安全+
SECURITY
2023/04 总第 056
技术版 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

从协议层面分析5G UPF存在的安全风险

绿盟科技云安全纲领（下）

云原生服务风险测绘分析（四）：Prometheus

容器逃逸即集群管理员？你的集群真的安全吗？

NSFOCUS

SECURITY+

安全+ 技术版
与安全人士分享技术心得
Share technique experience with security professionals

本期看点 HEADLINES

主办：绿盟科技
策划：《安全+》编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-5462
传真：(010)6872 8708
网址：www.nsfocus.com

2023/04 总第 056

欢迎您来信nsmagazine@nsfocus.com 与我们交流，
分享您的建议和评论。（《安全+》部分图片来源于网络）

安全+ SECURITY

目录 CONTENTS

卷首语

数字化进程不断加速，网络安全乘云而上，持续为信息安全产业带来机遇与挑战。新时期，党的二十大报告从党和国家事业发展战略全局出发，对国家安全体系和能力现代化作出全面部署，提出强化网络和数据安全保障体系建设，为实现更高水平的网络安全提供了根本遵循。

本期《安全+》将继续着眼网络安全行业现状，探析网络安全发展趋势，从前沿技术、安全理念应用等视角出发，探索网络安全新发展所需的整体脉络和发展路径。

数字中国建设需要网络安全行业横纵双向全方位支撑，数字经济向深向实发展，催生更广泛的安全需求，保障企业业务的持续性、可靠性和稳定性已成为必然选择。

面对数字化经济的加速发展，安全公司如何实现创新突破，以适应新场景的变化？绿盟科技认为，安全公司的本质，是以安全对抗能力为核心构建公司的核心竞争力，打造可信可控的网络和数据安全综合防控体系。绿盟科技对数字化经济趋势持续适应，通过智慧安全3.0理念，构建“全场景、可信任、实战化”的安全运营能力，以体系化建设为指引，契合数字化时代的安全建设需求，夯实数字中国建设框架的数字安全屏障。

面向多变、复杂的网络攻击和数据安全威胁，绿盟科技积极拥抱变革，不断求索，寻找更科学、更合理的安全发展模式，构建以“新安全格局”为基石的网络安全发展体系，为长久的网络安全事业递一分绿盟之力。

叶晓虎

5G安全

从协议层面分析5G UPF存在的安全风险

绿盟科技 安全建模技术组 皮靖

摘要：UPF 即用户平面网元。它既会与核心网的 SMF 网元进行信令的交互，同时也承载着转发用户平面数据的作用，因此是一个比较关键的网元。而 UPF 下沉，也为 UPF 带来了一些安全挑战。本文从 UPF 上两个比较关键的协议 PFCP 和 GTP-U 出发，分析协议层面可能存在的一些安全风险及可能造成的后果，并给出安全建议。

关键词：UPF 网元 PFCP 协议 GTP-U 协议 安全风险

1.UPF 网元和协议

UPF 即用户平面网元（User Plane Function），它与 SMF 网元（Session Management Function）通信，根据 SMF 网元基于 PFCP 协议（Packet Forwarding Control Policy，数据包转发控制协议）下发的规则，来进行用户面数据的转发和处理。UPF 网元既会与核心网网元进行交互（SMF，交互控制面信令），也会与接入网设备交互（基站等，转发用户面数据），同时业务数据也承载于 UPF 网元之上，因此它是一个比较关键的网元。

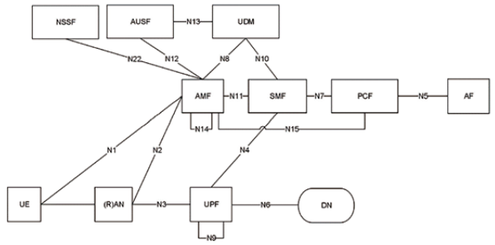


图 1 5G 网络结构及 UPF 所处的位置

UPF 主要通过 N4 接口与 SMF 网元进行通信，其上的协议为 PFCP 协议。PFCP 协议基于 UDP 协议，默认端口为 8805。如图 2 所示，为 PFCP 会话建立报文。里面的 SEID 字段即为会话唯一标志符，如果需要对其进行修改、删除，需要提供 SEID 这个字段：

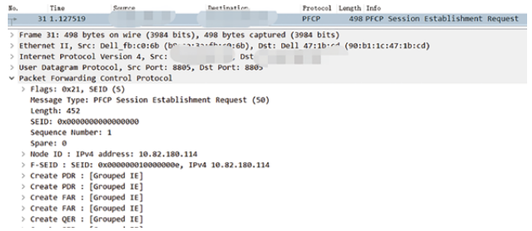


图 2 PFCP 会话建立报文

另外，里面有两个比较关键的部分：

PDR: 包识别规则（Packet Detection Rule）。数据包只有命中了包识别规则，才会走后面的处理流程。如果数据包没有命中 PDR 规则，那么 UPF 将会直接丢弃该数据包。

FAR：转发动作规则（Forwarding Action Rule）。FAR 的作用是告诉 UPF 怎样处理数据包。FAR 中有个比较关键的字段，叫作 Apply Action。Apply Action 的值对应的标志为表示了不同的处理动作，包括 DROP(丢弃)、FOWD（转发）、BUFF（缓存）等，如图 3 所示。

```
Apply Action :
    IE Type: Apply Action (44)
    IE Length: 1
    0... .... = DFRT (Duplicate for Redundant Transmission): False
    .0.. .... = IPMD (IP Multicast Deny): False
    ..0. .... = IPMA (IP Multicast Accept): False
    ...0 .... = DUPL (Duplicate): False
    .... 0... = NOCP (Notify the CP function): False
    .... .0.. = BUFF (Buffer): False
    .... ..0. = FORW (Forward): False
    .... ...1 = DROP (Drop): True
```

图 3 FAR 中的 Apply Action 字段

UPF 主要通过 N3 接口与基站进行通信，其上的协议为 GTP-U 协议（User Plane Part of GTP，GPRS 用户平面部分）。GTP-U 协议基于 UDP 协议，默认端口为 2152。如图 4 所示，为 GTP-U 数据包，它就是在普通数据包之上加上了 GPRS 隧道头部。

```
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
Ethernet II, Src: Dell_47:1b:cd (90:b1:1c:47:1b:cd), Dst: RealtekU_ee:0
Internet Protocol Version 4, Src [redacted]  Dst: [redacted]
User Datagram Protocol, Src Port: 2152, Dst Port: 2152
GPRS Tunneling Protocol
    Flags: 0x30
    Message Type: T-PDU (0xff)
    Length: 32
    TEID: 0x00000001 (1)
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 32
    Identification: 0x0001 (1)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
```

图 4 GTP-U 报文

GPRS 隧道头部有一个比较关键的字段，即 TEID 字段（Tunnel Endpoint Identifier，隧道端点标识符），它标志了数据属于哪一个隧道。

2. 风险场景示例

2.1 PFCP 协议风险场景示例

从前面对于 PFCP 协议的解释我们可以了解到，UPF 主要是依据 PFCP 协议里的 PDR 来识别数据包，而基于 PFCP 里的 FAR 来处理数据包。这就意味着，如果攻击者在某种场景下可以访问到 UPF 的 8805 端口（例如 UPF 下沉到客户侧，且关键端口直接暴露在了外网），且通过某种方式嗅探到了部分关键字段（如 SEID），或者仅仅是暴力遍历某些关键字段的值。那么就可以构造恶意的 PFCP 报文，来影响 UPF 对于用户平面数据的处理。

如第一小节所述，数据包首先会过 PDR 规则，如果数据包没有命中 PDR 规则，那么 UPF 将会直接丢弃该数据包。这就意味着，如果我们构造 PFCP 会话修改请求（PFCP Session Modification Request），删除掉指定 PFCP 会话里的 PDR 规则。那么该会话对应的用户面数据将会无法命中 PDR 规则，而被 UPF 直接抛弃。造成的影响就是，该终端会出现断网的情况。

```
Frame 294: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
Ethernet II, Src: HuaweiTe_e3:39:35 (5c:e8:83:e3:39:35), Dst: RealtekU_69:f0:8c (52:54:00:69:f0:8c)
Internet Protocol Version 4, Src: [redacted]  Dst: [redacted]
User Datagram Protocol, Src Port: 8805, Dst Port: 8805
Packet Forwarding Control Protocol
    Flags: 0x21, SEID (S)
        001. .... = Version: 1
        ...0 .... = Spare: 0
        .... 0... = Spare: 0
        .... .0.. = Follow On (FO): False
        .... ..0. = Message Priority (MP): False
        .... ...1 = SEID (S): True
    Message Type: PFCP Session Modification Request (52)
    Length: 22
    SEID: 0x0a0400000000076
    Sequence Number: 0
    Spare: 0
    Remove PDR : [Grouped IE]: PDR ID: 257
        IE Type: Remove PDR (15)
        IE Length: 6
        PDR ID : 257
    [Response In: 295]
```

图 5 PFCP 会话修改请求中删除 PDR

同时，因为 UPF 主要是基于 FAR 来处理数据包的。这就意味着，如果攻击者构造 PFCP 会话修改请求（PFCP Session Modification Request），修改 FAR 里的 Outer Header Creation 里的 IP 为恶意的 IP，即可以令用户面数据被重定向到恶意的主机。

```
Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_47:1b:cd (90:b1:1c:47:1b:cd), Dst: RealtekU_69:f0:8c (52:54:00:69:f0:8c)
Internet Protocol Version 4, Src:  Dst:
User Datagram Protocol, Src Port: 8805, Dst Port: 8805
Packet Forwarding Control Protocol
    Flags: 0x21, SEID (S)
    Message Type: PFCP Session Modification Request (52)
    Length: 52
    SEID: 0x0a0400000000048
    Sequence Number: 0
    Spare: 0
    Update FAR : [Grouped IE]: FAR ID: Dynamic by CP 16641
        IE Type: Update FAR (10)
        IE Length: 36
        FAR ID : Dynamic by CP 16641
    Apply Action :
    Update Forwarding Parameters : [Grouped IE]
        IE Type: Update Forwarding Parameters (11)
        IE Length: 19
        Destination Interface : Access
        Outer Header Creation :
            IE Type: Outer Header Creation (84)
            IE Length: 10
            Outer Header Creation Description: GTP-U/UDP/IPv4  (256)
            TEID: 0x00000022
            IPv4 Address:
```

图 6 PFCP 会话修改请求中修改 FAR 里的 Outer Header Creation

因此，基于 PFCP 协议，可以想到的风险场景如下：

场景	可造成的后果
恶意构造PFCP会话删除请求	终端断网
恶意构造PFCP会话修改请求删除PDR	终端断网
恶意构造PFCP会话修改请求修改FAR	1.终端断网 2.流量被重定向

2.2 GTP-U 协议风险场景示例

我们知道，UPF 会转发基站的 GTP-U 数据包，其中 TEID 是隧道的标识信息。假设攻击者在某种条件下可以访问到 UPF 的 2152 端口，且嗅探到了关键字段（如 TEID 等），或者仅仅是暴力遍历其中某些字段的值。那么就可以构造恶意的 GTP-U 报文，从而使得 UPF 转发攻击者构造的数据。如图 7，是一个构造的 GTP-U 报文，其下包含的 UDP 数据正文内容为 test（需要注意此攻击构造符合约束的数据包是存在难度的，需要攻击者已经掌握了 TEID、UE IP 及 DN IP 的相关信息），直接发给 UPF 设备后，UPF 会将其转发到 DN。其风险点在于，攻击者可以在 GTP-U 内部包裹恶意数据包，例如包裹 SYN 包，然后大量发送给 UPF 使其转给 DN。DN 收到 SYN 包后，会回复 SYN-ACK 消息，但由于此消息并非由真实的 UE 发送，所以 UE 收到 SYN-ACK 后会回复 RST 消息。当包到达一定量级，大量的 SYN-ACK 和 RST 数据包拥塞网络，在终端会出现网络断开的现象。

```
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
User Datagram Protocol, Src Port: 2152, Dst Port: 2152
GPRS Tunneling Protocol
    Flags: 0x30
    Message Type: T-PDU (0xff)
    Length: 32
    TEID: 0x00000001 (1)
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
User Datagram Protocol, Src Port: 1234, Dst Port: 1234
Data (4 bytes)
    Data: 74657374
    [Length: 4]

0000  52 54 00 ee 0a 1e 90 b1  1c 47 1b cd 08 00 45 00   RT·····  ·G····E·
0010  00 44 00 01 00 00 40 11  fc d1 0a 52 b4 71 0a 52   ·D····@·  ···R·q·R
0020  b4 c1 08 68 08 68 00 30  0a 10 30 ff 00 20 00 00   ···h·h·0  ··0··· ··
0030  00 01 45 00 00 20 00 01  00 00 40 11 b0 a1 0a 0a   ··E···· ··@·····
0040  0a 04 ac 10 0a 0d 04 d2  04 d2 00 0c 44 2d 74 65   ········  ····D-te
0050  73 74                                              st
```

图 7 构造的 GTP-U

另一方面，假设攻击者已经可以接触到某个 UPF 网元，但是并不能接触到其他网元。如图 8 所示，他可以在 GTP 隧道消息体里，包裹 GTP 消息。在某些 UPF 内，可能内置了安全策略，即限制 GTP-U 内部包裹的普通消息的目的地址只能为特定的地址，例如 DN 的地址（因为用户面的消息主要用于基站和 DN 之间的数据

交互）。而 GTP-GTP 则可以绕过这个限制使得 UPF 在剥离了头部之后发现内部依旧是一个 GTP 消息，从而将消息发送给攻击者本不可能接触到的网元。而如果被包裹的 GTP-U 消息也是恶意的话，就可以令这个攻击者本不能接触到的网元出现一些处理方面的异常。

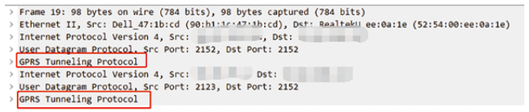


图 8 GTP-IN-GTP 攻击

因此，基于 GTP-U 协议，可以想到的风险场景如下：

场景	可造成的后果
TEID爆破	获取真实的TEID，用于其他攻击
GTP-U 包裹恶意消息大量发送（如 TCP SYN）	终端断网
GTP-GTP攻击	令本不能接触到的网元出现异常

3. 安全建议

（1）不论是核心网 UPF 还是下沉到客户机房的 UPF，都需要做好安全策略。尤其是关键端口，不应该被外部或者不需要访问此端口的主机访问。

（2）UPF 应支持内置安全功能，可以拒绝恶意主机发送的恶意消息。

（3）部署旁路安全检测设备，辅助及时发现威胁。

参考文献

[1] 3GPP. 5G Security Assurance Specification (SCAS); User Plane Function (UPF). [DB/OL]. 2022.

[2] 3GPP. Interface between the Control Plane and the User Plane nodes. [DB/OL]. 2022.

[3] Positive Technologies. 5G Standalone core security research. [DB/OL]. 2020.

[4] Philippe Z Lin, Charles Perine, Rainer Vosseler, Wen-Ya Lin. Attacks From 4G/5G Core Networks：Risks of the Industrial IoT in Compromised Campus Networks. [DB/OL]. 2021.

[5] Seongmin Park, Daeun Kim, Youngkwon Park, Hyungjin Cho, Dowon Kim, Sungmoon Kwon. 5G Security Threat Assessment in Real Networks. [DB/OL]. 2021.

全面深入的5G安全评估创新方案

绿盟科技 创新研究院 陈佛忠 产品服务部 温才进

摘要：5G 技术近些年来发展迅速，5G 的安全问题也慢慢得到了各行各业的重视。本篇文章结合 5G 安全评估实际的需求，提出了一套全面覆盖、由浅入深的 5G 安全评估创新方案。用户可以根据自己的实际情况来选择适合的评估模块，以便以最高性价比的方式满足自身的 5G 安全需求。

关键词：5G 安全 云原生安全 5G 核心网 5G 安全评估

1. 5G 安全评估背景及相关政策

第五代移动通信技术（以下简称 5G）近些年来发展迅速，5G 技术在电力、煤矿、钢铁、港口和医疗等垂直行业的应用也正在逐年深入。5G 的高带宽和低延迟可以支持新兴的数字服务，如虚拟现实和增强现实，同时还可以改善传统的移动应用，如高清视频流和在线游戏。此外，5G 的更高连接密度和更广泛的覆盖范围可以帮助解决物联网的难题，从而实现工业自动化和智能城市的愿景。5G 技术给现代社会带来诸多便利与革新的同时，5G 网络也给各行各业带来了新的安全问题。

为了进一步保障垂直行业安全可靠地使用 5G 网络，工信部在 2022 年印发的基础电信企业网络与信息安全工作考核文件中新增了“5G 行业应用安全风险评估”要求，明确了三大运营商需建立 5G 行业应用安全风险评估机制，开展 5G 行业应用安全风险评估工作，并在规定时间内完成 5G 项目清单及评估报告的报送。

2. 解决之道的探索

面对 5G 安全的新型挑战，绿盟科技在 5G 安全研究领域持续耕耘、不断积累。2021 年，绿盟科技与信通院一同成立了“5G 安全联合实验室”[1]；2022 年，绿盟科技成功入选首批工信部“5G 应用安全创新推广中心”[2] 和首批 5G 应用产业方阵开展的“5G 应用解决方案供应商推荐名录”[3]，并作为唯一安全厂商受邀在 5G 网络创新研讨会上发表了《以攻促防，5GC 安全评估创新研究》[4] 的主题演讲。

针对 5G 行业应用安全风险评估，绿盟科技结合自身的研究与积累提出了一套全面覆盖、由浅入深的安全评估创新方案，该方案包含三部分核心内容，分别是：5G 基本项安全评估、5G 进阶项安全评估和 5G 高阶项安全评估，下文将对这三部分内容进行具体阐述。

3. 5G 基本项安全评估

5G 基本项安全评估旨在通过一个覆盖面全、成本较低的方案对 5G 网络进行一个全方面的安全性评估，以最优性价比发现 5G 网络中存在或潜在的威胁并进行修复与完善。

3.1 评估内容及框架

根据信通院发布的 5G 安全评估规范相关要求，评估内容涵盖 5G 典型应用场景安全、5G 行业通用安全、5G 专网安全、5G 关键技术安全、5G 行业应用安全保障、5G 行业应用数据安全 6

个方面，涉及 91 项要求，以下是 5G 行业应用安全评估框架：

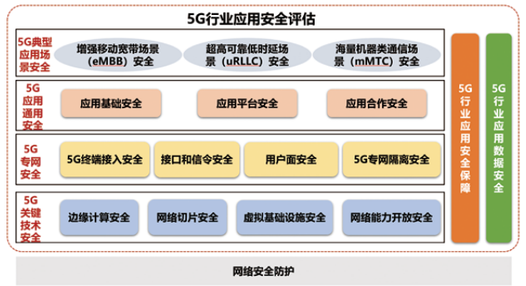


图 1 5G 行业应用安全评估框架

5G 典型应用场景安全主要结合 eMBB、uRLLC、mMTC 三大 5G 典型应用场景特点和风险，分别提出了基础安全保障能力和高安全要求应用场景下的安全措施增强两类评估要求。

5G 应用通用安全从应用基础安全、应用平台安全、应用合作安全 3 个方面提出了评估要求。其中，应用基础安全包括行业用户的应用规模情况、应用类型情况、行业用户身份认证情况、设备及网络环境情况、对公共安全的影响 5 项要求；应用平台安全包括应用服务器、机房、节点的地理位置和计算存储资源 / 云服务安全 2 项要求；应用合作安全包括合作方式合规性评估、合作企业安全保障能力评估 2 项要求。

5G 专网安全主要对 5G 终端接入安全、接口和信令安全、用户面安全和 5G 专网隔离安全 4 个方面提出了评估要求。其中，5G 终端接入安全包括终端接入认证安全、终端信令和数据安全、终端访问控制安全 3 项要求；接口和信令安全主要从 AS 层信令安全、NAS 层信令安全、N2 接口安全、N4 接口安全和核心网服务化接口安全 5 个维度提出了 10 项要求；用户面安全包括终端与 gNB 之间用户面数据保护、5G 专网 gNB 和 UPF（N3 接口）之间的用户面数据保护、UPF N4 接口会话防劫持机制 3 项要求；5G 专网隔离安全包括 5G 专网 UPF 与行业网络之间的安全隔离机制、5G 专网对行业网络访问的认证鉴权和最小边界访问策略、边缘 UPF 或下沉核心网的安全防护、5G 专网与公网之间的物理 / 逻辑隔离、跨运营商网络之间的安全边界控制 5 项要求。

5G 关键技术安全聚焦 5G 网络中引入的关键新技术带来的安全风险，对边缘计算、网络切片、虚拟基础设施和网络能力开放提出了 4 类评估要求。其中，边缘计算安全从组网安全、UPF 安全和 MEP 安全 3 个维度共提出 14 项要求；网络切片安全从切片隔离、切片访问控制和切片身份认证 3 个维度共提出 11 项要求；虚拟基础设施安全包括虚拟设施操作统一管理、不同虚拟机功能内部安全域划分，物理 / 虚机操作系统、虚拟化软件、第三方开源软件定期安全加固，网元容器配置安全检查和运行时安全检测 4 项要求；网络能力开放安全包括网络能力差异化开放机制和 5G 网络能力开放接口安全保护 2 项要求。

5G 行业应用安全保障聚焦企业管理措施保障能力，从安全管理制度、安全人员配置、安全运维管理、账号权限管理、应急处置机制 5 个维度提出了 8 项要求。

5G 行业应用数据安全重点关注业务通用数据安全，从管理制度、数据分级分类、重要数据安全管理、违法不良信息管理、数据全生命周期安全、网络数据安全 6 个维度提出 16 项安全要求。

3.2 评估实施流程

安全评估实施流程主要涉及三个阶段，分别是：评估准备阶段、评估实施阶段和评估总结阶段。

在评估准备阶段，应梳理需要开展的工作内容，并制订评估实施计划，沟通、准备评估材料，包括相关技术文档、管理文档、涉及的设备列表（包括业务平台、MEC、5G 设备等），明确已有的安全管理措施和技术保障措施情况等。

图 2 评估准备阶段中应收集的材料

在评估实施阶段，应采用文档审查、现场勘验、演示查看、测评验证等方式进行评估，首先对客户自查调研结果进行梳理，根据提供的证明材料判断该项结果是否满足要求，评估小组成员将梳理的问题逐一与提供材料的人员进行访谈确认，核查被评估系统及单位的安全保障能力并做好记录，针对发现的安全风险问题，提出整改建议并记录整改计划和风险隐患整改措施。

在评估总结阶段中，应针对被评估系统的基本信息和规模类型，结合实施阶段的各项评估结果及相应的证明材料，完成安全评估报告编写。

依赖权威的评估内容及框架，制定详细的评估实施流程，5G 基本项安全评估可以做到定期、全面、体系化、低成本地对整个 5G 网络进行安全评估，及时发现并修复相关安全问题。

4. 5G 进阶项安全评估

4.1 安全风险分析

如图 3 所示，5G 核心网中包含了多个网元，如 NSSF 网元、AUSF 网元、AMF 网元、SMF 网元、PCF 网元、NRF 网元、UDM 网元和 UPF 网元等。

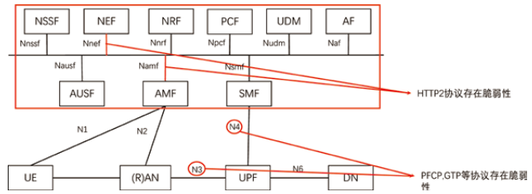


图 3 5G 核心网网元示意图

上图红框中的各个网元通过 HTTP2 协议进行互相通信，但由于 HTTP2 协议未启动 TLS 加密，攻击者可以对网元展开威胁程度逐步递增的安全攻击，该类网络安全攻击包括：注册恶意网元、恶意注销网元、窃取网元信息、窃取用户隐私信息、恶意删除关键信息和恶意删除已配置策略等。

对于 UPF 网元来说，UPF 可以通过 PFCP 协议（N4 口）与 SMF 网元进行通信、通过 GTP-U 协议（N3 口）与基站进行通信。根据我们在现网环境的实际测试得知，N3 口通信的 GTP-U 协议和 N4 口通信的 PFCP 协议存在脆弱性，存在被攻击者攻击的可能，涉及的安全风险包括：UPF 瘫痪（拒绝服务）、UPF 信息泄露、终

端设备断网、终端信息泄露、通信流量信息被窃取、构造虚假信息发送给数据网络和构造虚假信息发送给信令面网元等。

4.2 安全风险发现及处理

5G 进阶项安全评估通过模拟真实攻击的方式，在安全、可信的环境下验证上述可能会出现的安全风险并进行指导修复。通过部署自动化工具，我们可以实现持续识别信令面网元和 UPF 网元的恶意流量，及时发现并阻断与上述 5G 网元相关的安全风险。

例如，在真实现网场景中，黑客可以通过利用 GTP-U 协议包裹大量 tcp syn 消息的方式使得终端断网（如图 4 所示）。该类攻击场景可以造成连接此 UPF 网元的所有终端出现断网的情况，如果该类攻击发生在真实的生活之中，则势必会对多方的利益造成损失。我们通过部署自动化安全评估工具，可以及时发现此类攻击场景的恶意流量并进行阻断，从而有效提升 5G 核心网的整体安全水平。

