

OT 安全市场指南

发布时间：2022 年 8 月 4 日 ID: G00743794

编辑人员：Katell Thielemann、Wam Voster、Barika Pace、Ruggero Contu

OT 安全产品和服务发展迅速，Gartner 为安全和风险管理领导者提供了 OT 安全市场状态的概述，并建议如何使用合适的 OT 安全产品，应对不断变化的格局。

概述

主要发现

- 随着 IT 系统与 OT 系统不断连接，带来了全新设计的网络化物理系统 (CPS)，OT 安全状态正在从以网络为中心发展为以 CPS 资产为中心。
- 81%的企业已意识到需要改变 OT 安全策略。其中，大部分企业开始执行崭新的 OT 安全运维。
- 平台式解决方案是 OT 安全产品的重心，众多 OT 供应商和 IT 网络安全厂商建立联系，进行合并和收购，致使特定垂直供应商涌现。当安全和风险管理 (SRM) 领导者在选择 OT 安全供应商时，拥有了比以前更多的选择性。

建议

负责 OT 系统安全技术、信息和弹性风险的 SRM 领导者，可以参考以下做法：

- 在风险不断增长的情况下，采用超越传统 OT 集成安全策略，将安全工作发展为运营弹性。即，融合所有 CPS（如，OT、物联网 [IoT]、工业物联网 [IIoT] 和医疗物联网 [IoMT]）和 IT 系统管理模式。
- 评估 OT 安全供应商在典型最终用户 OT/CPS 安全体系中所发挥的作用。判断其能否为加速优化路径奠定基础、能否提供安全之外的价值。
- 审查企业当前正在使用的 OT 安全解决方案，同时，比较现今市场上所有新兴的 OT 安全解决方案。经过对比分析后，便可得出最适合您企业的 OT 安全供应商。

战略规划假设

到 2025 年，70%的资产密集型企业将在企业办公环境、生产运营环境中融入安全功能。

市场定义

Gartner 把 OT 定义为：通过直接监测控制工业设备、资产、流程和事件来检测或变更管理硬件和软件。

OT 安全是保护它们的操作和技术。

市场变化

OT 安全市场正在迅速变化。传统细分的 OT 安全市场将产品聚焦于传统工业系统、纯运营网络、防火墙。如今越来越多的新功能出现，创新的工具与服务也同时出现。随着 OT 不断连接到 IT 系统，带来了全新设计的 CPS，而 OT 管理、运维、基础设施和安全也在陆续发展（请见图 1）。

图 1：从 OT 到 CPS 的安全变化



来源：Gartner 743794_C

Gartner

OT 安全体系的演变：

- **缺乏全面的安全管理**：在许多企业中，OT 最初是用于执行特定任务的，是定制化部署的。OT 安全不是生产系统设计和架构的核心。尽管后来发现这在很大程度上是一个谬论，但“air gapped”概念导致了一种“缺乏全面的安全管理”的心态。没有人会发现和重视生产系统的安全性，没有安全重点。
- **OT 网络中心安全**：随着生产系统开始相互连接，然后连接到企业 IT 系统，出现了以网络为中心的安全体系。它是以 OT 五层网络建模为基础，由防火墙、DMZs 和单向数据防火墙提供支持。

中央化管理的网络化物理资产系统：新旧资产的复杂性和多样性是许多企业的现状，因此需要一种全新的安全解决方案。企业了解到，OT 只是他们现在必须应对的一种网络化物理资产，紧接着还有物联网、工业物联网、智能建筑甚至医疗设备技术。这些技术都有一个共同点：不仅处理数据，还跨越了网络和物理环境。以资产为中心的 OT 安全体系，其首要执行工作是发现和厘清资产。

当涉及安全体系时，IT 与 OT 功能进化存在差异，两极分化的安全投入程度会对攻击者有利。并且，由于 OT 生产系统的设计、寿命年限和功能差异等原因，其独特性不可被忽视，以至于增加了 IT 安全问题。现代化工作模式将 OT 风险、可靠性和安全性的问题推到了风口浪尖。

