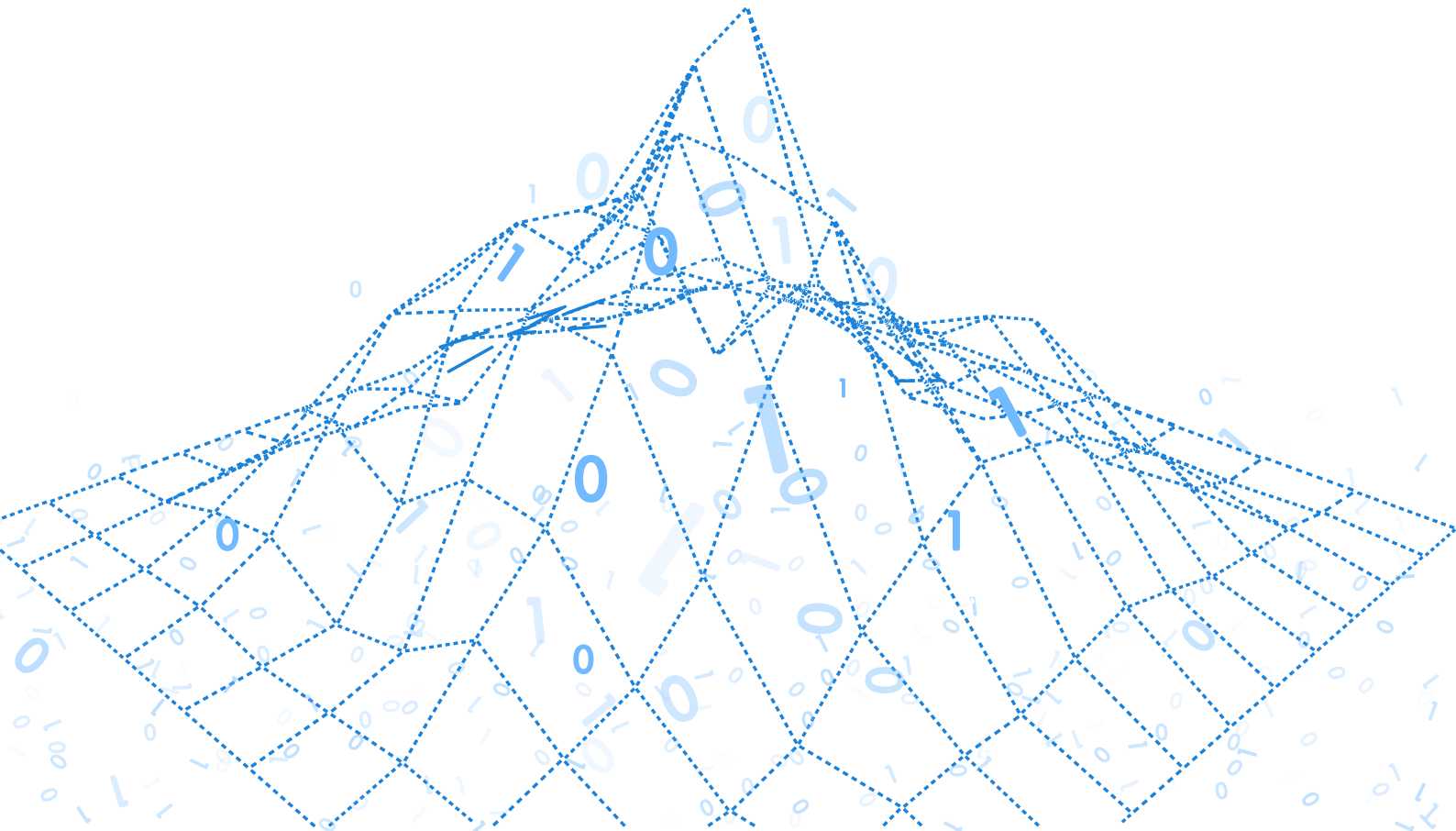
2023年第三期 | 总第五期

全球开源发展态势洞察



开放原子开源基金会出品
2023年2月20日

目录

国际开源基金会

KubeEdge 达到软件供应链 SLSA L3 等级

KubeEdge 社区已于 2022 年 7 月，完成整个 KubeEdge 项目的第三方安全审计，已发布云原生边缘计算安全威胁分析和防护白皮书，并根据安全威胁模型和安全审计的建议，对 KubeEdge 软件供应链进行持续安全加固。

在 KubeEdge 社区的不断努力下，在 2023 年 1 月 18 日发布的 v1.13.0 版本中，KubeEdge 项目已达到 SLSA L3 等级（包括二进制和容器镜像构件），成为 CNCF 社区首个达到 SLSA L3 等级的项目。这意味着，KubeEdge 实现 SLSA L3 等级标准后，可以端到端的从源码构建到发布流程进行安全加固，保障用户获取到的二进制或容器镜像产物不被恶意篡改。

行业发展

麦肯锡收购从事人工智能和机器学习的 Iguazio

近日，麦肯锡收购了总部位于以色列特拉维夫的 Iguazio，该公司专门从事人工智能和机器学习。通过此次收购，麦肯锡将能够快速扩展 AI 部署，实现加速生产路径并在极短的时间和有限的资源范围内，为客户提供行业特定的 AI 解决方案，横跨金融服务、医疗保健、制造、电信、娱乐等广泛行业。这些解决方案的生产率将提高五倍，从概念验证到生产的速度将提高八倍，可靠性将提高一倍。足以预见，此次收购将会帮助麦肯锡能够以更少的资源、更低的成本实施人工智能部署。

Istio 宣布 2023 年贡献席位结果

近日，据 Istio 官方消息，根据席位分配流程，今年谷歌将分配到 5 个席位，IBM/Red Hat 将分配到 2 个。作为过去 12 个月里 Istio 的第三大贡献者，华为获得了 2 个贡献席位。

Cilium 发布安全审计报告和模糊测试审计报告

通过借助第三方的安全审计和模糊测试，以帮助项目识别代码在改进过程中存在的潜在漏洞，进而提高安全状态。近日，Cilium 项目发布了两份报告：安全审计和模糊测试审计。

本次安全审计和模糊测试共计发现 30 个问题，但并未发现关键风险漏洞。其中，包含两个中风险问题，第一个问题是缺少易于访问的关于安全运行 Cilium 的文档，该问题正在处理中；第二个是在配置错误的情况下，可能无法解锁互斥锁 mutex，该问题已修复，其余的都是低风险或信息性的问题。总的结论是，Cilium 是一个非常安全的项目，审计并未发现严重的漏洞。