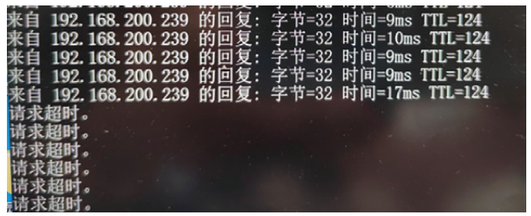


图 4 GTP-U 协议包裹大量 tcp syn 消息使得终端断网

5. 5G 高阶项安全评估

5.1 安全风险分析

相比于 4G，5G 引入了两项新的核心技术，分别是软件定义网络(Software Defined Network，SDN)和网络功能虚拟化(Network Function Virtualization ，NFV)，SDN 和 NFV 技术的出现使得电信服务更有弹性，可以根据客户的动态需求提供针对性的服务，但同时 NFV 和 SDN 技术也给 5G 引入了新的云安全风险。

随着各行各业云化趋势的逐步深入，云原生的安全问题也在逐步增加。 对于 5G 网络来说，5G 网元容器化部署引入了新的云原生安全问题，如容器可能存在漏洞被黑客利用、微服务的复杂性可能导致安全隐患、云原生环境中的网络通信可能存在安全风险、云原生环境中可能出现恶意资源访问等，这些安全问题需要通过合适的技术和流程来解决，以确保 5G 网络的安全性。

5.2 安全风险发现及处理

5G 高阶项安全评估通过模拟真实攻击的方式，在安全、可信的环境下验证上述可能会出现的安全风险并进行指导修复。通过真实现网环境的测试，我们发现了许多 5G 云原生环境中可能存在风险的安全问题，因此需要周期化、真实地对 5G 云原生环境进行安全评估。

图 5 为 5GC 云化基础设施安全评估会涉及的评估内容，其中主要包括三部分，分别是：容器化 5GC 基础设施信息收集、容器化 5GC 基础设施渗透攻击、容器化 5GC 基础设施渗透后利用。相关的攻击评估场景如：对宿主机上 SSH 服务进行暴力破解，测试其是否存在弱口令风险；在容器内执行高危系统调用，测试 Seccomp 安全机制是否开启且配置良好；在容器内匿名访问 K8s API Server 服务地址，验证是否存在未授权访问；在容器内进行端口扫描，验证云原生环境中是否支持网络异常行为的检测等。

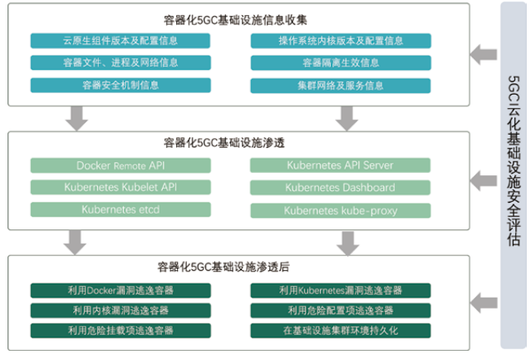


图 5 5GC 云化基础设施安全评估

例如，在真实现网场景中，恶意攻击者可以利用内核 notify-on-release 机制进行容器逃逸攻击，从而获取到宿主机的权限。该类攻击属于容器运行时安全的范畴，针对于此类攻击我们可以通过启用 Apparmor 机制禁止赋予容器 CAP_SYS_ADMIN 权限的方式来进行防护。下图为我们在某现网环境进行安全评估时，利用 coogo 工具实现该场景并完成容器逃逸的截图。

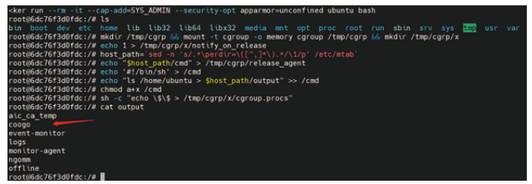


图 6 利用 notify-on-release 机制逃逸

在 5G 云原生环境中，类似上述的安全问题层出不穷且呈逐年递增的趋势。通过部署自动化安全评估工具，我们可以对 5GC 中云原生环境进行持续、真实、自动化的安全评估，及时在武器库中更新与云原生相关的安全漏洞，及时发现并修复 5GC 中云原生的安全问题。

6. 总结与展望

随着 5G 技术的普及，人们将更多地依赖于移动网络，而其安全性直接影响着个人、企业和国家的安全。如果 5G 网络不安全，数据可能被窃取或损坏，从而造成严重后果，因此确保 5G 网络的安全对于保护用户数据和隐私至关重要。

本文结合政策、考核、业务、创新等 5G 安全评估实际的需求，提出了一套全面覆盖、由浅入深的 5G 安全评估创新方案。该方案包含三部分核心内容，分别是 5G 基本项安全评估、5G 进阶项安全评估和 5G 高阶项安全评估。用户可以根据自己的实际情况来选择适合的评估模块，以便以最高性价比的方式满足自身的 5G 安全需求。

参考文献

[1] 中国信通院 - 绿盟科技 5G 安全联合实验室成立，https://www.nsfocus.com.cn/html/2021/21_0802/1113.html.

[2] 绿盟科技作为联合发入选首批工信部 5G 应用安全创新示范中心，https://www.sohu.com/a/515370697_476857.

[3] 5G 应用解决方案供应商推荐名录 ,http://www.5gaia.org.cn/dynamic/detail/532.

[4] 5G 网络创新研讨会 ,http://www.c114.com.cn/expo/15/a1214843.html.

[5] 浅谈云原生 BAS,http://blog.nsfocus.net/bas/.

构筑全流程可信安全体系，助力5G医疗急救业务发展

绿盟科技 运营商售前技术二部 胡仁峰

摘要 :5G+ 医疗的深度融合，提升了医疗数据流转效率、加速了医疗诊断的决策流程，但随着 5G+ 医疗场景不断推广与应用，安全风险与问题也会逐渐扩大。本文基于 5G 智慧院前急救场景来探讨主要的安全风险和问题，以及如何基于“可信安全”的理念，构建起全面的安全体系，探索出安全风险解决之道。

关键词 :5G+ 医疗 院前急救 终端认证 数据安全 可信计算

1. 背景介绍

自 2021 年以来，工信部等多部委联合发布 5G 应用“扬帆”行动计划和“十四五”医疗产业发展规划，推动智慧医疗全面发展。院前急救体系作为急危重症患者寻求医疗帮助的重要组成部分，院前急救质量与急危重症患者的治疗效果密切相关，对此各医疗组织都在不断就院前急救工作体系进行完善，以提升医疗急救服务能力与水平。5G 技术作为网络通信技术，在医疗院前急救体系中的应用，能够突破传统医疗工作局限性，实现对急危重症患者的远程医疗指导。[1]

为了构建5G智慧院前急救场景，我们可依托5G新型网络架构、全民健康信息平台，整合院前急救、二三级医院、基层医疗卫生服务机构等卫生资源，从自动分析救治资源、远程专家及时协同、5G急救专网数据传输、高效采集节点时间、开辟交通绿色通道、自动记录急救任务等关键流程上，实现“医疗救治更精准、调度指挥更可靠、急救转运更高效”的模式。[2]

2. 安全风险

在构建 5G 智慧院前急救场景的同时，我们也应考虑如何应对随之而来的安全风险，例如医疗终端不可信接入、医疗数据非法篡改、院前急救边缘基础设施遭受攻击、安全态势无法感知等问题。

（1）医疗终端不可信接入：救护车上超声诊疗设备、心电图机设备、智能手环、智能血压计、高清音视频互动设备、医护 PC、医护手持等终端存在非法接入5G网络和非法访问业务的不可信风险。

（2）医疗数据非法获取、篡改、泄露：患者位置数据、患者病历数据、远程会诊数据、全救治过程数据，在获取、传输、存储、共享被泄露篡改，导致数据安全无保障而不可信。尤其是下图全救治过程数据一旦存在被篡改风险，或者无法证明其准确性，极易造成医患纠纷，引发社会冲突。

（3）5G 基础设施安全风险：院前急救专属边缘 MEC 物理、系统、应用基础设施如果没有有力的可信手段，容易遭受病毒攻击、网络入侵攻击，影响全救治过程的可用性。

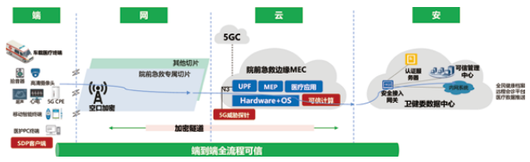
（4）缺乏安全态势感知手段：在 5G 院前急救端到端的全流程中，缺乏统一监控、分析和可信管理的手段，无法实施主动防御。

3. 设计理念

我们将“可信安全”理念引入 5G 智慧院前急救场景，从可信接入、数据可信、可信计算、可信管理四个方面出发，构筑全流程可信安全体系，为群众生命安全保驾护航，在保证 5G 网络与应用安全的基础上，提供安全、可信的运行环境和及时、便捷的医患服务。

4. 解决方案

我们基于“可信安全”理念，在 5G 智慧院前急救场景中，构建起“端—网—云—安”安全体系，探索出端到端的全流程可信、标准化的安全风险解决之道。



4.1 多层鉴权认证机制实现终端接入可信

（1）5G 自身安全认证保障 5G 网络接入安全

在 5G 医疗急救场景中，医疗终端完成接入 5G 网络接入认证后，应先由网络识别终端的切片标识信息，然后建立会话，保障接入的合法性；同时网络切片应对切片标识进行加密保护，对非目标终端和网络设备屏蔽相关信息，保护终端及用户隐私，防止非授权终端接入院前急救专属切片，也需要防止院前急救终端误接入到其他切片。

（2）5G 增强二次认证建立 5G 网络接入鉴权

医护人员通过 5G 专网接入后，到 120 急救指挥系统进行 5G 增强二次认证。5G 增强二次认证需要在卫健委数据中心认证服务器上增加网元 DN-IAM，采用 IMSI（必选）、IMEI（必选）、MSISDN（可选）、ULI（可选）组合检验的方式，对接入数据中心

的医疗终端进行二次认证，并可自主实现机卡绑定功能、接入位置控制功能。

（3）SDP 认证机制保障医疗业务应用访问安全

在院前医疗救治过程中，医护人员需要使用 PC、pad、手机进行信息获取、远程救治。为防止此类易被非法控制的终端接入急救业务平台实施攻击行为，本方案进一步采用零信任 SDP 认证机制实现院前急救的医疗业务应用在网络中的隐藏，需要手机、pad、电脑等设备安装可信 SDP 客户端，通过 SDP 网关认证后方可访问院前急救业务应用。

4.2 数据可信获取、传输、共享和存储

（1）端到端加密防止数据篡改泄露风险

一方面采用空口加密方案，发送方和接收方通过 RRC 消息协商出某一加密算法，发送方使用协商的加密算法对消息进行加密，然后将加密后的消息发送给接收方，接收方使用协商的加密算法对加密的消息进行解密。无线空口通信保护可以防止 5G 基站和终端间的数据被非法拦截、泄露、篡改。

另一方面采用切片级加密方案，可以实现为指定急救医疗业务应用提供专属通道的加密。5G 终端 UE 使用 DNN 和切片请求网络建立专有的 PDU 会话。在建立 PDU 会话的过程中，5G 基站根据 PDU 会话的安全需求激活基站与终端之间的该 PDU 会话的加密方式，以及确定 5G 基站与 UPF 之间用于传输 PDU 会话的数据包的加密隧道。切片加密支持多种加密算法，包括国密算法。

（2）区块链保障院前急救全流程可溯源

区块链技术是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，其形式为由区块组成的链式结构，每一个区块都包含上一个区块的信息，按照各自产生的时间顺序连接成链条。该链条被保存在联盟链中所有的节点中，只要联盟链中有一台服务器可以工作，整条区块链就是安全的。相比于传统的网络，区块链具有两大核心特点：一是数据难以篡改，二是去中心化。

基于这两个特点建设区块链院前急救存证平台，可有效保障院前急救数据的真实性及安全性，可为医疗机构提供更加真实可靠的急救数据，可有效减少涉及医疗纠纷时医疗机构自证时所消耗的各类成本。我们利用区块链技术可从如下三个维度来保障医疗数据的可信：

一是时间信息可信存储：将院前急救时间数据上链，使得数据无法篡改，实现全程留痕、全链路可信，高效解决自证问题。

二是存储数据可信验真：将院前急救业务系统数据库里的记录，通过存证 ID 作为关联纽带，与区块链上的数据进行比对，并返回相应结果。

三是环节数据可信取证：通过存证上链获得查询存证内容，返回区块链相关的参数，如区块高度、区块 Hash 等。

4.3 采用可信计算技术保障工作负载安全

通过采用可信计算技术，在院前急救边缘 MEC 基础设施的物理链路、软硬系统中加入可信验证，通过安全监控，构建起可信赖的计算环境，主动检测和抵御潜在的攻击。通过从硬件层、系统层、虚拟层、业务层构建安全的软硬件环境，为院前急救业务运行提供安全保障。

（1）硬件层为 OS 和业务运行提供基础安全保障，通过硬件可信根、硬件加固等维度构建安全的硬件环境，防御针对硬件的攻击。

（2）系统层为业务进程运行提供 OS 环境，系统层的安全设计一方面通过安全可信启动、可信度量、内存防护、隔离沙箱、系统安全加固等技术，构建安全可信的操作系统；另一方面，通过设备安全检测技术，及时发现针对系统的攻击，如溢出攻击、权限提升、越权访问等。

（3）虚拟化层提供云化场景下所需要的虚拟化组件。虚拟化层的安全一方面通过虚拟化隔离、容器隔离、内存防护等技术构建安全的虚拟化环境；另一方面，通过安全检测技术，检测逃逸攻击、非法访问等攻击行为。

（4）业务层是 5G 设备的业务功能，业务层的安全设计一方面将管理、控制、用户三面隔离，通过进程沙箱和权限最小化管理，严格控制业务进程能够执行的操作符合业务规范要求；另一方面，通过安全检测技术，检测针对应用层的各类攻击行为，如非法访问、注入类攻击等。

4.4 构建可信管理中心统一管理和分析

通过构建可信管理中心，采集网络接入、数据使用和基础设施的安全数据，实现业务整体可信策略管理和安全状态监控分析，主动检测和防御潜在的安全风险。

可信管理中心应包含数据采集、数据存储分析、业务应用管理等能力，具体说明如下：

（1）数据采集

基于大数据底座构建可信管理中心，可有效柔性接入各类数据，如告警数据、日志数据、流量数据、终端数据、应用数据，解决海量数据采集困难无法统一的问题，为运维者提供基础数据信息支撑。

（2）数据存储与分析

通过数据源管理、数据处理、数据分析和数据服务形成围绕信息数据的完整运营大数据集，统一提供各类数据的标准化、数据调用、数据查询、数据计算、数据建模分析等能力，借助威胁建模分析引擎和安全治理分析引擎，实现行为和威胁的关联和场景分析。

（3）业务应用管理

为适应 5G 智慧院前急救场景的安全管理业务需求，可信管理中心提供多项安全管理模块功能，如终端接入管理模块、区块链存证模块、可信策略管理模块、流量威胁管理模块等，协助运维者快速发现、分析和解决安全问题，通过建设全面的态势场景，如医疗终端接入安全态势、医疗业务数据安全态势、5G 基础设施安全态势、5G 网络流量安全态势等，支撑运维安全管理和指挥协同决策。

5. 总结

建设基于 5G 通信技术、共享互通、区域协同的院前急救信息通道，是各级政府及卫生应急部门的迫切需求。医疗救治关乎每个人的生命，对整个 5G 院前急救信息通道的网络可信接入、数据安全和个人隐私保护要求极高，因此构建可信安全体系旨在为群众生命安全保驾护航、创造社会价值与效益、提升院前急救群众满意度、降低医疗机构运营成本。

参考文献

[1] 刘磊 , 盛伟 . 浅谈 5G 技术在院前急救体系中的应用 [J]. 中国新通信 , 2022(001):024.

[2] 路辰，杨建斌，袁克虹 . 5G 移动式互联网急救医院重构院前急救体系 [J]. 中国医院院长 , 2020(8):70-71.

绿盟科技云安全纲领（下）

绿盟科技

绿盟科技自 2012 年开始研究并打造云计算安全解决方案，并于 2022 年正式推出“T-ONE 云化战略”，将安全产品与方案全面向云转型，并构建开放的云化生态。本文将对绿盟科技的云计算安全风险与发展的认知、价值主张、合作体系、参考体系、技术体系与建设方案进行阐释。因篇幅限制分为上中下三篇，本篇为下篇。

1. 云安全参考体系

1.1 与 NIST 安全标准的关系

为了增强美国关键基础设施的韧性以应对网络安全风险，2014 年《网络安全加强法案》（CEA）更新了国家标准与技术研究院（National Institute of Standards and Technology，NIST）的职责，包括制定和开发网络安全风险框架，供关键基础设施所有者和运营商自愿使用。这项法案将 NIST 之前在 13636 号行政命令（Executive Order 13636）“改善关键基础设施网络安全”（2013 年 2 月）下开发网络安全框架（Cybersecurity Framework，CSF）版本 1.0 的工作正式化，并为未来框架演变提供了指导。

2018 年 4 月，NIST 发布了 NIST CSF 1.1 版本。NIST CSF 是根据 13636 号行政命令制定并基于 CEA 持续演进的框架使用通用语言，以业务和组织需求为基础，以兼顾成本和收益的方式处理和管理网络安全风险，而无须对业务提出额外的监管要求。至此，该框架适用于所有依赖技术的组织，无论其网络安全关注点是信息技术（IT）、工业控制系统（ICS）、网络物理系统（CPS）、物联网（IoT），或是更普遍的连接设备。

1.1.1 NIST CSF框架

NIST CSF 由框架核心、框架实施层和框架轮廓三部分组成，其框架核心包括五个功能，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Respond）和安全恢复能力（Recover），如图 1 所示。这个能力框架实现了网络安全“事前、事中、事后”的全过程覆盖，帮助企业主动识别、预防、发现、响应安全风险。

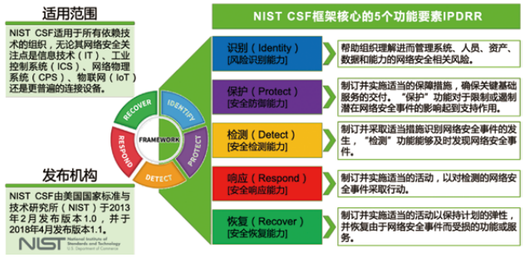


图 1 NIST CSF 框架的关键内容

NIST CSF 的框架核心的 5 个功能要素介绍如下：

识别（Identity）：帮助组织理解进而管理系统、人员、资产、数据和能力的网络安全相关风险。“识别”功能中的活动是有效使用框架的基础。只有在理解组织业务、支持关键业务的资源以及相关的网络安全风险时，才能使组织根据其风险管理策略和业务需求将资源集中投入到优先级高的工作中。此功能中的类别（Categories）有“资产管理”“业务环境”“治理”“风险评估”和“风险管理策略”等。

保护（Protect）：制订计划并实施适当的保障措施，确保关键基础服务的交付。“保护”功能对于限制或遏制潜在网络安全事件的影响起到支持作用。此功能中的类别有“访问控制”“意识和培训”“数据安全”“信息保护流程和程序”“维护”和“保护性技术”。

检测（Detect）：制订计划并采取适当措施识别网络安全事件的发生。“检测”功能能够及时发现网络安全事件。此功能中的类别有“异常和事件”“安全持续监控”以及“检测流程”。

响应（Respond）：制订计划并实施适当的活动，以对检测的网络安全事件采取行动。“响应”功能支撑对潜在网络安全事件影响进行遏制的能力，此功能中的类别有“响应计划”“沟通”“分析”“缓解”和“改进”。

恢复（Recover）：制订计划并实施适当的活动以保持计划的弹性，并恢复由于网络安全事件而受损的功能或服务。“恢复”功能可支持及时恢复至正常运行状态，以减轻网络安全事件的影响。此功能中的类别有“恢复计划”“改进”和“沟通”。

1.1.2 NIST云计算安全标准

除了 CSF 外，NIST 针对云计算具体场景，设计了相关的模型和安全框架。例如，NIST 发布了《SP500-291 云计算标准路线图》和《SP 500-292 云计算参考架构》，给出了云计算定义模型。

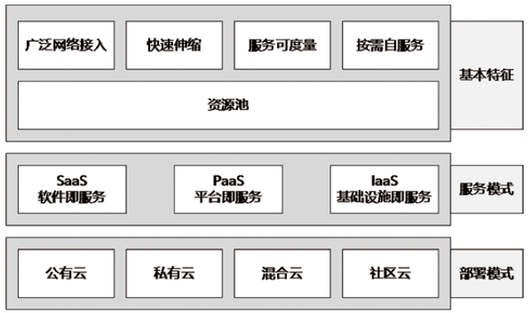


图 2 NIST 云计算定义模型

云计算定义模型定义了云计算的 3 种基本服务模式（PaaS、SaaS、IaaS），4 种部署模式（私有云、社区云、公有云和混合云），以及 5 个基本特征（按需自服务、广泛的网络接入、资源池化、快速伸缩、服务可度量）。

2013 年 5 月 NIST 发布了《SP 500-299 NIST 云计算安全参考框架(NCC-SRA)》，指导构建安全云环境，安全参考模型如图 3 所示。

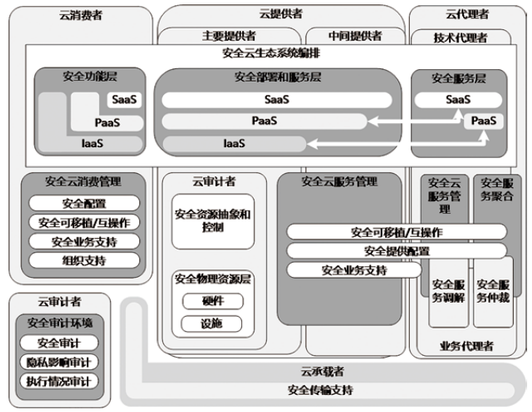


图 3 NIST 云计算安全参考架构

1.1.3 基于 NIST CSF 框架构建绿盟云安全体系

绿盟云基于 NIST CSF 框架对网络安全体系进行了优化，并在日常运营中遵循 PDCA 循环模型对其进行维护和持续改进，但这并不意味着客户使用绿盟云的服务就可以通过 NIST CSF 认证，客户与绿盟云基于上文的责任矩阵共同承担安全责任，参见《绿盟科技云安全纲领（中）——云安全责任模型》，客户应根据其自身的情况，采取相应的措施。

绿盟云打造集识别、保护、检测、响应和恢复为一体的云安全保障体系，动态协同多种安全防御措施，实现了网络安全“事前、

事中、事后”的全过程覆盖，帮助企业主动识别、预防、发现、响应安全风险，保障客户的云安全。

其中，绿盟云安全，基于 NIST CSF 的核心功能要素识别、保护、检测、响应和恢复构建云安全体系，绿盟科技也在积极应答由全球公认的权威标准组织英国标准协会（BSI）组织的 NIST CSF 等级认证评估，通过对该认证的评估应答，充分说明绿盟云在风险检测、处置、响应、恢复等方面的能力成熟度。另外，绿盟云提供的产品和服务可以针对 NIST CSF 框架核心中五项功能中的部分类别提供帮助，协助解决客户管理网络安全风险时遇到的问题。绿盟云携手全球云服务用户，构建安全生态，为用户提供更多安全选择。

针对绿盟在识别、保护、检测、响应和恢复阶段的应答说明：

在识别阶段与 NIST CSF 框架的对应关系可参见后续发布的文档 4-1《绿盟云安全对 NIST CSF 框架之识别类应对表》；

在保护阶段与 NIST CSF 框架的对应关系可参见后续发布的文档 4-2《绿盟云安全对 NIST CSF 框架之保护类应对表》；

在检测阶段与 NIST CSF 框架的对应关系可参见后续发布的文档 4-3《绿盟云安全对 NIST CSF 框架之检测类应对表》；

在响应阶段与 NIST CSF 框架的对应关系可参见后续发布的文档 4-4《绿盟云安全对 NIST CSF 框架之响应类应对表》；

在恢复阶段与 NIST CSF 框架的对应关系可参见后续发布的文档 4-5《绿盟云安全对 NIST CSF 框架之恢复类应对表》。

1.2 与 CSA 标准的关系

云安全联盟（Cloud Security Aliance，CSA）于 2008 年 12 月在美国发起，是中立的非营利世界性行业组织，致力于云计算安全在全球全面发展。CSA 在全球共有 500 多家单位会员，9 万多个个人会员。2009 年，绿盟科技成为 CSA 在亚太区的首家企业成员。

2010 年，CSA 发布了一套用于评估云 IT 运营的工具：CSA Governance、Risk Management & Compliance（GRC）Stack。其目的在于帮助云服务客户（Cloud Service Customer，CSC）对云服务商遵循行业最佳做法和标准以及遵守法规的情况进行评估。

2013 年，英国标准协会（BSI）和云安全联盟联合推出的国际范围内的针对云安全水平的权威认证（Security, Trust & Assurance Registry Program，STAR），这是一个可公开访问的免费注册表，云服务商可在其中发布其与 CSA 相关的评估。

