公司 Salt Security 的《State of API Security Report Q3 2022》报告统计：与 2021 年 7 月相比，过去一年平均每个客户的 API 数量增长了 82%，从 89 个增加到 162 个以上，同时平均每个客户的 API 流量增长了 168%。知名 CDN 与安全公司 Akamai 的一项报告也表明：API 请求已占所有应用请求的 83%，预计 2024 年 API 请求数将达到 42 万亿次。

## API 安全已不容忽视

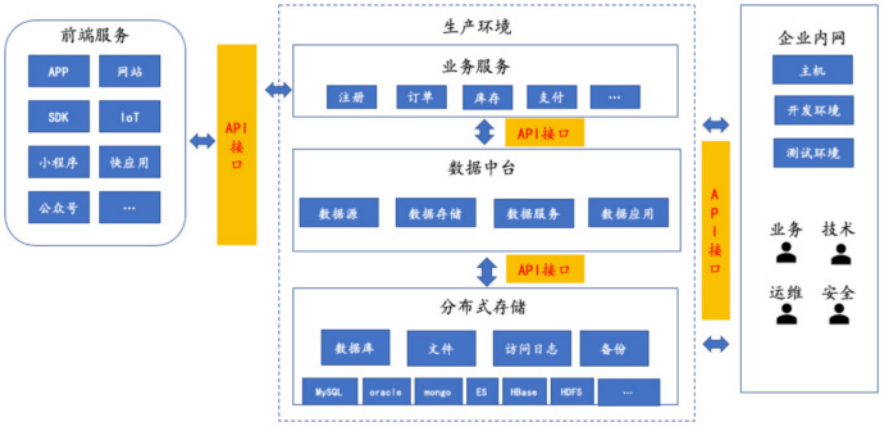
云化、微服务化的变革，使得 API 成为对外业务的最主要入口。业务系统上云后，云上会存在大量承载南北向及东西向流量的 API 接口。

我们可以按照承载的业务类别、暴露面两个维度对 API 进行分类。

承载业务类别：可以划分为对外提供服务的 API 和对内的 API。 主要的类型有自研的业务 API，公共组件 API 及第三方 API。

暴露面：可以分为已知 API 和未知 API 的暴露面。如没有进行登记就使用的、开源组件默认开放的 API、僵尸 API 等。

这些 API 形成了新的暴露面，让攻击面变的更加多样复杂，API 成为企业数据泄露及被攻击的最大风险敞口。由于 API 安全防护的缺失，组织对外暴露了哪些 API、有哪些 API 存在风险、是否涉及非法传输敏感数据等问




题都成了“灯下黑”。风险一旦演变为真实威胁和事件，后果会非常严重、恶劣。

以数据泄露为例，下面是两个因 API 安全问题而导致最终发生数据泄露事件的典型案例：

2021 年 4 月，Facebook 平台上有 5 亿的用户数据泄漏，起因是因为在线业务 API 遭到滥用；

2021 年 6 月，某电商企业 11 亿条用户信息泄露，调查结果显示有黑产通过订单评价的 API 绕过平台风控批量爬取信息。

考虑到涉事机构自身的安全能力、这两起恶性安全事件发生的时间及最终数据泄露的规模，越来越多政企单位的安全负责人已经意识到，API 的安全已经不能再置之不理。

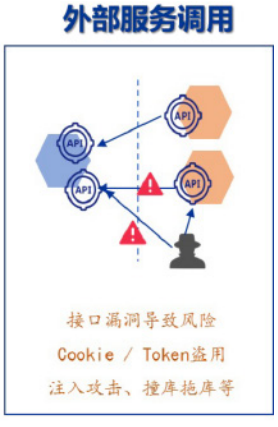
## 云原生时代需要新的 API 安全

云原生时代，新的技术栈层出不穷，让人应接不暇。新场景也催生了不同新的 API 的发展及应用。除了大家熟知的 RESTFUL API，GraphQL、gRPC 等不同的 API 技术也得到了大量应用。这些新技术栈、新 API 类型，让传统的 API 安全手段越来越难以起到应有的效果，给攻击留下空间。

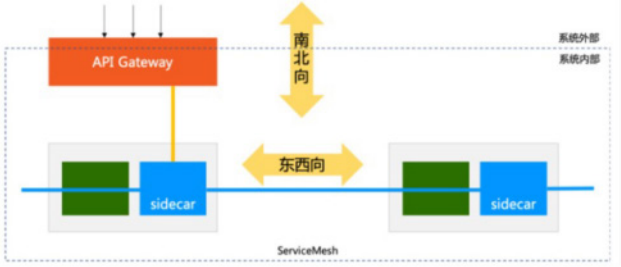
## 更复杂的暴露面、更多样的 API 攻击

企业对外提供服务的南北向 API，一般会通过 API 网关、k8s ingress、Istio gateway 等方式对外暴露；业务系统之间也存在大量的东西向 API 交互，可能存在未知的 API，如某些开源组件默认开放等情况。业务间不断增多的 API 调用也让利用 API 漏洞进行横向攻击的风险不断增加，如存在未授权访问的漏洞等，这些因素使得云原生场景下安全问题更加复杂严峻。






从 API 的攻击手法来看，针对 API 的攻击出现了许多新的攻击手法， 典型的如 OWASP API security TOP 10，当然还有更多针对 API 的攻击手法。 同时 API 攻击也包含了大家所熟知的一些攻击手法，如注入攻击、DDoS 攻击等，但是这些传统的攻击手法，在表现形式上也发生了很大变化。如 API 的拒绝服务攻击，可能只需要很小的流量就可以让 API




瘫痪，而且攻击的门槛变的更低，可能只需要一个简单的脚本就可完成攻击。

## 传统 API 安全手段的局限性

目前，针对 API 安全防护的传统做法是改造 WAF 或 API 网关，这种方式存在着较明显的局限性。

首先是核心能力的局限性。

API 网关偏业务保障方向，主要作用一般是以认证、授权、格式转换、业务发布、路由及负载均衡等业务属性为主。

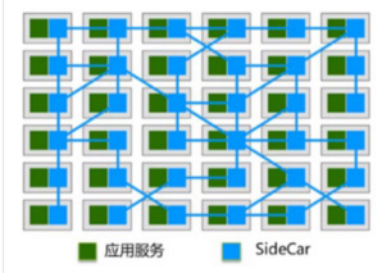
WAF 则是为防护网站而生，网页交互的内容主要是 HTML，主要是静态或动态页面，以前台的操作为主。在防护方面，WAF 主要的能力是以防护网站的漏洞攻击为主，可以做到第 7 层防护。

而 API 安全防护需要做到第 8 层防护。API 交互内容以 JSON/XML 为主，以后台操作为主，重点针对 API 调用过程中的逻辑、参数、数据字段、文件等维度，关注的焦点是以API为核心的调用过程及数据传输过程，应以 API 作为资产核心来进行安全防护。

其次是适用场景的局限性。

WAF 及 API 网关通常部署在出口网关位置，无法解决云原生复杂的东西向安全问题。而 API 安全需要能部署在云原生架构中的多个节点，包括南北向出口、东西向业务节点之间，对整个架构中各类 API 都做安全防护。

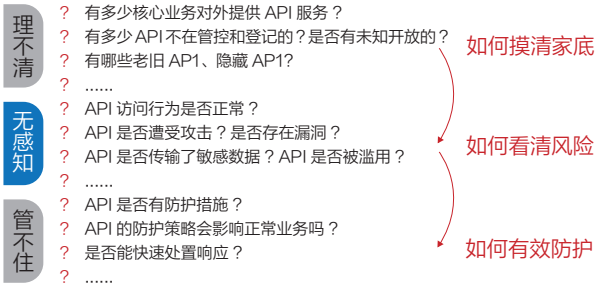
所以 WAF 或 API 网关上功能堆砌的方式，无法真正解决 API 安全问题。 API 安全防护的目标是承载在 HTTP 之上的 RESTFUL、GraphQL、gRpc 等各类




型 API，应足够轻量灵活去适用云原生环境与之融为一体，重点要解决 API 数据通道上的数据安全问题， API 从本质上来说是个数据安全问题。

## 新的对抗空间需要新的 API 安全防护体系

API 当前有三大亟待解决的安全问题：

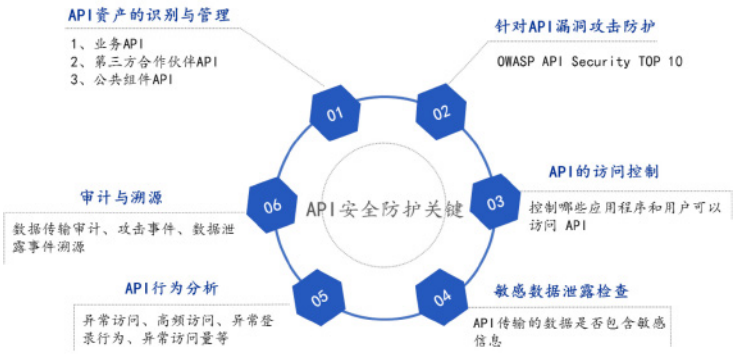



云原生时代的特点与变化，以及当前 API 安全的核心挑战，决定了传统的边界防护思路无法有效应对 API 安全问题。根本原因在于防护模型、防护维度没有发生本质变化。

传统边界防护是以网络通信 4~7 层防护为主，以端、网、云为边界的纵深安全防御体系主要关心南北向流量的安全。而云原生的 API 安全防护则应把重点放在解决 HTTP 之上第 8 层的安全威胁，API 安全能力不仅要围绕云原生、微服务架构进行，同时关注南北向和东西向全流量，还需更关注数据安全问题。

咨询机构 Gartner 在其 API 安全保护的创新洞察《Innovation Insight for API Protection》中表示，API 安全保护产品应具备三个主要能力——即发现、状

态管理和运行时保护。拆解来看，我们认为应对云原生 API 安全问题，应具备下图所示的六大核心能力：




具体到云原生场景，API 安全应覆盖微服务南北向、东西向的检测与防护，应足够灵活去兼容适应不同情况，这就需要将 API 安全检测、防护、分析的能力下沉到容器、微服务内部来完成南北向 + 东西向的安全防护。

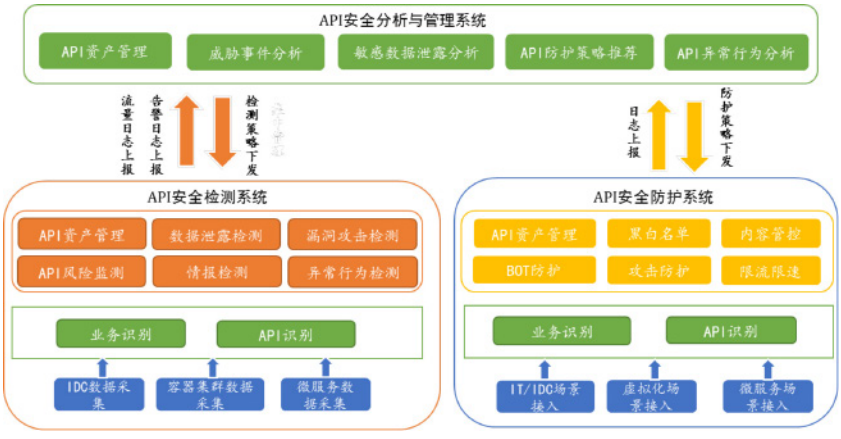

围绕上述关键点，奇安信形成了一整套围绕云原生架构，从发现、检测、分析，到防护的持续闭环监测，一整套的 API 安全解决方案。

奇安信 API 安全卫士适用于任何有 API 存在的场景，其优势在于场景适应全面、分析智能化、全方位的资产梳理和全面的监测与防护能力。API 安全卫士以 API 资产为核心，实现对 API 资产的检测、分析与防护，达到缩小 API 暴露面，关闭 API 的攻击面的目的，帮助客户摸清家底、看清风险、实现有效管控，充分应对云原生时代 API 安全挑战。

奇安信 API 安全卫士绝非凭空出现，而是与奇安信多年在平台能力、安全能力等方面的积累密切相关，这也是我们的核心优势所在。

如 API 的识别能力，奇安信网络探针团队多年在流量侧积累了大量的样本及经验，不同的 API 类型，在海量的样本池中反复训练从而提升识别率；威胁检测能力则集成了集团强大的威胁情报能力；API 安全分析平台基于奇安信大禹平台底座研发，大禹为新一代实战攻防的态势感知平台，其在互联网、工业物联网、移动互联网等不同领域有着广泛的实战应用。

随着数字化转型的发展，API 安全市场将呈爆发式增长，在这个新的安全领域，奇安信 API 安全卫士将继续以客户需求为核心，面向云原生时代，依托集团强大的安全能力、平台能力，不断迭代升级产品核心能力，为客户提供更好的 API 安全解决方案与服务。



# 云安全态势管理（CSPM）：有效管理复杂云环境配置风险

作者 奇安信云安全高级产品经理 马志伟

## 什么是 CSPM？

研究显示，几乎所有对云服务的成功攻击都是客户错误配置、管理不善和错误的结果。如 2017 年，澳大利亚网络安全评估初创公司 UpGuard 研究人员发现，由于亚马逊云服务 S3 存储桶错误配置，上千万 Verizon 客户个人数据存在被泄漏风险。企业网络安全和风险管理领导者应该投资云安全配置管理流程和工具，主动识别和修复这些风险。

在云原生业务场景下，云上配置更加复杂、繁琐，开发模式也转为 DevOps，需要更注重安全左移，即把安全隐患更多地在业务上线阶段排查出并解决。因此，对基础设施（如 IaaS、PaaS、Kubernetes）、开发环境配置（如镜像中的高危配置）等环境设定策略检查也显得尤为重要。

对此，咨询机构 Gartner 提出云安全态势管理（CSPM，Cloud Security Posture Management），专门针对多云、混合云环境，解决 IaaS 或 PaaS 的安全性配置持续验证的难题。CSPM 的最终目标，是基于通用框架、合规要求和企业策略，以自动化的手段，发现现有云服务配置和安全设定中的风险，并提供解决措施。

需要注意的是，此“态势（Posture）”非彼“态势（Situational）”。CSPM 中的态势强调状态，这种状态是基于配置参数、可改变的；而我们熟知的态势感知（Situational Awareness）中的态势，更多是指客户 IT 环境的安全处境，是以客户为原点发散的感知。

## CSPM 的三大关键价值

首先，CSPM 能够让用户从安全角度来看清云资产和云服务配置，进而进行持续的风险评估和管理，在日常安全运营工作中真正做到可验证的缩小暴露面。

安全的基础是保障风险的可见。CSPM 能够对云上

包括计算、存储、网络、数据库、身份（IAM）、容器等资产及其配置进行全方位清点，进而梳理出云上暴露面，做到及早发现、提前处置。

其次，CSPM 能够让运维人员高效的完成云服务配置风险的发现和处置工作，让安全与发展真正统一而不是对立。

CSPM 支持多租户或单个租户多云账号的统一对接。评估任务同时支持人工触发和自动化下发，能够灵活满足对云服务持续“评估 – 验证”的需求。对已发现的错误配置，CSPM 还能实现基于风险的处置优先级建议，以及可选的一键修复响应。这些“智能化”的能力，都让 CSPM 更加易用和友好，成为运维人员得力助手而不是累赘麻烦。