基于 Kubernetes 事件驱动自动缩放项目 KEDA 公布安全审计结果

基于 Kubernetes 事件驱动自动缩放（Kubernetes-based Event Driven Autoscaling）项目，在 2022 年底由 Trail of Bits 进行安全审计。在战略合作伙伴 OSTIF 的帮助下，KEDA 加

入了越来越多的 CNCF 项目审计名单，以改善安全状况，并帮助达到毕业阶段。威胁建模、手动代码审查和自动化测试工具的组合被用于这项工作。

本次审计发现了 Redis Scalers 中的一个重大缺陷，该缺陷可能会影响系统的机密性、完整性或可用性。这个问题与加密和绕过 TLS 有关，从而允许潜在的 MitM（中间人）攻击。目前，该问题已修复。此外，基于审计结果，KEDA 还更新了现有的安全工具链，引入了 semgrep 工具和 TLS 证书管理。

SUSE 推出企业级容器管理平台 Rancher Prime

为致力于满足企业用户的使用场景，SUSE 正式推出 Rancher Prime，Rancher Prime 是 Rancher 的一种分发版，核心功能代码均来自于 Rancher 社区版，不仅更加重视平台安全方面的管理建设，而且面向企业用户强化了相关功能和服务。

Rancher Prime 的新功能和增强能力在于：

• 综合安全治理能力得到提升，为企业用户提供可信的镜像仓库；

• 引入 UI 扩展功能；

• 对 Native Cloud 的支持，扩展到对阿里云、腾讯云以及华为云的托管集群的全生命周期支持；

• 对国产 OS 的支持，扩展对 openEuler Linux 的支持，并将其列入长期支持列表中；

• 对 ARM 体系的支持。

Red Hat 云原生 CI/CD 解决方案 OpenShift Pipelines 1.9 发布

OpenShift Pipelines 是基于 Kubernetes 资源的云本地、持续集成和持续交付（CI/CD）解决方案。它使用 Tekton 构建块，通过抽象底层实现细节，实现跨多个平台的自动化部署。

近日，红帽云原生 CI/CD 解决方案 OpenShift Pipelines 1.9 版本发布，其新功能和增强能力在于：

•Pipelines as Code 已正式可用，且支持在源代码存储库中定义 Tekton 模板；

• 支持存储库 CRD 的并发限制；

• 支持对管道中的 URL 进行身份认证；
• 新增 Resolvers 功能用于处理远程任务和管道的请求。

Red Hat 高级集群管理平台 Advanced Cluster Management for Kubernetes 2.7 发布

红帽高级集群管理平台 Advanced Cluster Management for Kubernetes，其是红帽专为混合云环境设计的 IT 管理技术产品系列的成员，能帮助企业利用跨混合云和多云环境的企业级管理能力，进一步延伸并扩展红帽 OpenShift，使其能够管理多个 Kubernetes 集群，在确保策略和治理措施执行的同时，实现跨混合云的多集群应用部署。

近日，红帽高级集群管理（Red Hat Advanced Cluster Management for Kubernetes）2.7 版本发布，其新功能和增强能力在于：

• 支持根据依赖关系进行执行策略的排序、策略生成器支持引用本地和远程定制配置、扩大边缘可管理的集群数至 3500 个；
• 支持在 ARM 架构上创建集群；
• 针对大规模环境的搜索组件正式可用；
• 支持使用新的 Submariner LoadBalancer 模式来简化集群部署；
• Submariner 支持无网络环境的集群。

Tigera 发布 Kubernetes 容器安全防护方案 Calico Runtime Threat Defense

据官方消息，Tigera 致力于为 Kubernetes 容器部署提供安全和合规解决方案，于 2023 年 2 月 15 日，正式发布 Kubernetes 容器安全防护方案 Calico Runtime Threat Defense。通过结合签名和基于行为的技术来检测已知威胁和零日威胁，能够检测出 MITRE 最常见的容器和网络的攻击。Calico Runtime Threat Defense 与传统运行的安全防护检测平台存在不同，其无需编写复杂的规则即可持续监控和分析网络和容器行为，寻找并获取攻击指标（IOA）。

AtomicJar 发布集成测试工具 Testcontainers Cloud

Testcontainers Cloud 是基于轻量级、易使用的开源测试框架 Testcontainers 进而构建的，主要是通过 Docker 容器以创建更真实的测试环境。云原生应用开发者可以实现在将代码通过持续集成（CI）平台转移到生产环境之前，独立完成测试应用程序，而无需借助专门应用测试团队的帮助，即可完成依赖关系的测试。

云原生安全检测器 Narrows，在 Harbor 上增加容器安全的动态扫描

近日，Narrows 与 Harbor 进行了集成。Narrows 允许用户通过简单的界面来定义对 Kubernetes 集群中工作负载的安全期望，并根据用户指定的扫描器和扫描周期对工作负载进行扫描，对于不满足安全要求的工作负载进行隔离。具体的更新内容如下：

• Narrows 能够对 Kubernetes 集群和其中的工作负载进行运行时的安全态势评估，发现 Kubernetes 集群的错误配置，终止工作负载运行时中的攻击；

• 对扫描报告进行汇总、聚合和分析并提供开放的 API 接口；

• 与 Harbor 无缝集成，对于外部公共镜像仓库的镜像，可以自动同步到 Harbor 中，以生成安全数据。

用于 GitHub Actions 的 SLSA 3 Container Generator 正式可用

近日，用于 GitHub Actions 的 SLSA 3 Container Generator（1.4.0 版）正式可用。其允许任何 GitHub 项目生成符合 SLSA 第 3 级标准的溯源声明，因此用户可以验证他们使用的容器镜像的来源。以前的工具允许用户为文件制品生成溯源信息，但是容器生成器（Container Generator）能够支持容器生态系统。它通过允许溯源声明与容器注册表中的镜像一起分发，并直接与 Sigstore 兼容的工具集成以进行检查和验证。

NASA 招募 Microchip、SiFive 为自主太空任务开发 RISC-V12 核处理器 SoC

NASA 的喷气推进实验室（JPL）任命 Microchip 来设计和制造基于 SiFive 的 8 个 RISC-V X280 核的多核高性能航天计算机（HPSC）SoC，并为 VPU 的 2 个集群增加了 4 个 RISC-V 核用于通用计算。该项目的运营目标是提供与较当前航天计算机相比，100 倍的飞行计算技术计算能力。在最近的 RISC-V 峰会上，HPSC 领导团队成员、JPL 顾问 Pete Ficco 解释了 HPSC 项目的总体目标。