CSA STAR 基于 CSA GRC Stack 的两大关键组成部分：

云控制矩阵（Cloud Controls Matrix，CCM）：其中列出了云计算的安全控制，并将它们映射到多个安全和合规标准。该矩阵还可以用来记录安全责任。CCM 涵盖基本安全原则的控制措施框架，它可帮助云客户对 CSP 的整体安全风险进行评估。

共识评估倡议调查表（CAIQ）：一份根据 CCM 制定的调查表，其中有客户或云审计师可能想要要求 CSP 根据 CSA 最佳做法对其合规性进行评估的一百多个问题。为云服务商提供的标准模板以记录他们的安全与合规控制。

STAR 提供三种级别的保障：CSA-STAR 自我评估是第 一 级别的入门级服务，它免费提供并向所有 CSP 公开；在保障堆栈中更深一步，第 二 级别的 STAR 计划涉及第三方基于评估的认证；第 三 级别涉及基于持续监视授予的认证。

此外，CSA 发布了《云计算关键领域安全指南》《云计算的主要安全威胁报告》《云安全联盟的云控制矩阵》《身份管理和访问控制指南》等报告。其中，《云计算关键领域安全指南》是云安全领域奠基性的研究成果，得到全球普遍认可，具有广泛的影响力，被翻译成多国语言。其中，《云计算关键领域安全指南 V4.0》共 14 章，第一章描述了云计算概念和体系，其他 13 章着重介绍了云计算安全的关注领域，以解决云计算环境中战略和战术安全的“痛点”。这些域分成了两大类：治理（governance）和运行（operations）。其中，治理域范畴很广，解决云计算环境的战略和策略问题，在治理域中，要求对云平台进行合规化和审计管理；而运行域则更关注于战术性的安全考虑以及在架构内的实现。

图 4 CSA 云计算关键领域安全指南 V4.0 云安全架构

1.2.1 CSA CCM矩阵

在过去的十几年中发布的云安全定义、架构、标准、指南中，CSA 云控制矩阵（CCM）被世界各国公认为全球通用的黄金标准。CCM 可以用作对云计算实施的系统性评估工具，也可以作为云计算供应链中各角色与安全控制关系的指导。CCM 与《云计算关键领域安全指南》高度匹配，成为云安全保障与合规的事实标准。

CSA 于 2021 年 4 月发布最新的云控制矩阵（CCM v4），CCM v4 对 CCM v3.0.1 的内容作了大幅更新，确保覆盖来自云计算新技术、新控制、安全责任矩阵的要求，改善控制项的问责制，增强互操作性及与其他标准的兼容性。

CSA CCM 的目标是：

(1) 确保覆盖来自新云技术的需求（如微服务、容器）和新的法律和监管要求，特别是在隐私领域。

(2) 改善控制的可审核性，并为组织提供更好的实施和评估指导。

(3) 在共享责任模型中明确云安全责任的分配。

(4) 改善与其他标准的互操作性和兼容性。

CCM v4 包括 17 个控制域中的 197 个控制目标，全方位涵盖了云计算技术的安全领域，具体的安全控制领域，如表 1 所示。CCM 结构包含控制域、控制措施、对于每个控制措施对应的架构内容、公司治理的相关性、涉及的云服务类型、与云服务供应商和客户的相关性以及同标准、法规、最佳实践的映射关系。

CCM 构建了统一的控制框架，通过减少云中的安全威胁和弱点加强现有的信息安全控制环境，提供标准化的安全和运营风险管理，并寻求将安全期望、云分类和术语体系，以及云中实施的安全措施等标准化。

表 1 CSA CCM v4 控制域

控制ID	控制领域	控制领域（英文）
A&A	1. 审计与保障	Audit & Assurance
AIS	2 应用与接口安全	Application & Interface Security
BCR	3. 业务连续性管理与业务弹性	Business Contnuity Mgmt &Op Resilience
CCC	4. 变更控制和配置管理	Change Control & Configuration Management
CEK	5. 密码学、加密与密钥管理	Cryptography, Encryption and Key Management
DCS	6. 数据中心安全	Datacenter Security
DSP	7. 数据安全和隐私	Data Security and Privacy
GRM	8. 治理、风险管理和合规	Governance, Risk Management and Compliance
HRS	9. 人力资源	Human Resources Security
IAM	10. 身份和访问管理	Identity & Access Management
IPY	11. 互操作性和可移植性	Interoperability & Portability
IVS	12. 基础设施和虚拟化安全	Infrastructure & Virtualization
LOG	13. 日志记录与监控	Logging and Monitoring
SEF	14. 安全事件管理、电子发现和云取证	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	15. 供应链管理、透明度和问责制	Supply Chain Mgmt, Transparency & Accountability
TVM	16. 威胁与漏洞管理	Threat & Vulnerability Management
UEP	17. 统一终端管理	Universal EndPoint Management

1.2.2 基于CSA CCM 构建绿盟云安全体系

CSA STAR 以 ISO/IEC 27001 认证为基础，结合云端安全控制矩阵 CCM 的要求，运用 BSI 提供的成熟度模型和评估方法，综合评估组织云端安全管理和技术能力。CCM 与行业接受的安全标准、法规和控制措施框架相对应，如 ISO 27001、PCI DSS、HIPAA、AICPA SOC 2、NERC CIP、FedRAMP 和 NIST 等。

绿盟科技参考 CSA 云安全控制矩阵中 17 个控制域中的控制目标构建云安全体系框架，以下以审计与保障、应用程序和接口安全、供应链管理、威胁与漏洞管理为例进行说明。

在审计与保障方面，绿盟建立了一个正式、定期的审计计划，包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证绿盟云控制环境的实施和运行有效性。

在应用程序和接口安全方面，绿盟科技的云计算相关产品与服务在发布前均需完成静态代码扫描，扫描出的漏洞告警清零才可进行发布，有效降低应用程序存在编码相关的安全问题的可能性。绿盟科技对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。

在供应链管理，透明度和问责制方面，绿盟科技制定了供应商安全管理要求，定期对供应商进行审查，验证其是否符合绿盟安全和隐私标准。绿盟科技建立了应对网络安全事件的响应流程，并针对关键基础设施、网络进行监控，可及时监测可能的网络攻击，避免数据泄露事件的发生。

在威胁与漏洞管理方面，绿盟科技所有的办公计算机均需安装公司指定的安全防护软件，仅可以安装指定软件列表的软件。对于 IT 基础系统、组件则通过 IDS/IPS 等进行保护。

针对其他控制域的要求，在此暂不详细罗列。

绿盟科技在云平台安全、云安全产品等方面，从硬件到应用构建了全面、纵深防护体系，以保障整个云计算体系的安全合规。

此外，绿盟科技在安全服务上，全面布局，在网络安全、主机安全、应用安全、数据安全等领域，推出了多款安全服务，并利用自身安全领域的优势，在全球构建安全生态，携手合作伙伴，为用户提供更多安全选择。

1.3 与等级保护 2.0 的关系

1.3.1 概述

《网络安全法》于 2017 年 6 月 1 日实施，“网络安全等级保护制度”首次从法律层面提及，标志着网络安全保护进入有法可依的等级保护 2.0（以下简称等保 2.0）时代。网络安全等级保护对象由信息系统调整为基础信息网络、信息系统（含采用移动互联技术的系统）、云计算平台 / 系统、物联网、大数据应用 / 平台 / 资源、物联网和工业控制系统等。自 2019 年 12 月 1 日起，《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》（以下简称《基本要求》）等系列标准正式实施，落实网络安全等级保护制度是每个企业和单位的基本义务和责任。

1.3.2 安全合规责任

从传统数据中心的视角来看，云安全是指保护云服务本身在基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）中的技术资源的安全性，以确保各类云服务能够持续、高效、安全、稳定地运行。云服务与传统数据中心存在明显差异，前者对云安全整体设计和实践更侧重于为云服务客户提供完善、多维度、按需定制、组合的各种安全和隐私保护功能和配置，涵盖基础设施、平台、应用及数据安全等各个层面。同时，不同的云安全服务又进一步为云服务客户提供了各类可自主配置的高级安全选项。这些云安全服务需要通过深度嵌入各层云服务的安全特性、安全配置和安全管控来实现，并通过可整合多点汇总分析的、日趋自动化的云安全运维运营能力来支撑。

在云计算环境中，任何云服务客户业务应用系统安全性由云服务商和云服务客户共同保障，云服务客户业务系统所部署的云计算服务模式不同，双方安全责任边界也相应产生差异，详细的差异如《基本要求》中所描述。按业界定义的安全责任共担模型，云服务客户使用不同模式的云服务（IaaS、PaaS 或 SaaS）时，对资源的控制范围不同，安全责任边界也根据控制范围的差异而有所不同。

等保 2.0 标准中将安全技术要求重新划分为 4 个层面：物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全。在网络和通信安全方面要求安全审计。云服务方和云租户分别收集各自的审计数据，并根据职责划分提供审计接口，实现集中审计。在设备和计算安全方面，云服务方负责基础设置的安全审计，云租户提供计算服务中的安全审计，审计要求提供数据接口实现集中审计。在应用和数据安全方面，要求根据职责划分，提供各自的审计接口实现集中审计。

1.3.3 基于等保2.0构建绿盟云安全体系

绿盟科技最早于 2006 年开始提供等级保护咨询和建设服务，拥有 10 余年、5000+ 次的等级保护建设经验。

绿盟科技对等级保护 2.0 下的安全建设，通过建设“一个中心”管理下的“三重防护”体系，分别对通信网络、区域边界、计算环境进行管理，实施多层隔离和保护措施，构建网络安全纵深防御体系。

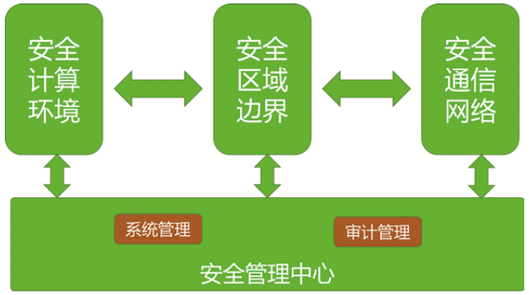


图 5 等级保护安全技术设计框架（第二级）

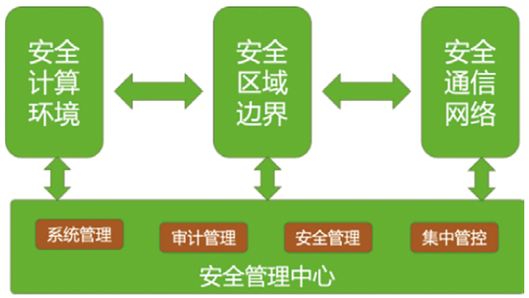


图 6 等级保护安全技术设计框架（第三级）

网络安全等级保护安全技术框架各个功能部件功能设计如下：

- 安全计算环境：对定级系统的信息进行存储、处理及实施安全策略的相关部件。
- 安全区域边界：对定级系统的安全计算环境边界，一级安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。
- 安全通信网络：对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。
- 安全管理中心：对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。

绿盟科技的总体安全体系架构设计如图 7 所示，其中，等级保护三级的系统总体安全体系架构包括总体安全策略、网络安全等级保护制度、安全技术体系、安全管理体系和安全服务体系五个有机组成部分。

图 7 绿盟科技等保 2.0 总体安全体系架构

- 总体安全策略

单位整体安全策略是立足本单位现状和将来一段时间内，以保护单位整体信息安全而制定的安全方针，需要单位全体人员遵守并执行。总体安全方针、策略具有战略高度，并且根据单位面临的安全风险，进行定期更新。

- 网络安全等级保护制度

在安全建设中，需要落实国家网络安全等级保护制度，安全保障建设首先需要对单位系统进行科学定级、备案，落实安全整改建设，通过等级测评对单位安全防护能力进行有效检测，在安全运营中持续进行安全监测和响应，同时需要配合上级单位和监管单位的安全监督检查。

- 安全技术体系

从计算环境安全、安全区域边界、安全通信网络和安全管理中心四个方面分别设计。其中，安全计算环境主要是对单位定级系统的信息进行存储处理，并且实施安全策略保障信息在存储和处理过程中的安全，安全计算环境包括：用户身份鉴别、用户身份鉴别、自主访问控制、标记和强制访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、客体安全重用、程序可信执行保护。

通信网络安全主要实现在网络通信过程中的机密性、完整性防护，重点对定级系统安全计算环境之间信息传输进行安全防护。安全通信网络包括：安全审计、数据传输完整性保护、数据传输保密性保护、可信接入保护。

安全区域边界主要实现在互联网边界以及安全计算环境与安全通信网络之间的双向网络攻击的检测、告警和阻断。安全区域边界包括：区域边界访问控制、区域边界包过滤、区域边界安全审计、区域边界完整性保护。

安全管理中心主要实现安全技术体系的统一管理，包括系统管理、安全管理和审计管理。同时，按照权限划分提供管理接口。

- 安全管理体系

从安全策略、管理制度、管理机构、人员管理、安全建设管理和安全运维管理等方面分别设计。重点内容包括安全管理机构的组建，安全策略、管理制度、操作规程、记录表单等内容的安全管理制度体系的补充和完善，安全相关人员的录用、培训、授权和离岗管理，围绕信息系统全生命周期安全的安全建设管理和安全运维管理。

- 安全服务体系

从信息系统安全角度出发，通过网络安全风险评估、安全加固、渗透测试、应急响应、安全重保、应急演练、安全培训等服务，和安全技术体系、安全管理体系相辅相成保障信息系统的安全风险始终处于可控、可管的安全状态。

绿盟科技等保 2.0 安全保障体系全景图如图 8 所示。绿盟科技遵循网络安全等级保护 2.0 基本要求和云计算相关标准要求，充分分析云计算安全需求，以“纵深防御，持续监控”为指导思想，逐步建立自适应安全防护体系，形成包含预警、防护、检测和响应等能力的安全闭环，分别从云平台和云上客户两个层面进行防护，并为云上客户提供专业和可配置的安全服务，全面控制云平台自身和云上客户的安全风险，不止满足云平台等保三级和云上客户等保

合规性要求，更可以持续防护云计算环境。

图 8 绿盟等保 2.0 安全保障体系全景图

总体而言，等保 2.0 是基础框架，云等保是补充，云等保是等保 2.0 的子集。

相应地，绿盟科技云等保解决方案整体架构如图 9 所示。

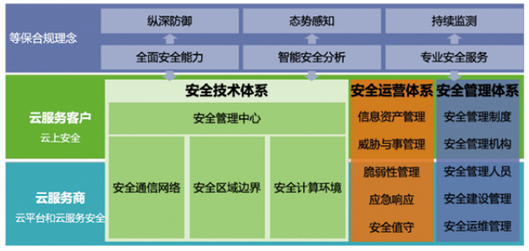


图 9 云等保解决方案整体架构

基于等保 2.0，绿盟科技的云安全产品部署如图 10 所示（其中以 v 为前缀的产品为虚拟化版本）。

图 10 绿盟云安全产品示意图

2. 云安全能力发展趋势

云计算技术始终在快速发展中，很难给出云安全能力发展的全景图，然而可以根据产业和安全技术的发展，预测云安全能力的发展趋势。按照“使用一代、建设一代、预研一代”的原则，绿盟科技不断迭代研究新的云计算安全前沿技术，积累云计算新的安全能力，研制下一代云计算安全创新产品与平台。

2.1 云上攻防

除了合规驱动外，越来越多的云安全事件也在促进云安全防护能力的提升。攻击者是逐利的，随着越来越多企业选择云计算来开发、承载业务，云上业务的价值在飞速增长，也因此成为黑产团伙的重点关注对象。

近年来，云安全事件层出不穷，例如：

(1) 2018 年 2 月 20 日，特斯拉公司的 Kubernetes 云原生集群被曝出曾在数月前被入侵，黑客在特斯拉的 Kubernetes 集群中部署了挖矿程序。

(2) 2019 年 10 月 15 日，一款名为 Graboid 的挖矿蠕虫程序被曝光，该病毒通过不安全的 Docker 守护进程暴露出来的远程端口获得目标主机的控制权，然后下达指令从 Docker Hub 上拉取并运行恶意镜像。被发现时，它已经感染了超过 2000 台 Docker 宿主机。

(3) 2020 年 4 月 8 日，微软 Azure 安全中心公告称检测到大规模 Kubernetes 集群挖矿事件；同年 6 月 10 日，Azure 再次公告称检测到大规模 Kubeflow 挖矿事件。

(4) 2021 年 8 月，微软提供的 Cosmos DB 数据库服务被曝光存在一系列严重的安全漏洞，可能导致大规模商业数据泄露。

(5) 2021 年，TeamTNT 组织多次被曝针对云计算对象发起攻击，包括投放针对 Kubernetes 集群的非法加密挖矿软件、在 Docker Hub 上投放恶意镜像、利用存在未授权访问漏洞的 Docker 控制服务器等。

由此可见，攻击者已经将战场从传统环境扩展到了云计算环境。在此背景下，未知攻焉知防，防守方必须跟进掌握最新的云安全攻防技术，不断迭代、不断进化，实现云上攻防能力的持续运营和向云安全防御能力的持续转化，才能够实现云计算业务和环境的有效防御。

对此，绿盟科技星云实验室创建并开源了 Metarget 云原生攻防靶场项目，希望将云原生脆弱场景固化，提供自动化的脆弱环境构建能力，不断积累沉淀云原生攻防研究，进而实现以攻促防，持续赋能云原生安全产品。

对于具体的攻防技术来说，归纳和分类是非常重要的，能够帮助我们降低复杂度，梳理已有攻击技术，制订防护能力发展规划，评估安全能力对攻防技术的覆盖度。目前 Mitre 归纳了云计算（含几大公有云）、容器的 ATT&CK 技战术[2]。在此基础上，我们扩展了一个云原生 ATT&CK 矩阵，读者可结合这几个矩阵构建云上整体的威胁视图。

表 2 云原生 ATT&CK 矩阵

初始访问	执行	持久化	权限提升	防御绕过	获取凭证	发现	横向移动	收集	危害
利用对外开放的应用程序	容器管理命令	外部远程服务	逃逸到宿主机	在主机上构建镜像	暴力破解	容器和资源发现	逃逸到宿主机	私有镜像	资源劫持
外部远程服务	部署容器	植入内部镜像	通过漏洞利用实现权限提升	部署容器	不安全凭据	容器网络扫描	窃取凭证		破坏系统及数据
有效账户	计划任务/容器编排任务	部署后门容器	计划任务/容器编排任务	损害防御	恶意准入控制器	权限组发现	访问云资源		影响服务
用户执行/恶意镜像	用户执行/恶意镜像	有效账户	有效账户	清除入侵痕迹		云厂商服务	集群中的网络和服务		
	利用对外开放的应用程序	恶意准入控制器		伪装		镜像仓库			
	外部远程服务	计划任务/容器编排任务		有效账户					
	云厂商服务	逃逸到宿主机		通过代理访问					
		Webshell							

2.2 云安全态势与安全能力的评估

随着合规性要求和攻防需求迅速增加，企业纷纷部署众多的安全产品以确保云环境和云上业务的安全性，但即使如此，也很难回答“云计算平台和应用是否安全”这一问题。因为错误配置与缺乏及时更新都可能会产生系统的风险。事实上，无论是真实的攻击，还是大型攻防对抗演练，都出现攻破云平台或云上应用的案

例。考虑到云上业务变化频繁，云计算应用规模庞大，仅仅依靠人工手段去评估（如红蓝对抗、渗透测试等）很难达到完备。因而，云环境中的持续性安全评估,特别是云原生入侵和攻击模拟（Cloud Native Breach & Attack Simulation，CNBAS）应运而生，其可评估云环境是否安全，并可验证云上部署的安全能力是否有效。

从功能上来看，CNBAS 既能对云计算平台本身安全性进行评估，又能可对第三方安全能力和策略进行评估。一方面可依托于针对云计算 ATT&CK 矩阵的攻击武器，对云环境进行自动、持续、无害化的攻击模拟；另一方面，参考国内外针对云原生系统的合规性要求和成熟度评估机制，评估系统整体的安全成熟度。

从架构上来看，CNBAS 以云原生的方式部署和工作，既具备云计算的可靠、伸缩、易扩展等特性，也能利用云原生平台的接口、资源，减少对被评估环境依赖和侵入，提升整体运营的效率。

2.3 云上风险发现

云计算技术栈已经被广泛使用。开发运营一体化（DevOps）、编排系统、微服务、声明性 API 与无服务器等新技术的使用，使得对应用运营变得更加便捷方便，但也带来了极大的安全风险。因为：

- 云上服务需要对外暴露，但如果因不当配置、弱访问凭证、服务软件版本信息泄露，都可能造成攻击者发现并利用脆弱性，造成数据泄露等后果。在Gartner发布的2022年安全和风险管理的主要趋势中，将攻击面的暴露作为第一条纳入其中，可见对攻击面的管理的重要程度。
- 当前软件系统依赖大量开源软件库、中间件，这些软件如出现严重漏洞能被利用，攻击者发现后就可能直接攻陷云上系统。
- DevOps的闭环链条非常长，其中某个环节出现不可控的风险，就会危害整个业务系统的安全。例如，外包员工将代码仓库外泄到代码平台或自托管的主机，都可能被攻击者所窃取并利用。在2021年的3月就曾爆出PHP的Git服务器被入侵，源代码被添加后门事件。

因而，绿盟科技在云上风险发现方面构建完整的外部攻击面发现的监控体系，包括：

- DevOps软件供应链监控：开发中使用的大量的第三方开源服务或者依赖库，使用的服务镜像，都有可能存在漏洞。
- 云计算基础设施监控；监控Docker、Kubernetes等云计算基础设施，特别是对外暴露的服务与自身的安全漏洞，可对云上云原生服务组件潜在的脆弱性进行快速识别或无害性高精度验证。
- 微服务安全：微服务依赖的服务网格，各种服务发现组件，消息队列等中间件，对外暴露的大量API等安全风险。
- 公开服务配置监控：例如，Kubernetes的API对外未授权暴露可导致攻击者接管整个Kubernetes集群，恶意利用集群资源集群。
- 源代码仓库监控：通过对云上的资产进行持续测绘，获取源码仓库的特征利用人工智能识别仓库真实属主，并对存在错误配置或者未授权的仓库进行仓库内容分析识别。具体包括以下功能： 代码仓库基础信息识别；识别代码仓库地区信息、人名信息、组织机构信息等；发现代码仓库中的敏感信息，如个人隐私、SQL数据库账号密码、服务器公私钥等；归因代码仓库相关领域、开发和发布机构等。

我们预测，云上风险的发现将成为攻守双方在云计算系统、应用与服务前的首战之地，包括网络空间测绘技术、自动化漏洞验证、软件供应链安全等一系列技术将快速发展，读者应在这些领域适度投入资源，尽可能降低对外暴露的攻击面。

2.4 API 与服务类安全

云原生环境中，应用由传统的单体架构转向微服务架构，云计算模式也向为函数即服务（Function as a Service，FaaS）发展。应用架构和云计算模式的变革会导致进一步的风险。例如：

- 云原生应用架构的变化进而导致应用API交互的增多，大部分交互模式已从Web请求/响应转向各类API请求/响应 ，如RESTful/HTTP、gRPC等。
- 由于应用架构变革，云原生应用遵循面向微服务化的设计方式，从而导致功能组件化、服务API数量和东西向流量激增，配置复杂等问题，进而为云原生应用和业务带来了新的风险。例如，攻击者可利用某服务API漏洞，在内部容器网络进行横向移动，造成数据泄露的后果。
- 无服务器计算是一类新的云计算模式，在提升整体开发效率的同时，也引入新的风险，如拒绝钱包服务攻击（Denial of Wallet DoW）、函数滥用等。

因而，绿盟科技构建了面向云原生应用和 API 的安全防护体系，包括：

- 微服务API资产发现：提供微服务API资产信息、API调用链路追踪及关联关系，同时，提供基于IP/域名/业务/API数据实体多角度资产画像可视化，数据标签、数据风险、安全事件探索以及全方位的访问记录可视化能力。
- 微服务API业务安全：基于基线的异常检测可对微服务业务间调用异常序列、参数、逻辑等进行异常行为告警。
- 微服务API安全网关：提供针对微服务应用场景下的全流量防护能力，可适应云原生环境下应用普遍容器化、面向微服务架构、容器编排调度等特性，解决微服务间东西向流量难以防护的问题，特别对微服务API滥用、Webshell连接上传、SQL注入等常见攻击有着较为明显的防护效果。

3. 场景化的云安全建设

3.1 大型公有云上的安全建设

国内云计算总体处于快速发展阶段，据中国信息通信研究院发布的《云计算白皮书（2022 年）》[1] 的数据，2021 年我国公有云 IaaS 市场规模达 1614.7 亿元，增速 80.4%，PaaS 同比正增长 90.7% 达 194 亿元，SaaS 同比正增长 32.9% 达 370 亿元。推动公有云快速增长主要用户群体为企业、个人和政府，政府方面因数据敏感度、安全性比较高出台了各类政务云的规划，多数非敏感业务也逐渐转移到政务云上；此外，中小企业是大型公有云市场的核心群用户，因为成本和便捷性考虑，相当一部分的企业选择公有云托管业务或直接采购 SaaS 服务。