市场方向

威胁在递增和转移

OT 系统对企业非常重要，它们是创造价值和收入的核心系统。如果它们故障，就会停止生产运营。OT 系统之间的联系越紧密，攻击面越来越大。这使得它们容易成为勒索软件、目标恶意软件的攻击目标。自 2021 年以来，关于 OT 生产运营环境被攻击的头条新闻数量在攀升，例如，南非港口运营被中断、美国佛罗里达州一家自来水公司被企图投毒。此外，诸如 Industroyer2¹ 和 Pipedream² 之类的恶意软件出现，它们功能新颖且易于部署。

更多的漏洞被披露

OT 系统中披露的漏洞数量逐年增加。³ 在许多方面，漏洞数量的增加是由于更多的安全研究人员和供应商将注意力集中在这些生产运营资产上。因为在很长一段时间里，原始设备制造商将漏洞的复杂性视为下游、售后的问题（请见注 1）。此外，生产运营环境中的漏洞是无法随意修补（请见注 2）。

安全专业技能仍然短缺

安全工程、安全评估和工业安全运营等领域的技能短缺表明，制定跨 IT、OT 和其他 CPS 环境的有效安全体系非常复杂。由于缺乏技能，对提供安全评估、安全框架、开发和实施的咨询服务的需求增加。对事件响应、自动化和行动准则的兴趣也导致对这些服务的需求不断增加。

更多法规、指令和机制在出台

2021 年瞄准基础设施建设相关的企业，不管是水务公司，还是管道运营商。加速了解它们生产运营环境中的技术，是国家安全和经济繁荣的关键。为此，出台了新的法规、指令和机制（请见注 3）。

市场分析

一些重要的载体直接影响 OT 安全市场的演变。

企业正在跨越觉醒阶段

Gartner 记录了企业的安全布局变化（请见图 2）。调查结果显示，82% 的企业已经历了觉醒阶段。

图 2：OT/CPS 安全布局变化



来源：Gartner 743794_C

Gartner

安全布局变化的 6 大阶段：

- **阶段 1. 觉醒：**在这个阶段，会出现新的安全优先级和重点，这是触碰安全警报底线的违规行为所驱动的。另外，来自联邦调查局（FBI）、国土安全部（DHS）和欧盟网络安全机构（ENISA）等政府机构的警告和公告、以及关系到特定垂直的遵从法规需求在增加。董事会、高管、CIO 的决策和数字化转型，让企业要重新审视风险状态。通常负责解决这些问题的是 IT 安全团队，他们利用 IT 思维处理。但是，他们很快就会意识到自己在陷入一个困境之中。
- **阶段 2. 资产发现、网络拓扑映射：**一旦企业达到了觉醒阶段，下一步就是找出生产运营环境中存在哪些连接系统、风险状态。这要与负责 OT 资产管理的团队沟通，了解企业范围内的 IT 体系结构、OT 安全策略和程序。在现实中，一般很快就会出现这样的情况：“已开发而被荒废”的生产运营环境是为了提高生产效率、控制成本而连接起来的，缺乏安全可见性。而且，寻求数字化转型的业务部门，其管理的工业物联网（IIoT）、物联网（IoT）工作部署的全新 CPS 也缺乏安全监控。如今，越来越多的安全供应商提供资产发现和网络拓扑映射平台，那么下一步部署，会涉及一个或多个 CPS 保护平台解决方案的概念验证（POC）工作。
- **阶段 3. 发现问题：**这些概念验证（POC）总会让人大开眼界。例如：
 - 非托管资产无处不在。