沃达丰通过 CAT-M 物联网链路首次进行欧洲语音通话

CAT-M 网络旨在通过单个移动电话站点支持许多物联网（IoT）设备，并保证不会降低智能手机用户的服务质量。但是带宽可能会被故意限制。这是全球最小 LTE-M/NB-IoT RISC-V 芯片方案。

全球首届 RISC-V 高性能计算征文通道已经开启

全球首届 RISC-V 高性能极计算研讨会将于 2023 年 5 月 25 日在德国汉堡举行。此次大会征文通道已经开启：

https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines

论文截止日期：2023 年 3 月 24 日

入选通知日期：2023 年 4 月 10 日

最终稿日期：2023 年 5 月 1 日

开源安全

GitHub 更新 Copilot 编码助手，增加漏洞过滤系统

近日，GitHub 更新了其 Copilot 编码助手，增加了新功能，包括“漏洞过滤系统”以阻止不安全的编码模式。例如，SQL 注入或硬编码凭据。改进的 AI 模型和技术也提高了建议代码的接受程度，自 2022 年 6 月首次推出 GitHub Copilot for Individuals 时，平均超过 27%的开发者会选择使用 GitHub Copilot 生成代码。发展到今天，选择使用 GitHub Copilot 生成代码的比重上升到 46%。

Redpanda 存在凭据泄露漏洞

Redpanda 是一个数据流处理平台。

在该项目受影响版本中，存在凭据泄露漏洞，由于该项目的 import.go 代码在导入 rpk 文件时会以明文形式将 AWS Access Key ID 和 Secret 记录到标准输出中。具有本地用户权限的攻击者可以通过控制台中查看密钥，或通过 Kubernetes 日志查看。

Django 存在拒绝服务漏洞

Django 是一个开放源代码的 Web 应用框架，由 Python 编写，最初用于管理劳伦斯出版集团旗下的一些以新闻内容为主的网站，即 CMS（Content Management System，内容管理系统）软件，于 2005 年 7 月在 BSD（Berkeley Software Distribution）许可证下发布。

在该项目受影响版本中，存在拒绝服务漏洞，由于 multipartparser.py 中的 parse 函数在处理上传的文件时没有限制文件数量。远程攻击者在上传文件时，可同时上传多个文件致使 Django 因打开文件过多而内存耗尽，进而造成拒绝服务。

Apache Sling JCR Base 存在 JNDI 注入漏洞

Apache Sling JCR Base 提供 JCR 实用程序类和对存储库挂载的支持，是 ApacheSling 项目的一部分。

在 JDK 1.8.191 或更低版本中运行 Apache Sling JCR Ba

se 且项目版本小于 3.1.12 时，可能存在 JNDI 注入漏洞，由于 RepositoryAccessor.java 中的 getRepository 方法和 getRepositoryFromURL 方法对传入的参数验证不当导致 JNDI 或 RMI 注入。远程攻击者可以通过 JDNI 和 RMI 连接访问存储在服务器上的任意数据。

Git apply 存在路径穿越漏洞

Git 是一个免费的开源分布式版本控制系统工具，旨在快速高效地处理从小型到大型的所有项目。它是由 Linus Torvalds 在 2005 年创建的，用于开发 Linux 内核。

在 Git 受影响版本中，存在路径穿越漏洞。由于 Git 中 git apply 命令用于将补丁应用到代码仓库中，为了防止恶意补丁在工作空间之外创建文件，git apply 会限制通过符号链接绕过的行为。但当恶意补丁先创建符号链接时，即可绕过此机制。

在用户使用 git apply 命令时，如果应用了攻击者构造的恶意补丁，则可在受害者的文件系统上写入任意文件。

当 git 被用在服务端中时(如在 Gitlab 的 Gitaly 服务中)，可能会导致攻击者能在服务端执行任意命令。

Argo CD 存在权限管理不当漏洞

Argo CD 是以 Kubernetes 作为基础设施，遵循声明式 GitOps 理念的持续交付（continuous delivery, CD）工具，支持多种配置管理工具，包括 ksonnet/jsonnet、kustomize 和 Helm 等。

在该项目的受影响版本中，存在权限管理不当漏洞，由于 cluster.go 文件的 Update 方法对于用户权限限制不严格，如果攻击者能够修改至少一个集群 secret，则可以利用该漏洞修改任何集群的 secret，进而控制 Kubernetes 资源，或阻止其与外部集群的连接。

node-jose 存在拒绝服务漏洞

node-jose 是一款开源的 JSON 对象签名和加密（JOSE）的 JavaScript 包。

在使用 node-jose 2.2.0 版之前的 JS 环境中，当使用非默认的降级加密算法时（即 WebCrypto API 和 Node crypto 模

块都不可用时），由于 node-jose 内部计算中的 ECC 操作存在无限循环，进而导致拒绝服务（DOS）。该问题已在版本 2.2.0 中进行了修补。此问题仅存在于降级加密实现中，建议用户在运行 node-jose 的 JS 环境中可用 WebCrypto API 或 Node crypto 模块来避免。

Apache Commons SCXML 存在远程代码执行漏洞

Apache Commons SCXML 用于创建和维护 Java State Chart XML（SCXML）引擎，支持 JEXL, Javascript, Groovy 和 XPath 表达式。

攻击者可向 Commons SCXML 传入嵌入 script 标签的恶意 XML 文件，当存在 SCXMLExecutor#go()方法调用时，XML 中的表达式代码将被执行，从而执行任意系统命令。

Apache Kafka Connect 模块 JNDI 注入漏洞

Kafka 最初是由 Linkedin 公司开发的，是一个分布式的、可扩展的、容错的、支持分区的（Partition）、多副本的（replica）、基于 Zookeeper 框架的发布-订阅消息系统。它是分布式应用系统中的重要组件之一，也被广泛应用于大数据处理。Kafka 是用 Scala 语言开发，它的 Java 版本称为 Jafka。Linkedin 于 2010 年将该系统贡献给了 Apache 软件基金会并成为顶级开源项目之一。