大型公有云服务商一般会提供较为完善的安全服务，其中相当一部分为云服务商自身的安全能力，而其他非标准、特定需求、高级、跨云的安全能力则由第三方安全厂商提供。一般公有云计算场景的安全产品选购途径有 4 种：安全厂商提供可安装的安全软件、安全厂商提供独立的安全 SaaS 服务、驻公有云市场的安全厂商的安全产品、云服务商自己提供的安全服务。

公有云租户如希望进行云上的安全建设，首先需要考虑自身的业务与安全责任，依照云安全责任模型，承担租户自身部署的资源和业务的安全，负责采购安全产品、配置安全策略和安全运营。因而，租户应对比自己的需求与云服务商的安全能力，重点考虑两者不一致处。如存在，则或通过第三方安全厂商产品，或通过独立的安全服务解决。

从目前的实践看，建议用户在安全建设前结合业务需求和经济投入、法律政策的要求，着重针对漏洞利用、口令破解、偏离基线、横向扩散等风险进行安全防护。

3.2 私有 / 行业云的安全建设

2015 年“互联网 +”概念兴起至今，影响国民经济的主要行业均着手实现云化转型，而各行业的龙头企业在相当程度上成为云计算平台建设的排头兵，在此期间对影响国民经济各主要行业，国家发布了云化建设的行业政策。其中覆盖了制造业、政府、医疗、教育、金融、物流、能源、互联网、交通等行业。在《云计算三年行动计划（2017—2020 年）》和《推动企业上云实施指南（2018—2020 年）》中，可以看出政府在积极推动云计算在各个场景的应用，尤其是政务和金融领域。

相当一部分数量的行业或区域的头部客户是从虚拟化系统转到云计算系统，并且有合规性和数据安全的考虑，所以他们是采用了私有云的方案，而没有采用直接上公有云的方案。当然，有一些大型行业（如运营商、政府、金融）的头部机构，也在从为自己服务的私有云转向为行业内其他客户提供具有本行业特点服务的行业云。

与大型公有云不同之处在于，私有云与行业云的运营方不是公有云服务商，而是行业客户。根据责任共担模型，如果是私有云，那么全部责任均由行业客户承担；如果是行业云，那么责任分界线以下的所有安全责任，均由该行业客户承担。所以，行业客户应在方案设计、平台建设与安全运营整个生命周期，与安全厂商紧密协作，全方位保护云平台和应用的安全。

具体地，结合私有云与行业云本身的安全风险以及各行业的特点，在满足法律法规的要求下，以 CARTA（持续自适应风险与信任评估）为原则，遵循“建立自适应安全防护模型和责任共担模式”的设计思路，坚持“协作、共享、智能和服务”的设计原则，采用“1+2+3+5”的顶层设计，即实现自适应安全防护体系一个目标，保护云平台和云上信息系统两个对象，同步规划、同步建设和同步使用安全管理体系、安全技术体系和安全运营体系等三个体系，开展覆盖决策规划、纵深防护、监测预警、安全响应和评价提升五个阶段的工作，保障云安全运行，为行业实现数字化转型护航。

私有云与行业云的具体云安全建设，可参见绿盟科技后续发布的相关行业的云安全建设方案。

3.3 多云 / 混合云的安全建设

虽然多云 / 混合云的发展非常迅猛，然而其应用增加了整个系统的复杂性、异构度和攻击面，攻击者有可能利用一个系统的脆弱性移动到另一个核心系统，因而，企业应考虑在多云或混合云环境中部署统一、全方位的安全防护能力。此处给企业有两点建议：首先，采用零信任的架构，如 SSE、SDP 和身份访问管理机制，构建基于身份与上下文的边界；其次，采用第三方厂商构建跨云的安全编排能力，动态地在公有云、企业环境部署一致的安全能力，并可根据业务进行弹性伸缩和迁移，避免云服务商单一安全能力锁定。

更具体地，在面对多云 / 混合云环境下需要着重注意资源的统一管理能力，只有具备资源的统一管理能力才能对防护、运维起到良好的基础支撑。首先是资产清查能力，需要对多云统一管理为客户提供基础的资产概览，资产拓扑，账号管理，主机资产如虚拟主机，镜像，网络，用户权限管理，具备横向可扩展的 CMP 能力等，其安全能力对接多云有一定要求。其次是安全建设能力分散，运维管理成本较高，需要统一进行策略管理，需要根据资产分布情况进行云安全能力建设，根据客户需求，自动化投放和部署安全服务。最后是需要满足等保合规以及安全体系和人员提升，做到威胁闭环处置的运营反制能力。

多云与混合云的具体云安全建设，可参见绿盟科技后续发布的《多云 / 混合云场景的云安全建设方案》。

3.4 云化新型基础设施（5G/ 边缘计算）的安全建设

我国的“十四五”规划提出，系统布局新型基础设施，加快第五代移动通信、工业互联网、大数据中心等建设。新型基础设施（包括 5G、边缘计算和工业互联网等）的建设已经成为国家政策与经济发展的重要抓手，也是各行各业数字化转型的重要驱动力。

随着云计算作为支撑技术的快速发展，新型基础设施多以云计算为技术底座，如 5G 核心网、MEC 平台，以及工业互联网及其边缘网关等，都使用了虚拟化或容器技术提供弹性伸缩、敏捷部署的能力。因而，保护这些新型基础设施，就需要首先保护其云计算底座的安全。

结合 5G/MEC 风险，以运营商为例，边缘计算安全防护方案是由两个部分构成——运行体系和生态体系，其中运行体系由云、管、端、边构成安全能力的纵深防御和深度协同。通过运营商通信安全增强能力、云端安全能力协同共同构成整个体系。生态体系覆盖了与边缘计算相关的基础设施、软件平台和 APP 的生命周期管理，以及边缘计算相关生态的安全测试验证，包括测试环境、测试工具、基础资源。结合用户业务能力将安全能力分别以云、管、端、边 4 个位置进行部署。边缘计算的安全能力部署在最靠近行业用户的位置，为本省、云端能力提供信息基础，为客户实现最直接的安全防护、检测和安全基础设施。

运营商行业的具体云安全建设，可参见绿盟科技后续发布的《运营商行业场景的云安全建设方案》；工业互联网的具体云安全建设，可参见绿盟科技后续发布的《工业互联网场景的云安全建设方案》。

参考文献

[1] https://github.com/Metarget/metarget.

[2] https://attack.mitre.org/matrices/enterprise/cloud/.

[3] 中国信通院，云计算白皮书（2022 年）。

企业访问国际互联网信道合规管理指引

绿盟科技 总体技术部 张睿

摘要：企业组织为获得持续发展，通过互联网进行信息获取与传播、远程办公、线上交易已经成为日常业务开展中的基本需求。随着我国企业组织不断加强并深度参与国际经济贸易，通过国际互联网信道进行数据信息交换的需求强烈且频繁，所以为规范和保障国际信息交流的健康发展，当前对国际联网流量进行审查过滤，也因此对部分网络资源的高效获取带来影响。与此同时，伴随我国当前信息领域法律法规体系日趋完善，明确组织非法外联违什么法、如何惩罚、合规如何建设管理成为一个重要议题，其能够帮助企业明确使用非法定信道的合规风险，进而推动企业组织将国际联网合规纳入本机构信息安全管理体系建设，合法访问国际互联网资源。

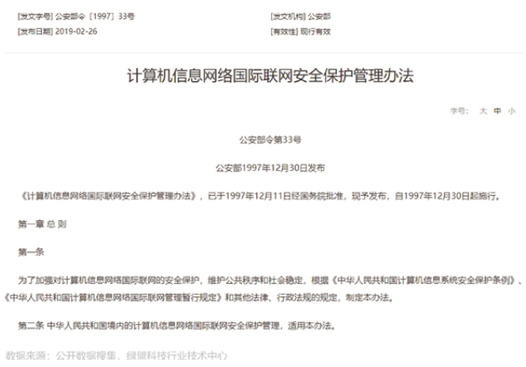
关键词：合规管理 非法定信道 行政处罚 计算机犯罪

数字信息化时代，企业组织利用互联网参与国际经济贸易活动日益频繁，通过数字信息化技术进行技术创新，实现数字化新发展、业务新成长成为当前各类企业机构积极探索的热点主题。信息技术产业技术更新迭代频繁，拥有广泛的横向跨产业影响效应，从 2022 年的“元宇宙”到 2023 年的“ChatGPT”，既表征了互联网数字化产业异于传统行业的活力，同时也表明企业组织必须积极加入国际化技术竞争，与全球的互联网产业保持积极互动，从而获得发展优势。国际互联网是当前各大企业组织机构实现跨区域、国家进行通信与业务往来，实现数据资源交互，完成项目产品交付等关键任务的重要通道。受网络安全监管体系日趋严格以及流量内容过滤清洗的双重影响，部分国际互联网站点与资源容易出现访问效率受限、拒绝访问的情况[1]。

针对相关问题，企业组织机构通过法定信道合法、合规获取国际互联网资源异常重要，尤其从 2021 年开始，信息领域法律法规持续细化完善，部门规章、行业准则不断出台实施，国家、行业、团体标准每年的发布规模与更新效率也不断达到新的高度。企业组织早期“无法可依”的“裸奔”时代已经过去，“合规必须执行到位、责任必须落实到人”的时代已经到来。除此之外，我国刑事领域网络安全犯罪的打击日益精准，执法能力日益增强，围绕企业组织因互联网管理不合规受到行政处罚的案件不断增多，所以组织机构必须积极将此纳入日常管理体系，防止因疏于管理，因为诸如非法外联、搭建境外服务器以及各类“翻墙”行为受到监管机构的行政处罚，甚至因制作、传播或贩卖“翻墙”工具而触犯刑法。

1. 互联网信道法规要求

针对非法定信道的管理，除一般法《刑法》分则妨害社会管理秩序涉及的网络安全领域相关罪名，特殊法《网络安全法》《数据安全法》乃至《个人信息保护法》联合构成上位法体系化要求。但因单纯使用非法定信道这一行为相对具象，不适合于法律层面为此细节单独阐述相关法律责任，所以在行政规章、部门规章的层面得到了细化。针对行政规章，现行有效并且经常作为各省、直辖市网络安全监管机构执法依据的行政规章有两部，首先为 1996 年 2 月 1 日国务院 195 号令发布，并于 1997 年 5 月 20 日修正的《中华人民共和国计算机信息网络国际联网管理暂行规定》[2]，该规定第六条明确了任何单位和个人不得自行建立或者使用其他信道进行国际联网，与此同时确定了由公安机关进行执法，可以执行诸如警告、通报批评、责令停止联网、罚款相关行政处罚。其次为 1997 年 12 月 11 日国务院批准发布，并于 2011 年 1 月 8 日修订的《计算机信息网络国际联网安全保护管理办法》[3]，该办法进一步细化了诸如打击单位或个人利用国际联网违法活动的类型，明确了各主体安全保护责任，进一步指出公安机关的安全监督范围涉及联网备案、安全保护管理制度、通知删除关闭以及网络犯罪追踪查处。该行政规章基于 1997 年公安部第 33 号令发布，所以也是公安机关对于企业组织通过非法定信道访问国际互联网，实施监管处罚最常引用的行政规章。


[发文字号] 公安部令［1997］33号　　[发文机构] 公安部
[发布日期] 2019-02-26　　[有效性] 现行有效

计算机信息网络国际联网安全保护管理办法

字号：大 中 小

公安部令第33号

公安部1997年12月30日发布

《计算机信息网络国际联网安全保护管理办法》，已于1997年12月11日经国务院批准，现予发布，自1997年12月30日起施行。

第一章 总 则

第一条

为了加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和其他法律、行政法规的规定，制定本办法。

第二条 中华人民共和国境内的计算机信息网络国际联网安全保护管理，适用本办法。

数据来源：公开数据搜集，绿盟科技行业技术中心

图 1《计算机信息网络国际联网安全保护管理办法》

除公安机关针对企业组织机构利用非法定信道访问国际互联网的监管要求外，企业组织还应关注自身所属的行业监管要求，尤其是行业内部门规章，将与上位行政规章组合形成监管机构执行行政处罚的基准，同时结合行业特性，会围绕利用互联网进行发布、传输的内容进一步细化监管要求。以教育行业为例，2021 年发布的行政规章《教育部办公厅 工业和信息化部办公厅关于提高高等学校网络管理和服务质量的通知》，以及 2000 年发布的围绕网络站点管理的一般管理性规定《教育网站和网校暂行管理办法》。

此外，工业和信息化部作为电信领域业务关键政府监管机构，2017 年发布的《工业和信息化部关于清理规范互联网网络接入服务市场的通知》，也再次强调了任何组织机构未经电信主管部门批准，不得自行建立或租用专线等其他信道开展跨境经营活动的要求[4]。

2. 行政与刑事责任

针对行政责任，对于通过非法定信道访问国际互联网，以北京市为例，涉及两项行政处罚，分别为“对未经允许，建立非法定信道进行国际联网的行为进行处罚”（公安职权编号：C05782）[5]，以及“对未经允许，使用非法定信道进行国际联网的行为进行处罚”（公安职权编号：C05783）[6]，两者违法情形均为《中华人民共和国计算机信息网络国际联网管理暂行规定》（以下称《规定》）第六条，即单位和个人自行建立或者使用其他信道进行国际联网。行政处罚依据也均基于《规定》第十四条，行政处罚种类包含罚款、警告、停止联网、没收违法所得。

图 2 北京市公安 C05782 行政处罚职权

基于《计算机信息网络国际联网安全保护管理办法》，统计北京市近六个月公安机关相关行政处罚案例，时间覆盖 2022 年 8 月至 2023 年 1 月，总体案件数量 33 件，处罚种类全部为警告，相关处罚原因主要围绕不履行国际联网备案职责、未落实安全技术保护措施。此外以 2023 年 1 月为例，围绕信息领域的行政处罚，还有基于《网络安全法》的处罚 5 件，处罚种类也全部为警告 [7]。

北京市公安基于《计算机信息网络国际联网安全保护管理办法》行政处罚案件统计

时间	处罚数量	警告
2023年1月	6件	6件
2022年12月	0件	0件
2022年11月	3件	3件
2022年10月	3件	3件
2022年9月	12件	12件
2022年8月	9件	9件

数据来源：北京市公安官网，绿盟科技行业技术中心

根据北京市公安机关相关数据，基于《规定》围绕非法定国际互联网信道的行政处罚主要以警告为主，通过检索外省相关案例 [8]，涉及罚款的数额较低，一般不会超过 1 万元人民币，罚款数额以及处罚类型均较违反《网络安全法》《数据安全法》更少。其一方面受行政执法单位执法权限的约束，另一方面主要源于违反行政规章与违反法律的罪过程度和负面影响差异甚大。对比近三年生效的网络信息领域相关法律责任追究形式，因违法而采取罚款的，一般依据影响程度分梯级设定，并习惯采用处罚企业加责任人的双罚制，所以往往中等程度以上处罚会对企业组织带来非常大的不利影响。一般违法企业组织不但要缴纳罚款，还会因此引发商誉贬值、客户流失甚至被吊销执照的风险。但企业组织不能因此放松基于《规定》对互联网信道合规履行的审慎义务，因行政处罚负面记录会直接影响甚至钳制诸如企业对外投标、融资、并购等关键市场活动，且往往会被设定为限制准入、否定排除条件，对企业组织的综合合规风险仍然巨大。

针对刑事责任，在不考虑企业组织以从事非法活动而设立或通过非法定信道主动制作、发布传播违法内容的情况下，仅以企业为发展正常业务而违规使用非法定国际互联网信道 (如利用境外 VPN“翻墙”)，在负面影响可控的情况下，一般均通过警告的行政处罚方式督促相关企业组织整改，其有利于市场经营主体的健康发展，防止过度执法，同时也体现了《刑法》的谦抑性。

但部分企业组织因合规管理意识与能力薄弱，甚至知法犯法，存在制作、传播非法信道访问工具或提供非法国际互联网信道服务的行为，此已明确定性为犯罪行为，并有众多刑事案例。根据《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》[9]，针对计算机信息系统安全保护措施，具有“越权获取数据、越权控制，以及其他同等功能的”，属于“专门用于侵入、非法控制计算机信息系统的程序、工具”。当前针对此类软件（“翻墙”软件）是否属于上述工具，各地法院根据实际情况，一般认定的可能涉及两类罪名。第一种情形肯定此类软件属于上述犯罪工具，会被认定提供侵入、非法控制计算机信息系统程序、工具罪，受《刑法》第二百八十五条规定约束；第二种情形否定属于上述犯罪工具，从技术上不具有上述工具的特性，不能满足上述罪名的犯罪构成要件，而是从非法销售盈利的角度出发，被认定为非法经营罪，受《刑法》第二百二十五条规定约束。

3. 合规管理方案

针对企业组织访问国际互联网信道合规管理与建设，结合监管要求与企业内控，本文提供如下三项建议。

首先，企业组织应当加强监督内部审计，于日常业务开展中，能够有效监测组织跨境流量与终端应用，识别非法定信道工具的使用与敏感或非法信息外发、发布，防止先通报后调查、先问责后整改的被动失效管理，完善事前合理审慎、预案先行，事中明确责任、追溯到人的能力建设。

其次，将访问互联网服务纳入组织管理体系，基于企业组织的管理成熟度与规模，可以分情况纳入合规管理体系、信息安全管理体系或质量管理体系，保障风险管理的落地，实现信道合规、境外网络资源访问相关业务流程的闭环化管理与管理成熟度的持续提升。

最后，对于国际互联网资源有高要求的企业组织，依法通过电信运营商申请接入国际专线，并申请备案，在成本方面可以考虑就近接入的方式，如选择申请我国香港、澳门地区网络。同时，需持续监控企业组织访问国际互联网资源的合理性、业务相关性，防范利用备案信道从事非法内容的制作、传播等活动。

4. 结语

企业组织通过合法国际互联网信道访问并使用网络资源是合规建设必不可少的工作，对内加强违规事件的发现能力与管理体系成熟度建设水平，对外积极完善并满足合规备案、依申请接入专线等监管要求，是企业保持互联网信道合规接入进而满足网络安全大合规框架的可行路径。我国企业组织信息与网络安全合规建设还有很远的路要走，而在国际互联网合法信道的合规问题上，未来也会有安全、成本、效率平衡的解决方案，而针对流量审查过滤，我们也将以更积极开放的姿态于全球化的浪潮中不断成长前行。

参考文献

[1] 沈逸 . 超越推墙与守墙之争，推进长城防火墙改革 [BD/OL]. 复旦发展研究院，https://fddi.fudan.edu.cn/c9/fb/c18965a182779/page.htm.

[2]《中华人民共和国计算机信息网络国际联网管理暂行规定》，https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE2ZjNlOTc4NDAxNmY0MWZjMWMzMjAyNTU%3D.

[3]《计算机信息网络国际联网安全保护管理办法》，https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE2ZjNjYmIzYzAxNmY0MGRkYTNkZDA4MmY%3D.

[4]《工业和信息化部关于清理规范互联网网络接入服务市场的通知》，http://www.cac.gov.cn/2017-01/23/c_1120366809.htm.

[5] [C05782] 对未经允许，建立非法定信道进行国际联网的行为进行处罚，http://gaj.beijing.gov.cn/wsgs/zqxx/xzcfqd/202004/t20200403_1787296.html.

[6] [C05783] 对未经允许，使用非法定信道进行国际联网的行为进行处罚，http://gaj.beijing.gov.cn/wsgs/zqxx/xzcfqd/202004/t20200403_1787292.html.

[7] 北京市公安行政处罚公示，http://gaj.beijing.gov.cn/wsgs/sgszl/xzcfgs/index.html.

[8] 行政处罚结果信息公开，浙江政务服务网，https://www.zjzwfw.gov.cn/zjservice/matter/punishment/index.do?webId=1&tabid=00001.

[9]《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》，https://pkulaw.com/lawexplanation/7129e689f4c469a8f5660c9825371149bdfb.html?way=textRightFblx.

浅谈数字化转型下的企业安全运营体系建设

绿盟科技 行业技术中心 刘艳东

摘要：数字技术推动企业战略转型与业务发展，网络安全与信息化业务深度融合，传统的网络安全体系逐渐无法有效应对复杂的网络安全威胁。企业安全运营是通过人、工具、流程、数据和流程的有机融合，持续提升企业安全价值，成熟的安全运营在企业数字化业务发展中将发挥重要作用。本文将通过对企业网络安全现状进行分析，提出一种企业安全运营建设思路和设计框架，围绕企业安全运营建设的具体措施进行阐述，最后对安全运营建设促进企业发展的意义进行总结。

关键词：数字化转型 安全运营能力 自适应安全

1. 前言

“十四五”期间，随着“数字中国”和“网络强国”等国家重大战略进程的加快推进，我国数字经济与实体经济融合发展。云计算、大数据、人工智能、5G 等数字技术加速创新与应用，持续推动企业数字化变革与进程发展，有效提升企业生产力和创造力。数字技术为企业数字化转型带来新模式和新动能的同时，也引入了更多的网络安全风险。近年来，我国网络安全法律法规和政策要求的相继出台与实施，网络空间安全治理已上升至国家战略高度，企业依据国家、行业监管要求和业务需求进行了网络安全建设。随着网络攻击技术的迭代进化以及新型数字技术与业务的深度耦合，以边界防御为主的传统网络安全体系逐渐无法有效应对新型、灵活、复杂多变的网络攻击形态，合规驱动安全建设正在向风险和数据驱动安全建设转变，边界、非体系化的安全防护体系，在一定程度上制约了企业数字化高质量发展。

2. 企业安全运营现状与分析

在经过多年的网络安全建设后，企业形成了基于边界防护为主的安全机制。为持续提升市场竞争力，企业通过使用数字化技术来驱动业务转型与模式创新，但同时也面临着更加复杂的安全威胁，现有的网络安全保障体系已无法适应企业长期发展的需要，主要在以下几个方面还存在不足。

2.1 缺乏有效的安全管理组织制度体系

企业信息化建设与业务伴生发展，通过体系化、流程化和精细化的信息化管理流程来提升企业生产运营效率和降低运营风险及成本。企业网络安全管理与信息化发展相辅相成，但在建设进度上具有一定的滞后性。在安全管理制度体系建设方面，企业仍然存在组织建设不完善、流程制度不规范、责任落实不明确的问题，在某种程度上制约了企业网络安全管理工作的开展。

2.2 安全防护体系建设尚不完善

在数字化转型深化过程中，云原生、人工智能、移动办公等广泛应用，企业网络安全边界持续瓦解。业务云化加速与分布式企业经营模式扩大了受攻击面，网络攻击的隐蔽性、复杂性和持续性将进一步加剧，企业 IT 网络与数据安全环境更加恶化。企业不仅要满足数据结构的开放度和弹性，同时也要求安全架构设计上能够确保网络安全。多数企业尚采用边界防护建设模式，以传统安全技术为基础构建的企业防御能力，将难以遏制不断向企业内部渗透的威胁，被动式防御体系逐渐无法适应企业快速发展的需求，碎片化的安全能力建设将无力应对数字业务变革所带来的安全风险。

2.3 缺少专业的安全运维能力

多数企业的网络安全工作是通过内部信息化部门进行统一管理。对于企业信息化技术体系建设以及运营维护的管理部门，安全运维工作多数是由信息化运维人员兼职负责，他们往往在系统信息技术体系建设和运行维护管理方面拥有丰富的经验，但缺乏有效的安全运维技能、方法和流程。网络安全运营是相对独立的系统工程，需要具有专业知识背景的安全运营团队进行全面和流程化管理。

3. 企业安全运营建设思路与架构

在管理学中，对运营的定义是对运营过程的计划、组织、实施和控制，是与产品生产和服务创造密切相关的各项管理工作的总称。安全运营是为了实现组织的安全目标，提出安全解决构想、验证效果、分析问题、诊断问题、协调资源、解决问题并持续迭代优化的统筹管理过程，满足组织网络安全的动态性、持续性和整体性需求。安全运营的核心是将人、数据、技术工具和流程等要素进行有机结合，以数据为基础，以安全分析为手段有效地发现网络安全威胁，并以处置响应为闭环来实现对网络安全威胁的阻断或抑制。通过运用先进的技术能力和管理手段，对企业网络安全进行可持续的风险管控。企业为更好地适应数字化业务发展的需要，创新技术的应用、资产的动态变更、管理和业务数据的弹性变化将促进企业数字安全管理处于随时调整的状态，以应对企业数字化转型所面临的网络安全风险与挑战。

3.1 理念与思路

体系化、常态化和实战化成为当下网络安全建设的新标杆和新风向。借鉴 Gartner CARTA 模型，贯彻“基于数据分析为核心的安全运营闭环管理”安全运营理念[1]，以体系化、层次化的安全能力建设为指引，构建基于企业信息化场景的可信任、可持续的安全运营能力。通过打造一体化、联防联控机制，构建可编排策略、可信任访问、可验证攻防、可度量运营、可联动响应和可闭环流程，为企业打造“全面化防护、智能化分析和自动化响应”的弹性、自适应安全防护体系。