最后，CSPM 是云原生的。这就意味着，用户可以像使用云服务一样便捷的使用 CSPM，同时对主流云平台的基础架构及多云、混合云等场景已经适配，有良好体验和稳定性的。

## 奇安信的 CSPM 落地实践

基于 Gartner 对 CSPM 产品能力的定义及结合国内客户实际业务痛点，奇安信推出的 CSPM 具备以下七大核心能力：

①资产梳理

资产的梳理是安全防护的基础，不仅可以梳理基础的云上资源，还可以梳理出资源之间的访问关系，这样做不仅能以更友好的方式让客户快速梳理出自身资产，还能发现其中某个资源有错误配置时，对整个业务系统的影响做到“心中有数”；

②保护对象覆盖 IaaS 和 PaaS 层

不仅可以对 IaaS 层的资源和服务配置检查，还可以针对云原生环境下广泛应用的公有云或者自建云的 Kubernetes 平台提供资产梳理和配置检查的功能，并且可根据 Kubernetes 下所有容器的访问流量，采集并绘制出拓扑关系图；

③配置的实时、持续检查

针对云配置信息提供实时、持续的检查，一旦发现错误配置及时告警，在最短时间内提醒负责人修复错误配置，并且绘制出配置状态的趋势图供管理员掌握整个云上资源配置的安全趋势；

④可自定义符合客户实际情况的基线检查规则

提供开发定义基线的接口，客户可根据业务实际场景，结合一些基线框架，总结出适用于自身环境的基线检查规则；

⑤报表输出

可以根据时间、基线种类等多个维度输出各种报表，供管理者掌握整体云上配置态势；

⑥开箱即用的基线标准

系统内置多种基线标准，如 CIS 基线、最佳安全实践等。可以满足大部分客户开箱即用；

⑦支持云原生环境部署

产品采用云原生的部署方式，客户可以很便捷地获取安全能力，并且产品自身可以适用多种云平台架构。

目前，某家近万人 IT 企业已部署上线奇安信的 CSPM。该企业业务采用“私有云 + 公有云”的混合云模式部署，使用了多个云厂商提供的云平台。由于采取多云、混合云的部署模式，管理存在难度，尤其公有云部分管理起来较为松散、暴露面多，管理员不清楚云上资产的安全配置状况如何，缺乏整体的配置管理能力。

该 IT 企业的 CSPM 共对接了阿里云、腾讯云、华为云 3 个云平台，采集到的资源包括千余项 IAM（用户、密钥、角色、策略等）、数百个计算虚机、近百项存储（硬盘、文件等）、4 个数据库、7 项网络（负载均衡、ACL 等）及 3 项审计信息。

运维人员通过 CSPM 下发扫描任务，识别出 170 条高危配置项，71 条中危配置项。高危配置项中包含密码策略不合规导致的弱密码可登录问题、开启高风险端口、对象存储 OSS Bucket 允许匿名或公开访问、对象存储 OSS 数据明文传输等存在极高安全风险的问题。

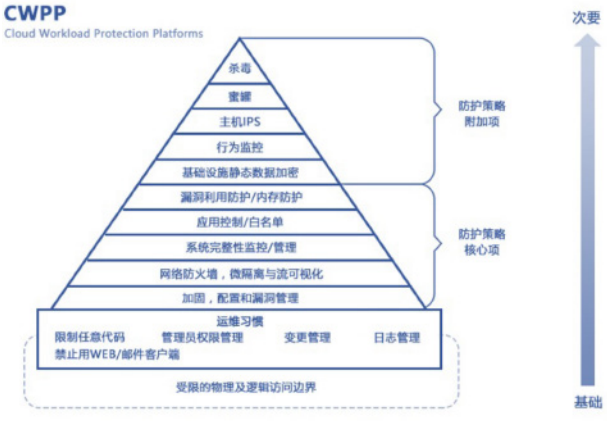
随着混合云、多云及云原生的不断普及，云环境日益复杂化，CSPM 的重要性也愈加凸显，值得更多企业进行深入探索和实践。

# 安全左移与右移，CNAPP 和 CWPP 谁才是工作负载最强守护者

作者 奇安信服务器安全资深专家 李栋

主机安全、服务器安全、杀毒、容器安全已是安全架构中的必备产品，但很多人对于云工作负载保护平台（CWPP）这个词还比较陌生。

简单地说，云工作负载保护平台 (Cloud Workload Protection Platform， CWPP) 就是用来保护物理机、虚拟机、云主机、容器这类工作负载的，Gartner 对 CWPP 的能力做了明确定义，在前几版的能力层次中，包含了对工作负载权限配置、系统、应用、访问权限等多个层次的防护策略，覆盖了 CWPP 整个生命周期。




## Workload 工作负载的演进经历了漫长的过程

在说工作负载安全前，先谈谈工作负载这些年的演进。笔者在十几年前曾就职于某数据中心 IDC 公司，负责客户工作负载的运维和托管，当时最常见的工作负载形态是虚拟空间和物理机。虚拟空间也叫虚拟主机，算是 serverless 的最初形态，客户不需要部署、配置或管理服务器服务，只要上传 dedeCMS、phpwind、discuz 等程序代码就能建立独立网站，这在当时很受中小企业和个人用户的欢迎。在物理机上部署业务是个复杂的过程，物理机上架需要经过“设备采购 – 设备运输 – 机房上架 – 安装系统 – 配置 IP– 部署业务 – 上线运行”的繁琐过程。

出现云主机和容器之后，业务部署效率大幅度提升，一台云主机的部署几分钟内就能完成，容器的加入更是让业务上下线效率大幅度提升。


图：工作负载的演进

## 百炼成钢，CWPP 统一了工作负载的安全需求

“安全需要伴随着业务需求的变化而变化”，前面我们提到工作负载经历了漫长的演化过程，比如，我们看到的一个网站，它背后的工作负载是虚拟主机、服务器、

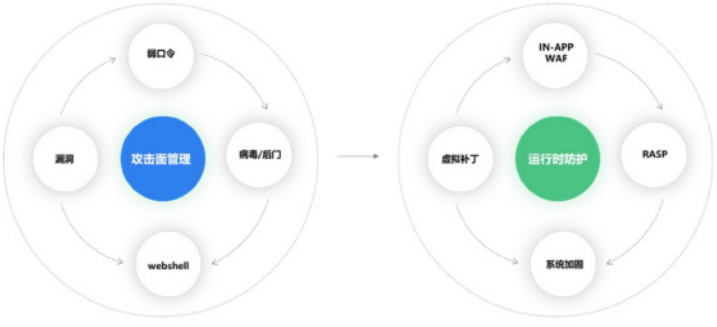
云主机还是容器？工作负载不同，这个网站所需要做的安全防护就不同；一个网站面向的客户群体不同，它的防护需求也同样不用，比如，政府类网站主要需求是网页防篡改、游戏类需求是抗 DDoS 和 CC 攻击、金融类的需求是数据防泄密。

需求的多样性也导致工作负载曾经出现了多种形态，包括杀毒、基线检查、HIDS/HIPS、网页防篡改、EPP 等。


图：工作负载安全的演进

直到 CWPP 的出现，才第一次统一工作负载的安全需求，从能力上看，CWPP 覆盖配置管理、资产与漏洞管理、工作负载防火墙、系统防护、应用防护、恶意代码检测、日志管理等 11 项能力，基本覆盖了工作负载在运行时的全部安全需求，也有部分市场需求剥离了安全防护的需求，仅作为工作负载端的数据采集探针，演化出服务器 EDR 这类产品。

不同于防火墙、WAF 等传统安全设备，CWPP 涵盖的能力范围非常广，曾一度被认为可以取代多种安全设施，将 CWPP 安全能力进行分类，可以分为攻击面管理、运行时防护两个维度。



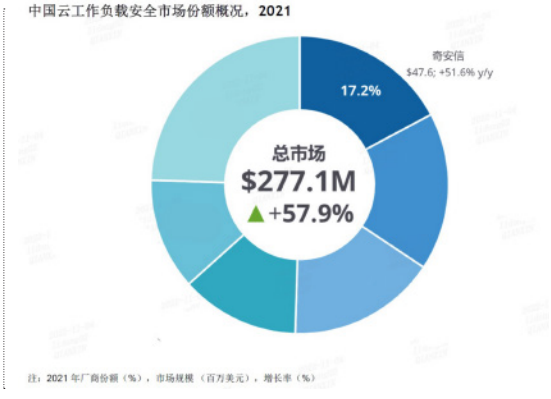

攻击面管理可以持续发现漏洞、弱口令、病毒 / 后门、webshell 等安全风险，在黑客攻击发起提前修复安全风险，缩小工作负载的被攻击面；

在业务运行时阶段通过微隔离、虚拟补丁、in-app waf、RASP、系统加固构建了流量、中间件、语言解释器、系统层面的四层防御体系，在不干扰业务的前提下，为业务提供最大程度的安全防护。

## IT 变革、HW、重保、合规建设等因素推动 CWPP 快速发展

IDC《中国云工作负载安全市场份额，2021：云原生与安全左移驱动技术持续创新》显示，中国云工作负载安全市场在 2021 年实现了规模和增速的双爆发，市场规模达到 2.8 亿美元，同比增长了 57.9%。

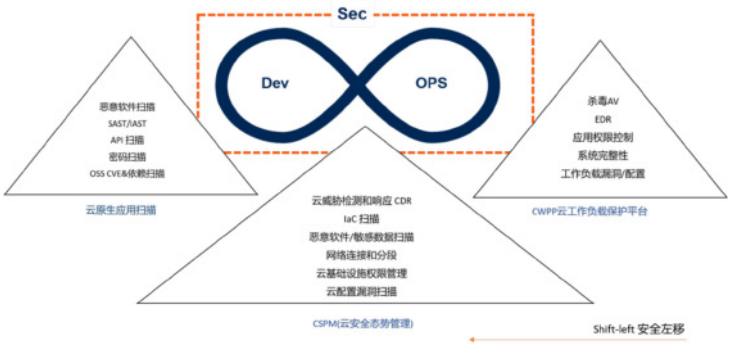
IDC 认为“中国公有云、私有云市场的持续快速发展为云工作负载安全的应用提供了广阔的客户资源，而网络威胁的持续肆虐及由此带来的巨大风险进一步促使云上企业提升对安全的关注及投入”，除此之外，等保、关键基础设备保护等相关政策中也对工作负载安全防护提出了明确了要求，再加上在攻防演练和重保中发挥的重要，CWPP 迎来了快速发展的时机。



## 云原生和 DevSecOps 推动安全左移：从 CWPP 到 CNAPP

目前 CWPP 有两种形态：插桩在工作负载内部、平行于 K8S&VM 等工作负载管理工具，其中插桩在工作负载内部的 agent 模式最常见，这在物理机和云主机时代几乎是一种完美的解决方案，但随着容器和 Serverless 的大规模使用，插桩模式已经出现水土不服，相应的平行于 k8s&VM 等工作负载管理工具的无代理模式能更贴合新 IT 架构下的安全需求。

由于具备极强的适应性，CWPP 也在贴合 DevOps 的需求而变化，除了在 Ops 环节保护工作负载安全，在 Dev 开发环境检查阶段，也演进出风险组件、云配置、API 发现等能力，推动“业务的安全”向“安全的业务”转变，推动 DevSecOps 的落地。但是 CWPP 本身能覆盖 Dev 开放阶段的能力有限，出现了短板，如对 API 的防护、在开发环境的 SAST/IAST 检测等，因此 Gartner 提出了 CNAPP 原生应用保护平台，CNAPP 开始在开发阶段就对业务进行完整的保护，填补了 CWPP 的短板，真正实现“开发 – 上架 – 运行时”的 DevSecOps 全栈式安全。




如上图，最新版本的 CNAPP 包含了 CWPP、CSPM( 云安全态势管理 )、云原生应用扫描和中控这 4 个部分。我们把在 CNAPP 框架下的 CWPP 模块和 CWPP 做了对比，发现运维管理、网络防火墙、漏洞管理等 6 项能力发生左移，成为 CNAPP 框架下 CSPM 的一部分，这也验证了 CWPP 最初的设计，把重要但不一定要在工作负载内部完成的工作左移，提升效率的同时也降低了对工作负载自身资源的损耗。

| 安全能力 | CWPP 原框架 | 左移后 CWPP 框架 |
|---|---|---|
| 运维管理（限制任意代码、管理员权限、变更管理、日志管理等） | √ | |
| 配置和漏洞管理 | √ | √ |
| 网络防火墙（工作负载隔离） | √ | |
| 系统完整性监控 / 管理 | √ | √ |
| 应用控制 / 白名单 | √ | √ |
| 漏洞利用防护 / 内存保护 | √ | |
| 基础设施静态数据加密 | √ | |
| 行为监控 | √ | √ |
| 主机 IPS | √ | |
| 蜜罐 | √ | |
| 杀毒 | √ | √ |

## CNAPP 和 CWPP，谁才是工作负载的最强守护者

毫无疑问，CNAPP 比 CWPP 覆盖的场景更多、对业务的保护也更加完整，但从目前阶段来说，要完成 CNAPP 的落地还很难，需要厂商具备云原生、CWPP、CSPM 的数项安全能力，从产品成熟来说 CNAPP 还远不及 CWPP，但 CNAPP 的出现给 CWPP 的发展规划了方向：CWPP 未来需更聚焦于工作负载核心防护，而将网络分段、配置检查等非必须在工作负载内部完成的能力左移，以进一步提升效率、降低资源占用，同时，CWPP 应该具备足够的开放性和兼容性，在未来更好地接入 CNAPP 框架下的安全中控。安

奇安信

新一代网络安全领军者

# 「零事故」安服团队重磅力作

## 900余次实战攻防演练的经验总结

## 从红队、蓝队、紫队视角全面解读攻防演练


扫码购买

# 数据“高速公路”需要遵守什么交通规则?

1988 年 10 月 31 日，一位住在沪嘉高速公路附近的阿婆看见汽车飞驰而过，惊讶地揉了揉眼睛，汽车“哧溜”一下飞过去了。

原来车可以在公路上开得这么快。

而这一天，正是中国大陆首条建成的高速公路——沪嘉高速公路正式通车的日子。

高速公路的通车，对经济发展的带动作用肉眼可见。1984 年，嘉定县级财政收入仅为 1.9 亿元。到 1989 年，嘉定县级财政收入达到了 4.28 亿元，足足翻了两倍多。