在 Kafka 2.3.0 至 3.3.2 版本中，具有 Kafka Connect worker 访问权限且可以创建/修改 Connect 的攻击者可通过将 Connect 的任意 Kafka 客户端的 sasl.jaas.config 属性设置为 com.sun.security.auth.module.JndiLoginModule（此操作可通过 producer.override.sasl.jaas.config、consumer.override.sasl.jaas.config 或 admin.override.sasl.jaas.config 属性完成），进而可将 Connect 的属性 user.provider.url 设置为攻击者可控的 LDAP 服务器地址，并通过 Connect 反序列化可控的 LDAP 响应远程执行恶意代码或造成拒绝服务。

OpenSSL 存在拒绝服务漏洞

OpenSSL 是一个开源的软件库，使用包含了众多加解密算法，用于传输层安全性（TLS）和安全套接字层（SSL）协议的强大、商业级和功能齐全的工具包。

在受影响版本的 OpenSSL 的 X.509 GeneralName 中，存在 X.400 地址类型混淆漏洞。由于 X.400 地址被解析为 ASN1_STRING，但 GENERAL_NAME 的公开的结构体定义中错误地将 x400 Address 字段类型声明为 ASN1_TYPE，导致 OpenSSL 的 GENERAL_NAME_cmp 函数将此字段解释为 ASN1_TYPE。当 OpenSSL 启用 CRL 校验时（如应用程序设置 X509_V_FLAG_RL_CHECK 标志），攻击者向 memcmp 调用传递任意指针，进而读取内存或造成拒绝服务。

前沿技术

分布式云原生平台 Kurator v0.2.0 发布

Kurator 是华为云开源的分布式云原生平台，帮助用户构建属于自己的分布式云原生基础设施，助力企业数字化转型。Kurator v0.1 版本通过一键集成 Karmada、Volcano、Istio、Prometheus 等主流开源项目，提供了分布式云原生的统一多集群管理，统一的调度，统一的流量治理以及统一的应用监控能力。

在最新发布的 v0.2.0 中，Kurator 新增两大类关键特性，增强了可观测性并新增了集群生命周期管理，具体包括以下重大更新：

- 基于 Thanos 的多集群监控及指标持久化存储；
- 基于 Pixie 实时的 K8s 应用监控；
- 支持本地数据中心集群生命周期管理
- 支持 AWS 云上自建集群生命周期管理

Kurator 由此开始提供分布式云原生基础设施的管理。这意味着，从此 Kurator 可以依托基础设施、Kubernetes 集群，更好的管理各种云原生中间件，为用户提供开箱即用的分布式云原生能力。

OpenShift 日志管理方案 Logging 5.6 发布

近日，OpenShift 日志管理方案 Logging 5.6 发布，更新内容：

- 兼容 OpenShift 容器平台集群范围内的加密策略；
- 支持通过 LokiStack 创建自定义租户资源、流和全局策略和保留策略，并按优先级排序；
- 新增日志转发输出选项 Splunk；
- Vector 取代 Fluentd 作为默认收集器。

服务网格 Istio v1.17 发布

近日，服务网格 Istio v1.17 发布，更新内容：

- 金丝雀升级的修订标签升级为 Beta；
- 基于 Helm 安装 Istio 升级为 Beta；
- 完全兼容最新版 Kubernetes Gateway API（0.6.1）；

• 优化 IPv4/IPv6 双栈支持；
• 增加对监听器过滤器补丁的支持；
• 支持使用加解密技术 QuickAssist Technology（QAT）PrivateKeyProvider。

云原生存储 OpenEBS v3.4.0 发布

OpenEBS 是一种开源云原生存储解决方案，托管于 CNCF 基金会。OpenEBS 是 Kubernetes 本地超融合存储解决方案，它管理节点可用的本地存储，并为有状态工作负载提供本地或高可用的分布式持久卷。作为一个完全的 Kubernetes 原生解决方案的另一个优势是，管理员和开发人员可以使用 kubectl、Helm、Prometheus、Grafana、Weave Scope 等 Kubernetes 可用的所有优秀工具来交互和管理 OpenEBS。

近日，云原生存储 OpenEBS v3.4.0 发布，更新内容：

• 支持通过 OpenEBS helm chart 安装 Mayastor；
• 支持在故障检测时按需切换 Mayastor 节点；
• 支持使用 NDM 的 NVMe 虚拟路径检测；
• 修复 LVM LocalPV helm chart 的拉取镜像密钥错误；
• 在 NFS 服务器部署中添加后端卷 PVC 上下文作为标签。

CNI 插件 Cilium v1.13.0 发布

近日，CNI 插件 Cilium v1.13.0 发布，更新内容如下：

• 支持 Gateway API v0.5.1；
• 增加 IPv6 BIG TCP 支持；
• 支持 LoadBalancer IP 地址管理；
• 初步支持 SCTP；
• 支持根据标签选择器对节点进行细粒度的配置；
• 支持 k8s 1.26；
• 支持通过 BGP 控制平面宣告 LoadBalancer 服务的功能；
• 支持通过内置 Envoy 代理实现现有 Kubernetes service 的 L7 负载均衡；
• Ingress 资源可以共享 Kubernetes LoadBalancer 资源；
• datapath 支持 mTLS；

• 支持 Service 内部流量策略；
•对所有镜像创建 cosign 签名，为每个镜像创建 SBOM。

Envoy Gateway v0.3 发布

Envoy Gateway 可以被认为是 Envoy Proxy 核心的一个封装器。它不会以任何方式改变核心代理、xDS、go-control-plane 等（除了潜在的驱动功能、bug 修复和一般改进以外）。

近日，Envoy Gateway v0.3 发布，更新内容如下：

• 支持扩展的 Gateway API 字段；
• 支持 TCP 路由 API、UDP 路由 API、GRPC 路由 API；
• 支持全局速率限制；
• 支持请求认证。

GitOps 工具 Argo CD v2.6.0 发布

近日，GitOps 工具 Argo CD v2.6.0 发布，更新内容如下：

• ApplicationSet 资源增加渐进式发布策略；
• 允许用户为应用程序提供多个资源；
• 允许多个 CRD 共享健康检查；
• 支持反向代理扩展；
• argocd CLI 添加跨平台的文件加密工具 bcrypt 支持。

Falco v0.34.0 发布

Falco 是由 Sysdig 贡献给 CNCF 的云原生运行时安全相关项目。Falco 实现了一套可扩展的事件规则过滤引擎，通过获取事件、匹配安全规则、产生告警通知系列操作，能够发现系统中的安全问题。