- 部署操作系统时，默认凭据保持不变。
- 最初设计为高度隔离的 OT 网络，已变得比想象中更简单。
- 不同远程位置上的各种系统端口都是开放的。
- 原始设备制造商正在远程访问他们销售的机器，然而没有企业团队发现此状况，也没有对此进行管理。
- 旧操作系统上披露的漏洞从未进行修补评估。
- 不同安全体系（例如，网络安全、物理安全、供应链安全、产品安全、健康安全）之间的功能孤岛，正在形成漏洞，供不良行为者利用。
- 大多数企业的价值创造中心缺乏安全的运营环境。由于没有集中式管理，各种安全相关流程、决策的角色和责任从未明确，更不会有意见达成一致的时候了。

阶段 4. 解决问题：在这个阶段，确定行动的优先级并部署。例如，当风险评估发现高价值资产需要优先考虑安全时，可以通过创建指导委员会来解决管理差距。例如，网络分段审查、端点强化、威胁情报、在可行的情况下进行修补、事件响应计划更新等等，应按照优先级处理。对于部分企业而言，达到阶段 4 对决策制定有所帮助；也有部分企业既没有需要，也没有资源推进到第 5 阶段，因为这会改变它目前固有的稳定状态；还有部分企业，第 4 阶段的行动部署创造了一个崭新认知。他们发现，整合和优化阶段不仅为安全提供了价值，而且为企业提供了投资回报。

阶段 5. 整合：这是 OT 安全与 IT 安全和其他安全管理、监控、报告整合、协调的阶段。新岗位——首席安全官（CSO）把以前孤立的安全体系融合在一起。例如安全工具融合，提供了更广泛的态势认知，以及更新安全策略来应对非 IT 特定环境。此阶段可能整合安全信息和事件管理（SIEM）或安全编排自动化和响应（SOAR）解决方案。企业可能会开始在其运营或关键任务环境中采用端到端更广泛的安全办法。这些办法反映了 IT 安全实践，包括事件响应、威胁情报、威胁追踪或行骗。值得注意的是，这些反映并不意味着成效相同。OT 生产运营环境仍然具有独特性，IT 安全体系需要相应地调整。

阶段 6. 优化：随着融合取得成果，更多数据来自部署以 OT 为中心的安全工具。如今企业意识到，他们可以访问到前所未有的可见性和数据量，这附加功能会使得安全团队以及负责运营、维护、采购和工程的非安全团队受益。Gartner 与企业互动交流得出，一些企业已经开始使用 CPS 保护平台的数据来支持预测性维护工作。例如，根据资产使用指标，来为采购决策提供参考。

CPS 保护平台成为重心

随着越来越多的 OT 系统与 IT 系统互通互联，物联网（IoT）、工业物联网（IIoT）、智能建筑或工厂自动化运营加速，现在企业必须保护其环境中所有类型的网络化物理系统。在过去几年里，CPS 资产发现平台出现，这帮助了安全领导者厘

清庞大的技术资产。这类平台通常是无代理的，可以向运营部门解释为不会增加额外的风险。它们与其他安全工具（如，SIEM 或 SOAR 解决方案）会产生越来越多的互操作性。

最初的平台功能以资产发现、可见性和网络拓扑为中心。然而，随着供应商不断向这些平台添加新功能，它们变成了 CPS 保护平台。现在可用的功能包括威胁情报 (TI)、漏洞管理、风险评分或安全远程访问。

基于平台的特性和功能模块化，对于最终用户很有吸引力，因为最终用户可以根据当前的需求和熟练度去操作它们。平台业务模式还意味着，供应商可以提供基于软件即服务 (SaaS) 的定价模式，并为更多基于云和以分析为中心的解决方案打开大门。一些供应商现在既为“已开发而被荒废”系统提供被动本地解决方案，又为“未开发使用”系统提供基于云的解决方案。