在此后的数年间，沈大高速公路、京津唐高速公路陆续建成通车，中国的高速公路网在 960 万平方公里的土地上徐徐展开。

截至 2021 年年底，我国高速公路总里程达到了 16.91 万公里，位居世界第一。

从南到北，从东到西，一条条高速公路上呼啸而过的汽车，正是高速公路经济腾飞的缩影。

## “要想富，先修路”

高速公路带来了商品经济的进一步繁荣，因为商品经济的本质是交换；而在赛博世界，应用程序也并非要成为一个个孤岛，你中有我，我中有你，才应该是常态。

比如，一款地图导航软件，除了单独的出行导航功能，其部分功能还可以用在打车软件或者订餐软件。

而在这个过程中，必然伴随着不同应用程序之间功能、服务和数据的频繁流动。

但在互联网发展早期，调用其他应用程序的功能和数据，对于开发者来说并不是一件容易的事情：你得理解程序内部的工作机制，甚至读懂源代码。

众所周知，即便是在程序开发语言已经非常简化的今天，在缺乏代码注释的情况下，自己写的代码经常只有自己才能看懂，甚至自己也看不懂。

所以得有一种方法，能够让开发人员在不了解具体细节的情况下，可以轻松调用所需要的功能和数据。应用程序也应该修建自己的“高速公路”。

这种方法叫作 API，中文翻译为应用程序编程接口。

API 的数据调用效率，足以和高速公路相媲美：当你使用订餐软件的时候，可以瞬间调用支付功能来完成订单支付；当你使用打车软件的时候，可以瞬间调用地图软件进行导航……

2000 年，销售管理软件巨头 Salesforce 发布了他们 Web API 的首个版本，允许第三方通过这些 Web API 调用 Salesforce 部分功能，实现自动化管理交易流程。

Salesforce把需要开放给第三方应用的功能和数据，封装成一个个 API 接口，方便开发人员“一键调用”。就像高速公路上奔驰的车辆一样，“哧溜”一下就把货物就送到了你手中。

“API 经济是将企业能力或竞争力作为 API 服务而进行商业交换的经济模式。”奇安信网络探针事业部总经理刘洪亮说，API 大幅缩短了应用程序之间“商品交换”的效率，也让数据的流动变得更加自由。

## 应用程序的“高速公路网”

实际上，最开始的 API 是放在企业内部，供不同应用之间互相调用的。

千禧年以来，企业内部信息化建设如火如荼，ERP、CRM、OA 等各类管理软件，逐渐成为了支撑企业财务、进销存、客户管理等日常工作流程的工具，并且积累了大量数据。

为了便于企业日常业务的开展，不同应用系统之间，

需要 API 支持数据调用。

比如，一家制造企业在使用 CRM 管理客户关系时，可能需要调用 ERP 软件的企业进货、存货及销货等各类资源数据。

此时，API 还没显现出什么安全问题。置身企业内网环境中的它，可以受到防火墙、IDP/S 等设备很好的保护。外部人员想要在未经授权的情况下访问内部 API，需要绕过一大堆防御设备。

并且，此时 API 的整体数量并不算大，部署相对集中，管理起来也十分轻松。

很快事情发生了变化。互联网技术尤其是以电商、社交为代表的移动互联网技术的发展，上下游产业链紧密的融合在了一起，信息化再也不能局限在组织的围墙之内。

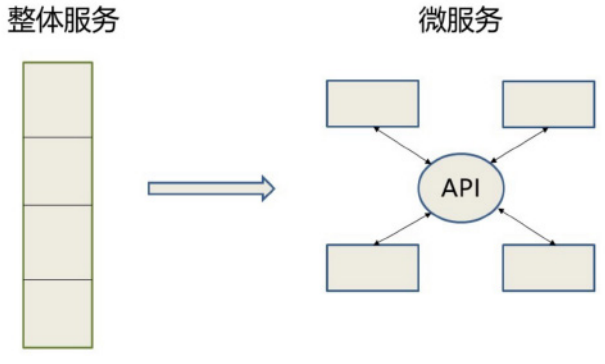
这就意味着，API 必须得开放给企业外部应用使用。

事情还没有结束。2015 年前后，云计算，尤其是公有云，开始在数字经济领域强势崛起，在云服务的帮助下，人们就像用水、用电一样，对应用程序“予取予求”。

从那时起，把 API 托管在云上迅速流行开来，这样可以方便开发者在云上调用相应的 API。

比如，目前大火的微服务架构，它允许开发人员将应用程序微分成一组独立的服务，每个服务都围绕着具体业务进行构建，并且能够独立地部署，而服务与服务之间便需要通过 API 进行数据通信。

应用程序数量的爆炸式增长，自然带来了 API 数量的爆炸式增长。作为敏捷开发的重要实现形式，没有人能够拒绝 API 带来的便利。




## 频繁发生的“交通事故”

路多了，车多了，“交通事故”的数量自然也上来了。

尤其是 “API 号”高速公路甚至没有配套的“交通规则”和防范措施。

如前文所述，API 的本意是为了方便不同应用程序之间合法的调用某些特定的功能和数据。可总有人并不是很喜欢守规矩，尤其是现在大量的 API 都直接托管在云上，所有人随时随地都可以访问。

可以想象，一旦 API 上发生安全问题，必然会给其中流动的数据造成损失。

比如，2020 年 3 月，国内知名社交媒体因其用户查询接口滥用导致数据泄露，影响用户数量高达 5.38 亿；

再如 2021 年 7 月，知名职场社交网站被曝出因为 API 漏洞被攻击者爬取了超过 7 亿条用户数据；

……

尤其是，最危险的漏洞往往能够绕过脆弱的身份验证机制，使攻击者在未经授权的情况下可以访问 API 资产。

这下让攻击者如同发现了新大陆：原本在内网“重兵防守”的数据，现在开始频繁出现在几乎“无险可守”的 API 上。

“2017 年前后，我们开始在实战攻防演习期间，不断检测到针对 API 漏洞的利用行为。”刘洪亮说，而且近几年这个数量上升很快。

从前，窃取数据需要攻入内网，再经过一系列复杂的横向移动最终访问目标数据库，难度大、战线长，还容易被发现。现在只需要守在 API 边上“打伏击”即可，隐蔽性较强，攻击成功率可以说大大提高。

但历史不能开倒车。数据一旦流动起来，就绝不会因为安全问题缩回去。

《中国人民共和国数据安全法》第一条明确说了，为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

显然，保护数据安全的目的是为了促进数据的开发和利用，并不是让数据躲在隔离网环境，成为“温室里的花骨朵”。

因此，API 的规模只会不断扩张，除非出现一种可以完全取代 API 的新技术。

既然这样，解决 API 的安全问题成了奇安信必须要做的事情，而这个任务就落在了刘洪亮的肩膀上。

## 身份仿冒、暴力破解 or 漏洞利用，防得住吗?

奇安信对于 API 安全的布局始于 2019 年，那一年国家级的网络安全攻防演习逐渐走向了深水区，攻击队各种五花八门的攻击手法层出不穷。

其中，最常见的针对 API 的攻击方法就以下三种：

第一，窃取 API 账户的登录凭证，从而仿冒合法用户身份。登录凭证经常会通过各种意想不到的方式泄露，比如更新社交媒体时一不小心就泄露了，再比如身份信息被明文写在代码中，并且代码被分享到了某些技术社区。

第二，对使用弱口令的 API 账户进行暴力猜解，获得账户的登录权限，弱口令不仅仅局限于 123456 这种简单的口令，还包括规律口令，如首字母 + 出生日期、企业邮箱之类的，很容易被攻击者猜到。

第三，利用 API 自身的漏洞，绕过其安全机制，在未经授权的情况下获得 API 账户访问能力。

只要获得了 API 的访问权限，就可以拿到经 API 调用的数据。

事实上，在专门的 API 安全产品出现之前，有很多组织采用 WAF（Web 应用防火墙），部署在 Web 服务器前面，来试图阻止针对 API 的攻击行为。

但 WAF 有自己的规则。

从名字上来看，再厉害的 WAF，其本质仍然是一道“围墙”。围墙就注定了它在保护 API 方面的最大缺点——没办法保护围墙之外的 API。

但API的本质就是开放和连接，这一点是不能接受的。

并且，对于依靠静态规则匹配来检测入侵行为的 WAF 而言，想要发现未知威胁也十分困难，尤其是 0day 漏洞的利用行为。

所以从一开始，奇安信就摒弃了这种传统围墙式的建设思路，无论是 WAF 还是其他什么墙。

至于到底怎么做，奇安信或许早已有了定论。刘洪亮说，API 安全卫士应该能够解决 API 运行时的安全问题，从 API 资产识别管理、攻击检测、敏感数据检测到 API 风险检测、行为审计、访问控制、攻击防护等方面。

在接手 API 安全这个任务之前，刘洪亮带领的团队主要负责网络探针的建设。探针就好比网络空间的摄像头，能够将所有的事情都记录下来。

要知道，探针早已广泛应用于天眼、NGSOC、态势感知等产品中。

那么如果在关键节点部署上探针，再配合上一些其他的技术手段，是不是能把所有的 API 及安全风险都看得一清二楚？有什么攻击行为也都能了如指掌呢？

带着这些疑问，刘洪亮决心一试。

## 看不见的 API 是最危险的

很快，第一个问题出现了，大多数组织并不清楚自己都有哪些 API。

奇安信做过一次统计分析，客户少则部署了上千个 API，多则甚至有十几万个 API，很多 API 的开发过程也是跟着业务拓展“赶鸭子上架”，随着业务变革、人员更替，早就把这些 API 抛之脑后了。

就像不知道揣在哪个口袋里的几张红票票，如果不洗衣服根本想不起来在哪。那些原本应该在业务生命周期结束之后就该下线的 API，最终也就不了了之了。

试想，如果连家门口有几条道、这些道都通向哪里都搞不清楚，就更不要说搞清楚哪条道安全、哪条道不安全了。

看不清楚 API 在哪里才是 API 面临的最大风险，也是安全防护首先要解决的问题。

不过让刘洪亮也没有想到的是，仅仅是解决 API 安全的第一步，就成为了奇安信面临的最大难题。

其实，识别 IT 资产都有着类似的方法。无论是计算机、打印机等硬件设备，还是网站、虚拟机、API 这些软件资

产，都有自己唯一的识别码，为了便于理解，你可以管这些识别码叫作“资产指纹”。

通常情况下，“资产指纹”都会按照行业通用规则，被开发人员写入资产内部。系统通过不断扫描、识别资产指纹，从而对 IT 资产进行统一管理。

这个过程就如同上课点名（没有重名），听到我的名字我就答到，老师也就知道我来上课了。

但 API 的情况有点特殊。

在互联网“野蛮生长”的那些年里，为了追求业务上线速度，很多开发者并没有按照规范去开发 API 接口，导致“资产指纹”五花八门。

如果简单的按照 API 标准规范去识别 API 资产的话，大量的 API 就会识别不出来。

比如，大部分人的身份证号码都是 18 位数字，其中有些人的身份证号最后一位是“X”。早些年，某些身份信息录入系统就不支持输入“X”。

所以，API 安全卫士应该对各种“指纹”都了如指掌，否则系统在点名的时候，部分 API 内心 OS：“What are you 弄啥嘞，我也听不懂啊！”

这让刘洪亮一下子都犯了难。如果全中国的程序员一人一个 API 开发方法，单单是 API 资产识别的工作量，还不得大到姥姥家去。

说句实在话，即便是现在回头看，也没什么捷径可走。

但当时那种情况，数据安全已经提到了和国家安全同等的高度上去了，没办法也得硬着头皮上，至少得先摸摸底，看看程序员们都是怎么开发 API 的。

常见的程序开发语言也就那么几种，没准能从中找到什么规律。

功夫不负有心人。作为拥有足够体量的安全公司，奇安信能够拿到足够数量的样本，可以说，能想的到的、想不到的 API 类型，都能在这里见到。

把这些样本拿到机器学习的样本池里进行反复训练，最终得到了一个让所有人都喜出望外的结果：系统可以自动识别出大部分 API 资产的类型、位置、功能等基本信息。

有了这些信息，才能全面掌握自身 API 的安全性到底如何，比如，是不是直接暴露在互联网上，是不是配置有错误，存不存在弱口令和高危漏洞等。

掌握这些信息正是 API 安全防护的前提。

## 一个好汉三个帮

在解决完这个问题之后，前路似乎平坦了起来。

奇安信 API 安全卫士聚焦打造持续监测响应的 API 安全防护能力，建立基于用户访问行为的用户画像或行为模型，发现 API 未认证访问、弱口令登录、未授权访问、异常访问行为等。此外，该产品还具有基于自动化发现并可视化展示及管理 API 能力，能够及时发现与预警僵尸、未知等异常 API，以及避免在 API 设计之初由于缺乏统一规范导致后期大量 API 无法统一管理而引入的安全问题。

“借助奇安信的安全能力、大数据能力、安全中台的能力，奇安信 API 安全卫士为客户提供了摸清家底、看清风险、防住攻击闭环解决方案。”刘洪亮说，一个好汉总得三个帮啊。

比如，借助大数据和机器学习能力，奇安信 API 安全卫士解决了 API 资产自动发现的问题；

再如，借助用户实体行为分析能力，建立基于用户访问行为的用户画像或行为模型，只要 API 安全分析平台发现了针对偏离行为基线的异常访问，即可产生告警。

还有，借助奇安信 CERT 的漏洞情报能力，可以第一时间掌握最新漏洞情况，上线针对该漏洞的防护规则，同时根据漏洞的危害、影响范围，为客户提供漏洞处置的优先级排序。

……

所有 API 安全卫士所需要的能力，都可以在奇安信的“武器库”里找到。

而这远比在 API 面前摆一道围墙，要有效得多。

“随着数字经济的发展、微服务的发展，以及云原生的发展，安全对抗已由原来的技术空间的对抗，转移到数据空间的对抗。”刘洪亮感慨到，看着在 API 这条铺满应用程序世界的高速公路上奔驰的数据，没有交通规则和安全措施是万万不行的。

但是我们还应该明白，或许对于数据安全而言，奇安信 API 安全卫士只是万里长征中最微不足道的一步。安

# 打破孤岛，协同联防

## 某运营商打造全省市跨域跨网统一威胁感知自运营样板

作者 安全攻防 BG

“如果把某省运营商近 20 个市分公司四通八达的 DCN 网络比作全国道路交通网，网络流量就可以类比成车流量。当网络安全遭遇‘交通事故’时，就会导致 DCN 网络运行不通畅，引发集团在线交易、电商平台、政务云等业务瘫痪。”该省运营商网络安全部门相关负责人表示，不光要重视省公司网络安全，所有地市公司的业务网络威胁可视、可控也是当下亟需解决的问题。