近日，运行时安全项目 Falco v0.34.0 发布，更新内容如下：

• 支持手动下载和应用相关的规则 application_rules.yaml；
• 新检测规则使用 PTRACE 向进程注入代码；
• 规则结果添加编译条件上下文；
• 允许现代 bpf 探针为一个环形缓冲区分配一个以上的 CPU；
• 添加 webserver 端点以检索内部版本号；
• 在 systemd unit 中支持多个驱动。

KubeSphere 3.3.2 发布

近日，KubeSphere 社区宣布 KubeSphere v3.3.2 正式发布，本次发布的 KubeSphere v3.3.2 带来了更多的优化增强，主要集中在对 DevOps 和应用商店易用性的提升和问题修复。

服务网格 Kuma 改进策略处理和调试体验

近日，服务网格技术 Kuma 发布了 2.1 版本，改进了策略并更新了 UI。改进后的策略建立在 2.0 版本的基础上，并将剩余的策略移至新的 targetRef 系统。targetRef 系统为定义策略提供了改进的匹配系统。

Kuma 是基于 Envoy 的容器、Kubernetes 和 VM 的开源多区域服务网格。它为安全性、流量控制、发现和可观察性提供服务网格策略。最近的 2.0 版本改变了这些策略的匹配方式。这个新模型使用受 Kubernetes Gateway API 启发的 targetRef 系统。

Grafana Tempo 推出新的查询语言并支持 Apache Parquet

Grafana 是一款用 Go 语言开发的开源数据可视化工具，可以做数据监控和数据统计，带有告警功能。目前使用 grafana 的公司有很多，如 paypal、ebay、intel 等。

近日，Grafana 发布了 Grafana Tempo 2.0，它引入了新的 TraceQL 查询语言并支持 Apache Parquet 格式。Grafana Tempo 是一个与对象存储一起使用的开源跟踪后端。新的 TraceQL 查询语言与 Apache Parquet 格式配合使用，以提供改进的搜索时间和与跟踪对齐的查询。

AutoK3s v0.7.0 发布，离线环境更友好

近日，AutoK3s v0.7.0 发布，更新内容：

- 支持离线部署/升级 K3s 集群；
- SSH Key 管理；
- K3d Provider 升级至 v5.4.4 版本；
- 全新的 UI 体验，所有的 Cloud Provider 均支持与公有云资源的联动；还包括其余更新内容。

开源政策

《人工智能法案》在欧盟会议遭阻

2021 年 4 月，欧盟委员会提出《人工智能法案》条例草案，法案对人工智能系统的定义、禁止人工智能应用的领域、人工智能系统的高风险分类、与执法机关有关的范围和规定、支持创新的措施等方面进行了界定。2022 年 12 月 6 日，欧盟理事会就法案形成共识，旨在确保投放到欧盟市场并在欧盟范围内使用的人工智能系统是安全的。然而，近日欧盟议会未能就《法案》达成一致，将于 3 月底欧盟议会再次表决，届时欧盟各国家将开始谈判立法的最终条款。

从立法初衷来看，欧盟希望为人工智能在整个单一市场的发展制定一个统一、横向的法律框架，既能推动人工智能的投资和创新，又能促进保障公民基本权利和安全的现行法律得到有效执行和加强。负责数字政策和竞争事务的欧委会执行副主席玛格丽特·韦斯塔格表示，法案有助于制定“新的全球规范，确保人工智能可以被信任”。捷克负责数字化事务的副总理兼地方发展部长伊万·巴尔托什表示，欧盟尝试在人工智能发展和保障公民基本权利之间达成平衡，将促进整个欧洲人工智能技术的创新和发展。

从法案争议来看，议会争议的核心在于监管是否会阻碍创新，即如何平衡数据隐私与避免扼杀人工智能创新和投资，以及决定哪些人工智能系统被归为“高风险”。绿党议员谢尔盖·拉戈金斯基表示，议员之间的冲突在于公民基本权利和人工智能创新之间的潜在矛盾。业界争议的核心在于禁止有风险的不当行为，以及对企业使用人工智能系统的审查是否必要。渣打银行数据管理风险和人工智能主管维贾伊·贾伊拉杰表示，法案将迫使企业密切关注人工智能产品的第三方供应商，一旦监管机构发现人工智能系统风险，则需要向欧盟国家提供有关技术和供应链细节。国际隐私专业人士协会首席研究员凯塔琳娜·柯纳表示，部分企业可能意识到了人工智能的风险，但他们缺乏正确处理这些风险的工具和指导方针。

开源报告

《2023 年开源状态报告》发布

近日，Open Source Initiative（OSI）联合 OpenLogic 发布了他们的年度开源调查的结果——《2023 年开源状态报告》。

该报告通过 Perforce（社区开源软件技术支持和服务提供商），进而获取到 OSI 和 OpenLogic 合作创建的全球开源用户调查数据进行分析，该调查数据覆盖全球八个地区、20 多个行业以及各种规模组织。

《2023 年开源状态报告》共阐述了推动开源软件采用的因素、最受欢迎的开源技术以及 OSS 团队最常遇到的挑战。该报告还提供了关于开源如何在不同规模、行业和地理区域的组织中日益发展走向成熟的重要见解。

该报告指出，80%的组织在过去的 12 个月中增加了对开源软件的使用。五分之四的公司依赖 OSS 来实现广泛的关键业务应用程序，包括数据和数据库管理、容器和容器编排以及 DevOps 和 SDLC 工具，开源在广泛的技术应用中无处不在。