3.2 总体架构

企业安全运营架构主要包括安全管理体系、安全技术体系和安全运维体系三个主要部分。通过融合人、技术工具、制度流程和数

据等全要素，构建预测、预防、检测与响应的安全闭环流程，以打造体系化、实战化的安全运营能力，实现网络安全体系建设从合规驱动到风险和数据驱动的转变 [2]。

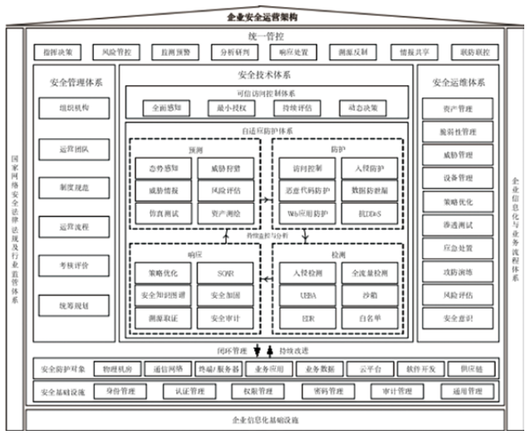


图 1 企业安全运营架构

4. 企业安全运营体系建设具体举措

当前，面对安全攻防态势的日趋恶化，企业要借鉴业务风险管控的思想建立持续性安全运营能力，主要从组织管理制度体系完善、安全运营团队建设、安全技术能力提升和安全运维体系优化四个方面进行思考。

4.1 持续完善组织管理制度体系

安全管理是企业安全运营工作的基础，通过建立健全安全管理体系，对组织、制度、流程进行规范化管理，依据国家和行业监管要求开展网络安全管理工作。安全技术体系、安全和安全运维服务体系需要依赖安全管理体系才能发挥有效作用。进一步完善安全管理组织架构和责任落实机制 [3]，加强组织建设，以制度和标准为管理手段，抓好安全制度的制定、完善与落实工作，打造合理有效的组织保障体系。在管理制度和运营操作流程方面，遵循安全合规建设要求，结合数字化业务发展，优化现有安全管理制度、流程和规范，形成顶层安全工作方针和策略、制度规范、操作流程和工作记录表单的体系化、可执行的安全制度体系。企业可围绕安全策略、安全管理制度、操作流程和记录表单四层架构，与企业 IT 流程进行调整与适配，构成全面的安全运营管理制度体系。

企业安全制度和流程与人、技术工具在安全运营工作中相辅相成，适配企业信息化战略与业务发展的管理制度与流程才能发挥其最大的效能。

4.2 加强安全运营团队建设

在安全运营过程中，人是最核心的要素，要明确安全运营团队的组织架构。在企业安全运营团队中，根据安全运营维度的不同分为红队和蓝队，对于安全运营能力较为成熟的企业根据业务的特点，对其进行更精细的划分。红队（国内有公司也称为蓝队）主要工作职责是通过渗透测试、对手仿真到 APT 攻击模拟等进阶式的攻击方式，例如通过近源攻击、供应链攻击、钓鱼邮件、水坑攻击、多源低频攻击甚至是物理攻击的方式对企业安全防护效能进行度量评估，同时能够发现安全防护体系当中存在的缺陷和短板，并配合蓝队完成安全能力体系的完善与优化。在蓝队方面，根据工作内容的不同可分为通报预警组、分析研判组、应急响应组和溯源分析组，围绕攻击事件或行为开展从威胁监测和识别到日志告警、恶意代码和情报分析以及应急处置工作。

网络安全与业务深度耦合，安全运营工作是企业业务发展的重要基础。因此，持续有效的安全运营工作离不开企业各业务部门与安全运营团队的协同与配合。

4.3 强化安全技术能力体系

当前，企业安全防护理念逐渐从被动防御向主动检测防御、自动化响应转变，在网络安全能力设计方面，企业要从实际业务和风险对安全需求的角度出发，企业在建设身份与访问控制、入侵检测与防护、安全审计、防病毒、漏洞扫描等传统安全能力的基础上，需要进一步提升自适应安全能力，主要从以下几个方面进行考虑：

- 动态可信访问控制能力

基于 SDP 最佳实践，通过建立统一化的可信安全访问架构，借助反向代理的方式将业务和 API 隐藏，利用多种强认证、MFA 等技术实现先进行身份认证再完成连接，基于用户身份、设备状态、上下文的动态自适应授权，同时结合细粒度的访问控制策略，精准过滤非法的访问，有效实现精准化的应用访问控制、安全链路和边界隐藏，收缩企业业务资产暴露面，确保企业用户安全可控地访问业务系统。

- 威胁情报能力

对于企业安全运营团队来说，其核心工作就是与黑客或攻击组织进行攻防博弈以保障企业业务连续性。通过构建威胁情报能力体系，安全运营团队可提前了解当前热门事件、漏洞、IOC 甚至是 APT 攻击组织 TTP 的高级情报信息，可以提前做好安全防护防范措施，有效降低潜在安全风险。另外，威胁情报在风险资产感知、互联网敏感信息发现和企业资产测绘等方面也同样发挥着重要作用，已经成为安全运营能力建设中必不可少的组成部分。

- 网络资产测绘能力

资产信息是威胁情报的重要组成部分，利用测绘技术可以对企业信息系统和网络环境各类资产进行精确的识别和标注，对内可以梳理所属资产，监测其动态变化；对外可以主动识别和监测恶意资产的动态，发现已失陷资产的特征并进行通报预警。通过结合资产指纹、地理、情报等知识进行分析，识别和标记资产数据 [4]，形成企业资产库数据。基于资产的地理、位置构建网络拓扑，经过对资产指纹、网络攻击和漏洞等脆弱性数据的关联分析，形成对企业互联网资产暴露面的分析展示。资产信息恰恰具有联结各种防御技术的核心技术属性。通过资产信息可以实现多种防御技术的协同。

- 威胁狩猎能力

威胁狩猎是一种主动识别网络攻击行为和入侵痕迹的技术和方法，由安全运营人员利用威胁诱捕 / 数据分析工具、威胁情报信息和攻防经验对攻击数据进行筛选、鉴别和分析网络侧与终端侧数据，寻找可疑的异常网络入侵行为和异常或非法流量等正在产生的攻击痕迹，并举证攻击或威胁的假设与存在。在威

胁狩猎过程中，依然是以人为核心，其次是多维度的数据分析和自动化研判处置。

- 端点检测与响应能力

EDR 技术可实时检测未知威胁并快速响应，对主机系统内部的动态行为进行检测、分析和关联。通过碎片化痕迹与行为的关联，为精准威胁事件过程溯源分析取证提供重要支撑。绿盟科技通过自主研发的智能行为追踪检测技术，不依赖病毒特征库即能识别检测出各类活跃的恶意程序、针对主机系统的恶意攻击以及对主机系统的恶意破坏等。

- 全流量检测能力

对网络数据包进行全流量存储和实时智能化分析，基于多模匹配协议识别、解析模板智能提取和流识别等关键技术对流量数据进行高效、完整、准确的协议类型识别与解析，建立全面的协议、日志、数据包全字段索引，提取多维度的网络元数据并进行异常行为建模，以快速识别和检测企业 IT 网络中的异常流量与安全威胁。通过回溯分析数据包特征、异常网络行为，结合威胁情报和未知威胁分析等能力发现潜在的高级未知威胁。

- 用户实体与行为分析能力

基于多维用户行为数据，融合运用大数据分析、行为基线检测和机器学习等技术，对异常用户和终端侧行为进行建模分析，结合异常行为检测规则和机器学习模型，对用户行为进行深度分析和异常检测，快速识别感知出内部用户的可疑或非法行为。UEBA 技术聚焦对异常用户和用户异常行为的分析与判定，侧重于在攻防对抗场景对企业内部威胁的分析场景更具优势，更关心用户行为的研判，从其他视角去发现威胁或攻击行为。

- 安全编排自动化与响应能力

依托 SOAR 的策略剧本编排、智能决策与自动化响应能力，充分融合人的安全技能、安全数据、安全运营流程和安全运营工具，有效提升安全运营工作的效能和成熟度。安全编排通过剧本的方式进行表述，通过工作流引擎支撑剧本的执行过程。以剧本方式固化分析场景、研判策略和响应手段，形成从安全分析、研判到响应的自动化编排能力库。基于安全事件或者确定的安全威胁事件，自动触发剧本的执行完成从安全分析、安全研判到安全响应的自动化闭环流程 [5]。

4.4 不断优化安全运维体系

企业安全运维是安全运营工作落地的有力支撑，要与企业赋能建设同步思考，以“业务发展”为核心，以“风险管理”为指引，以“数据治理”为抓手 [6]，将企业网络安全建设过程与业务系统匹配。借助威胁情报、大数据、人工智能、威胁建模等技术沉淀安全能力，打造以人为本、持续优化的安全运维体系在安全运维体系中。主要包括资产管理、脆弱性管理、威胁管理、设备管理、

渗透测试、应急处置、攻防演练和安全意识培养等内容。安全运营团队可参考 PDCERF 模型制定企业的应急响应流程，并形成行之有效的安全事件应急预案。通过流程化、规范化的本地化或云端安全服务交付方式，为企业打造云地协同、精准化安全服务范式。企业需要通过对安全运营指标的建立和完善，来度量安全运营人员的服务能力和效率，如单位周期内的资产识别率、漏洞处置率、威胁发现率、应急事件处置率等内容，为可持续的安全运营服务能力提升和优化提供保障。

网络安全运营工作主要将多种安全能力服务化 [7]，制订安全运营能力提升计划，定期对安全运营能力进行评估并找出差距，持续完善提升计划，驱动企业安全运营体系逐渐成熟。

5. 总结与展望

在数字化转型与业务治理数字化的浪潮下，企业网络安全建设正在从合规驱动向业务和风险驱动转变。安全运营是为了实现组织的安全目标 [8]，提出安全解决构想、验证效果、分析问题、诊断问题、协调资源、解决问题并持续迭代优化的统筹管理过程，满足组织信息安全的动态性、持续性和整体性需求。通过打造持续性安全运营能力，可以更好地指导和管理企业网络安全工作，着力提升企业风险管控能力以保障业务连续性，为企业信息化发展提供重要支撑，有效助力现代化企业长远发展。

参考文献：

[1] 阎彩应 . 新形势下省级电子政务外网网络安全运营体系建设思路 [J]. 保密科学技术 ,2019.

[2] 王晟 , 赵建福 , 李超峰 , 张怡晨 , 赵帅 . 持续化网络安全运营体系研究 [J]. 电信工程技术与标准化 ,2020(12).

[3] 于江 . 网络安全运营在企业安全保障中应用研究 [J]. 网络安全技术与应用 ,2021(6).

[4] 赵粤征 , 叶建伟 , 员珊 , 郭兰杰 . 基于 SOAR 的安全运营自动化关键技术构建及未来演进方向 [J]. 信息技术与网络安全 ,2021,40(3).

[5] 邓晓晖 , 李伟辰 , 曹文杰 . 基于测绘技术的网络资产安全管理研究 [J]. 保密科学技术 ,2021(3).

[6] 刘吉林 . 构建数字经济下的持续安全运营服务能力 [J]. 网事焦点 ,2020(10).

[7] 李伯恺 . 电力企业网络安全综合防护体系构建探析 [J]. 长江信息通信 ,2021(12).

[8] 李昀磊 . 智慧安全 3.0 下的网络安全运营能力成熟度模型 [J]. 绿盟博客 ,2021(6).

云原生服务风险测绘分析（四）：Prometheus

绿盟科技 创新中心&星云实验室 浦明

1. 概述

Prometheus 是一套开源的监控、告警、时间序列数据库的组合工具。与 Kubernetes 由 Google 内部 Borg 系统演变而来相似，Prometheus 由 Google 内部的 Borgmon[6] 监控系统演变而来，最初在 2012 年由前 Google 工程师 Matt T. Proud 于 SoundCloud[5] 进行研发使用并在短时间内迅速得到业界广泛认可，后于 2015 年初在 GitHub 上开源，目前已有 42.2K 的 Star 数和 7.1 的 Fork 数。其用户社区非常活跃，拥有超过将近 700 位贡献者，并在多数云原生组件中被集成。

2016 年 5 月，Prometheus 成为继 Kubernetes 之后第二个正式加入 CNCF 的项目，同年 6 月发布 1.0 版本，并于 2018 年 8 月顺利毕业。Prometheus 现已被众多的企业、互联网公司和初创公司在其微服务业务环境下使用。

本篇为云原生服务测绘系列的第四篇，主要从资产发现、资产漏洞、资产脆弱性发现三个维度分析了 Prometheus 所存在的风险，最后笔者针对 Prometheus 提供了一些安全建议，希望各位读者通过阅读此文可对 Prometheus 服务风险暴露有更清晰的认识。

2.Prometheus 资产风险测绘分析

2.1 Prometheus 资产暴露情况分析

借助测绘数据，我们可以了解到国内 Prometheus 资产地区和版本的分布情况，笔者也以这两个维度为各位读者进行介绍。

2.1.1 Prometheus资产地区分布

笔者从测绘数据中得到 Prometheus 相关资产共 5908 条数据，地区分布如图 1 所示（资产数较少的由于篇幅原因不在图中显示）。

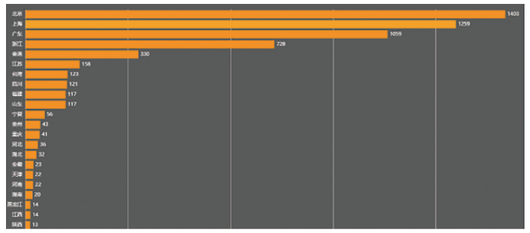


图 1 Prometheus 资产地区分布

笔者针对以上 Prometheus 资产暴露的端口情况进行了统计，如图 2 所示。

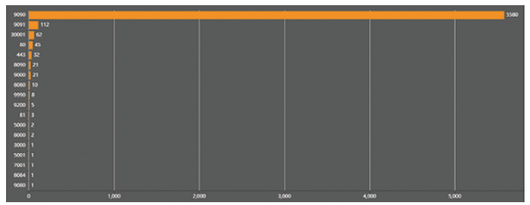


图 2 Prometheus 资产端口分布

由图 1、图 2 我们可以得出如下信息：

国内暴露的 Prometheus 资产信息中有约 81% 的数据来源于北京市、上海市、广东省、浙江省、香港特别行政区、江苏省，其中北京市暴露 1403 条数据，位居第一。

国内暴露的 Prometheus 资产使用的端口主要分布在 9090 端口，9090 为 Prometheus Dashboard 提供 HTTP 服务的默认端口，使用 9090 端口的资产数约占整体资产数的 94%。

2.1.2 Prometheus资产版本分布

借助测绘数据，笔者对国内暴露的 Prometheus 资产版本进行了分析，其分布情况如图 3 所示（资产版本数较少的由于篇幅原因不在图中显示）。

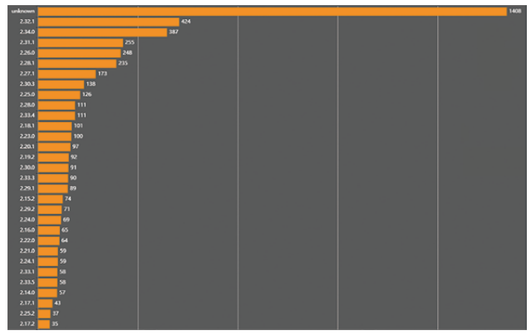


图 3 Prometheus 资产版本分布

上图可以看出在统计的 Prometheus 资产中，24% 的资产未获取到具体版本信息，剩余约 76% 的资产中，绝大多数资产暴露版本分布在 2.32.1、2.34.0、2.31.1、2.26.0、2.28.1、2.27.1、2.30.3 之中。

2.2 Prometheus 脆弱性风险和漏洞介绍

2.2.1 脆弱性风险介绍

Prometheus 的 2.24.0 版本（2021.1.6 发布，当前版本为 2.35.0）发布之前，也许是官方不认为通过 Prometheus 捕获的数据是敏感数据，故在 Prometheus 中未内置认证授权等安全机制，同时也意味着只要用户对外暴露 Prometheus 的 9090 端口，那么任何人都可以对 Prometheus Dashboard 进行未授权访问。虽然 Prometheus 在 2.24.0 版本后针对 Dashboard 引入了 TLS 及 Basic 认证方式，但由于引入时间较晚，许多企业及组织已在云上部署了 Prometheus，且未及时启用官方提供的认证机制，从而导致大量 Prometheus 服务暴露在互联网，导致可能存在敏感数据泄露的风险，笔者也将一些敏感的数据接口进行了梳理，如下所示：

- /api/v1/status/config

访问该接口将返回 Prometheus 服务相关的配置文件内容，文件格式为 yaml，该文件内容包括 Alertmanager 组件（Prometheus 告警组件）相关的配置、告警匹配规则、Prometheus 任务配置、Prometheus 监控的目标节点信息等，完整的内容可参考官方文档 [4]，示例配置文件如图 4 所示。

图 4 Prometheus 数据泄露接口返回内容 1

- /api/v1/targets

访问该接口将返回 Prometheus 目标服务的当前状态，包括活动状态（activeTargets）、下线状态（DroppedTargets）等，示例如图 5 所示。

图 5 Prometheus 数据泄露接口返回内容 2

我们还可以通过“/targets”接口看到目标服务状态的可视化 UI，如图 6 所示。

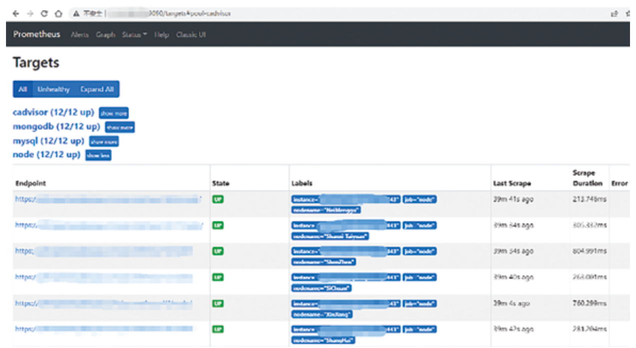


图 6 Prometheus 数据泄露接口返回内容 3

- /api/v1/status/flags

访问该接口将返回 Prometheus 配置的 flag 值，如图 7 所示。

图 7 Prometheus 数据泄露接口返回内容 4

其中,config.file 参数提供用于存放 Prometheus 配置文件(该配置文件与 /api/v1/status/config 接口返回的配置文件信息一致）的完整目录。 此外，该接口返回的内容中还包含 web.enable-admin-api 参数，该参数代表用户是否可以使用其它 Web Admin API 的权限，默认值为 false，如下所示：

图 8 Prometheus 数据泄露接口返回内容 5

根据官方文档 [3]，若用户将 web.enable-admin-api 项参数值设为 true, 则将额外开启一些管理 API 供操作者调用，这些管理 API 允许用户删除 Prometheus 所有已保存的监控指标以及关闭相应的监控功能。

- /api/v1/status/buildinfo

访问该接口将返回 Prometheus 服务的构建信息，其中包括 Prometheus 版本、Go 版本、构建日期等敏感信息，如图 9 所示。

图 9 Prometheus 数据泄露接口返回内容 6

2.2.2 漏洞介绍

CVE编号	漏洞类型	描述	影响版本	漏洞风险级别	CVSS2.x评分	是否存在POC	是否存在EXP
CVE-2021-29622	开放式重定向	在2.23.0-2.27.0版本中，Prometheus将其旧版UI界面更换为新UI界面。为确保界面调整可以无缝过渡，Prometheus将以"/new"为前缀的URL重定向到/，但由于代码逻辑存在缺陷，可导致攻击者制作一个URL 该URL可重定向到以/new为前缀的任意地址。例如，用户访问 http://127.0.0.1:9090/new/newhttp://www.google.com/，访问将被重定向到 http://google.com。	v2.23.0-2.26.1 2.27.0, 2.27.0-rc0	中危	5.8	是，POC链接[1]	是,POC链接 [1]
CVE-2019-3826	XSS	在2.7.1及之前版本中，Prometheus存在存储型XSS漏洞。攻击者可利用此缺陷诱导用户访问其精心制作的URL，并执行恶意脚本。	<2.7.1	中危	4.3	否	否

图 10 Prometheus 漏洞介绍

Prometheus 于 2013 年开源至今，已有约九年时间，在此期间一共曝出两个漏洞 [2], 漏洞数量相对较少，从 CVE 编号信息我们可以看出漏洞披露时间分别在 2019 年和 2021 年，根据 CVSS2.0 标准，两个漏洞均为中危漏洞。CVE-2021-29622 漏洞类型为开放式重定向、CVE-2019-3826 为 XSS，其中 CVE-2021-29662 漏洞在市面上曝光度较大，笔者也针对这两个漏洞进行了信息汇总，其中包括公开暴露的 PoC 及 ExP 信息，如图 10 所示。

2.3 Prometheus 资产脆弱性暴露情况分析

借助测绘数据，笔者从 Prometheus 漏洞维度，统计了现有暴露资产的漏洞分布情况，如图 11 所示。

图 11 Prometheus 漏洞介绍

可以看出，在国内互联网暴露的 Prometheus 资产中，有 713 个资产被曝出含有 CVE-2021-29622 漏洞 (XSS)，通过上图我们也可以看出命中 CVE-2021-29622 漏洞的资产数约占总资产数的 12%，该漏洞是个重定向漏洞，虽然对业务自身运行无影响，但重定向漏洞可用来做钓鱼攻击，仍存在一定危害。CVE-2019-3826 漏洞在互联网上并未发现有相似暴露信息，通过前面的 Prometheus 漏洞介绍，我们可以进一步了解这两个漏洞，篇幅原因此处不再赘述。

2.4 安全建议

升级 Prometheus 版本为最新版本。

Prometheus Dashboard 使用认证机制，如 Prometheus 提供的 Basic 认证，使用 TLS 保证数据传输安全。

禁止将用户名密码等敏感信息以明文形式写入 Prometheus 的配置文件中。

3. 总结

Prometheus 是 CNCF 第二个毕业的项目，也是除了 Kubernetes 之外被开发者普遍认为最火爆的项目，在其被大规模部署的同时，由于脆弱性配置及漏洞导致的风险也不容忽视，本文从测绘角度分析了国内暴露的 Prometheus 服务及其存在的风险，下一篇笔者将继续针对云原生环境下的其他组件进行相应的测绘风险分析，欢迎各位读者持续关注，若有任何问题欢迎提出，互相交流学习。

参考文献

[1] https://security.archlinux.org/CVE-2021-29622.

[2] https://www.cvedetails.com/vulnerability-list/vendor_id-20905/product_id-61503/Prometheus-Prometheus.html .

[3] https://prometheus.io/docs/prometheus/latest/querying/api/#tsdb-admin-apis .

[4] https://soundcloud.com/ .

[5] https://sre.google/sre-book/practical-alerting/.