随着网络通信技术和计算机技术的不断发展，电信业的网络安全问题日益引起通信运营商的重视，因为这直接影响着运营商的生存和发展。通常，运营商受网络攻击后，黑客可能会秘密侦听电信网络传递的信息内容，盗取运营商大量的用户数据，还有可能利用电信网络作为通路，侦测各种信息业务系统，甚至投递蠕虫病毒、木马病毒，拥塞电信网络，恶意控制和破坏网络，使电信网络全面瘫痪。

由此可见，通信运营商的网络安全问题不容小觑，建立健全地适应于通信业务、技术发展的网络安全管理

体系，落实常态化运行机制是通信运营商的首要之举。

某运营商作为国内三大运营商之一，是国家网络安全保障的主力军，承担着从底层提升网络安全的重任。而某省运营商作为该运营商最大的省级分公司，下辖包括近 20 个市分公司，服务网点覆盖城市和乡村。在此基础上，该省运营商对内要保障省公司和所有地市管理网的安全，对外还要保证各类业务系统正常运转的安全，确保为制造、能源、医疗教育等不同行业的客户及个人用户提供安全稳定的电信服务。

基于运营商的网络安全现状，以及全省、各地市公司的安全需求，某省运营商于 2019 年起陆续与奇安信天眼达成四期合作，通过多期流量扩容，以“分布式集群”的部署方式，实现省公司对全省 21 个地市公司 150G 业务流量的全面监测，达到了跨域跨网统一流量威胁感知的目标，对该省运营商业务出口的威胁防范起到了关键作用，提升了省、市公司网络安全协同联防能力及电信网络安全风险管理水平。

## 电信网络复杂，三大网络安全痛点亟需破解

不同于其他行业的关键信息基础设施，承载话音、数据、消息的电信网络与绝大多数其他行业的关键信息基础设施不同，电信网络要复杂得多。电信网络涉及移动接入网络、固定接入网、传送网、IP 网、网管支撑网等多个通信网络，任何一个网络被攻击，都会对承载在电信网上的话音或数据业务造成影响，尤其是面对高级威胁的时候，可能会导致网络瘫痪，甚至造成更严重的后果。

因此，某省运营商在没有部署天眼之前，所面临的第一个问题如下。

**安全设备老旧，缺乏发现高级威胁的能力：**电信网络的复杂程度使某省运营商的网络安全变得极其脆弱，而安全问题并非传统意义的安全设备所能解决，尤其是难以发现隐蔽 APT 威胁，这些高级威胁一旦被忽略，就会绕过运营商原有的安全防护设备，对集团重要的数据资产进行攻击，造成泄露、破坏或篡改等严重损失。

其次，作为内部支撑业务的“数据通信网”，DCN 网络信息资产的价值不断提高，其安全问题也日益显现出来，除了会遭到物理攻击破坏，还会面对恶意软件攻击、内部员工误用、黑客入侵破坏等网络攻击。某省运营商 DCN 网络汇聚省干核心层和地市汇聚层，部署节点遍布全省各地市。而由于 DCN 组网方式随意性很强，网络区域之间边界不清晰，互通控制管理难度大，因此一旦遭遇网络攻击就很容易扩散。

基于此，该运营商所面临的第二个问题如下。

**无法掌握全局安全态势，全省各市缺乏协同联防的能力：**当网络资源比较分散的近 20 个市公司 DCN 网络受到攻击时，省公司如何无一遗漏的做到全面感知、可视监测、统一指挥。

另外，通常情况下，攻击者在进行攻击之前总是会搜集各种情报，包括开放的端口、联网的硬件设备资产、办公软件漏洞等，有了这些信息，攻击者可以针对性地构建攻击武器和攻击载荷，从而大幅度提升攻击的成功率。但是处于防守角色的客户却不同。在部署天眼之前，该省运营商部署了防火墙、WAF 等各类设备，但是却无从得知攻击者会利用什么样的漏洞、采用什么样的方法来入侵其系统，入侵后也不知道威胁究竟潜伏在哪里。

所以，该省运营商所面临的最后一个问题如下。

**威胁数据不能贯通，无法追溯到攻击源头：**当该省运营商的任一家分支单位遭受攻击，省公司如何发现攻

击者是否对其他分支单位也进行了攻击，以及攻击者的具体的攻击信息，并溯源到攻击者的源头，防止攻击者再次入侵其他分支单位。

## 分布式集群部署，省、市网络安全协同联防

基于某省运营商的网络安全现状，以及下属市分公司整体情况，天眼与该省运营商达成合作。天眼通过“分布式集群”部署模式，对运营商省公司 DCN 出口、互联网出口、云平台出口，以及省内近 20 个地市公司 DCN 出口总计约 150G 大流量实时监测，帮助该运营商实现省公司、各地市公司流量的全面采集与威胁检测，最终达到告警在省平台统一分析和展示的目标，提升了省、市公司网络安全协同联防能力。

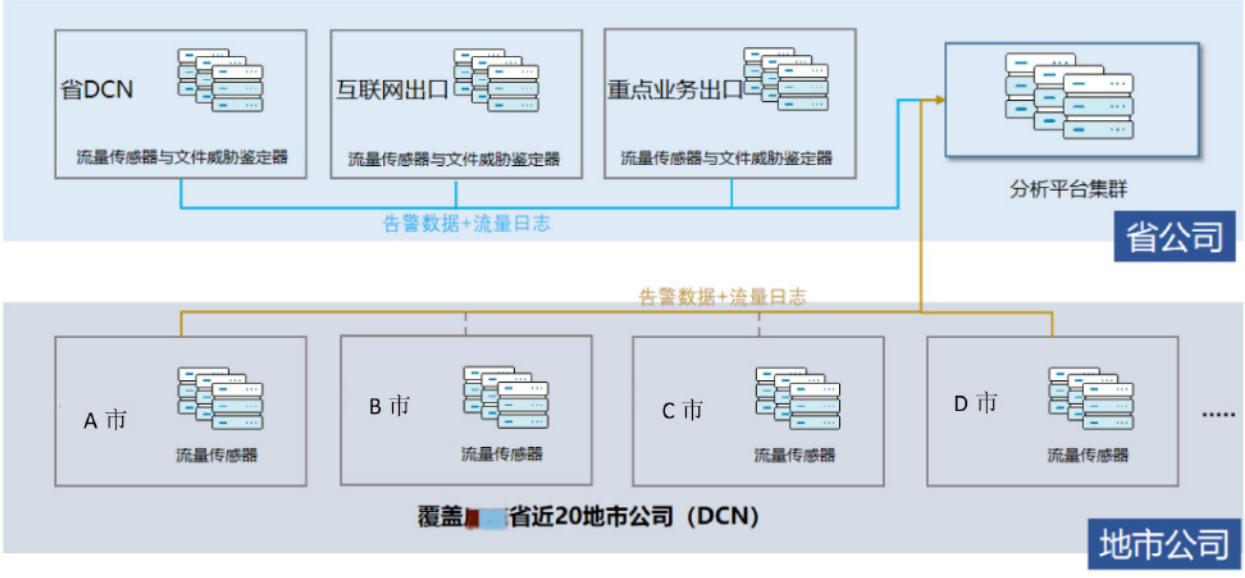
在省公司侧，通过部署在省机房的天眼流量传感器，对省公司 DCN 出口、互联网出口、重点业务出口逾 100G 流量进行采集监测。经天眼探针检测分析后，把相应的告警数据及流量日志转发到本地机房的天眼分析平台集群，同时把还原出的文件转发至本地机房的天眼文件威胁鉴定器。接着，文件威胁鉴定器对文件进行检测分析后将告警数据转发至分析平台集群。分析平台再通过对收集到的探针、沙箱数据进行整体分析后，精准定位省公司存在的网络安全威胁。

在各地市侧，将天眼探针部署至近 20 个地市公司机房，对各地市 DCN 流量进行采集分析，并将检测后的告警数据、流量日志通过专线转发至省机房的分析平台，分析平台基于收到的数据进行集中分析，实现省公司对各地市公司网络威胁的统一监测与管理。

## 应用效果明显，自运营让天眼价值最大化

“在部署了天眼之后，我们现在可以通过省统一的分析平台可视化查看到全省及所有地市公司的安全态势，包括威胁事件态势、资产态势、脆弱性态势等各类展现攻击情况的态势。”正如该省运营商网络安全部相关负责人所说，天眼帮助运营商全省各市公司持续监控攻击、统一处理威胁，就像交通路网智能监测系统一样，可以对重大突发事件预测预警及应急处置，还可以对全省路网运行及重大交通突发事件指挥调度。

省各地市单位部署天眼之后，分别将流量的原始数据和日志数据传输到省公司天眼分析平台，与省公司各节点探针搜集上来的数据进行碰撞、综合关联分析，自



动将数以万亿的零散告警形成智能化的攻击事件链条，并对受害目标及攻击源头进行精准定位，最终达到对攻击者入侵途径的研判与溯源。“原来近 20 个地市的网络安全各做各的，现在天眼帮我们把省市的安全都串联起来。换个角度来讲，只要攻击者从任何一个市进来，我们都能掌握他它的行踪轨迹，看它是否也侵犯到了其他市，从而追溯到攻击源头。”该省运营商网络安全部相关负责人表示，天眼系统帮助集团有效提升了网络安全持续防护能力，保证了省运营商业务的正常开展。

不光在攻击检测有效性上发挥了作用，在事件响应处置高效自动化方面，天眼与终端、防火墙等设备协同联动的能力，也切实帮助该省运营商快速定位到感染主机和恶意软件，及时阻断威胁，提升了威胁响应和处置的效率。

如果在终端上检测出恶意软件，通常需要调用杀毒软件尽快查杀；检查出内网在连接外部非法 IP，可能需要调用防火墙去封禁……这些设备都需要人工调用，既费时费力，威胁响应效率也不是很高。“而天眼的自动化能力，则完全摆脱了这种模式。我们日常发现恶意告警之后，通过天眼平台可以 1 秒内联动其他设备下发操作，如联动防火墙封禁 IP”。该省运营商客户表示，有了天眼之后，安全人员的威胁运营效率大大提升。

2021 年，为满足政企客户“建党百年庆典期间”对信息基础设施的安全防护与保障需求，助力各级政府、企事业单位营造建党百年的良好氛围，该省运营商启动建党百年“守护行动”，活动期间防护准确率 100%，有效保障了关键信息基础设施和政企客户的网络安全稳定。

“我们没有用乙方的安服同事，运营天眼设备的人员都是我们集团内部自己的人，因为天眼设备的易用性，让我们有信心把天眼设备用好，天眼设备的管用性，也让我们想投入自己的人员去运营。”该省运营商网络安全部相关人员表示，从威胁监测到响应处置，再到溯源分析，每一个环节他们都亲历过，也真真实实感受到了天眼在检测能力和检测效率上的优势，他们愿意主动投入人员自运营，让天眼的价值充分发挥。

## 后记：

电信行业在保证数据存储、传输等方面发挥了关键作用，它本身既是关键信息基础设施，同时又为其他行业的关键信息基础设施提供网络通信和信息服务，在网络数字化浪潮中扮演着重要的角色，关系国计民生。

天眼作为网络威胁监测与分析领域的领头羊，充分发挥在网络威胁监测与分析领域的优势，已经为电信行业——移动、电信、联动三大运营商搭建了网络流量采集和监测分析系统，提升了网络安全防护能力。未来，天眼将继续为电信行业客户的网络安全保驾护航，助力电信产业数字化转型，赋能传统产业转型升级。 安


天眼网络安全态势大屏

# 云深不知处，安全为始

## ——走近奇安信集团副总裁刘浩

作者 公关部 孙丽芳

许久没见刘浩的人，猛得见到他，可能会觉得他有点逆生长。半年多的时间，刘浩每天晨跑 6、7 公里，体重从 200 斤减到了 150 多斤，体态看起来年轻了不少。见微知著，奇安信云安全的这位领头人是个“狠人”。

### 真正想干的事

求学时期的狠，是勤奋、刻苦，学习成绩优异。刘浩本硕均毕业于 C9 高校计算机系，期间多次获得国家级奖学金，目前还在北大读博。

工作之后的狠，是好学、坚韧，在新领域开疆拓土。这个新领域就是云安全。

云安全伴随着云计算的发展而兴起，而早在云还是“无名之辈”的时候，刘浩就已经被云计算及其前景深深吸引。

“我一直在跟踪云技术的发展。2010 年我在百度做运维自动化平台，工作之余参加了兴趣组，尝试一些虚拟化的项目，当时 openstack 在国内还只是被当作一个热门开源项目在跟踪，没有什么商用场景。”

云寂寂无名的阶段转瞬即逝，之后的几年，阿里、华为等云计算专业玩家们纷纷入场，行业进入了精彩的探索时代。2016 年年初，刘浩加入了奇安信，负责筹建云安全产线。“奇安信的安全基因和云计算积累的结合，一定能在云安全领域拔得头筹，这是我真正想干的事”。

### 并不好做的云安全

从想干到能干，切入的时间点非常关键。

“云的概念是 2006 年提出的。2006 年到 2016 年，这十年，云的发展速度并不是很快，对于云计算到底是不是变革性技术还有些不确定性。因为在信息领域有太多的新技术、新概念涌现，后来又慢慢销声匿迹。但是从 2016 年开始，云的普及速度大大加快，渗透到了各行各业，改变了整个 IT 产业格局。云上的应用和数据越来越密集，与云相伴而生的安全问题也越来越突出。黑客很注重攻击的 ROI。云所承载的业务和数据价值越高，越容易受到攻击。云安全已成为数字时代新的‘重要战场’”。

太早，市场不成熟。太晚，失去了先机。2016 年被称为云快速增长元年，奇安信在这个时间点进入云安全市场可谓审时度势，刚刚好。

即便踩准了时机，刘浩还是认为，云安全并不好做。

“第一个难点是和云融合。在信息化上面做安全，首先要对信息化了解。很多传统安全厂商在云时代掉队，主要原因就是只懂安全，不懂云，自然就不知道该怎么在云上面做安全；第二个难点是兼容性。不同于美国以公有云为主，私有云很少的情况，中国的大型客户基本部署的都是私有云。美国主流的云其实就出自三家：微软、亚马逊、谷歌。而中国这个领域的厂商却非常多，三大运营商悉数入场，还有数通厂商（如华为、华三），服务器厂商（如曙光、浪潮），互联网厂商（如阿里、腾讯、京东），以及金山云、青云、UCloud 等一批独立的云创业公司。这就造成中国的云技术路线很多，版本很多，呈现碎片化。出于分散业务风险的考虑，客户基本上又都进入到了混合云的状态，要在这种状态下做好安全，难度显而易见。”

刘浩认为，做云安全的第三个难点是运营。“云计算落地是一个体系化的工程，不只是一次性的建设投入，更是长期的运营。运营中存在责任划分等一系列难题。传统模式下，按照谁主管谁负责、谁运行谁负责的原则，安全责任相对清楚。在云计算场景下，云计算平台的管理和运行主体与数据安全的责任主体不同。比如，地方政府的政务云，由大数据局来建，各个局委办在用，安全责任是谁的？是谁提供谁负责，还是谁使用谁负责？这是大家很关心的问题。责任的重新划分意味着组织流程的重建、现有制度的调整。”