特定垂直供应商正在兴起

由于部署系统、协议类型、独特销售周期或安全安保差异，一些垂直行业（如，医疗保健、国防、铁路或海运）具有独特的安全需求。一些供应商正在接受这类独特需求，他们将向市场提供对特定垂直环境量身定制的解决方案，并根据垂直行业的专业知识，精心挑选人员进入市场。另外，渴望将市场占有率扩大到运营环境的云提供商，也瞄准了行业合作伙伴关系，并展示了其解决方案嵌入的安全实践。

近两年显著的并购和投资风险变动

过去两年，OT 安全市场发生了多起并购事件（请见注 4）。如果 OT 制造商和 IT 网络安全厂商因合作伙伴关系导致收购，最终用户就要考虑互操作性。大多数工业环境都由各种设备制造商的系统提供支持。令人担忧的是，如果某制造商的设备，只能由已成为同一安全厂商产品的 CPS 保护平台进行监控，将会发生什么。

OT 和 IT 安全供应商继续搭建桥梁

在过去两年，OT 安全和 IT 安全解决方案之间的联系越发密切。大多数 OT 安全供应商（以及所有 CPS 保护平台供应商）都与成熟的 IT 安全供应商建立了战略合作伙伴关系。

OT 安全供应商代表

本 OT 安全市场指南列出的 OT 安全供应商名单，并不是市场上全部供应商。我们尽可能提供详尽的 OT 供应商发展情况。

OT 安全供应商	企业总部位置
Accenture	爱尔兰都柏林
AirEye	以色列荷泽利亚
Airgap	美国加利福尼亚州圣克拉拉
Armis	美国加利福尼亚州帕洛阿尔托
Barracuda	美国加利福尼亚州坎贝尔
BeyondTrust	美国佐治亚州约翰斯克里克
Blue Ridge Networks	美国弗吉尼亚州尚蒂伊
Booz Allen Hamilton	美国弗吉尼亚州麦克莱恩
Capgemini	法国巴黎
Cervello	以色列特拉维夫
Claroty	以色列
Cylus	以色列特拉维夫
Darktrace	英国剑桥
DeNexus	美国加利福尼亚州索萨利托
Dispel	美国纽约
Dragos	美国马里兰州汉诺威
Forescout	美国加利福尼亚州圣何塞
Fortinet	美国加利福尼亚州桑尼维尔
Hexagon	瑞典斯德哥尔摩
Kudelski Security	瑞士洛桑河畔切索
Microsoft	美国华盛顿州雷德蒙德
Mission Secure	美国弗吉尼亚州夏洛茨维尔
Nozomi Networks	美国加利福尼亚州旧金山
NTT	日本东京
Onclave Networks	美国弗吉尼亚州麦克莱恩
Open Cloud Factory	西班牙毕尔巴鄂
Optiv	美国科罗拉多州丹佛
Orange Group (Orange Cyberdefense)	法国巴黎

Ordr	美国加利福尼亚州圣克拉拉
Owl Cyber Defense	美国马里兰州哥伦比亚
Palo Alto Networks	美国加利福尼亚州圣克拉拉
Radiflow	以色列特拉维夫
Red Trident	美国德克萨斯州休斯顿
SCADAfence	以色列特拉维夫
SecurityGate.io	美国德克萨斯州休斯顿
Shift5	美国弗吉尼亚州阿灵顿
Tenable	美国马里兰州哥伦比亚
Verve	美国伊利诺伊州芝加哥
Waterfall Security Solutions	以色列罗什哈因
Xage Security	美国加利福尼亚州帕洛阿尔托

市场建议

负责 OT 系统安全技术、信息和弹性风险的 SRM 领导者，可以参考以下做法：

- 将安全工作与运营弹性挂钩。
- 评估 OT 安全供应商在典型最终用户 OT/CPS 安全布局变化中所处的阶段。
- 厘清企业所拥有资产，加速 IT/OT 安全堆栈融合。