电信领域重要数据和核心数据识别报备机制解读

绿盟科技 咨询设计部 曾令平

1. 背景介绍

《数据安全法》第二十一条明确规定了“对重要数据进行重点保护，对核心数据实行更加严格的管理制度”。《网络数据安全管理条例（征求意见稿）》第二十七条进一步规定了“各地区、各部门按照国家有关要求和标准，组织本地区、本部门以及相关行业、领域的数据处理者识别重要数据和核心数据，组织制定本地区、本部门以及相关行业、领域重要数据和核心数据目录，并报国家网信部门”；以及第二十九条提出了“重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案”。

在国家标准层面，《信息安全技术 数据出境安全评估指南（征求意见稿）》于 2017 年以附录的形式给出了“重要数据识别指南”。全国信安标委在 2019 年设立“重要数据识别指南”标准研究项目。经过几年的研究，2021 年 9 月 23 日，发布了《信息安全技术 重要数据识别指南》征求意见稿。而随着法律法规及环境的不断变化，《信息安全技术 重要数据识别指南》不断调整，并改名为：《信息安全技术 重要数据识别规则》，做出了“重要数据”的定义修改等四方面重大改动。

在行业应用方面，2021 年 5 月 17 日电信行业已率先出台了《YD/T 3867-2021 基础电信企业重要数据识别指南》，并于 2021 年 7 月 1 日正式实施。主要针对基础电信企业的重要数据保护工作现状需求，提出了基础电信企业重要数据的概念、识别方法和安全保护指导原则并给出了基础电信企业重要数据示例。

2. 指南解读

2022 年 4 月，《2022 年省级基础电信企业网络与信息安全工作考核要点与评分标准》中明确提出重要数据安全管理要求。第一条便是重要数据识别备案，即按照《电信领域重要数据和核心数据识别指南（试行）》要求，梳理识别本企业重要数据和核心数据，于 2022 年 8 月底前将《电信领域重要数据和核心数据备案登记表》报送至属地通信管理局。

2022 年 4 月 27 日，工业和信息化部网络安全管理局发布了《工业和信息化部网络安全管理局关于组织开展电信领域重要数据和核心数据识别规则机制测试验证工作的通知》（工网安函〔2022〕328 号），提出了重要数据和核心数据识别、备案等工作要求，同时，也通过给出附件 1：《电信领域重要数据和核心数据识别指南（试行）》（以下简称《指南》）帮助企业梳理数据资源情况，有效识别重要数据和核心数据，形成本企业电信领域重要数据和核心数据目录。本文将从内容框架、术语与定义、主要内容、关注重点等方面对《指南》进行解读。

2.1 内容框架

《指南》共分为三个章节，分别对重要数据和核心数据识别原则、规则等内容进行规定，如图 1 所示。

图 1《指南》总体内容框架

- 第一章 总则：明确了目的依据、适用范围、相关定义以及总体原则等内容。其中，适用范围明确提出了涉及军事、政务、国家秘密信息、密码使用等数据处理活动，按照国家有关规定执行，不适用本指南；以及涉及其他领域数据时，则遵照其主管部门明确的重要数据和核心数据管理要求进行识别工作。
- 第二章 重要数据识别规则：将电信领域重要数据分为四类，并对每一大类、二级子类明确了识别规则，同时也描述了重要网络设施和信息系统的特征。
- 第三章 核心数据识别规则：将电信领域核心数据分为四类，并对每一大类、二级子类明确了识别规则，同时也描述了核心网络和信息系统的特征。

2.2 术语与定义

《指南》主要沿用了法律法规及国家标准中的定义，并基于行业特征进行了部分调整，主要涉及如下术语定义。如图 2 所示。

术语名称	定义	解读
电信数据	是在电信业务经营活动中产生和收集的数据。	从《数据安全法》对“数据”的定义来看，数据包括了电子和非电子两种形式，但电信行标（对“数据资产”的定义）以及具体实践过程中，更多的关注电子（电信）数据。
重要数据	电信领域重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的电信数据。仅影响电信数据处理者自身的电信数据，一般不作为重要数据。	电信领域属于重要数据国标定义中的特定领域，而电信行标明确提出了不涉及国家秘密，本定义明确了影响对象仅限于国家安全和公共利益。
核心数据	电信领域核心数据是指关系国家安全、国民经济命脉、重要民生、重大公共利益的电信数据。	基于《数据安全法》中的定义，并在重要数据的基础上增加了对影响对象的“重大”、“重要”等用词描述。
电信数据处理者	是指取得电信业务经营许可证，自在电信数据处理活动中自主决定处理目的、处理方式的电信业务经营者，包括基础电信业务经营者和互联网数据中心、互联网接入服务、在线数据处理与交易处理、互联网信息服务等增值电信业务经营者。	中国信通院发布《国内增值电信业务许可情况报告（2022.8）》，报告显示，截至2022年8月底，全国增值电信业务经营许可企业共134177家。如四大基础运营商：中国电信、中国移动、中国联通、中国广电。
电信主管部门	是指工业和信息化部，以及各省、自治区、直辖市通信管理局。	/

图 2 术语定义及对应解读

2.3 主要内容

2.3.1 总体原则

《指南》第四条提出了总体原则，即电信领域重要数据和核心数据识别工作应统筹发展和安全，遵循科学性、实用性、时效性、扩展性的原则，坚持立足中国实际情况与符合国际通行规则相结合，分类识别和定性定量相结合，企业主体、行业指导和属地管理相结合。而在具体实践过程中，主要通过逐级监管模式执行，如图 3 所示。

图 3 重要数据和核心数据识别逐级监管模式

2.3.2 分类维度

参考《重要数据识别规则（征求意见稿）》中重要数据的识别

因素的描述，重要数据和核心数据在考虑安全影响（如影响对象和影响程度）、关键基础设施、关系国家科技实力、影响国际竞争力或关系出口管制物项等因素的基础上，可以采用面分类法从业务属性、安全属性等多个维度进行分类，对不同维度的数据类别进行标识，每个维度的数据分类也可采用线分类法逐次进行细分。目前主要分为四个大类，每个大类下采取二级或三级子类形式进行细分，如图 4 所示。需特别注意的是，《指南》也为电信主管部门确定的其他电信数据为重要数据或核心数据预留了口子，即可归为其他情况类。

重要数据			核心数据		
一级子类	说明	二级子类	二级子类	说明	一级子类
网络规划运维数据域	能够反映重要网络设施和信息系统规划建设、运维等总体发展情况的数据	网络规划建设数据	网络规划建设数据	能够反映核心网络设施和信息系统规划、建设、运维等总体发展情况的数据	网络规划运维数据域
		网络运行维护数据	网络运行维护数据		
安全保障数据域	能够反映重要网络设施和信息系统安全保障情况以及重大应急通信保障情况的数据	网络与数据安全保障数据	网络与数据安全保障数据	能够反映核心网络设施和信息系统安全保障情况以及特别重大应急通信保障情况的数据	安全保障数据域
		物理安全保障数据	/		
		应急通信保障数据	应急通信保障数据		
经济运行与业务发展数据域	能够反映我国电信领域经济运行总体情况与核心业务发展情况的数据	发展战略与重大决策数据	/	能够直接反映我国电信领域经济运行总体情况与核心业务发展情况的数据	经济运行与业务发展数据域
		关系国家安全和公共利益的非公开统计数据	关系国家安全、国民经济命脉和重大公共利益的非公开统计数据		
关键技术成果数据域	能够反映我国先进信息通信技术与产品发展水平的数据	涉及电信领域出口管制物项相关数据	/	能够直接反映我国国际领先信息通信技术与产品发展水平的数据	关键技术成果数据域
		重大科技成果数据	特别重大科技成果数据		
		国家科技计划活动中产生的先进技术数据	国家科技计划活动中产生的先进技术数据		
其他情况	其他被电信主管部门认定的电信数据		其他被电信主管部门认定的电信数据		其他情况

图 4 电信领域重要数据和核心数据分类维度

另外，以上数据分类维度中关于重要网络设施和信息系统和核心网络和信息系统特征，多体现在影响大且波及深、数字庞大（用户基数、数据量级、市值等）、关基设施、等保三级及以上网络设施和信息系统等方面，此处详细内容不再描述。

2.3.3 识别流程

电信数据处理者结合数据分类规则对电信数据进行识别时，可参照重要数据和核心数据识别流程，如图 5 所示。

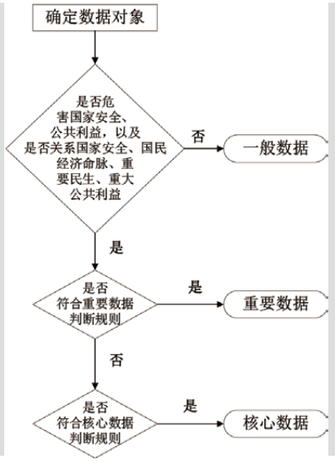


图 5 重要数据和核心数据识别流程

2.3.4 判断规则

经过整理和分析，重要数据判定规则包括但不限于：

直接影响国家主权、政权安全、政治制度、意识形态安全；

直接影响市场秩序或国家经济命脉安全，如电信领域核心业务运行的数据；

关系国家科技实力、影响国际竞争力，或关系出口管制物项；

反映重要网络设施和信息系统总体运行、发展和安全保护情况，可被利用实施对其的网络攻击；

可被利用实施对关键设备、系统组件供应链的破坏，以发起高级持续性威胁等网络攻击。

经过整理和分析，核心数据判定规则包括但不限于：

可被犯罪分子 恐怖分子等利用，对物理目标或以物理手段发动攻击，危害国家安全、国民经济命脉、重要民生、重大公共利益的数据；

直接关系国家特别重大科技实力、特别影响国际竞争力；

反映核心网络和信息系统总体运行、发展和安全保护情况，可被利用实施对其的网络攻击；

其他一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可导致大范围停工停产，核心网络和信息系统大量业务处理能力丧失的数据。

2.4 关注重点

结合以上对《指南》的解读，建议对重要数据和核心数据识别报备工作关注以下四点和对应动作，如图 6 所示。

关注点	对应动作
确认重要网络设施和信息系统和核心网络和信息系统	一是基于已有的特征点，各部门进行确认；二是安全部门等相关部门对其进行审核；三是电信主管部门认定的网络设施和信息系统。
重要数据和核心数据识别	可先基于重要/核心网络设施和信息系统，通过专业的技术工具进行识别梳理，并结合人工的方式进行确认。
哪些部门需要配合	优先考虑信息安全中心、IT信息中心、网络中心、战略规划部、应急通信保障等建议优先参与进来。
如何做好备案登记	首先，是梳理好重要数据和核心数据的基本情况；其次，是理清楚数据处理情况；最后，是需要对接已开展的等保测评、风险评估等工作成果。

图 6 关注重点及对应动作

3. 实践方案

3.1 解决方案

按照数据分类分级保护机制，重要数据和核心数据识别工作可看作整个数据分类分级工作比较特别的，它们有专门的识别规则，且不易通过常见的工具或产品等进行简单识别，目前一般做法多以人工为主 +工具为辅的方式形成解决方案，具体可拆为策略预设定、数据梳理与调研、重要数据和核心数据梳理、重要数据和核心数据清单（或目录）四个主要阶段，如图 7 所示。

图 7 重要数据和核心数据识别解决方案

3.2 操作流程

在以上解决方案的基础上，进一步对重要数据和核心数据识别操作流程进行设计，主要分为了六个操作步骤，如图 8 所示。

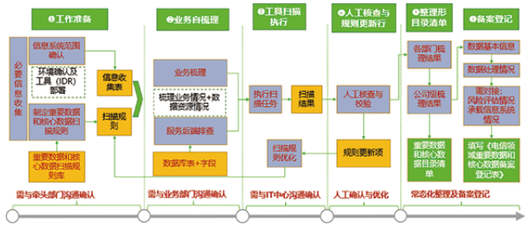
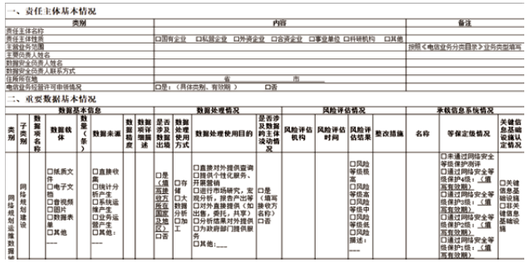


图 8 重要数据和核心数据识别操作流程

第一步，工作准备。需与牵头部门进行沟通确认，并通过必要信息表收集相关信息，包括客户的期望、信息系统大概范围、工具所需环境确认等，并基于《指南》中相关规则，制定重要数据和核心数据扫描规则。

第二步，业务（自）梳理。各部门基于业务情况，对涉及重要数据和核心数据进行自梳理，牵头部门给予梳理指导，可委托第三方机构进行梳理。



一、责任主体基本情况

类别	内容	备注
责任主体名称		
责任主体性质	□国有企业 □私营企业 □外资企业 □合资企业 □事业单位 □科研机构 □其他	
主管业务范围		按照《电信业务分类目录》业务类型填写
主管负责人姓名		
数据安全负责人姓名		
数据安全负责人联系方式		
注册位置	省 市	
电信业务经营许可申领情况	□暂；（具体类别、有效期） □否	

二、重要数据基本情况

数据基本信息							数据处理情况		风险评估情况				承载信息系统情况		
类别	子类别	数据来源名称	数据载体	数量（条）	数据来源	数据敏感度	数据领域描述	是否涉及数据出境	数据处理使用方式	数据处理使用目的	是否涉及数据跨主体流动情况	风险评估机构	风险评估时间	风险评估结果	整改措施	名称	等保定级情况	关键信息基础设施认定情况
同电信领域重要数据目录清单对应			□纸质文件 □电子文档 □音视频 □图片 □数据库集 □其他 ____		□直接收集 □统计分析产生 □系统运维产生 □业务运营产生 □其他： ____	□是（高度敏感/一般敏感） □否	□是 □否	□直接对外提供查询 □提供个性化服务，开展营销 □进行市场研究，发现分析，报告产出等 □对外直接提供（如出售、委托、共享） □为价值累计对外提供服务 □为政府部门提供报告 □其他：____	□大数据分析 □人工智能 □其他 ____	□是（填写具体内容） □否						□风险等级高 □风险等级较高 □风险等级中 □风险等级低 □风险描述： ____		□不通过网络安全等级保护测评 □通过网络安全等级保护4级（上报完整效期） □通过网络安全等级保护3级（上报完整效期） □通过网络安全等级保护2级（上报完整效期） □通过网络安全等级保护1级（上报完整效期）	□关键信息基础设施 □相关信息基础设施 □其他

图 9《电信领域重要数据和核心数据备案登记表》

第三步，工具扫描执行。与 IT 中心或涉及系统运维部门进行沟通确认，部署数据扫描工具，并对扫描策略进行确认，通过新建扫描任务对电子数据（数据库中数据）执行扫描动作。

第四步，人工核查与规则更新。通过人工对扫描结果进行调整，并对识别规则进行优化，进一步完善数据识别能力。

第五步，整理形成目录清单。各部门将梳理结果上报牵头部门，牵头部门整理形成公司级梳理结果，即输出《重要数据和核心数据目录清单》，本目录清单可与日常《数据分类分级清单》的格式保持一致。

第六步，备案登记。牵头部门对数据基本信息、数据处理情况进行统计分析，并与其他部门对接风险评估情况、承载信息系统情况，填写《电信领域重要数据和核心数据备案登记表》，如图 9 所示。

4. 总结与启示

目前，国家标准《重要数据识别规则（征求意见稿）》仍在进一步调整，但对重要数据的特征描述已逐渐清晰。而电信领域出台的《指南》，正是对重要数据和核心数据识别工作的试点，为标准的适用性和可操作性提供了实践数据，同时也为其他行业探索重要数据和核心数据识别提供了前行依据。总而言之，重要数据的识别已逐渐形成了“拨开云雾见青天”之势，而核心数据总体上仍不太明朗，需进一步探索。

容器逃逸即集群管理员？你的集群真的安全吗？

绿盟科技 创新研究院&星云实验室 李来冰

摘要：本文介绍了在集群中利用危险的 RBAC 配置提权至集群管理员的案例，并总结了同类的技术和方法及对应的防御思路。

1. 简介

在 2022 年的 KubeCon 会议上，来自 Palo Alto Networks 的安全研究员 Yuval Avrahami 和 Shaul Ben Hai 分享了议题 *Trampoline Pods：Node to Admin PrivEsc Built Into Popular K8s Platforms*[1]，介绍了攻击者在容器逃逸之后如何利用节点上“TrampolinePods”的权限来接管集群，其中涉及的技术和思路十分值得学习与思考，本文主要介绍该技术的原理和步骤，扩展了同一类型的方法，希望云安全人员在深入了解攻击技术之后，能够发现并缓解生产环境中存在的类似风险，共同建设云环境安全。

本文涉及的技术仅供教学、研究使用，禁止用于非法用途，所有操作均为本地实验环境进行。

2. 事出有因

该技术的分析来源于针对恶意软件 Siloscape 的分析[2]。2021 年 3 月，研究员第一次发现针对 Windows 容器的恶意软件并将其命名为 Siloscape，在还原其攻击链时（图 1 所示）发现 Siloscape 展示了一种未曾见过的在野攻击思路：在入侵 Kubernetes 集群的一个节点后，它会检查节点上是否有 create Deployments 的权限，如果有则在集群内创建一个 Deployment 后门，如果没有则停止继续攻击。

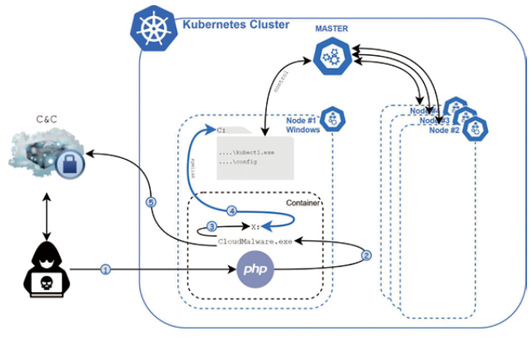


图 1 Siloscape 的攻击链（图片源自针对恶意软件 Siloscape 的分析[2]）

该思路引发人思考：如何配置 Kubernetes 集群节点的权限才能防止此类攻击？如果配置不当又会造成什么风险？带着这两个问题我们继续深入其中。

3. 容器逃逸的真正影响

容器技术在被广泛应用的同时，也带来了对应的安全问题——容器逃逸。我们在《容器逃逸技术概览》中，系统地将容器逃逸的根源划分为 4 个类型：危险配置导致的容器逃逸、危险挂载导致的容器逃逸、相关程序漏洞导致的容器逃逸、内核漏洞导致的容器逃逸，不论通过何种方式从容器逃逸到宿主机，直接的影响

似乎只是控制了容器所在的宿主机。若该宿主机是 Kubernetes 集群的一个普通节点，从渗透测试的角度来看，下一步需要进行的便是横向移动或权限提升。关于 Kubernetes 集群的权限提升，不论是 CVE-2018-1002105 还是 CVE-2020-8559，漏洞的利用都依赖相关组件存在漏洞这个前提，倘若目标集群 Kubernetes 的相关组件都是安全的，如何在集群内进行权限提升呢？笔者通过整理现有的技术并类比针对容器逃逸的类型划分，将 Kubernetes 集群的权限提升手法划分为两个类型：相关程序漏洞导致的权限提升、危险的 RBAC（基于角色的访问控制）配置导致的权限提升。本文主要讨论危险的 RBAC 配置导致的权限提升，为了更加容易理解后文涉及的技术手法，下面将介绍一些相关背景知识。

4. 背景知识

4.1 DaemonSets

当希望 Pod 在集群中的每个节点上运行时，需要创建 DaemonSet 对象，如 Kubernetes 的 kube-proxy 进程，负责节点的网络代理，需要运行在每个节点上。当有节点加入集群时，DaemonSet 会为它们新增一个 Pod，当节点从集群中移除时，这些 Pod 也会被回收。删除 DaemonSet 将会删除它创建的所有 Pod。

4.2 ServiceAccount

Pod 自身在访问 Kubernetes API Server 时，需要使用内置的 ServiceAccount（以下简称 sa）。sa 在创建时，会在同一命名空间下生成一个与之关联的 Secret 资源，Secret 存储认证所需的 token、ca.crt 等内容。默认情况下，Pod 会自动挂载同一命名空间下的名为 default 的 sa，相关文件挂载在 Pod 中容器 /var/run/secrets/kubernetes.io/serviceaccount/ 路径下。

5. 危险的 RBAC 配置

“人类才是系统中最大的漏洞”，不论是传统应用场景，还是如今的云原生场景，权限配置一直是困扰安全人员的最大挑战之一。权限配置不当导致的安全事件比比皆是，因此诞生了各种标准来规范应用程序的权限以防止发生风险。

一般情况下，Kubernetes 集群中节点上主要运行的 Pod 类型有三种，如图 2 所示。

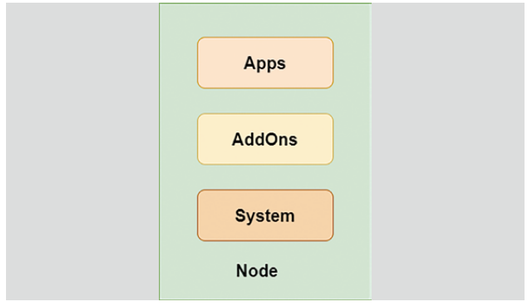


图 2 节点上运行的 Pod 类型

- 业务Pod
- 附加组件（Prometheus，Istio此类）
- 系统组件（Kube-proxy，coredns）

业务 Pod 的权限一般较小，附件组件和系统组件提供集群管理的服务，它的权限也不应等于集群管理员的权限，但在实际场景中，集群管理员可能配置不当，赋予对应角色过高的权限。当攻击者从外部进入容器环境中并逃逸至宿主机时，往往会关注节点上 Pod 的权限，若发现高权限的 sa，则可以凭借它完成集群内的权限提升。现根据利用功能将角色涉及的敏感权限和对应的风险进行整理，如图 3 和附录 A 所示。

操控认证/授权	获取凭证	命令执行	管理Pod	中间人
impersonate	list secrets	create pods/exec	modify nodes	modify endpoints
escalate	create secrets	update pods/ephemeralcontainers	modify nodes/status	modify services/status
bind	create serviceaccounts/token	create nodes/proxy	create pods/eviction	modify pods/status
approve signers	create pods	control pods	delete pods	modify pods
update certificatesigningrequests/approval	control pod controllers	control pod controllers	delete nodes	create services
control mutating webhooks	control validating webhooks	control mutating webhooks	modify pods/status	control mutating webhooks
	control mutating webhooks		modify pods	

图 3 根据利用手段划分权限

注：

操控认证 / 授权：有权修改认证标识或角色权限，如 escalate clusterrole

获取凭证：有权获取或下发凭证，如 list secrets

命令执行：有权在 Pod 或 Node 上执行命令，如 pods/exec

管理 Pod：有权转移 Pod 或更新节点，如 update nodes，delete pods

中间人：有权拦截通信流量，如 create endpointslices

6. 攻击案例

下面将以 CNI 插件 Cilium 为例，介绍攻击者在容器逃逸之后，如何利用高权限的 Pod 从工作节点获取集群管理员权限。

Cilium 的架构主要包含 Cilium Agent（以下简称 Agent）和 Cilium Operator（以下简称 Operator）组件，如图 4 所示。

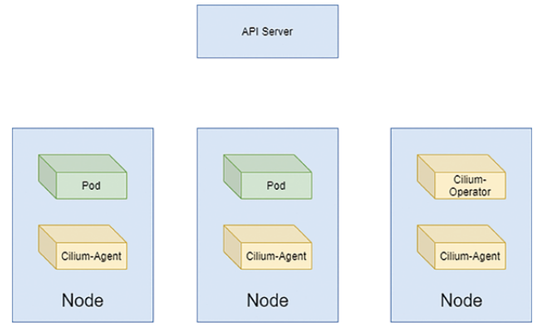


图 4 Kubernetes 集群中的 Cilium

其中 Agent 的功能是接收来自上层的配置，包括通过 Kubernetes 或 API 来定义网络、服务负载均衡、网络策略、可见性和监控需求，它以 DaemonSet 形式部署，在每个节点上运行。在较早版本（v1.12.0-rc2 版本之前）中的 Agent 内置的 sa 拥有集群内的 delete pods 权限和 update nodes/status 权限。

Operator 的功能是管理集群，主要是节点之间资源信息的同步、确保 Pod DNS 更新管理、集群 NetworkPolicy 的管理和更新等，它以 Deployment 形式部署，随机分配在集群中的某个节点上。同样，Operator 在较早版本中内置的 sa 拥有集群内的 list secrets 权限。需要知道的是，在 Kubernetes 集群中，list secrets 权限可以直接获得 secret 的内容，官网文档已经说明 [3]，具体效

果如图 5、图 6、图 7 所示。

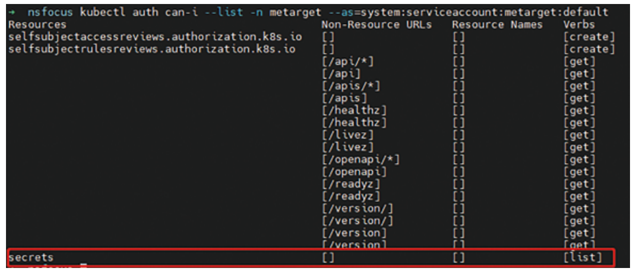


图 5 list secrets 权限示例

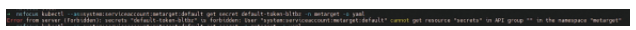


图 6 get secret name 效果

metarget 命名空间下名为 default 的 sa 拥有 list secrets 的权限，直接 get secrets+secretname 读取会提示 forbidden，但是可以改用 get secrets 来获取其内容，如图 7 所示。

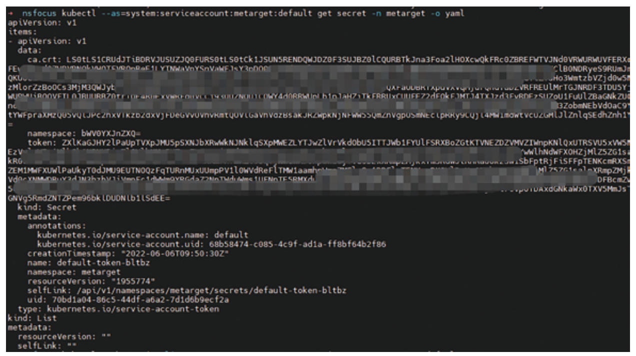


图 7 list 权限获取 secret 值

当获取到 Operator 的 sa 时，可以利用它来读取一些更高权限账户的 secret。但当攻击者通过一系列手段从容器逃逸至宿主机时，该宿主机可能只是集群中的一个普通节点，而 Operator 是以 Deployment 的形式随机部署在某个节点上的，并不一定会在当前节点，如图 8 所示。

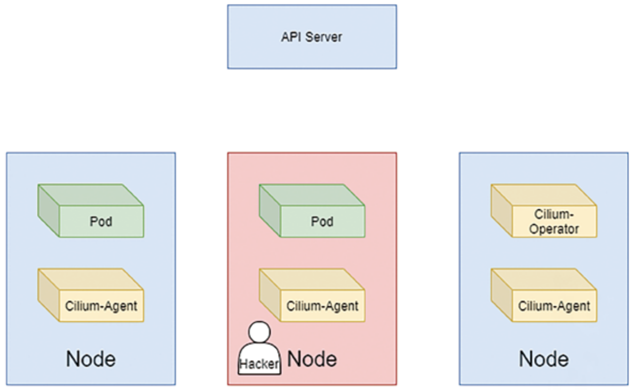


图 8 攻击者入侵至普通节点

因此需要通过一定手段将 Operator 从其他节点转移至当前节点，由此可将攻击大概分为以下三个步骤：

第一步：转移 Operator

如何转移 Operator？需要利用 Agent 的 sa。在节点上可以通过文件系统或进入容器内部获取 Agent 的 sa，先利用 update nodes/status 权限将其他所有节点的 PodCapacity 置为 0，然后利用 delete pods 权限将 Operator 删除。Capacity 代表节点的资源容量，包括 cpu、memory、将 PodCapacity 置为 0，代表节点上 Pod 的容量为 0。当 Operator 被删除时，因为 Deployments 的特性，Kubernetes API Server 会重新创建一个副本，在资源调度时会检查节点上的 Capacity 值，当发现其他所有节点的 Pod-Capacity 值为 0 时，便会将 Operator 部署在攻击者控制的节点上，完成转移。