## 赢下首场大胜

做云安全不易，刘浩和团队当时的处境也有些难。

“刚开始的时候，我们笑称自己是‘三无’团队。第一无经验。我这个 Leader 是从互联网公司过来的，是个技术管理者，没有做 to b 的经验；第二无队伍。当时我们总共不到 10 个人，还都是做开发的，人员构成很单一；第三无产品。我们现在做的云安全资源池，云安全管理平台，当时还只是构想。”

不过，自嘲仅限于语言，行动上，刘浩和团队一点也不含糊。

“我们自己先做方案，然后去和客户交流，被客户质疑，回来再改，再去和客户交流，同时加紧方案实现，节奏非常快。我们也很注意第三方机构的动向，以及国外云厂商怎么做安全。通过自己钻研、反复交流和外部学习，2016 年我们已经摸出了一些门道。”

而最好的历练永远是通过战斗获得。很快，刘浩和团队就经历了这样一场战斗。

政务云是云计算在国内推广应用的排头兵。由华为联合中国电信承建的嘉兴政务云是浙江省内市级政府云服务模式的首个落地项目。2016 年，嘉兴市政务云公开招投标购买安全服务。

“嘉兴政务云是华为的标杆项目，客户对华为的云服务也很满意，所以开始我们只能说是全力争取，并无多大把握。我们先自己出了一版方案去跟客户讲，客户听完一通质疑。我们没有气馁，把客户的意见全部记下，回去逐一修改，再找客户交流。第二次交流就好多了，客户对我们方案的认可度明显提升了一大截。第三次交流，客户对方案就非常肯定了。客户认为我们是真的懂云又懂安全的，而不是拿传统安全来凑数。经过反复多次的打磨，最终我们击败了多个强劲对手，拿下了这个项目。”

从纸面方案到最终交付，还有距离。接下来，刘浩团队和安服团队一起驻守在嘉兴，用了一个多月的时间，按照拟定方案，把客户所有的制度流程、组织结构重新捋了一遍。“我们捋得非常细，整了一摞大厚本子。客户对我们很满意。这给了我们很大的信心。我们借这个机会，从公司内部想办法挤资源、投资源，最终交付了第一版的云安全管理平台。这个平台虽然现在来看有一些不完善，但却是一个很好的开端。现在奇安信在全国，尤其是省会城市和省级政务云安全上面的占有率非常高，这都始于嘉兴政务云。”

## 乘势快速发展

嘉兴政务云是刘浩和团队在政务云安全市场取得的首场大胜。这场胜利对刘浩、对公司都有很大的鼓舞作

用。“公司领导不仅对我们充分放权，还给予了很多支持，包括收购了安贤、椒图等优秀公司，快速补充了团队。”

队伍整齐，机制灵活，之后的几年，在刘浩的带领下，奇安信在云安全领域取得了快速发展。奇安信云安全产品多次上榜国内外权威机构报告、中标运营商集采大单。在工信部赛迪顾问的中国云安全和服务器安全市场报告，以及 IDC 中国安全资源池和云工作负载安全市场报告中，奇安信连续多年稳居首位。在 Gartner 今年 10 月发布的《2022 年中国安全成熟度曲线（Hype Cycle for Security in China, 2022）》报告中，奇安信在云安全资源池、CWPP、SASE 等领域也都作为代表供应商入选。奇安信的云安全实力深受政企客户与第三方调研机构的认可。

对于这些成绩，刘浩觉得，除了因为赶上了云迅速发展的大趋势，还因为奇安信有三个独特之处。

“第一，区别于很多传统的安全公司，我们是既懂云又懂安全的公司，诞生于云时代，很多业务也构建在云上。此外我们有一支云的团队自研云，供公司内部使用，这使得我们在对云的了解及技术积累比较深；第二，在云的适配兼容上，我们的积累是最多、最好的。我们的产品基本能适配市面上所有的云，我们也是最广泛融入到云的生态里的安全厂商；第三，很多安全厂商做云安全就是卖一个产品，而我们做云安全是搭建一个大的体系。云是基础设施，属于短期建设长期运营，就像盖房子，盖起来很快，长期维护得几十年。这意味着云安全要贯穿云计算的论证、规划、建设、运营全生命周期。我们对此都能覆盖。在论证、规划阶段，我们和公司战规部门一起给大型客户做云安全的顶层规划。在建设阶段，我们的安全产品覆盖是业内最全。到了运营阶段，我们是业内最早推云安全运营服务的厂商。我们既看云，又跳开云，关注云的全生命周期。”

冬奥表彰会上刘浩和获奖的云安全团队小伙伴合影

表 1　2021 年中国云安全市场品牌 TOP10 排名

| 排名 | 厂商 | 销售额（亿元） |
|---|---|---|
| 1 | 奇安信 | 8.13 |
| 2 | [redacted] | 5.55 |
| 3 | [redacted] | 5.29 |
| 4 | [redacted] | 3.11 |
| 5 | [redacted] | 2.7 |
| 6 | [redacted] | 2.08 |
| 7 | [redacted] | 1.5 |
| 8 | [redacted] | 1.09 |
| 9 | [redacted] | 0.73 |
| 10 | [redacted] | 0.6 |

注：部分厂商未参与此次调研。　　数据来源：赛迪顾问　2022，02

近日，赛迪顾问发布的报告显示，在市场竞争格局上，奇安信以 8.13 亿元的销售额位居市场第一位。

## 云安全的步伐永不停歇

云计算是数字经济时代不可忽略的基础设施。过去十年，云计算的高速发展推动传统行业数字化转型不断深入，企业 IT 建设所依赖的基础资源也经历了从服

务器到云化资源的发展历程，目前正在快速进入云原生阶段。

“理解云原生我们可以类比两个词‘移民’和‘原住民’。云计算改变了资源的使用方式，大家于是把业务系统迁移到云上。这个时期的应用可以理解为云平台上的移民。现在和将来的应用系统在构建的时候，就不用考虑传统环境，天然就是构建在云上，利用了云的所有特性。这个时期的应用可以理解为云系统上的原住民，也就是云原生。数字化转型新时代，云原生定义了下一代云计算。相应的，云安全的未来就是云原生安全，包括保护云原生体系、云原生平台的安全及用云原生的技术来做安全。”

目前，带着多年积累的大量成功的云安全实践，刘浩正带领团队进入云原生安全这个全新的领域。

“我最近在牵头梳理和融合奇安信的云原生安全体系。它涉及的内容很广，包括云原生的开发安全、基础设施安全、计算环境安全、应用安全等，是一个大的领域和体系。除了包括公司现有如API、CWPP、SWG 等可部署在云原生环境的产品，我们也在投入一些新产品。同时，产线和战规一起进行了详细的梳理设计，接下来会推出面向云原生安全的一系列解决方案。总体来说，在云原生安全这个新领域，我们的技术储备已经很充分，且具备体系化优势，下一步就是踩准时机全面进入，深耕这块增量市场。”

除了在云原生安全领域加紧布局，接下来，刘浩还有一个工作重点。“我们现在的业务主体是保护云平台的安全，但同时我们也涉足了用云的技术做安全。这也是云安全发展的一大趋势。过去都是交付到客户本地的安全，现在我们可以在云端或者用 SaaS 服务的形式来交付。这个领域，我们今年也会落一些标杆项目。”

虽然已经取得了很多成绩，但刘浩明白，云安全永远不可能毕其功于一役。“云安全相关的新东西很多，该做什么，不该做什么，以及推出的时间，其实是一个选择题，但奇安信能做好这道题。我们总体的思路是，平台型、入口型、关键点位我们要把控，但是我们不铺摊子，有些产品就交给生态去做。因为云就是个大生态，云安全也一样。择时机、有重点、做取舍，对度的把握一直是我们能做好云安全的重要秘诀。”


刘浩带队和联通数科进行交流

生活中，刘浩喜欢跑步。工作中，刘浩同样喜欢跑一线。重要的项目，从客户沟通到写标书到价格的制定，他都会全程参与。“我要保持来自一线最真的敏锐度，而不是单向接收层层传递过来的东西，这对决策很有帮助。我要求团队里的干部也都要这样。同时，我坚信团队的融合和成长，最重要的就是一起战斗打胜仗！”

云深不知处，安全为始。从初识云安全到跑进云安全的未来，可以预见，刘浩还会继续跑下去，带着对生活的自律与坚持，对云安全事业的热爱与执着。安

# 对老实人背锅说不！

## ——网络安全人“防甩锅指南”

作者 研究员 张少波


“你不去当厨师可惜了，甩锅甩得那么好。”

俗话说，“人在江湖飘，谁能不挨刀。”在职场江湖中，明面上的刀光剑影少了，但是暗地里的甩锅和背锅，却防不胜防。商务印书馆《现代汉语词典》（第7版）对于“背黑锅”的解释是：“比喻代人受过，泛指受冤枉。”近年来，大家将“背黑锅”简化成了“背锅”，并衍生出个新词汇——“背锅侠”，而与之对应的，就是甩锅，意指推卸责任，企图将自身的矛盾转移到其他地方去，让别人来背黑锅的意思。

在四大名著之一《三国演义》中，就有两个甩锅与背锅的小故事。

### 曹操甩锅、粮官背锅 曹军征伐路上的垫脚石

《三国演义》第十七回，“袁公路大起七军，曹孟德会合三将”表述，建安二年，曹操远征袁术。曹军先期进展顺利，后双方进入僵持阶段，袁军占据地利，坚守不出。

因曹军数量众多，粮食需求巨大，且恰逢彼时年景不好，曹军驻扎之地大旱，后勤供给十分困难。加上将士众多，曹军粮食急耗殆尽。

这个时候，老实人王垕登场了，他智谋比不上郭嘉、荀彧、程昱，武力比不上许褚、夏侯惇、徐晃，只是一位小粮官，相当于职能部门的经理。他看到这种情况，马上向曹操汇报。

曹操效率很快，立即给了指示，“那就改成小斛吧。”王垕幽幽地说：“士兵们埋怨怎么办？”曹操说：“不要紧，老夫自有妙计。”

王垕看到领导都拍板了，自己还说啥呀，按照吩咐去执行了。果然，如王垕所料，士兵们吃不饱肚子，怨声四起。眼看就要哗变了，王垕慌了，赶紧找到领导曹操，请示下一步怎么办才好，曹操意味深长地看了一眼王垕，说道，"我要借你的脑袋用一下，安抚一下军心"，王垕这才明白，敢情领导之前所说的"有应对的办法"，就是要让自己背锅。


很快，曹操以贪污军粮的罪名处死了王垕。可怜的背锅侠王垕，到死都没明白到底做错了什么，他只是曹操征伐天下路上的一个小小垫脚石。

## 孙权甩锅吕范 吕范甩锅贾华 贾华惨遭背锅

曹操将缺粮的罪名，甩锅给王厚，也许是突出了曹操“宁使我负天下人，休教天下人负我”的奸雄形象，在相对正面的孙权阵营，也有甩锅和背锅的故事。

“刘备招亲”是《三国演义》中的精彩一折，第五十四回“吴国太佛寺看新郎，刘皇叔洞房续佳偶”。周瑜为要回荆州，与孙权设下美人计，想用招亲把刘备诓到东吴囚禁。诸葛亮献出三条妙计化解孙、周之计，相当于只吃饵不上钩。

刘备到了甘露寺后，孙权就计划摔杯为号，弄死刘备，并安排吕范把这件事组织落实好，吕范于是安排手下得力干将贾华具体负责这件事，贾华埋伏了很多刀斧手，只等摔杯暗号。后来，贾华听到摔杯暗号，带人冲出来要砍刘备的时候，忽然发觉气氛不对，原来吴国太相中了刘备，不让杀这个得意女婿，吴国太当场把孙权臭骂了一顿，孙权挡不过，就谎称自己压根不知道有刀斧手这回事，说着便把锅甩给了吕范，吴国太又大骂吕范。吕范也是个官场老油条，反应也很快，转手又把锅甩给了贾华，贾华人老实，不知道再怎么甩，只得默默背锅，吃了这个哑巴亏。要不是刘备求情，贾华差点就在这里掉了脑袋。


贾华这位小小的配角，先是充当刺客，后又代人受过，免去上司的尴尬，最终被迫背锅，虽然侥幸保住性命，但小人物被迫背锅的命运，总让人有一种酸楚的感觉。

## 安全不投入、甩锅给员工还索赔 1000 万，某公司引发众怒

古往今来，甩锅和背锅的故事，始终在延续。职场中更是如此。

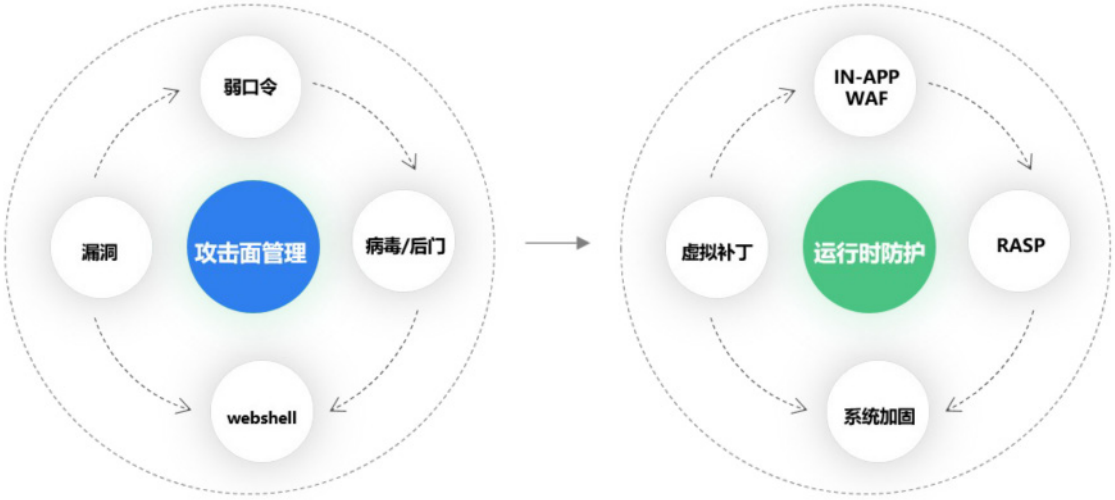
不久前，据媒体报道，某科技公司遭受黑客攻击，其研发数据遭受破坏无法恢复。令人匪夷所思的是，该公司没有去追查黑客，反而把自家员工郭某某告上法庭，并索赔 1000 万巨款。引发了各自媒体和网友的热议和声讨。