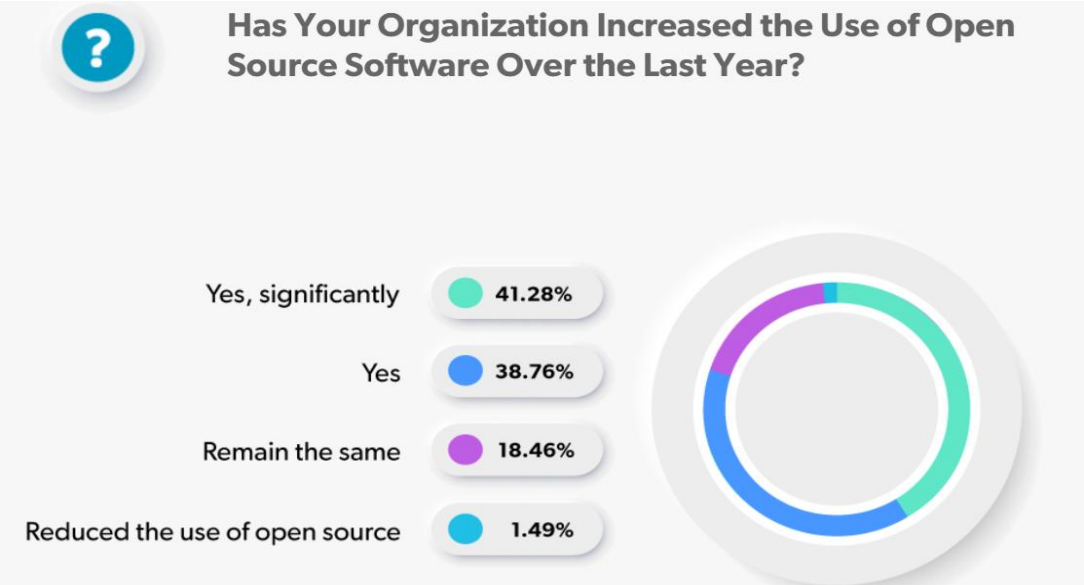


图 1 您的组织在去年是否增加了开源软件的使用？

在关于哪类开源软件正在被组织使用时，该报告显示：

• 容器和容器编排技术的使用量在显著增加，在今年达到 33.26%（去年仅为 18%）。其中，34%的公司使用开源软

件开发生命周期（SDLC）工具，22%的公司使用开源内容管理解决方案。容器和容器编排技术，以及软件开发生命周期工具，是投资业最多见、最常用的开源技术。

•Kubernetes 的使用率也在维持增长，在今年达到 23%，同比增长 5%，跃升成为使用率排名第三的云原生技术。在过去的一年中，几乎所有的云原生技术在一定程度上都获得了增长。例如，OpenTelemetry、Jaeger 和 Prometheus 的使用率都获得大幅增长。

• 在编程语言方面，JavaScript 以及 Python 持续处于领先地位，但在各行业的使用率仅稍有增加，为一到两个百分点。最受欢迎的三个开源 Java 运行时依旧是 OpenJDK、OpenJ9 和 Oracle Java。其中，OpenJDK 和 OpenJ9 的使用率维持稳定，而 Oracle Java 的使用率与去年相比下降 4 个百分点。

• DevOps 开源自动化和配置工具的使用率也得到了快速增长，该调查显示只有近 12%的受访者表示没有使用过任何此类技术（去年该比例为 50%）。同样，CI/CD 工具，特别是云原生 CI 和 CD 工具的使用率也在增加。总体来看，Jenkins X、Spinnaker 和 Tekton 的使用率都获得了增加。

然而，该报告显示，开源软件在发展的过程中仍然存在一定的挑战，该报告将挑战共分为九个方面，具体来看：

- 维护安全策略和合规性：41.97%。
- 缺乏技能、经验或熟练程度：37.50%。
- 更新和补丁：36.70%。
- 缺乏底层技术支持：36.47%。
- 维持生命周期终止（EOL）支持：36.01%。
- 缺乏实时的技术支持：35.89%
- 安装、升级、配置等问题：31.31%
- 没有足够的人员支持：21.90%
- 基础设施的可扩展性和性能问题：17.43%

图 2 在使用开源软件的时，面临的首要挑战？

对此，Perforce Software 的首席 OSS 布道师和主要作者 Javier Perez 说到“很明显的是，开源发展需要更多的技术支持，而人员经验和熟练程度也成为各类组织发展开源的关键关注点。OSS 的内部支持不应局限于仅掌握一种技术，还需要掌握构成软件堆栈的多种技术的专家级知识，进而丰富自身经验及熟练程度。”

在组织的关键核心任务中，被广泛应用的开源软件包括 Linux、Apache HTTP、Git、Node.js、WordPress、Tomcat、Jenkins、PHP 和 Nginx。总体上来看，软件已经成为许多组织发展业务的关键，开源软件成为其数字基础架构的关键组成部分。越来越多的组织获得了这些关键技术的专业知识，并认识到通过成为社区的一部分来持续参与、推动开源创新的重要性。

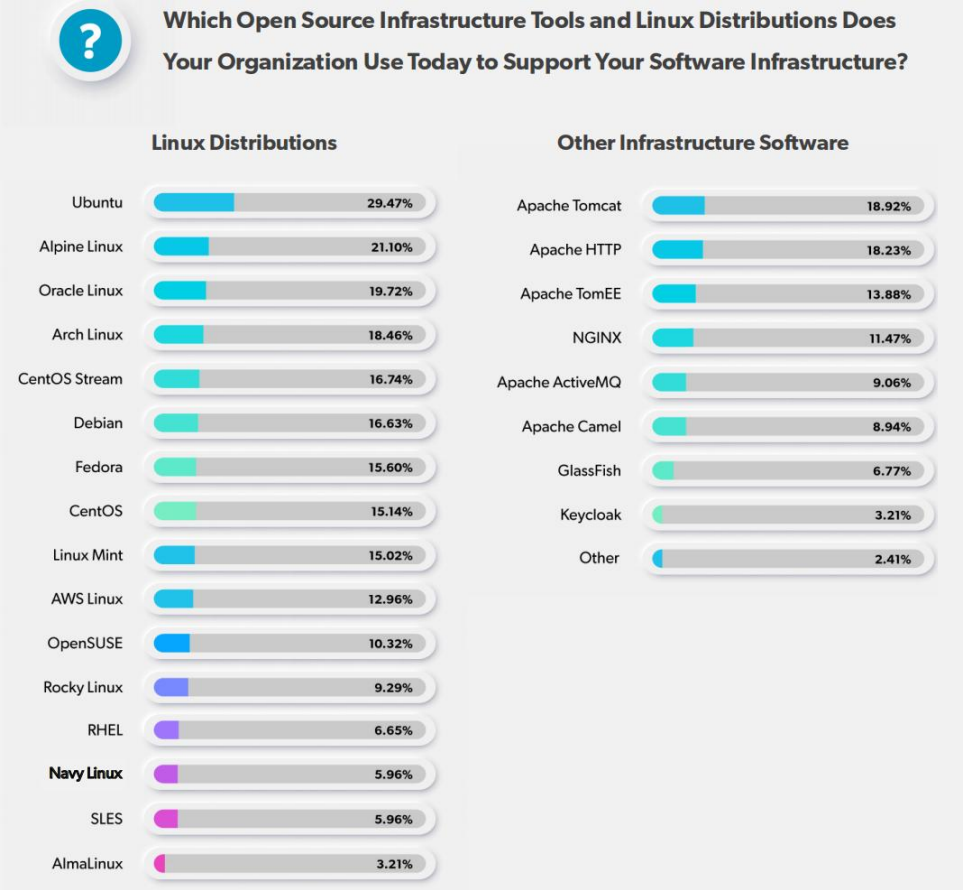


图 3 你的组织目前使用哪些开源基础设施工具或是 linux 发行版来支持你的软件基础设施？

总体上来看，目前至少有 37%的组织已经为开源做出了贡献，包括对开源项目或开源组织的贡献（代码或其他活动），相较去年增加 5%。其中，进行安全扫描活动的贡献者占比最高，达到 46%。