第二步：窃取凭证

当 Operator 可控时，同样可以通过文件系统或进入容器的方式获取 Operator 的 sa。那么问题来了，当拥有读取 secret 的权限时，需要读取谁的 secret 才能进一步扩大权限，甚至一步到位？经过调查，发现 Kubernetes 集群内有这样一个角色 :clusterrole-aggregation-controller（以下简称 CRAC），它的权限如图 9 所示。

图 9 CRAC 角色权限

值得注意的是其中的“escalate”权限。一般来说，role 或者 clusterrole 角色只能拥有在它们被创建时所赋予的权限。但 escalate 是个例外，它可以升级角色或集群角色的权限。为此我们需要利用 Operator 的 sa 获取 CRAC 的 ca.crt 和 secret 值，通过相关命令可以获取，如图 10 所示。

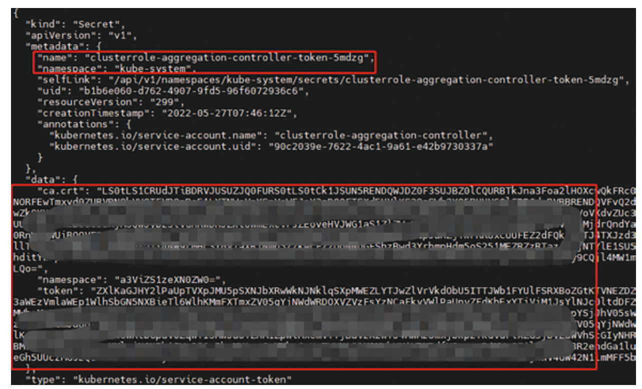


图 10 获取 CRAC 凭证

注：其中 token 为 Operator 的 secret 值。

第三步：权限提升

在经过上述步骤获取到相关凭证之后便可从节点上进行权限提升。使用 kubectl edit 相关命令给 system:controller:clusterrole-aggregation-controller 角色添加权限，效果如图 11、图 12、图 13 所示。

图 11 修改权限前

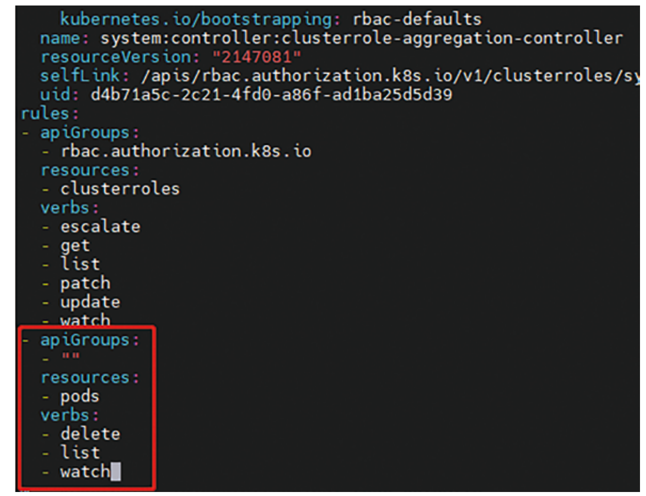


图 12 修改权限

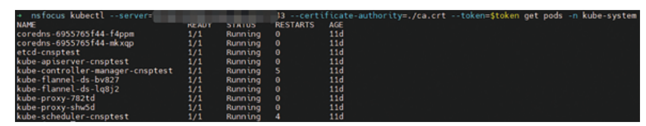


图 13 修改权限后

将权限修改为 cluster-admin，即可提权至集群管理员权限。

7. 方法扩展

回顾上文提到的利用 Cilium 在集群中提升权限的思路，大致路线如图 14 所示。

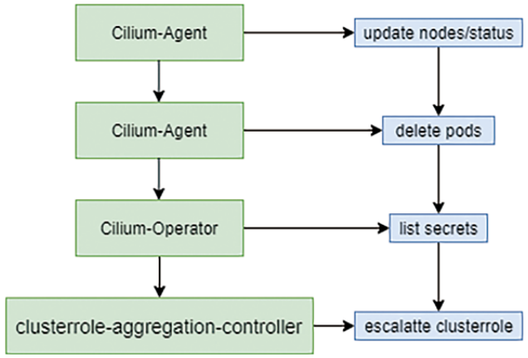


图 14 权限提升路线

观察发现，一旦攻击者获取到 kube-system 命名空下的 list secrets 权限，就可以利用 CRAC 角色提权至集群管理员，该角色的权限是集群默认赋予的，因此在生产环境中需要控制的是 list secrets 权限的赋予。那么除了上述思路外，是否还有其他权限能完成攻击链的构造进行权限提升？经过调研 [4] [5]，还发现下面两种权限提升思路：

利用 Node/Proxy 提权

在 Kubernetes 的机制中，Kubelet 工作在集群中的每个节点上，它负责执行来自 API Server 的请求并返回结果。正常情况下，访问 Kubelet API 是需要凭证的，但当攻击者拥有 get、create node/proxy 权限时，便可以与 Kubelet API 直接通信，绕过 API Server 的访问控制，同时因为 Kubelet API 不会被日志审计，也增大了检测的难度。

攻击者在获取到拥有 get、create node/proxy 权限的 secret 值后，若能访问到 master 节点上的 Kubelet API，便可以直接与其通信，获取到 API Server 的凭证，从而控制整个集群，如图 15 所示。

图 15 和 Kubelet API 通信

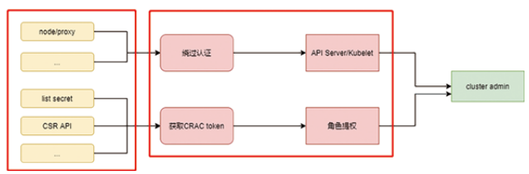
利用 CSR API 提权

CSR 即证书签名请求，Kubernetes 在多处使用客户端证书进行认证，包括用于 Kubelet 和 API Server 之间的通信。当攻击者拥有签名者为 kubernetes.io/kube-apiserver-client 的 create CSRs 权限和 update CSRs/approval 权限时，可以为高权限的系统账户创建一个新的客户端证书，用于和 Kubernetes 进行认证，能够获取到系统账户的权限。

其他更多思路和权限风险可以参考附录 A 中提及的风险项深入挖掘。

8. 思考与总结

通过对比分析不同的权限提升思路，总结了以下两条集群内的提权路线图：



若拥有的权限可以绕过认证，直接和 API Server 或 Kubelet 通信，便可以读取到 kube-apiserver 的凭证，获得集群管理员权限；若拥有的权限可以读取到 CRAC 角色的 token 值，便可以通过修改角色来获得集群管理员权限。

站在防御者的角度，高效的修复方案便是直接针对此类攻击路线进行阻断。在对角色的权限分配时，可以参考图 3 中涉及的权限和文中提及的攻击案例，仔细考虑每项权限的作用范围与危害，在生产环境中遵循权限最小化原则，进行合理分配。节点之间的隔离防护，如给 Kubelet 服务设置防火墙，尽可能控制攻击者的影响面。同时加强 API Server 的日志审计和异常检测，对于异常的 API 请求应及时记录、阻断和警报。

本文介绍了在集群内利用危险的 RBAC 配置进行权限提升的思路，以此说明权限配置不当对容器逃逸后的进一步影响，希望企业的集群管理员与云厂商在管理集群环境中的角色与权限时，能够合理分配，防范权限滥用攻击，共同建设安全的集群环境。

参考文献

[1] https://kccnceu2022.sched.com/event/ytlb/.

[2] https://unit42.paloaltonetworks.com/siloscape/.

[3] https://Kubernetes.io/docs/concepts/security/rbac-good-practices/#listing-secrets.

[4]https://blog.aquasec.com/privilege-escalation-kubernetes-rbac.

[5] https://blog.aquasec.com/kubernetes-rbac-privilige-escalation.

[6] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/kubernetes-privilege-escalation-excessive-permissions-in-popular-platforms.

附录 A

利用功能类型	RBAC权限	可利用点
操控认证/授权	impersonate users/groups/serviceaccounts	模拟身份，如用户、组和sa
	escalate roles/clusterroles	向现有角色或集群角色添加权限
	bind rolebindings/cluster role bindings	将现有角色或集群角色绑定至任意身份
	approve signers & update certificatesigningrequests/approval	让现有的签名者批准证书签名请求
	control mutating webhooks	修改已承认的角色或集群角色
获取凭证	list secrets	获取secret的列表和内容
	create secrets	为现有sa下发新的secret
	create serviceaccounts/token	通过TokenRequests为现有sa下发临时secret
	create pods	将指定sa挂载至新建的Pod中或以环境变量或卷的方式附加至新建的Pod中
	control pod controllers	将指定sa挂载至新建或现存的Pod中或以环境变量或卷的方式附加至新建或现存的Pod中.
	control validating webhooks	在创建sa时获取其secret
	control mutating webhooks	在创建sa时获取其secret或将sa附加至新的Pod中
命令执行	create pods/exec	通过API Server在Pod中执行命令
	update pods/ephemeralcontainers	容器注入至现有Pod中以执行命令
	create nodes/proxy	通过Kubelet在Pod中执行命令
	control pods	修改Pod为特权模式
	control pod controllers	通过pod controllers创建或修改Pod，如设置为特权模式以执行命令
	control mutating webhooks	修改容器的镜像、执行命令、执行参数、环境变量或卷等来执行命令
管理Pod	modify nodes	通过NoExecute驱逐节点上的Pod，使其转移至在指定节点上
	modify nodes/status	修改节点状态，如将其pod capacity设置为0
	create pods/eviction	驱逐Pod，迫使其重新生成
	delete pods	删除Pod，迫使其重新生成
	delete nodes	通过删除节点来删除Pod，迫使其重新生成
	modify pods/status	设置Pod标签以匹配标签选择器，同时设置Pod的生成时间以欺骗控制器删除现有副本，完成替代
	modify pods	设置Pod标签以匹配标签选择器，同时设置Pod的生成时间以欺骗控制器删除现有副本，完成替代
中间人	control endpointslices	修改现有的endpointslices以拦截流量或为现有服务新建endpointslices以拦截流量
	modify endpoints	修改现存服务的endpoints以重定向流量，对endpointslices无效
	modify services/status	附加一个负载均衡IP来利用CVE-2022-8554，进行流量劫持
	modify pods/status	修改Pod的标签以匹配服务的选择器进行流量劫持
	modify pods	修改Pod的标签以匹配服务的选择器进行流量劫持
	create services	创建一个ExternalIP服务来利用CVE-2022-8554，进行流量劫持
	control mutating webhooks	修改新生成的服务、endpoints和endpointslices来进行流量拦截

参考自 Palo Alto Networks 报告 [6]

浅析常见云安全解决方案在客户端的落地场景

绿盟科技 云安全产品部 赵怿政

摘要：本文讨论云计算安全问题及针对性解决方案，包括云安全资源池、安全 SaaS 服务、多云安全管理、云工作负载保护和容器安全解决方案等。文章从客户视角出发，分析了如何选择适合自己的解决方案、实现精准防护和避免重复建设等问题。

关键词：云安全 客户场景 T-ONE CLOUD

1. 云计算环境面临诸多风险

近年来云计算产业发展突飞猛进，技术手段日新月异，承载客户业务的云计算环境也是形态各异。云计算在带来高效、弹性、便捷的同时，新的风险也在增加，但原有的安全问题也并没有消除。随着远程办公的常态化与元宇宙技术的兴起，云上办公、业务上云、多云访问等模式逐步成为更多客户的首要选择，同时客户也逐步将更加重要的业务迁移到云上，使得云上客户的业务、数据、资产变得越来越重要。云上安全问题也成为用户在 IT 建设中首先要考虑的问题。如何让用户放心地使用云，就必须解决云计算本身面临的各种安全问题。无论是 IaaS、PaaS、SaaS 等传统云计算平台，还是云原生、多云等新的场景，都存在众多安全风险。

围绕客户在云计算场景下的安全风险，市场提供了多种类型的针对性解决方案，如云安全资源池方案、安全 SaaS 服务方案、多云安全管理方案、云工作负载保护方案、容器安全解决方案等。客户应用场景越来越复杂，安全解决方案也愈加丰富，那么客户如何在特定场景下选择适自己的解决方案？如何用成熟稳定的方案落地到客户端？如何实现精准防护避免重复建设？都是 IT 从业者需要思考的问题。笔者尝试站在客户视角，浅析业界主流云安全解决方案在不同需求下的落地场景，供大家参考。

2. 云安全解决方案

2.1 虚拟系统方案

2.1.1 方案介绍

虚拟系统（Virtual System）是指将一台物理防火墙划分成多台逻辑设备的技术，将一台防火墙从逻辑上划分为多个虚拟系统，每个虚拟防火墙系统都可以被看成是一台完全独立的防火墙设备，具有自己的接口、地址集、用户 / 组、路由表项以及策略，并可通过虚拟系统管理员进行配置和管理。图 1 展示了虚拟系统的基本原理。

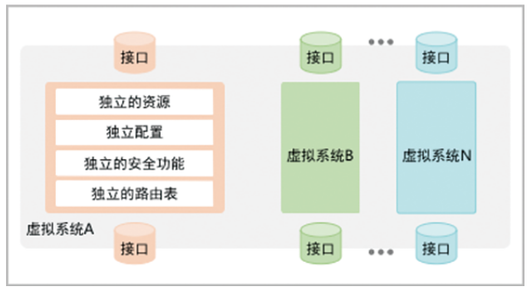


图 1 虚拟系统基本原理 [1]

2.1.2 应用场景

（1）租户安全网关

在集团企业或者政府部门内部，一般存在不同的二级部门，它们具有各自的业务系统，为了方便管理统一部署在中心机房的云环境中。由于各个业务系统之间开放度、隔离性、保密性、重要性不同，需要配置不同的安全策略。通过配置虚拟系统，可让部署在云计算中心出口的硬件防火墙具备云计算网关的能力，对不同租户流量进行隔离的同时提供差异化的安全防护能力。需求场景如图 2 所示。

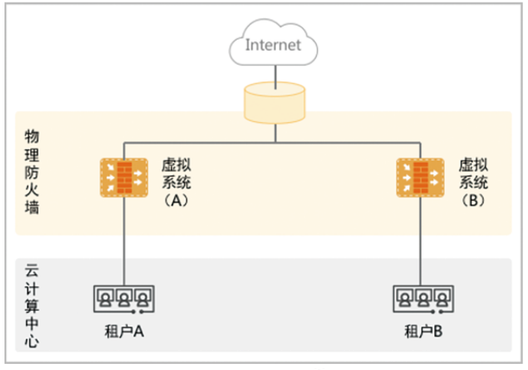


图 2 租户网关场景 [1]

2.1.3 客户价值

集中部署，权限可控：根管理员可配置开启虚拟系统功能，创建虚拟系统后，根系统管理员可以为虚拟系统创建一个或多个管理员。虚拟系统管理员能配置和查看的业务也仅限于该虚拟系统，根管理员可以配置任何一个虚拟系统的业务，方便灵活。

策略独立，快捷调整：虚拟系统管理员可登录权限内的虚拟系统配置适合于自身业务的策略和访问关系，快速完成安全能力的建设。

安全有效，性价比高：一台高性能硬件防火墙至少可以虚拟 32 个及以上的虚拟系统，为租户提供快速、有效、独立、可自定义的安全能力，性价比较高。

2.1.4 优劣分析

优势：

零部署：租户侧无须独立部署安全组件，即可实现边界网关的安全能力。

高性价比：通过一台硬件防火墙即可满足简单的多租户网络隔离、入侵防御、虚拟专用网络、网关杀毒等安全能力，极具性价比。

劣势：

功能单一：底层架构决定传统硬件方案只有防火墙、IPS、VPN 等功能，安全能力类型无法扩展。

性能瓶颈：单台高端硬件设备数据交换性能高，但是在开启安全功能后，尤其是应用层的防护功能开启之后，设备吞吐性能骤降。

平台适配：无法与其他安全组件统一管理，同时无法实现跟云平台的耦合对接，对外开放的端口有限。

2.2 云内 NFV 方案

2.2.1 方案介绍

NFV（Network Function Virtualization），即网络功能虚拟化。这个概念最初是由运营商的联盟提出的，就是通过使用通用的硬

件以及虚拟化技术，将很多硬件设备的安全功能抽离出来通过软件实现[2]。也就是将专用硬件实现的功能虚拟化到一个通用硬件里，如防火墙、入侵检测系统、Web 应用防护系统等，此方案可以灵活快速地进行安全组件虚拟化和安全能力编排，广泛应用于公有云及私有云场景，成为当下主流的云安全解决方案之一。图 3 展示了云内方案的典型部署模式。

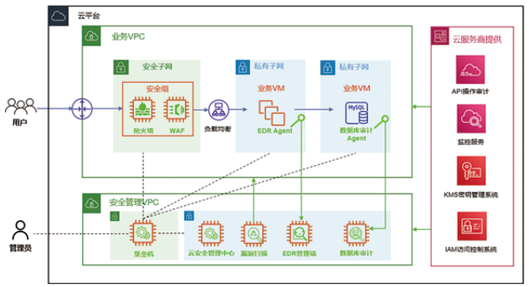


图 3 云内 NFV 部署模式

2.2.2 应用场景

（1）超融合架构场景

在中小型企业、政府、科教文卫等商业客户中，为了业务发展和数字化转型，越来越多的客户采用超融合架构下的私有云来承载自有业务。在这种模式下，客户对于安全建设的灵活性、兼容性、稳定性、经济性都有较高要求。因此，通过将安全能力作为超融合架构中的一个虚拟网元，构建到整体方案中，即可实现安全能力快速部署，同时整体架构的稳定性与可靠性都比较理想。不过，如果是不同供应商的安全能力，需要进行额外的系统测试与安全集成。

（2）公有云安全场景

随着敏态业务在整体业务系统中的比重逐年提升，无论是商业客户还是行业客户，使用公有云承载敏态业务的比例和意愿正在逐年提升，由此也激发了公有云上安全的蓬勃发展。在众多的公有云安全解决方案中，将虚拟化安全网元部署在客户 VPC 内部，同时利用公有云强大的网络编排能力实现业务安全防护方案，无疑是一个不错的选择。多数公有云厂商会为客户提供安全云市场，发布自有产品及合作伙伴安全厂商的安全产品，这些安全网元能够部署于统一管理的虚拟资源之上，并确保功能可用、性能良好、运行情况可监控、故障可定位，即使是不同厂商的安全组件也可实现灵活配置、数据互通、能力混用、集约管理。

2.2.3 客户价值

灵活部署，快捷开通：采用标准的虚拟化资源即可快速部署，无须独立专用的物理硬件，公有云场景可在云市场快速下单开通，方便快捷。

能力独享，自主配置：安全能力相对独立，每个客户可采购自身业务需要的安全能力，安全策略可根据业务需要灵活调配。

2.2.4 优劣分析

优势：

软硬分离：NFV 方案通过软硬件解耦的方式，使得网络设备开放化，软硬件可以独立演进，避免厂家锁定。

高性价比：采用虚拟化安全网元模式部署，在实现同等安全效果的情况下，大幅降低 TCO（Total Cost of Ownership）。

劣势：

厂商适配：多数情况下云和安全服务提供商由多个厂商组成，在部署前期需要从 NFV 各层之间的接口定义与数据类型，到层内功能的实现机制，乃至层间的协同处理均需要厂商之间通力协作，将流程与功能予以完善。

资源占用：NFV 模式会占用客户业务虚拟化资源，需要在建设前期为安全能力的部署预留相当一部分虚拟化资源。

性能衰减：由于 NFV 占用了业务服务器的 CPU 资源来处理安全业务，尤其在 NFV 处理应用层安全业务时会占用大量的计算资源，导致私有云服务器计算性能下降。

2.3 云安全资源池方案

2.3.1 方案介绍

云安全资源池 (Cloud Security Resource Pools)，指的是安全供应商将安全能力 SaaS 化，采用“软件定义安全 SDS”架构，以弹性、按需的“池”的方式提供给用户使用的产品。通过统一管理平台实现安全设备服务化和管理集中化，以及安全能力的订阅使用，满足客户租户安全、网站防护、等保合规等需求，提高云上安全运维效率。

安全资源池通常旁挂在云 IDC 的核心 / 汇聚交换机上，通过 SDN 对接或者利用 Netconf 协议等方式，牵引需要防护的租户的目标虚拟机的网络流量到安全资源池进行防护，流量检测和清洗完成过后，再回注到原有网络路径。在客户的中小规模数据中心场景下，网络架构采用的是 VLAN(虚拟局域网) 技术，不存在 IP 冲突的情况，即可直接通过引流交换机配置路由策略引流；在某些大规模数据中心场景下，网络架构多数采用的是 VXLAN(虚拟可拓展局域网) 技术，而 VXLAN 是一种 Overlay 网络，网络中的流量和传统流量不一样，有可能 IP 地址会出现重叠的情况。因此，这些流量往往通过隧道的方式引入安全资源池，同时安全资源池要能够识别不同的租户标签，才能提供正确的防护。

2.3.2 应用场景

（1）租户安全场景

在一些行业云环境中，如政务云、金融云、交通云、医保云、工业互联网云、能源云、警务云，以及一些大型企业集团内建设的私有云，往往都有租户的概念。云平台为不同的租户划分云资源供其搭建自己的业务系统，由于不同业务部门对于信息系统的风险偏好不同，无法让云平台统一提供所有的安全能力，因此云平台上租户需要具备独立的安全能力体系和可自定义的安全策略，从而满足业务系统自身的安全防护需要。云平台运维管理人员与租户管理员都有独立的操作界面，同时做了明确的责任边界划分，在满足安全灵活性的同时，保障了业务流程的合规性。部署模式如图 4 所示。

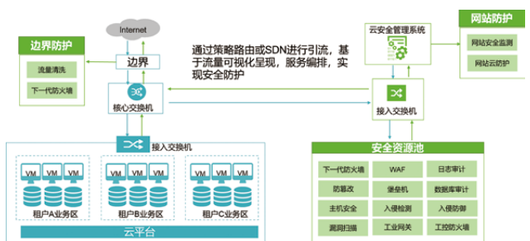


图 4 租户安全场景

（2）安全增值场景

云服务提供商在为商业及行业客户提供计算、存储、应用等云服务的同时，还会考虑逐渐把安全也作为一种增值手段一起提供给云上用户。典型的场景就是省 / 市级的运营商及本地 IDC 服务提供商，在提供 IaaS/PaaS/SaaS 服务的基础上需要加入“安全即服务”相关业务来更好地满足日益增长的云上客户对于安全的需求，同时也可获得更多的收益。部署模式如图 5 所示。

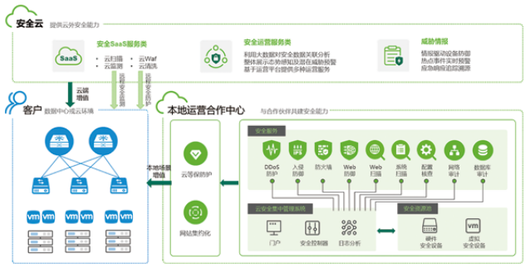


图 5 增值运营场景

（3）多云安全场景

随着企业及政府数字化转型不断深化，IT 架构转向以云为核心，融合大数据、人工智能、区块链等新一代技术的数字基础设施，多云、混合云成为主要形态，在混合云场景下，可以通过一套管理平台实现公有云内安全 + 私有云旁挂安全资源池方案的统一管理。

在公有云云平台上，NFV 安全组件需要完成云计算平台兼容性适配，通用云安全管理系统与云平台进行 API 的对接，即可与云平台紧耦合对接，完成自动部署组件，快速授权，实现 NFV 组件生命周期管理，并支持配置网络 IP、NTP、授权服务器等。部署模式如图 6 所示。

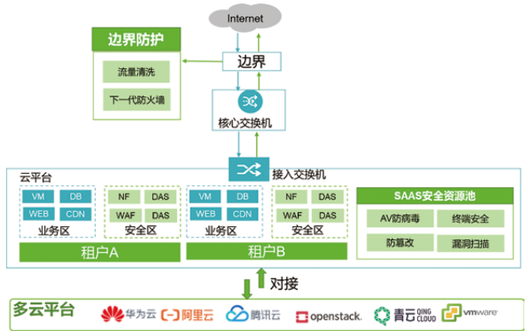


图 6 多云安全场景

2.3.3 客户价值

快速部署，简化管理：通过集中式安全平台管理安全资源池提供的多个安全产品，同一平台管理多种安全能力，简化运维管理工作。

权责分明，风险可控：方案提供独立的云平台侧管理平台和租户侧管理平台，权责划分清晰，同时提供事件报表、日志分析、态势大屏、威胁告警等服务，为风险的预防、发现、遏制、溯源等工作提供可靠保障。