有网友评论说，“为了 1000 块的工资，差点背了 1000 万的债。”一语道出了老实人背锅的无奈。

据该公司称，服务器遭遇黑客攻击后，系统数据库遭到篡改、重要数据遭到破坏，当初买系统花费的 135000 元和投入的研发经费 1000 万元均无法挽回。该公司认为，郭某某作为项目经理及系统管理员，从未对数据库进行本地备份及查杀，造成数据丢失，属于严重失职，给公司造成重大经济损失，应当进行赔偿。

经过法院的二审判决，最终认为该公司提交的证据未显示郭某某工作职责的具体指向，亦无法证明在系统遭遇黑客攻击的因素下，因郭某某的工作失职造成了具体损失。因此，要求郭某某赔偿损失的请求缺乏事实与法律依据，法院不予以支持。

这场闹剧虽然结束了，但这个案件本身却值得我们深思：如果当时该公司明确 PRISM 系统和服务器安全就是郭某某的工作职责，那么发生了黑客入侵事件后，这 1000 万元是不是就应该由郭某某赔偿？以此案件为开端，其他公司在制定服务器管理人员职责时，会不会明确因黑客攻击造成的损失应该由服务器管理人员赔偿？？？




其实，《网络安全法》早已给出了答案：网络运营者需要制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。也正是因为上诉公司在内部安全管理制度上的缺失，郭某某侥幸躲过一劫。

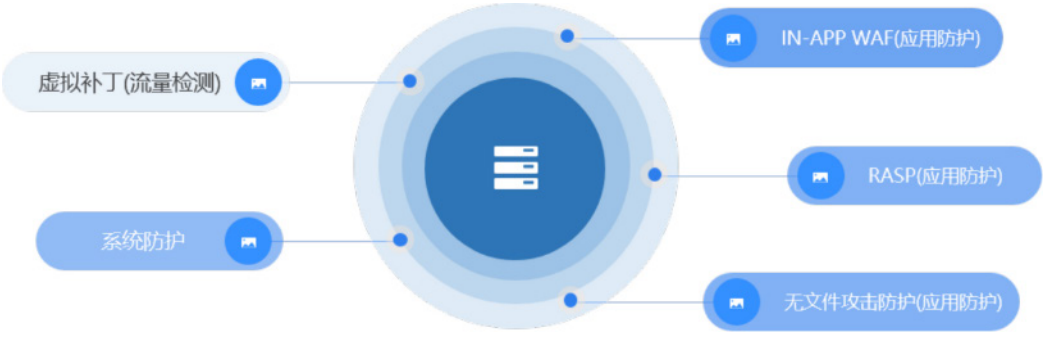
## 想“躺着”管好服务器 用椒图就行了

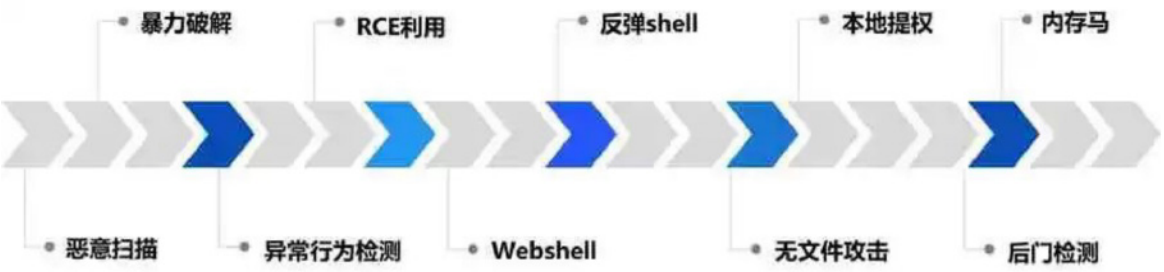
实际上，很多 IT 系统管理员并不是不想做好服务器安全，而是缺乏有力的“抓手”，对服务器安全风险看不清，缺乏有效的对抗手段，无法在遭到攻击后定位攻击者，以至于在黑客攻防中常常处于被动的位置。

**奇安信椒图云锁服务器安全管理系统（椒图）**是一款能够全面覆盖服务器攻击面管理、运行时防护的实战型服务器安全产品。椒图可以在服务器端构筑事前加固、事中对抗、事后溯源的全程防线，实现网络层、系统层、应用层一体化防护，可有效地保护服务器、虚拟机、云主机、容器等工作负载免受黑客及恶意代码攻击，满足实战攻防要求。

**首先，通过攻击面管理，显著降低被入侵风险。**

椒图通过从硬件配置、账户、进程、应用、端口、






网络连接等多个维度、细粒度清点服务器资产情况，为资产的统一管理、快速搜索、快速处置提供可靠抓手，有效避免 shadow IT(影子 IT)的出现，及时发现弱口令、危险端口暴露、漏洞等安全风险，对攻击面做有效收口。

除此之外，椒图还具备虚拟补丁能力，帮助客户实现在无法打补丁、无法重启的情况，依然可以对抗漏洞利用攻击，实现“漏洞检查 – 实体补丁 – 虚拟补丁”的闭环管理。

**其次，运行时防护，为服务器配上“免疫细胞”。**

椒图以 IN-APP WAF、RASP、无文件攻击引擎和系统加固为核心，构建了流量、应用、系统的全链路运行时防护体系，针对 web 攻击、无文件攻击、系统攻击分别提供相应的“针对性疫苗”，让防护能力、防护精准度大幅度提升。

**最后，攻击溯源，找到真凶，别再向员工“开枪”。**

椒图服务器威胁监测功能基于攻防实战打造，除了能对传统的暴力破解、恶意扫描、webshell、反弹 shell、本地提权、主机异常行为等常用攻击手段进行监测，还增加了无文件、内存马等新型攻击手段的监测。同时在告警中增加了进程树、可疑文件下载等多维度信息，提升告警的可研判性。并通过运营不断优化规则及检测引擎，持续降低误报率。

当发生安全事件后，用椒图可以精准定位黑客信息，无需再向员工“开枪”。

## 结束语：

从古代小说中的小人物背锅，到现实职场老实人屡屡“代人受过”，都充分说明一点，职场有风险，背锅需谨慎，不要只顾闷头赶路，不要一味盲目服从，在完成本职工作的基础上，一定要时不时的多思考、多权衡，不然，哪天一口大锅甩下来，吃亏的还是自己。

同样，对于网络安全而言，责任落实至关重要。今年 9 月，中央网信办会同相关部门起草了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（以下简称《网安法修订稿》）。其中明确指出，对于情节特别严重的违反网络运行安全一般规定的网络运营者和违反网络信息安全义务的网络运营者，除了保留对相关管理人员的罚款措施，《网安法修订稿》特别增加了“禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作”，有力强化了对涉及违法行为的相关管理人员的惩戒效果。

不仅仅是《网络安全法》，包括去年推出的《数据安全法》《个人信息保护法》《关键基础设施保护条例》一系列法律法规，都将责任落实放在至关重要的地位。只有制度清晰，责任落实，才能真正提升网络安全能力，将网络攻击销匿于无形，而不是出了事情之后，找老实人来背锅承受经济损失，损害名誉，可谓“一失万无”。安

# 超 950 亿条我国泄漏数据在海外非法交易

作者 奇安信行业安全研究中心

11 月 11 日，CEATI 威胁情报联盟牵头，奇安信行业安全研究中心、天际友盟等联合发布《中国政企机构数据安全风险分析报告》（以下简称《报告》），对 2022 年以来我国相关单位面临的数据安全风险进行了详细的解读。

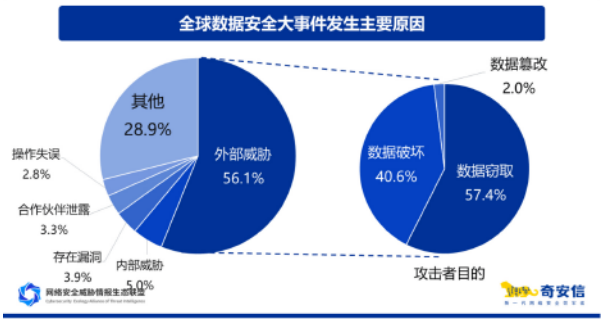
## 数据泄露是最大风险

《报告》显示，2022 年 1 月—10 月，安全内参共收录全球政企机构重大数据安全报道 180 起，其中数据泄露相关安全事件高达 93 起，占 51.7%。与近三年平均每月公开报道频次相比，2022 年相较前三年全球重大数据安全相关事件数量有小幅下降，略低于 2020 年和 2021 年。


并且，数据泄露已经超越数据破坏成为数据安全最大风险。与 2021 年相比，从数量来看，2021 年全球数据安全大事件，涉及数据破坏的有 102 件，占总量的 42.0%；涉及数据泄露的有 100 件，占总量的 41.2%。2022 年，全球数据安全大事件涉及数据破坏的大事件下降至 42 件，占总量的 23.3%；而数据泄露事件有 93 件，占 51.7%。可见近两年来，由于数据破坏导致的数据安全事件数量大幅减少，同时，数据泄露类事件一直较为严重。

从政企机构重大数据安全事件发生的原因来看，2022 年 1 月—10 月，超过五成安全事件是由于外部攻击（指没有获得认证的、未经授权的非法用户对内网进行的访问请求或攻击行为）导致的，但也有 5.0% 的事件是由于内部人员违规操作。3.9% 的重大数据安全事件是由于存在漏洞。

内鬼作案是数据安全事件发生的重要途径。我们不仅要防外也要防内，做好数据操作的审计，防止非授权信息读取，防止越权的敏感信息读取，还有一些过度的数据读取其实也是一种泄露。比如，在办一些业务的时候本来仅需知道该用户的姓名、性别及年龄，但是在相关资料上还有其联系方式、工作单位等信息，这样的过度读取或者暴露个人信息的行为也不合适。




## 超 950 亿条数据在海外非法售卖，个人信息占据大头

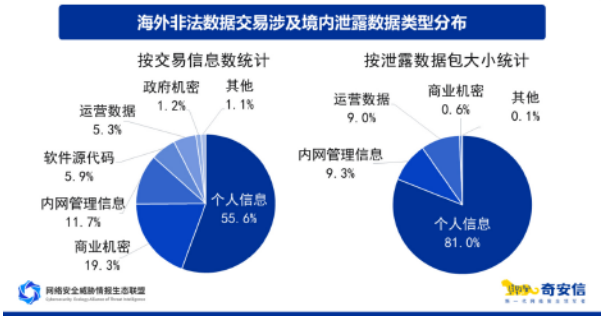
在数据被窃取后，有相当一部分数据被挂在非法网站上进行售卖。自 2022 年 3 月以来，奇安信威胁情报中心对 BreachForum 及各种暗网黑客黑产交易平台，以及 LeakIX（一个数据泄露监测的网站）、Telegram、Twitter 等海外网络平台上的数据泄露及交易信息（以下简称“交易信息”）进行了系统性的监测，并对其中涉及中国境内政企机构泄露数据的交易信息进行了评估和

验证。

截至 2022 年 10 月，奇安信威胁情报中心累计监测到境内政企机构泄露数据的海外非法交易信息 171 条。其中，共有 106 条交易信息明确给出了泄露数据的数量或数据包的大小，约占交易信息总量的 62.0%。

进一步分析显示，明确给出了泄露数据数量的交易信息共有 85 条，约占交易信息总数的 49.7%，合计约含有 950 多亿条各类数据；明确给出了泄露数据数据包大小的交易信息共有 40 条，约占交易信息总数的 23.4%，合计约有 46.4TB 数据信息。其中，有 19 条交易信息同时给出了泄露数据的数量和数据包大小。

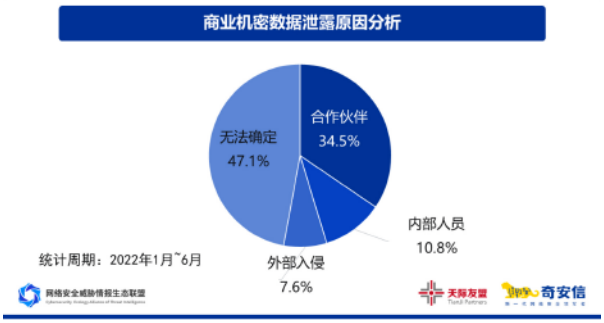
从交易信息的数量来看，55.6% 的交易，买卖的是个人信息数据；其次是商业机密数据，占比 19.3%；内网管理信息数据排第三，占比 11.7%。从泄露数据的数据包大小来看，个人信息至少有 37.6TB，占比高达 81.0%，同样排名第一；其次是内网管理信息，约有 4.3TB，占比为 9.3%；运营数据排名第三，约有 4.2TB，占比为 9.0%。




此外，从泄露数据的数量来看，个人信息数据约有 868.8 亿条，占比为 91.4%；其次是运营数据，约有 79.5 亿条，占比为 8.4%。二者之和占到了泄露数据总数量的 99.8%。

在商业数据泄露方面，2022 年 1 月—6 月，天际友盟共监测到商业机密数据泄露事件 1948 起，主要涉及文档数据泄露、代码数据泄露和文化版权数据盗版三大类数据泄露风险类型。

为全面了解政企机构商业机密数据泄露的原因，对部分数据泄露事件的原因进行了溯源分析。与人们一般的想象不同，商业机密数据泄露最主要的原因并不是黑客入侵或外部威胁，而是合作伙伴和内部人员的泄露。统计显示，约有 34.5% 的商业机密数据泄露是合作伙伴造成的；由内部人员泄露的商业机密，占比约为 10.8%；而真正是由于外部入侵造成的商业机密泄露，仅占比约为 7.6%。




而百度文库、道客巴巴、豆丁网、360 文库等文档分享平台，则是文档类商业机密数据泄露的主要渠道。

## 勒索病毒依然是国内数据安全的最大威胁

2022 年 1 月—9 月，95015 网络安全服务热线共接到全国各地大中型政企机构网络安全应急响应求助电话 697 起，其中，涉及到数据安全事件共 295 起，占比约为 42.3%。从事件损失来看，数据破坏事件 211 起，占所有应急响应事件的 30.3%；数据泄露事件 68 起，占比 9.8%；数据篡改事件 16 起，占比 2.3%。

对触发数据安全应急响应事件的原因进行分析发现，勒索软件是当前阶段对国内政企机构数据安全威胁最大的攻击方式，占到所有攻击方式的 59.7%；其次是漏洞利用，占比为 14.6%；钓鱼邮件排第三，占比 10.5%。此外，木马攻击（不含勒索软件）、非攻击事件也都是触发数据安全事件的重要原因。

从应急响应情况来看，数据安全问题也和内部人员的安全意识密切相关。比如，钓鱼邮件和非攻击事件，这两种攻击类型，都属于安全意识不足引发的数据安全问题。特别是非攻击事件触发的数据安全事件，绝大多数都是由于员工操作不当引起的。安