将安全工作与运营弹性挂钩

勒索软件攻击、全球流行病、供应链中断和地缘政治问题日益加剧，大多数企业重新评估其运营弹性。这包括协调风险评估管理、风险监控和执行控制措施。这些都会影响业务交付、价值实现过程中风险领域的劳动力、流程、设施、技术和第三方。随着 OT 安全风险成为网络物理风险，SRM 领导者应该抓住机会，将不断增长的安全认知与 OT 安全产品综合研判（相关最佳实践，请见注 5）。

评估 OT 安全供应商在典型最终用户 OT/CPS 安全布局变化中所处的阶段

了解处境相似企业的安全布局变化，这可以帮助 SRM 领导者在规划未来道路与请求资源时，能与高级领导沟通到预期效果。

虽然安全布局经常被视为成本中心，但具有商业头脑的 SRM 领导者很快就会意识到，保护能创造价值的资产，可以获得不同级别管理层的关注。如果对 OT 安全解决方案的投资，创造了对非安全团队有价值的信息。那么，这样的投资是十分明智（请见注 6）。

厘清企业所拥有资产，加速 IT/OT 安全堆栈融合

SRM 领导者需要评估最新入市的独立或基于平台的 OT 安全供应商，以便与其 IT 安全产品实现互操作性。为了实现这一目标，SRM 领导者都在寻求更多的选择性。好消息是，市场正在做出反应。针对生产运营或关键任务环境的新 OT 安全供应商、新安全特性和功能，目前均可落地。在评估解决方案时，向供应商提出的问题示例（请见 7）。

参考来源

本 OT 安全市场指南中的分析基于主要和次要研究，反映了 Gartner 与最终用户、供应商的许多日常交流。

¹ 针对乌克兰能源公司 Techstrong Group 的 Industroyer2 恶意软件。——来源 Security Boulevard

² 美联储发现入侵工业控制系统的“瑞士军刀”。——来源 WIRED

³ 半年度 ICS 风险和漏洞报告：2H 2021。——来源 Claroty

⁴ 欧洲同意采用旨在加强网络安全的新 NIS2 指令。——来源 The Hacker News

注 1：漏洞的复杂性

Forescout 的 Vedere Labs 发布的 56 个漏洞表明了这问题：

- 多家原始设备制造商。
- 一系列漏洞，从硬编码凭据到不存在或弱密码。
- 一系列利用选项，从远程代码执行到文件、固件、配置操作。
- 受影响的系统，包括旨在保护人类生命的安全仪表系统。

注 2：修补漏洞

- 需要执行详尽的计划，以免在操作中给正常生产运行时间带来更多风险。
- 原始设备制造商，在其产品生命周期的运营阶段发挥着关键作用。他们有责任在严控的物理环境中开发、测试和推出补丁。

- 最终用户需要知道这些漏洞在哪里，然后确定修补、隔离、升级，评估对企业的定制操作是否有意义。
- 配合生产过程中的计划停机时间，必须安排补丁和更新部署。
- OT 系统的补丁无法支持操作系统。

注 3: 新法规、指令和机制

- 美国的 CISA Shields Up 运动，以及其他国家开展类似活动。
- 美国运输安全管理局针对管道和地面运输运营商的各种指令：
 - 加强管道网络安全 — SD-Pipeline-2021-01B
 - 加强铁路网络安全 — SD 1580-21-01
 - 加强公共交通和客运铁路网络安全 — SD 1582-21-01
 - 加强地面运输网络安全 — IC 2021-01
 - 管道网络安全缓解措施、应急计划和测试 - SD-管道-2021-02B
 - 管道 — 实施时间表 — SD-管道-2021-02B 的附件 1
 - 加强管道网络安全的信息通报 (IC 管道-2022-02)
- 针对关键基础设施运营商，新的美国网络事件报告法。
- 在欧盟，即将出台的 NIS2 指令将加强所有欧盟国家的安全控制和事件报告规定。⁴