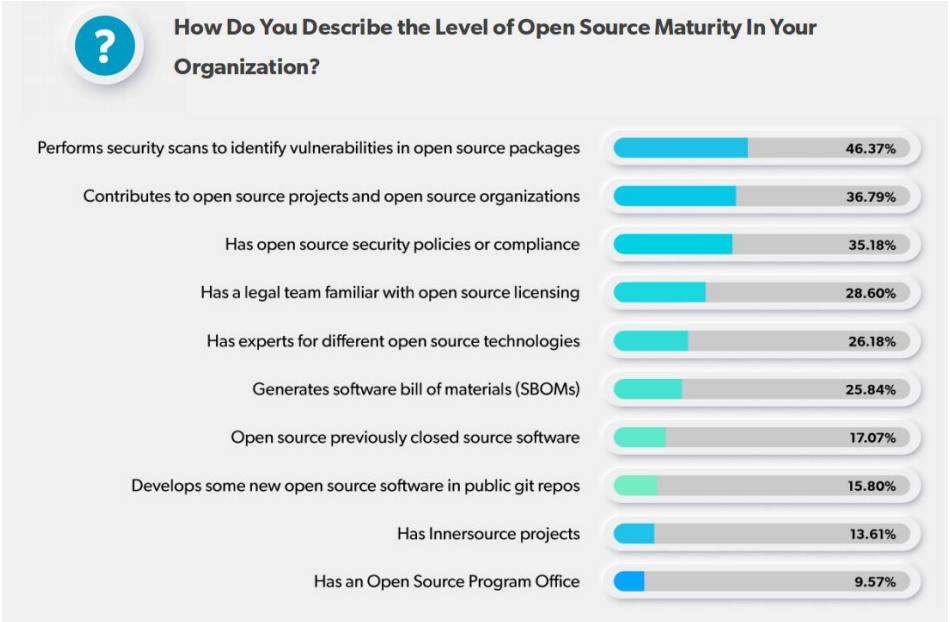


图 4 如何描述你的组织中的开源成熟度水平？

尽管存在诸多挑战，但《2023 年开源状态报告》同样表明了开源日益发展的积极趋势。其中，35%的调查者具有 OSS 安全和合规政策；28%的法律团队熟悉开源许可；多数行业中超过 25%的组织都会生成软件物料清单（SBOM），这是迈向更高安全性和透明度的关键第一步。这些数字表明，越来越多的公司正在从 OSS 的消费者转变为积极的参与者。调查发展，有超过三分之一（37%）的人表示他们正在积极为开源项目和组织的发展做出贡献。

该报告调查的最后问题是针对于调查者在未来采用 OSS 的优先事项。主要调查他们在未来的 18 个月内实施这些技术的意愿，进而对技术进行排名。多数调查者选择 AI/ML/DL 技术作为最理想的技术，此项选择相比于 Kubernetes 以及 Kubernetes Operators 要高出 1%。

In Order of Importance, From Not Important to Most Important, Rank the Following Technologies in Relation to Your Organization's Desire To Implement Them in the Next 18 Months

Technology	Not Important	Mildly Important	Important	Very Important	Most Important
Kubernetes or Kubernetes Operators	16.34%	20.30%	31.97%	21.00%	10.39%
Data Science	11.88%	23.52%	29.22%	27.20%	8.19%
Artificial Intelligence / Machine Learning / Deep Learning	11.29%	20.82%	30.12%	26.24%	11.53%
Virtual Reality or Augmented Reality	19.74%	20.21%	24.82%	24.94%	10.28%
Blockchain/Crypto	20.98%	20.38%	27.46%	21.22%	9.95%
Nonfungible Tokens	25.30%	17.87%	28.66%	20.02%	8.15%
Serverless/Functions	11.88%	21.26%	33.25%	25.06%	8.55%
Quantum Computing	20.72%	22.16%	26.35%	22.28%	8.50%

图 5 在未来的 18 个月内实施这些技术的意愿？

OSI 执行董事 Stefano Maffulli 表示：“现阶段来说，对由 AI/ML/DL 技术提供支持的服务的需求呈现出爆炸式增长。在这个快速增长及发展的时代，应用程序吸收的大量数据，对许可和隐私带来了严重影响。目前，Open Source Initiative 正在研究针对于 AI/ML/DL 的发展策略，以帮助企业和个人在数据和 AI 系统方面明确定义他们的权利和义务，维持良性、可循环的发展”。

《2022-2024 中型企业技术采用路线图》发布

近日，全球知名咨询公司 Gartner 发布《2022-2024 中型企业技术采用路线图》。该路线图汇集全球 400 多家中型企业技术领导者的集体智慧，涉及核心基础设施领域。其中包括计算、存储云、数字化工作场所、网络、安全和自动化等领域，共囊括 53 项技术。