扫描阅读报告原文

## 大事记

### 齐向东在北京市工商联（商会）领导班子学习宣传贯彻党的二十大精神专题座谈会上发言

11 月 17 日，北京市工商联（商会）领导班子学习宣传贯彻党的二十大精神专题座谈会在京召开。北京市商会副会长，奇安信集团党委书记、董事长齐向东在座谈会上发言，他表示，在我国实现现代化新征程中，奇安信将以“科技引领、数字护航”为关键词，积极响应中央号召，践行总书记指示，这项工作责任重大、使命光荣。

作为网络安全国家队的带头人，齐向东代表科技企业家发言，表示要从龙头创新引领、国家安全支撑、网安人才培养、企业社会责任四方面发力，按照总书记的讲话要求，加快企业发展，为快速实现中国式现代化新征程做好数字护航。


### 奇安信成为工业和信息化部 5G 应用安全创新推广中心（广东）联通分中心生态合作伙伴

11 月 17 日，由工业和信息化部主办的 2022 年 IMT-2020(5G) 应用安全高峰论坛在深圳召开。奇安信集团受邀出席会议，并正式成为工业和信息化部 5G 应用安全创新推广中心（广东）联通分中心生态合作伙伴。


### 金融信创再获突破 奇安信可信浏览器中标某大型国有银行

近日，奇安信中标某大型国有银行信创浏览器采购项目，项目规模为全集团采购。该项目为大型国有银行中第一个全集团浏览器采购案例，为奇安信可信浏览器在大型银行开拓和推广，打造了高质量、可借鉴和可复制的落地标杆。

此前，奇安信可信浏览器已陆续在全国股份制商业银行、城商行、农商行等各类银行多次中标，充分满足了各类金融客户对浏览器的统一纳管、信创迁移、国密改造等需求，为业务安全保驾护航。

### 奇安信亮相 2022 中国互联网大会

11 月 15 日—17 日，2022（第二十一届）中国互联网大会在深圳召开。奇安信集团受邀出席，全方位展示数据安全建设体系及冬奥网络安全保障“零事故”成果。

在大会开幕论坛上，奇安信集团副总裁刘进在主题演讲时指出，大数据环境下，业务与数据流转更为复杂，需要数据安全管理与技术相结合，从组织、制度、流程上完善数据安全管理体系，有效支撑数据安全技术与运营更好地落地。


在数据安全论坛上，奇安信虎符基地作为“电信和互联网行业数据安全人才强基计划”首批人才基地获得授牌。虎符基地是奇安信打造的培养网络安全人才的战略板块，致力于安全运营与服务和向广大企事业单位提供多层次的网络安全、数据安全专业人才，已于 2021 年被工业和信息化部选为重点领域人才能力评价支撑机构。截至 2022 年 10 月，虎符基地共举办 60 期网络与信息安全特训班，累计培养安全专业人才 3692 人。


会上公布了“互联网助力经济社会数字化转型”案例名单。奇安信“基于内生安全的态势感知整体解决方案”入选互联网助力经济社会数字化转型案例集的“数字经济”方向。

会上，中国互联网协会还为在推动行业自律、履行社会责任、热心社会公益等方面表现突出的企业颁奖。继获得“2018–2020 年度中国互联网行业自律贡献和公益奖”后，奇安信蝉联“2021—2022 年度中国互联网行业自律贡献和公益奖”。


奇安信科技集团股份有限公司


## 锦州市人民政府与奇安信达成战略合作，共塑“数字锦州”城市新名片

11 月 17 日，在 2022 辽宁国际投资贸易洽谈会上，

锦州市人民政府与奇安信正式签署战略合作协议，共塑“数字锦州”城市新名片。

根据协议，双方将紧密围绕“数字辽宁 智造强省”发展战略，构建辽宁网络安全发展新格局，充分发挥奇安信在网络安全等方面的技术、人才储备优势，就网络安全和大数据产业等领域开展深入合作，共同促进锦州市网络安全与大数据产业健康快速发展。

## 打造城市下沉标杆 奇安国投 500 万中标湖北某市安全运营中心项目

近日，由奇安信集团和宜昌产投集团联合成立合资公司奇安国投中标湖北某县级市智慧城市采购项目（城运中心安全运维项目），项目总额超过 500 万。

该项目的落地，充分证明了奇安信在县市级建设城市安全运营中心的可行性，更突出了公司对城市安全运营布局的前瞻性和战略性，为将来在县级市等下沉市场开拓和推广，提供了高质量、可借鉴和可复制的落地标杆。

## 奇安信吴云坤：数字化保障新安全体系建设的三个关键点

11 月 11 日，第 37 次全国计算机安全学术交流会在云南昆明举行。CCF 计算机安全专委会数据安全工作组组长、奇安信集团总裁吴云坤在主题演讲中表示，要以内生安全的思路，构建面向数字化保障的新安全体系，形成体系化防御能力，通过实战化运行，做到网络安全“零事故”目标，护航数字化发展。

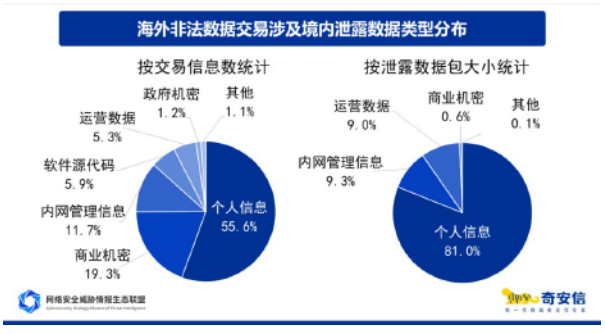
数字化保障必须建立体系化的防护能力。吴云坤提出了新安全体系建设的三个关键点：其一是建立能力导向、架构驱动的新安全体系；其二是用内生安全的方法指引新安全体系建设；其三是需要政企防御体系与网空对抗体系相互协同支援。


## 《中国政企机构数据安全风险分析报告》发布

11 月 11 日，由 CEATI 威胁情报生态联盟牵头，奇安信行业安全研究中心、天际友盟等联合发布了《中国政企机构数据安全风险分析报告》（以下简称《报告》），对今年以来我国相关单位面临的数据安全风险进行了详细的解读。

《报告》显示，2022 年 1 月—10 月，安全内参共收录全球政企机构重大数据安全报道 180 起，其中数据泄露相关安全事件高达 93 起，占 51.7%。

根据奇安信威胁情报中心监测信息分析显示，明确给出了泄露数据数量的交易信息共有 85 条，合计约含有 950 多亿条各类数据；明确给出了泄露数据的数据包大小的交易信息共有 40 条，合计约有 46.4TB 数据信息。



## 奇安信的 2022“乌镇时间”：引领安全市场发展 共创数字未来

11 月 9 日—11 日，2022 世界互联网大会在浙江乌镇举行。作为网络安全行业代表企业，奇安信集团连续四年亮相乌镇峰会，全面展示了我国网络安全行业的前瞻观点和先进成果。


在“互联网企业家论坛”上，吴云坤表示，数字经济蓬勃发展，让生产生活效率大幅提高，也放大了网络安全风险，勒索攻击、供应链攻击、数据窃取等安全事件频发。从中长期来看，未来网络安全产业会超过万亿规模。随着互联网新的应用场景的推动，网络安全涉及的范围也会更广，支撑着未来网络安全产业的规模。

在“数字技术论坛上”，吴云坤进一步提出，针对网络空间的复杂性，网络空间安全也是一个系统工程，要用系统工程的方法来解决安全问题，并与 IT、CT、OT 各方充分融合协同，才能有效推进中国的网络空间安全发展，保障国家的创新发展。

针对企业在数字经济时代的安全发展，奇安信集团首席战略官兼副总裁刘勇在“网安技术发展与国际合作论坛”上表示，全球数据安全正在形成大监管格局，无论是“走出去”还是“走进来”，企业都应当以数据安全合规为立身之本，做到“合规不踩线”。

在“开源技术生态创新发展论坛”上，刘勇表示，我国开源正处于空前的加速阶段，奇安信正积极推进国


内企业软件供应链安全建设，免费向中小企业提供开源软件的检测服务，积极构建开源安全生态。

为更好地挖掘数据要素价值，推进数据治理与利用，11 月 9 日下午，“之江杯”数据治理与利用大赛在乌镇举行启动仪式。大赛在浙江省委网信办、浙江省大数据发展管理局、中国网络空间安全协会指导下，由中国电子信息产业集团有限公司、之江实验室、浙江省网络空间安全协会、杭州未来科技城（海创园）管理委员会主办，杭州电子科技大学、浙江大学嘉兴研究院、奇安信集团承办。


## 奇安信中标约 1.45 亿海外某国家首都城市网络安全指挥中心建设项目

11 月 9 日，奇安信集团下属公司北京蔚灵科技有限

公司收到中标告知，确认公司为海外某国家首都城市网络安全指挥中心建设项目的供应商，预计项目交易金额约 2,000 万美元（约合人民币 1.45 亿元），中标产品主要为态势感知、威胁监测等软件类产品。

作为国内网安龙头企业，本次中标代表奇安信海外战略今年迈上新台阶，公司的相关产品和技术已经具备了较强的国际竞争力。此前，奇安信曾于 2021 年获得七千万海外业务大单，项目重点聚焦于 APT 监测方向。2022 年，奇安信集团海外业务持续保持高增长，新签订单相比去年增长了 100%。

## 奇安信亮相第十四届中国国际航空航天博览会

11 月 8 日，第十四届中国国际航空航天博览会在广东珠海国际航展中心正式拉开帷幕。奇安信作为网络安全“国家队”应邀参展，“冬奥网络安全保障中国方案”“汽车仿真平台漏洞攻防演示”、态势感知与安全运营平台（NGSOC）、电子取证等一众网安利器惊艳亮相，展现了网络安全领域的中国力量。


## MOSEC 2022 正式召开 移动安全研究百家争鸣

11 月 4 日，由奇安盘古（盘古实验室）和韩国 POC 主办的 2022MOSEC 移动安全技术峰会在上海隆重举行。大会吸引到了数百名来自移动安全领域的顶级白帽黑客及行业专家，围绕 iOS、Android、车载娱乐系统及 SoC 芯片等移动端软 / 硬件的漏洞挖掘、漏洞利用及安全防护等话题，为业界奉献了一场饕餮盛宴。

奇安信集团总裁吴云坤在致辞中表示，MOSEC 从 2015 年创立以来，一直坚持聚焦移动安全、专注于前沿技术，吸引聚集二进制漏洞攻防领域的顶级专家，还有他们的顶级成果和智慧，为移动安全领域的技术发展做出了贡献。


## 第六届补天白帽大会召开：多方聚力推动白帽人才实战化能力发展

11 月 3 日，2022 补天白帽大会在上海召开。来自政府、厂商、研究机构的重磅嘉宾和顶尖白帽汇聚一堂，

围绕培养实战化网络安全人才、构建多元化人才培养体系进行深入探讨，并分享先进白帽技术在实战场景中的应用。

为进一步推动相关领域安全建设，本次大会还专门设立了“数据安全”和“信创安全”两个分论坛，邀请了主管单位、信息化企业、网络安全及数据安全专家，围绕论坛主题进行研讨和分享。

## 奇安信与上海交大达成战略合作 打造一流网安创新和产业应用平台

11 月 3 日，奇安信集团与上海交通大学签约，成立“上海交通大学电子信息与电气工程学院 – 奇安信信息系统安全联合实验室”。联合实验室将搭建联合研究平台，支持信息系统安全领域的基础研究和应用基础研究工作。围绕安全基础理论研究、软件分析和漏洞挖掘、网络安全监测和防范、网络攻防对抗演练、物联网安全性分析、数据隐私安全合规、联合教学实践等方向展开深入合作，并推进相关技术成果的落地应用。


## 奇安信与茅台集团达成战略合作

10 月 27 日，奇安信集团受邀参加茅台集团 2023 年度采购与供应链大会，并与茅台集团签署战略合作协议。

双方将在网络安全咨询规划、网络纵深防御、数据安全防护、工业互联网安全防护、网络安全运行治理、网络安全人才培养等方面展开全面合作，共同探索白酒企业数字化安全建设新方案，为数字赋能茅台集团高质量发展保驾护航。

## 奇安信入选“奋进新时代”主题成就展

正在北京举行的“奋进新时代”主题成就展上，来自全国各行各业的一件件实物、一段段视频、一幅幅照片、一张张图表，集中向人们展示了十八大以来党和国家事业的伟大成就和巨大变革。

其中，奇安信冬奥会解决方案入选“坚定文化自信 建设社会主义文化强国”专题，北京网络安全大会（BCS2020）案例入选“全面践行总体国家安全观 开创新时代国家安全新局面”专题，记录了奇安信与新时代同频共振的成长印记。


## 荣誉墙

### 中国云安全市场达 120.6 亿 奇安信连续四年稳居市场第一

近日，赛迪顾问发布《2021—2022 年中国云安全市场研究年度报告》（以下简称《报告》）。《报告》显示，2021 年，中国云安全市场保持了 46.2% 的较高增长率，规模达到 120.6 亿元。在市场竞争格局上，奇安信保持快速增长态势，以 8.13 亿元的销售额位居市场第一位。

《报告》显示，2021 年，中国云计算安全市场规模达到 78.8 亿元，同比增长 47.6%，在整个市场中占比达 65.3%。在这个主力赛道，2021 年，奇安信以 10.3% 的份额，位居市场规模首位。

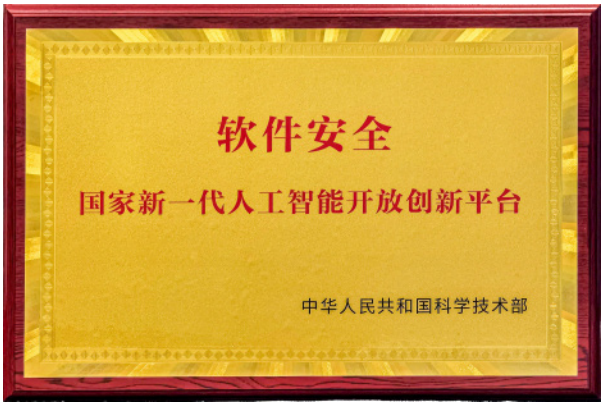
表 1　2021 年中国云安全市场品牌 TOP10 排名

| 排名 | 厂商 | 销售额（亿元） |
|---|---|---|
| 1 | 奇安信 | 8.13 |
| 2 | 绿盟科技 | 5.55 |
| 3 | 安恒信息 | 5.29 |
| 4 | 新华三 | 3.11 |
| 5 | 天融信 | 2.7 |
| 6 | 格尔软件 | 2.08 |
| 7 | 绿安科技 | 1.5 |
| 8 | 东软 | 1.09 |
| 9 | 云盾智慧 | 0.73 |
| 10 | 山石网科 | 0.6 |