能力丰富，满足合规：云安全资源池可提供数十种有效的安全能力组件，租户可自定义选择不同规格、不同种类的安全能力，实现自己的等保合规、业务防护、网站安全等诉求。

2.3.4 优劣分析

优势：

资源独立：云安全资源池方案一般会独立占用服务器资源，不占用业务资源，在不影响业务性能的同时还可实现资源的平滑扩容。

稳定运行：利用虚拟化特性和网络冗余特性，可实现组件级、主机级、链路级等多种高可用机制，保障业务稳定运行。

快速扩容：租户可通过订单变更的方式快速实现安全规格的扩容。

劣势：

多平台管理：云安全资源池有独立的管理平台，一般情况下是需要跟云计算管理平台解耦合部署，导致客户需要登录不同的管理平台实现云和安全的运维管理。

厂商开放度：由于安全组件厂商较多，安全组件接口开放程度较低，导致部分第三方组件纳入云安全管理平台统一管理存在一些困难。

2.4 云原生安全防护方案

2.4.1 方案介绍

云原生容器安全产品 CNSP(Cloud-Native Security Platform) 定位于云原生安全领域，秉承 DevSecOps 理念，践行安全左移原则，采用微服务架构设计，形态轻量可弹性匹配客户的容器环境，借助容器编排技术将安全容器部署在业务节点中，为容器编排环境、容器及镜像提供持续安全分析，实现容器环境的资源可视化管理并提供镜像安全、基础设施安全、运行时安全、合规安全等能力，保障容器在构建、部署和运行全生命周期的安全。为客户提供全能力、可运营的容器安全赋能体验。图 7 展示了 CNSP 的基本原理。

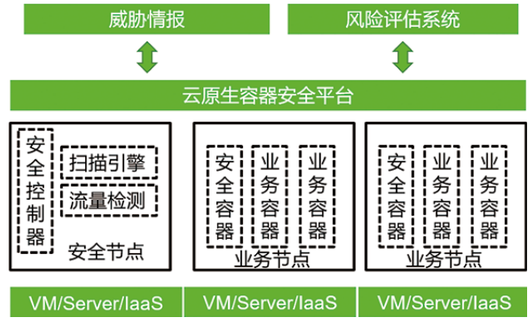


图 7 CNSP 基本原理

2.4.2 应用场景

（1）云原生架构数据中心安全

在金融、能源等行业，客户为了实现业务的敏捷和高效性、IT 架构的轻量化，客户业务系统将逐步从虚拟化环境迁移到容器环境运行并进行微服务架构改造。业务改造初期实现了快速发布、组件解耦、灵活移植、架构轻量化的目的，运行效率得到了很大提升。但是容器化改造是将传统的单体应用拆分为众多的微服务模式，其端口数量的暴涨必然导致攻击面增多。同时容器的隔离性差、镜像风险、逃逸风险等问题逐渐浮出水面。

利用 CNSP 解决方案，安全能力以镜像方式敏捷交付，通过资产清点、基线核查、容器微隔离、API 访问控制、流量威胁检测等能力，可以很好地解决云原生架构下的 Pod/ 容器 / 镜像等维度的安全风险，同时提供持续专业容器安全运营服务，保障客户容器环境安全。部署模式如图 8 所示。

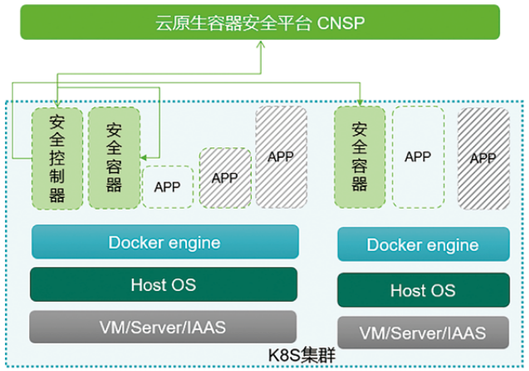


图 8 云原生数据中心安全场景

（2）DevOps 开发过程安全

在金融、运营商行业的客户开发环境中，越来越多的客户开始使用 DevOps 这种开发和运营的新模式，它帮用户缩短了软件生命周期中各个环节的等待时间，减少了诸多重复性、流程性的工作，使得开发、运维过程的成本明显降低。但是由于缺乏对流水线安全性的考虑，容器镜像风险、进程风险、隔离风险、API 风险、漏洞利用风险等问题逐步产生，对业务的开发运营造成了巨大威胁。

采用 CNSP 解决方案，以轻量化插件 / 北向 API 接口方式灵活集成客户流水线环境，及时识别开发风险，将安全融入 DevOps 阶段，提前规避危险镜像进入生产环境，助力构建客户安全开发体系，降低开发阶段引入安全风险。部署模式如图 9 所示。

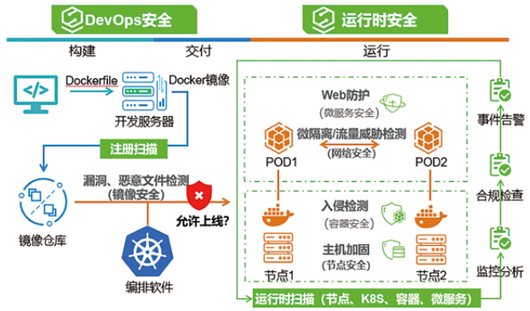


图 9 DevOps 开发过程安全场景

2.4.3 客户价值

非入侵式，敏捷交付：全产品以镜像方式敏捷交付，安全容器（资源占用极低）权限最小化运行并设置资源阈值保障不影响既有业务，利用自动化部署可快速完成上线，通过更新容器镜像快速升级，有效提升容器安全运维效率达 50%。

灵活扩展，随需而变：当业务容器弹性增长时，安全容器可以自动识别并进行安全监测，当扩容业务节点时可自动部署安全容器，只须通过便捷的引导式授权管理即可满足客户业务弹性变化时的安全场景。

CI/CD 环境，全程防护：可以与客户的开发 / 生产流程紧密配合，客户可以在全流程中调用所需安全能力，极大地降低了开发 / 生产过程风险点的引入。

2.4.4 优劣分析

优势：

云地联动：能够联动云端威胁情报中心来进行容器环境恶意文件检测，通过构建恶意文件云地双引擎检测机制，避免本地的威胁检测存在孤岛效应，有效提升恶意文件检出率。

轻量化：产品秉承云原生安全产品轻量化的设计理念，部署在宿主机上安全容器仅做必要的信息采集及监测，性能消耗不超过部署宿主机的 0.1 vCPU，保障不影响业务容器的正常运行。

流量检测：提供容器环境流量入侵检测，覆盖容器环境网络层和应用层的安全检测，联动微隔离为用户环境提供东西向横向威胁闭环管理。

劣势：

功能单一：产品定位决定了仅能提供容器层面的安全能力，对于数据中心整体安全，必须依赖其他产品配合才能完成全面防护。

组件适配：云原生安全防护平台仍旧处于发展初期，对于多平台的适配和多维度的网络插件的兼容还需更加广泛，才能全面满足更广泛客户的需求。

2.5 云工作负载保护方案

2.5.1 方案介绍

云工作负载保护平台 (Cloud Workload Protection Platform，CWPP)，旨在为所有类型的云工作负载（包括物理服务器、虚拟机、容器、无服务等）提供一致性的安全属性。云工作负载保护平台主要采用服务端 agent+ 远程控制台的部署模式，agent 支持物理、虚拟机、容器等混合云环境部署，部署方式更加灵活、防护层面更加丰富，能实现工作负载加固、微隔离、威胁检测、防范恶意代码等能力，同时提供了一体化的管理平台。主要是解决混合云、多云环境下云工作负载的安全问题。图 10 展示了云工作负载保护方案的典型部署模式。

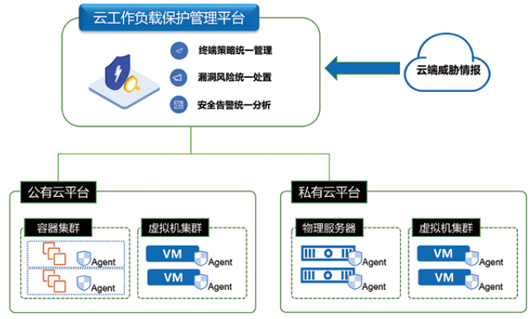


图 10 云工作负载保护方案

2.5.2 应用场景

（1）数据中心 IaaS 安全防护

在金融、能源、政府等行业，新建数据中心一般会具有多种工作负载模式，如物理服务器、虚拟机、容器等，承载稳态、敏态等业务。虽然不同的工作负载模式有不同的特点，但是信息安全管理人员还是希望通过一套管理平台实现业务风险可视化、策略管理一致化、安全能力全面化等特性。此时采用 CWPP 方案可实现系统完整性保护、应用程序控制、行为监控、基于主机的入侵防御和可选的反恶意软件保护等能力，保护数据中心多类型工作负载免受攻击。

2.5.3 客户价值

负载保护，降低难度：针对云原生等新兴的工作负载场景，依旧可以实现良好的安全防护效果，降低了云上工作负载安全防护的难度。

多种环境，策略一致：在多云和混合云场景下，业务频繁迁移带来的安全防护策略不一致是个巨大问题，CWPP 很好地解决了这一难题，实现了不同环境下安全策略保持一致性的效果。

单一插件，多维能力：通过提供一个终端插件，即可实现完整的云工作负载安全防护。

2.5.4 优劣分析

优势：

可移植性：当工作负载经常变换环境的情况下，CWPP 仍然具备相同的安全防护能力。

可视可控：提供对工作负载的威胁可见和策略控制。

劣势：

兼容性差 :CWPP 插件安装在操作系统之上，所以要根据不同的操作系统与环境做独立适配。

功能单一：提供完整的云工作负载安全能力，但是缺少访问管理、风险监控、流量审计等能力。

发展初期：国内 CWPP 仍在发展初期，在对于 Gartner 提出的完整的八个维度的安全能力支持层面，还有待加强，具体支持情况需要根据具体厂商提供的能力为准。

2.6 SASE 解决方案

2.6.1 方案介绍

安全访问服务边缘（Secure Access Service Edge）即安全访问服务边缘。SASE 是一种新兴的服务，它将广域网与网络安全（如 SWG、CASB、FWaaS、ZTNA）结合起来，从而满足数字化企业的动态安全访问需求。SASE 是一种基于实体的身份、实时上下文、企业安全 / 合规策略，以及在整个会话中持续评估风险 / 信任的服务。访问者的身份可与人员、人员组、设备、应用、服务、物联网系统等相关联 [3]，实现 SaaS 化的安全访问服务。图 11 展示了 SASE 解决方案的全景图。

图 11 SASE 解决方案

2.6.2 应用场景

（1）上网安全服务

在中小微企业需要的员工上网安全防护场景及分支单位的边界安全快速建设场景，都具有建设费用高、部署速度慢、安全能力不灵活等痛点。而 SASE 提供的订阅模式下的上网安全服务，可解决上网侧，包括对终端上网、SaaS 应用访问的安全问题。通过 SD-WAN 接入服务引流实现流量上云，实现上网行为管理、URL 过滤、流量管理、入侵防御、终端防病毒等安全模能力，从而在用户终端与互联网 / 应用服务之间隔离出一块安全缓冲区，建立企业新型 SaaS 化的安全防线。

（2）接入安全服务

在具有总部—分支场景或者员工大量出差外地办公场景的大型集团公司、中小企业单位等，都需要实现安全接入公司内网。SASE 提供的基于零信任 +SD-WAN 的安全接入方案，具备身份权限控制、入网认证、访问加速等功能，确保企业员工、合作伙伴在任何地方，任何时间通过全球各地 POP 点网络访问业务时，都能享受到更安全、更隐私、更稳定的访问体验。

2.6.3 客户价值

SaaS 订阅，灵活调控 :采用 SaaS 订阅模式，无须一次性大量投入硬件成本，客户可按需购买多种套餐服务，可按月、按功能模块订阅 SASE 服务。

近源接入，安全访问：无论是分支节点还是员工远程接入，都可以享受到 SASE 提供的近源 POP 节点快速接入，同时利用 SD-WAN 的应用加速和 QoS 等服务，提升接入效率和链路使用体验。

统一管理，服务至上：运维人员可以通过一套 SASE 服务，覆盖企业完整的办公安全需求，降低学习成本，提升运维效率。同时 SASE 服务提供运营团队支撑，节省了单位维护、升级和硬件更新等成本。

2.6.4 优劣分析

优势：

高性价比：与购买和管理硬件产品不同，利用 SaaS 化订阅安全服务模式将大大降低客户的成本和 IT 资源。

统一管理：将客户的安全堆栈整合到基于云的网络安全服务模型中，可实现统一平台一体化管理，充分降低 IT 基础架构管理难度。

全球接入：通过遍布全球的 POP 节点，客户可以轻松连接到就近的网络节点，并利用 SD-WAN 技术实现业务的快速访问。

劣势：

数据安全:现阶段 SASE 解决方案缺少专业的数据安全相关能力。

成熟度欠缺 :SASE 解决方案发展仍旧处于初级阶段，POP 节点数量与网络链路质量仍有待提升。

2.7 综合解决方案

2.7.1 方案介绍

网络安全建设复杂度高专业性强，这也意味着安全建设需要投入更大的成本，并且在建设完成后安全设备还需要专业的安全运维人员持续运营，才能让安全投入发挥价值，这又对建设方提出了新的要求。网络安全建设投入大、成本高、效果低、难维护几乎成了所有组织都会面临的建设难题。

在此情况下单一的安全产品或者单独某一方面的解决方案无法满足客户体系化的安全建设的诉求，基于以上现状，绿盟科技提出了云化时代下的用户价值主张：

(1) 采用云化交付的安全产品和服务以获得弹性全面的安全能力；

(2) 引入高效敏捷的安全运营体系，以达到最优的安全效能；

(3) 与专业安全公司建立持续可信任的连接以获得最新的安全能力。

因此提供产品 + 服务 + 运营的体系化的综合安全解决方案，应运而生，在绿盟科技的安全体系中，我们定义为“T-ONE CLOUD”。

T-ONE CLOUD（inTelligent First Security Cloud），即智慧安全优先云解决方案。旨在以云的思路重构安全运营体系，为用户提供弹性敏捷的安全闭环保障能力。T-ONE CLOUD 采用云地协同架构，提供云化交付的安全产品和安全服务。通过云端安全运营中心联动用户侧安全设备，统一全局视图，用户可通过云端运营中心全面掌握网络安全运行状况。云端门户提供丰富的安全产品服务和安全运营服务，用户可按需灵活订阅，按需引入弹性全面的安全能力，应对各类安全问题。基于场景化设计的安全服务便于用户匹配自身建设需求，同时还可实现降本增效。

方案主要由以下四个方面组成：

（1）安全运营中心：建立整合云地安全能力、产品服务的统一门户，帮助用户实现全天候全方位的态势感知，提供安全检测、攻击溯源、资产风险评估及智能响应的安全运营能力，满足监管

合规企业日常运营要求。

（2）产品即服务：用户侧安全设备或安全资源，通过与云端安全运营中心连接，获取 T-ONE CLOUD 安全能力。具体能力包括硬件魔力防火墙（NF-SSE），虚拟化安全能力如入侵防御、全流量威胁检测、云堡垒机、主机漏洞扫描等数十种安全能力。

（3）安全服务体系：包括可订阅的产品服务、实现闭环保障的运营服务，以及等保合规建设、挖矿主机治理、勒索病毒防治、紧急漏洞应急响应等专项服务。从服务规格的设计到服务价值在客户视图的体现，都强调了场景化的服务闭环效果。

（4）移动 APP：移动 APP 包括租户门户和运营门户。通过租户门户，最终用户可以随时随处监测安全风险，享受对安全服务的实时感知和交互。利用为运营人员提供的运营门户 APP，合作伙伴可以实现对用户安全 7*24 小时的无间断服务。

图 12 展示了 T-ONE CLOUD 整体方案架构图。

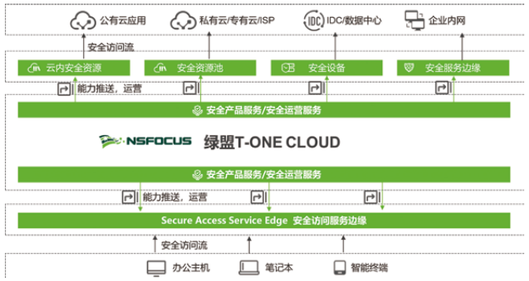


图 12 T-ONE CLOUD 解决方案

2.7.2 应用场景

（1）订阅式弹性边界场景

中小型企业对于网络安全的需求比较明确，希望供应商提供的解决方案可以做到轻资产、多能力、可扩展、易管理、高性价比等要求。在此场景下，轻量级 T-ONE 解决方案即可完美满足客户的这些诉求。

在中小企业、集团单位分支互联网出口部署 NF-SSE 设备，内置基础防火墙功能，实现网络接入与访问控制策略，保证互联网出口的安全。NF-SSE 是一款将安全能力服务化的产品，其在缺省提供下一代防火墙能力的基础上，本地化硬件可以弹性扩展安全流量深度检测、web 应用智能检测等能力，按需开通。通过云端 T-ONE 能力订阅的方式，还可获得如 SWG、终端安全等安全能力。安全能力服务化，使得安全能力可以按需开通，无须增加新的硬件设备，即可获得不同种类的安全能力，实现动态防御、立体防御点的效果。如图 13 所示。

图 13 订阅式弹性边界场景

NF-SSE 作为边缘接入设备，可接入云端 T-ONE CLOUD 平台。当硬件设备在本地完成建设，只须配置网络，保证与云端 T-ONE CLOUD 平台互通，即可通过设备注册接入云端，实现账号和设备点的绑定。此时，用户将在云端获得设备状态监控、设备管理、安全策略管理等服务，对设备自身以及业务安全的状况达到一目了然的效果，减少运维人员的投入、获得专业的安全业务风险呈现。

（2）云地协同 + 服务运营场景

具有总部—分支性质的大型集团企业，或者医疗专网、教育城域网、能源专网、交通专网等网络架构中，机构间呈现上级—下级关系，上级单位统一维护一张专网，供下级单位接入和使用。上级单位对专网内的网络安全负责，对下级单位接入专网的安全性有监管职责。接入专网的下级单位众多，上级单位没有足够的安全团队支撑专网内的安全监管和安全运营工作。

在此类场景下，可采用分支单位本地部署 NF-SSE 设备，总部部署本地化的 T-ONE CLOUD 运营中心（或采用云端 T-ONE CLOUD 平台）借助平台提供的云端安全专家和云上的智能安全分析能力，对威胁事件进行统一分析、统一响应，及时阻断，弥补下级单位技术能力储备不足的问题。 云端向下级单位发送安全告警和邮件报告的同时，也向上级主管部门发送全局安全分析报告，全面展示下级单位的安全状况，安全事件处置是否及时等。必要时，上级单位可通过 T-ONE CLOUD 平台的能力、联动下级单位部署的 NF-SSE，直接阻断存在安全问题的下级单位接入流量，实现对下级单位的有效监管。方案架构如图 14 所示。

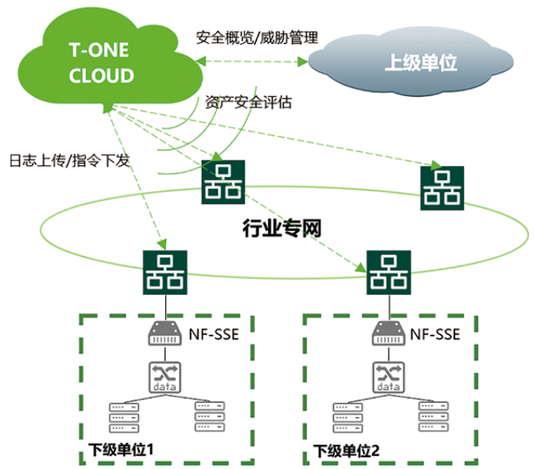


图 14 云地协同解决方案

当然上级单位还可以通过订阅 T-ONE CLOUD 平台具备的互联网资产核查、轻量化安全测试、网站安全监测等服务，对下级单位网络和行业专网中的应用进行周期性的安全评估，实现对下级单位和行业专网相关的脆弱性、威胁事件等安全风险的全局掌控，并在发生重大安全事件或紧急漏洞期间，结合云端安全专家的专业服务，通过统一的 T-ONE CLOUD 中心对全场景风险进行闭环处置。

（3）合作运营中心场景

在运营商、第三方云服务商提供基础设施服务的行业云场景，云服务商在提供计算 / 网络 / 存储等基础服务的同时，把安全也作为一种增值手段一起提供给租户。合作伙伴充分利用现有的云计算平台、运维人员和技术资源，与绿盟科技依托于 T-ONE CLOUD 提供的强大安全体系进行强强联合，开展安全增值业务，可以利用双方的优势相互赋能去应对当前越来越复杂的网络攻击场景，不仅可以提升现有业务的竞争力，还可以提升客户黏度，从而实现共赢和收益最大化。

基于 T-ONE CLOUD 强大的安全体系，可为客户提供等保合规安全能力、网站安全监测、网站安全防护、勒索病毒防治服务、挖矿治理服务等数十种安全能力及安全服务项。结合主动防御、动态感知的安全运营体系，帮助合作伙伴解决最终客户面临的安全风险和挑战。

不仅如此，绿盟还提供从能力建设、试运行、正式上线、持续运营一系列运营支持方案，包括团队组建、平台上线、市场分工、流程梳理、服务培训等工作。协助云服务提供商快速上手实现自主运营，帮助客户快速实现安全体系建设。整体运营架构如图 15 所示。

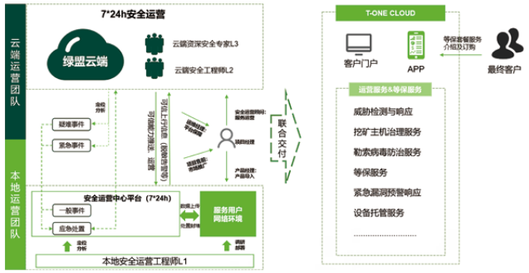


图 15 整体运营架构

2.7.3 客户价值

弹性订阅，降本增效 :T-ONE CLOUD 提供的安全能力可根据业务需要进行订阅和调整，能力的种类以及时间都可自定义，让安全始终以用户需求为主，云端一键开通，安全预算可灵活调配，提升安全效率。

云地协同，安全闭环：方案通过云地协同实现秒级检测，分钟级闭环，整个运营过程可视，应用 XDR、XSOAR 技术实践，通过丰富的观测指标体系，持续改进，不断提高安全运营闭环能力。

智能分析，安全可视 :T-ONE CLOUD 以客户实际需求为指引，基于场景化的专项服务提供实战化的攻防热点持续更新，云端威胁情报结合应急响应快速应对新的安全问题。

2.7.4 优劣分析

优势：

安全服务 :T-ONE CLOUD 解决方案配合专属云端安全专家服务，提供远程 7*24 小时服务,通过对威胁事件的实时监测、快速分析研判、主动处置闭环管理，提升客户威胁响应效率，提供精准的威胁分析结论。相比于仅提供安全能力方式，可以为客户带来更大价值。

APP 操控 :可通过手机 APP，随时随地进行安全产品服务管理及安全风险查看，支持售前电话咨询及工单、建议反馈在线提交，极大方便了客户的运维工作。

运维一体化：通过整合多种安全能力，客户可以降低复杂性、成本和用于定义安全策略的设备台数，有助于消除因使用多种不同供应商提供的不同产品的不一致而产生的管理风险。

劣势：

成熟度不足 :T-ONE CLOUD 解决方案仍旧处于发展初期，在方案与云网络融合、数据跟踪、运营流程成熟度等层面还需进一步完善。

3. 总结说明

上文阐述了业界常见的、在客户端有良好落地案例的一些云安全解决方案。随着云计算技术的发展和信息安全厂商的逐步探索，这些方案也会有更广泛的适用场景和更有效的应用模式，安全能力也会向着丰富化、精细化、运营化、服务化的方向发展，更好地服务于客户的业务和数据资产 [4]。当然仍然有很多云安全方向的新概念、新方案未能提及，如 CSPM、KSPM、CNAPP 等，它们还有待进一步的技术发展和市场验证。方案本身没有绝对的优劣之分，只有在确定场景下的最佳实践。

在面对纷繁复杂的客户需求和业务场景时，要求信息安全从业者协助客户详细梳理其基础架构、风险偏好和安全体系建设，选择最适合客户的产品方案去匹配，在解决客户实际问题的同时，也获得了自我价值的实现，取得双赢，甚至是多赢的局面。

参考文献：

[1] https://blog.k4nz.com/85c8ec3abaa74cd6e5ab5082f16aaad2/.

[2] https://zhuanlan.zhihu.com/p/394331330.

[3] Gartner,The Future of Network Security Is in the Cloud, August 2019.

[4] Gartner,Hype Cycle for ICT in China,2021, July 2021.

NSFOCUS

绿盟科技实验室年度研究巨献

重磅发布

扫描二维码
回复关键词“2022报告”
即可获取绿盟科技2022年报合集

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、金融、运营商、能源、交通、科教文卫等行业用户和各类型企业用户，
提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的后面，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技