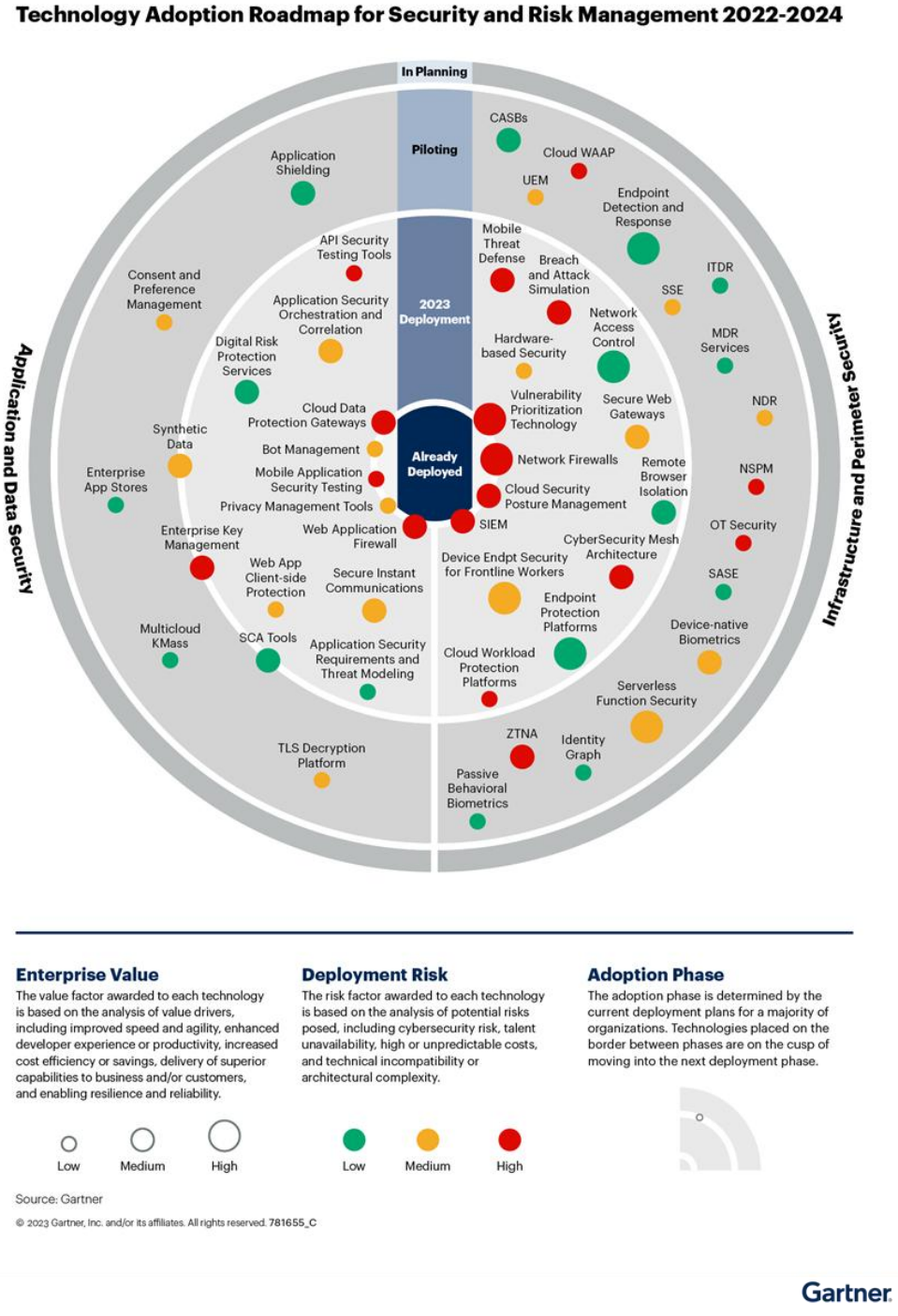


图 1 路线图共囊括技术路线范围

这项研究报告详尽的说明了中型企业[1]可实现商业回报的技术投资，以及相关技术的部署风险，可以帮助技术领导者了解相关技术的采用情况、对企业的价值和部署风险，了解中型企业的重点投资决策情况。该报告指出：

• 为应对不断变化的数字化风险，中型企业的技术投资侧重于托管检测和响应（MDR）以及威胁检测。

中型企业正在部署托管检测和响应（MDR）、网络检测和响应（NDR）、终端检测和响应（EDR）以及拓展威胁检测与响应（XDR）等技术。中型企业规划在 2022 年完成托管检测和响应（MDR）技术的部署。至于拓展威胁检测与响应（XDR）技术，中型企业希望在 2023 年前完成该技术部署，但该技术的市场仍处于早期形成阶段，还需要比较长的时间该技术才能走向成熟。

• 中型企业已经部署安全访问服务边缘（SASE）技术，零信任网络访问（ZTNA）仍处于实验阶段。

中型企业计划在 2022 年完成安全访问服务边缘技术的全面部署，实现从以硬件为中心的安全产品向以云为中心的安全服务转型。零信任网络访问（ZTNA）仍处于实验阶段，需要评估其优势与风险。

• 中型企业技术投资重视混合办公和远程办公模式。

中型企业将工作场所分析及工作流协作工具的部署计划推迟到 2023 年，并强化远程办公和混合办公模式的基础设施，优先部署云技术和安全技术。

• 为实现民主化交付，中型企业正在积极试点部署公民自动化开发平台（CADP）技术。

公民自动化开发平台（CADP）技术实际上是可以用来构建和管理自动化流程的技术。能够帮助企业更轻松地实现企业流程自动化，并将自动化过程集成到企业系统之中。中型企业计划在 2023 年完成公民集成者工具的部署，为了营造良好的低代码开发环境，目前正在对公民自动化开发平台（CADP）技术进行试点部署。通过投资这一风险较低的公民技术，企业能够降低数字化的成本，提高响应速度以及开发的敏捷性，赋能业务人员，实现业务主导型 IT。

[1] 中型企业（MSE）指营收高于 5000 万美元，低于 10 亿美元的企业机构。

• 中型企业将推迟完成其在 2022 年采用自然语言处理（NLP）技术的计划。

自然语言处理技术仍处于中型企业的实验部署阶段，但该技术已经取到了一定程度的进展。要想达到成熟，还需要跨越人类语言复杂性和模糊性两大主要障碍。

• 中型企业正在试点部署增强型互联网。

目前，已有 20%的中型企业部署了该项技术，其余中型企业还处在评估该项技术是否符合其现有的市场热度阶段。

• 中型企业已经部署了 AI、数据科学和机器学习平台。

中型企业已经部署了数据科学和机器学习（DSML）平台、AI 云服务和 AIOps。尽管人工智能的部署风险很高，但目前，超过 64%的中型企业正在部署或已经部署了 AI 云服务和 AIOps。

• 中型企业部署满足其更高的网络效率需求的技术。

尽管中型企业认为 5G 服务具有很高的价值，但由于覆盖范围不一致以及设备缺乏支持，并不利于该技术的持续推广。计划 2023 年，软件定义广域网和网络流量分析可实现安全且一致的网络覆盖。

• 中型企业投资 API 管理平台及服务。

中型企业逐渐意识到 API 管理平台及服务在支持云平台和自动化方面的优势，但专有人才短缺不利于中型企业雇佣相关人员来进行管理。

繁荣开源事业　共享开源价值

地址：北京市北京经济技术开发区科谷一街8号院8号楼22层2201
网址：https://www.openatom.org/home
资金捐赠：sponsorship@openatom.org　项目捐赠：sponsorship@openatom.org