### 建设首个软件安全领域国家开放创新平台 奇安信跻身“人工智能国家队”

近日，最新一批国家新一代人工智能开放创新平台企业名单公布，奇安信集团正式获得国家科技部批准，建设“软件安全国家新一代人工智能开放创新平台”。

为解决海量复杂软件的安全问题，夯实我国数字经济安全基础，此次批复建设的“软件安全国家新一代人工智能开放创新平台”，将依托奇安信集团，基于人工智能技术持续研究快速有效地发现软件安全问题的方法，面向软件开发、软件应用、安全分析三类用户提供服务，并通过开放平台支持创新创业，带动行业内的企业和个人共同研究运用人工智能解决软件安全问题。




### 总营收第一，三大赛道第一！赛迪报告显示奇安信行业龙头地位稳固

据赛迪顾问发布的《2021—2022 年中国网络信息安全市场研究年度报告》显示，2021 年，奇安信集团以 58.1 亿元的营业收入位居市场第一位，行业龙头地位进一步得以稳固。在终端安全、安全管理平台、安全服务等三大细分赛道，奇安信多年排名市场第一，而在竞争激烈的 UTM、Web 安全等领域，奇安信也持续保持市场前二的地位。

赛迪顾问在《报告》中指出，2021 年，奇安信集团通过打造认知、安全和授信三大能力，让网络安全体系

表 3　2021 年中国网络信息安全市场厂商 TOP10

| 排名 | 厂商 | 销售额(亿元) | 销售额占比（%） |
|---|---|---|---|
| 1 | 奇安信集团 | 58.1 | 6.8% |
| 2 | 启明星辰集团 | 43.6 | 5.1% |
| 3 | 深信服 | 36.9 | 4.3% |
| 4 | 新华三 | 35.2 | 4.1% |
| 5 | 华为 | 34.1 | 4.0% |
| 6 | 天融信 | 33.6 | 3.9% |
| 7 | 卫士通 | 27.9 | 3.3% |
| 8 | 绿盟科技 | 26.1 | 3.0% |
| 9 | 美亚柏科 | 25.4 | 3.0% |
| 10 | 安恒信息 | 18.2 | 2.1% |

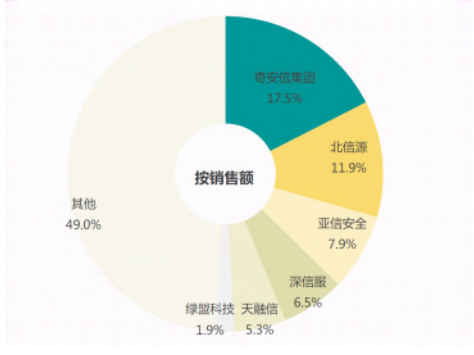
动起来，不断循环升级，让安全能力与日俱增。在“鲲鹏”“诺亚”“雷尔”“锡安”四大研发平台基础上进行全面升级，推出“川陀”“大禹”“玄机”“千星”新四大平台，以八大平台为基础核心组件，再配合少量定制化特殊组件，将大部分产品的研发速度从 3~6 个月，直接缩短到数周以内。

## EDR 营收超 3 亿元 奇安信终端安全位居国内市场第一

近日，国内知名研究机构赛迪顾问发布的《2021—2022 年中国网络信息安全市场研究年度报告》显示，在终端安全领域，市场规模达到 44.5 亿元，奇安信以 17.5% 的市场份额位居国内市场第一。

奇安信副总裁张庭透露在创新赛道终端安全检测与响应 (EDR) 方面，奇安信天擎终端安全响应系统优势地位明显，2021 年营收达到 3.02 亿元，成为国内首家突破三亿元营收的 EDR 供应商，并成为奇安信终端安全持续领跑的重要引擎。

图 14　2021 年中国终端安全市场品牌结构




## 中国网络安全企业 100 强发布 奇安信蝉联第一

11 月 15 日，国内网络安全媒体安全牛发布第十版《中国网络安全企业 100 强》。在申报的 300 余家安全厂商中，奇安信再次以 88.52 的总分荣登中国网络安全 100 强榜首，并在技术创新、行业应用等维度均位列第一，充分体现了网络安全龙头企业的整体竞争实力。


| 排名 | 企业简称 | 主营领域 | 总分 |
|---|---|---|---|
| 1 | 奇安信 | 综合性安全厂商 | 88.52 |
| 2 | 天融信 | 综合性安全厂商 | 88.05 |
| 3 | 绿盟科技 | 综合性安全厂商 | 83.65 |
| 4 | 华为 | 综合性安全厂商 | 83.03 |
| 5 | 安恒信息 | 综合性安全厂商 | 82.10 |
| 6 | 深信服 | 综合性安全厂商 | 81.56 |
| 7 | 新华三 | 综合性安全厂商 | 79.77 |

## 奇安信代码安全实验室研究成果成功入选国际顶会 USENIX Security 2023

日前，奇安信代码安全实验室研究员张之义以


FuzzJIT: Oracle-Enhanced Fuzzing for JavaScript Engine JIT Compiler

Authors:

Junjie Wang[1*], Zhiyi Zhang[2*], Shuang Liu[1*], Xiaoning Du[3], and Junjie Chen[1]

[1]College of Intelligence and Computing, Tianjin University
[2]CodeSafe Team, Qi An Xin Group Corp.
[3]Monash University

Abstract:

We present a novel fuzzing technique, FuzzJIT, for exposing JIT compiler bugs in JavaScript engines, based on our insight that JIT compilers shall only speed up the execution but never change the execution result of JavaScript code. FuzzJIT can activate the JIT compiler for every test case and acutely capture any execution discrepancy caused by JIT compilers. The key to success is the design of an input wrapping template, which proactively activates the JIT compiler and makes the generated samples oracle-aware themselves and the oracle is tested during execution spontaneously. We also design a set of mutation strategies to emphasize program elements promising in revealing JIT compiler bugs. FuzzJIT drills to JIT compilers and at the same time retains the high efficiency of fuzzing. We have implemented the design and applied the prototype to find new JIT compiler bugs in four mainstream JavaScript engines. In one month, ten, five, two, and 16 new bugs are exposed in JavaScriptCore, V8, SpiderMonkey, and ChakraCore, respectively, with three demonstrated exploitable.

*These authors contributed equally to this work.

共同一作身份与天津大学王俊杰教授团队完成学术论　文《*FuzzJIT: Oracle-Enhanced Fuzzing for JavaScript Engine JIT Compiler*》，被信息安全领域四大顶级会议之一 USENIX Security 2023 录用。

## 中国网安行业唯一 奇安信再摘“世界互联网领先科技成果”

11 月 9 日，2022 年世界互联网领先科技成果在乌镇峰会正式对外发布。奇安信集团“奇安信大禹平台及重大网络安全防护应用”项目作为中国网络安全行业唯一代表性成果，入选领先科技成果提名。此前，“内生安全框架”曾荣获 2020“世界互联网领先科技成果”。


## 连续三年位居网安企业头名！奇安信再登“中国先进计算企业百强榜”

11 月 5 日，在长沙举行的 2022 世界计算机大会发布了“2022 中国先进计算企业百强榜”。凭借领先的算力、算法等技术优势和优异的市场表现，奇安信连续三年入围该榜单，并且均位居网络安全企业头名。

此次“先进计算企业百强榜”的评选，企业的整体实力、成长潜力、研发水平、产品领先性、产业生态 5 大项一级指标和 26 项二级指标进行综合评估，是对中国企业界的数智化应用水平与创新能力的一次较全面呈现，将成为企业选择数智化转型路径的重要参考。

**2022先进计算百强榜Top20**

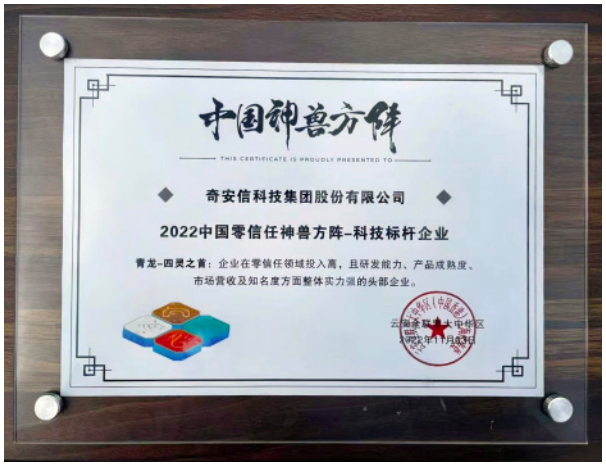
| 排行 | 企业名称 | 排行 | 企业名称 |
|---|---|---|---|
| 第一名 | 华为技术有限公司 | 第十一名 | 百度在线网络技术（北京）有限公司 |
| 第二名 | 英特尔(中国)有限公司 | 第十二名 | 戴尔（中国）有限公司 |
| 第三名 | 浪潮集团有限公司 | 第十三名 | 思爱普（中国）有限公司 |
| 第四名 | 英伟达半导体科技（上海）有限公司 | 第十四名 | 深圳市腾讯计算机系统有限公司 |
| 第五名 | 微软（中国）有限公司 | 第十五名 | 三星集团 |
| 第六名 | 用友网络科技股份有限公司 | 第十六名 | 中国电信集团有限公司 |
| 第七名 | 联想集团 | 第十七名 | 奇安信科技集团股份有限公司 |
| 第八名 | 超威半导体（中国）有限公司 | 第十八名 | SK海力士半导体（中国）有限公司 |
| 第九名 | 中芯国际集成电路制造有限公司 | 第十九名 | 希捷科技有限公司 |
| 第十名 | 苹果（中国）有限公司 | 第二十名 | 启明星辰信息技术集团股份有限公司 |

## 位居“四灵之首”！奇安信入围 CSA“中国零信任神兽方阵”

11 月 3 日，国际云安全联盟大中华区（CSA GCR）《中国零信任神兽方阵》报告重磅发布，奇安信凭借在零信任市场的技术实力、实践成果等多方面领先优势和市场影响力入围该报告，被评为“青龙－四灵之首”科技标杆企业。

“中国神兽方阵”是基于中国传统文化创立的分析模型，模型包含“青龙－四灵之首”“白虎－战斗之神”“朱雀－功力之神”“玄武－后起之秀”四象。报告基于该模型，从技术先进性和市场影响力两大维度评估中国零信任厂商，从研发能力、知识产权、产品成熟度、营收

情况等六个子维度做出分析评估。其中，青龙作为四灵之首，是指企业在零信任领域投入高，且研发能力、产品成熟度、市场营收及知名度方面整体实力强的头部企业。




## “数据安全服务前十家企业”榜单发布 奇安信集团荣登榜首

11 月 2 日，中国互联网企业综合实力指数（2022）发布会暨百家企业高峰论坛在厦门举行。会上发布了《中国互联网企业综合实力指数报告（2022）》，并首次发布数据安全服务前十企业名单，奇安信集团成功入选并位列第一。


凭借丰富的产品布局和扎实的技术基础，奇安信数据安全业务快速增长。2021 年奇安信数据安全与隐私保护产品收入超过 11 亿元，同比增长率超过 50%；2022 年前三季度，数据安全业务增速超 45%，继续保持高速增长，成为拉动公司发展的重要引擎之一。浙商证券、华泰证券、太平洋证券、华西证券等多家证券公司给予奇安信买入评级。

## “长沙市城市网络安全运营中心”获 IDC 2022 年亚太区智慧城市大奖

10 月 27 日，2022 年 IDC 亚太区智慧城市大奖（SCAPA）评选结果公布，“长沙市城市网络安全运营中心”项目被评为 IDC 2022 年亚太区智慧城市大奖（中国区）“灾难应对 / 应急管理” 类别最佳智慧城市项目。

## 奇安信入围上海经信委 2022 年度网络安全产业创新攻关成果目录

10 月 26 日，上海市经济和信息化委员会公布了《2022 年度上海市网络安全产业创新攻关成果目录》名单。奇安信网神安全访问服务（Q-SASE）以突出的创新性，在央企、国企等较好的应用推广效应及产业化潜力，成功入围该目录的安全访问服务边缘（SASE）方向。

附件

2022 年度上海市网络安全产业创新攻关成果目录

| 类别 | 序号 | 攻关方向 | 企业 | 成果名称 |
|---|---|---|---|---|
| 基础技术创新 | 1 | 隐私计算 | 上海富数科技有限公司 | 支持海量数据可信流通的隐私计算平台 |
| | | | 杭州锘崴信息科技有限公司 | 基于隐私保护的医疗多中心临床研究系统 |
| | 2 | 新一代数字身份认证 | 上海市数字证书认证中心有限公司 | 新一代数字身份认证服务体系 |
| | 3 | 人工智能安全 | 上海雾帜智能科技有限公司 | HoneyGuide 智能风险决策系统 |
| | 4 | 软件供应链安全 | 中电科拟态安全技术有限公司 | 电科·安测·探巡 |
| | 5 | 云原生安全 | 阿里云计算有限公司 | 阿里云云原生安全方案 |
| | 6 | 安全访问服务边缘（SASE） | 中国电信股份有限公司上海研究院 | 云化边缘安全网关 |
| | | | 奇安信科技集团股份有限公司 | 奇安信网神安全访问服务（Q-SASE） |
| | 7 | API 安全 | 上海斗象信息科技有限公司 | API 安全之眼监测系统 |
| | | | 上海派拉软件股份有限公司 | 派拉 API 安全平台 |

奇安信
新一代网络安全领军者

# 聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。


## 国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

## 首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

## 将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

## 重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

## 专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

## 市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一 ——数世咨询认证

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

网络安全 中国代表队 | 奇安信

2022年北京冬奥会胜利闭幕

# “零事故”

## 奇安信圆满完成冬奥会网络安全保障任务

# 奇安信蝉联“中国网安产业竞争力50强”第一名


6月23日，中国网络安全产业联盟（CCIA）
揭晓“2022年中国网安产业竞争力50强”榜单。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信蝉联第一名。


奇安信科技集团股份有限公司

CCIA 50强

2022年中国网安产业竞争力50强

编号：CCIA-2022JZL-01

中国网络安全产业联盟
2022年6月

## “2022年中国网安产业竞争力50强”榜单

| TOP15 | 公司名称 |
|---|---|
| 1 | **奇安信科技集团股份有限公司** |
| 2 | 深信服科技股份有限公司 |
| 3 | 启明星辰信息技术集团股份有限公司 |
| 4 | 天融信科技集团股份有限公司 |
| 5 | 华为技术有限公司 |
| 6 | 绿盟科技集团股份有限公司 |
| 7 | 腾讯云计算（北京）有限责任公司 |
| 8 | 阿里云计算有限公司 |
| 9 | 新华三技术有限公司 |
| 10 | 杭州安恒信息技术股份有限公司 |
| 11 | 360政企安全集团 |
| 12 | 亚信安全科技股份有限公司 |
| 13 | 成都卫士通信息产业股份有限公司 |
| 14 | 杭州迪普科技股份有限公司 |
| 15 | 山石网科通信技术股份有限公司 |