注 4: 并购事件

- OPSWAT 收购了 Bayshore Networks。
- Forescout 收购了 CyberMDX。
- Claroty 收购了 Medigate。
- Sabanci Group 收购了 Radiflow 的多数股权。
- Claroty 完成了由软银集团牵头的 4 亿美元 E 轮投资。
- Nozomi Networks 在 D 轮融资中额外筹集了 1 亿美元。
- Dragos 在 D 轮融资中又筹集了 2.1 亿美元。
- Ordr 在 C 轮融资中又筹集了 4000 万美元。

随着最终用户越来越重视 OT 安全，设备制造商将会加入安全供应商行列。市场上已经公布了一些值得被关注的合作伙伴关系。例如：

- Claroty 和 Yokogawa
- Nozomi Networks 和 Siemens
- Fortinet 和 Schneider Electric
- Dragos 和 Emerson

注 5: 将安全工作与运营弹性挂钩的最佳实践

- 回顾所有安全系统和安全管理的执行情况，记录所有缺口、重叠，以便更好地在 IT、OT、安全、隐私、供应链和面向客户的 CPS 之间进行协调。
- 认识到以 IT 为中心的解决方案不会普遍有效，甚至不可取，因此需要针对 OT 系统进行更新。
- 对整个运营威胁环境中的威胁向量进行建模。
- 明确和分散风险所有权，提高运营中的安全认知，同时集中安全持续资产的可见性和监控。
- 根据实体(如设施、生产线或高价值资产)的运营价值，用评分更新风险登记册。

注 6: CPS 保护平台为其他团队创造的价值

Gartner 的调查发现，一些部署了 CPS 保护平台的最终用户，能够与其他团队共享有价值的信息，例如：

- 运营和工程 —— 资产可用性、网络拓扑和资产连接、弹性冗余映射。
- 维护 —— 资产配置文件映射到维护间隔。
- 合规性 —— 仪表板和报告。
- 采购 —— 资产使用情况报告，可以为采购决策提供参考。
- 最高管理层 —— 增强运营态势感知能力。

这是一个将安全投资转变为业务发展投资的机会，从而提高了 SRM 团队在数字化转型决策层面的地位。

注 7: 在评估解决方案时，向供应商提出的问题示例

- 能否提供端口或设备控制解决方案？
- 能否提供便携式媒体管理解决方案？
- 能否提供恶意设备检测、隔离、管理解决方案？
- 能否提供资产发现、分析、库存解决方案？

- 在技术堆栈中处于多低的位置（例如，什么级别）？
- 提供被动还是主动解决方案？两者兼而有之吗？
- 解决方案是作为串联还是带外或两者兼而有之？如果带外，引入数据的过程是什么？
- 支持哪些协议？
- 提供的详细程度如何？
- 发现方法是持续的？还是时间点的？
- 能否提供网络拓扑映射解决方案？
- 能否提供单向安全数据传输解决方案？
- 能否提供基线和配置管理解决方案？
- 能否提供网络分段解决方案？
- 能否提供漏洞管理解决方案？
- 能否提供威胁检测解决方案？它是时间点还是持续的？
- 能否提供加密解决方案？
- 能否提供违规或事件响应解决方案？
- 能否提供调查或取证解决方案？
- 能否提供合规报告解决方案？内部制定的政策？符合标准？
- 能否提供安全远程访问或监控解决方案？
- 能否提供渗透测试服务？
- 能否拥有测试平台、模拟或以安全为中心的数字孪生解决方案？
- 能否提供硬件、固件、软件供应链安全解决方案？
- 能否提供与现有 IT 安全堆栈产品（例如 SIEM、SOAR、配置管理数据库 [CMDB]、SOC、NAC、防火墙和其他针对没有内联强制功能的被动侦测系统的强制控制）的开箱即用集成？
- 能否为 OT 提供托管检测和响应服务？
- 是与谁合作进行技术开发？用于服务交付？
- 是否可以交流类似规模、垂直行业的内容？