Gartner

创新洞察：CPS 安全远程访问解决方案

发布时间：2024 年 4 月 18 日　　ID：G00804283

作者：Katell Thielemann、Abhyuday Data 和其余 1 人

企业越来越需要为制造商、员工和承包商提供对生产或关键任务型网络化物理系统（cyber-physical system, CPS）的安全远程访问。本项研究为安全和风险管理（security and risk management, SRM）领导者提供了有关 CPS 环境新型安全远程访问解决方案的见解。

概述

主要发现

- 越来越多的企业开始采用远程访问解决方案，以在其生产或关键任务环境中操作、维护和更新 CPS。这是出于安全考虑、合同义务和成本、竞争和技术员工短缺的压力。
- 可能存在未记录且不安全的远程连接，然而，网络安全团队或生产团队均不知情。
- 事实证明，传统的 VPN 和基于跳转服务器的方法越来越不安全，管理起来也越来越复杂。此外，它们通常缺乏对单个设备的细粒度访问控制，而是提供对整个网络的访问。
- IT 远程特权访问管理（remote privileged access management, RPAM）和 CPS 安全远程访问解决方案均支持远程访问需求，但针对不同的用例和考虑不同的用户。

建议

希望通过有效的安全远程访问功能来增强其 CPS 环境安全性的 SRM 领导者应该：

- 在选择解决方案之前，先确定企业的需求和用例。在某些情况下，IT RPAM 工具可用于轻度触及权限的 CPS 访问。但如果需要手动操作、维护或升级设备，则需要 CPS 安全远程访问解决方案。
- 与 CPS 资产保管者（例如生产工程师或维护人员）密切合作，制定既能平衡多因素身份验证（multifactor authentication, MFA）等安全最佳实践、又能满足运营或生产需求的策略。
- 对企业的所有远程连接进行全面盘点。未经正式记录或未经授权的远程访问可能存在于整个运营网络中，特别是在现场。

- 在部署新的 CPS 安全远程访问解决方案时，请移除旧的远程访问解决方案。通常，企业在部署新解决方案时，没有注意遗留下来的旧方案。因此，被利用的 VPN 漏洞数量不断增加，这是一个重大盲点。

战略规划假设

到 2028 年，使用远程访问向量对 CPS 发动的攻击比例，将从现在微不足道的数字增长到 15%以上。

引言

虽然支持生产或关键任务流程的 CPS 技术（通常可互换称为 OT、IoT、IIoT、ICS、IACS、SCADA 等）最初是单独部署的，但它们变得越来越相互连接，并与企业系统相连。此外，企业现在需要原始设备制造商（OEM）、承包商和员工来远程操作、维护和更新它们。

虽然过去人们使用 VPN 和跳板机来实现这一点，但这些方法已被证明越来越不安全且难以管理。近年来，VPN 漏洞急剧增加，导致漏洞被利用，并引发紧急指令，如 CISA 的 ED-24-01。[1] 此外，大多数 VPN 提供广泛的网络访问。如试图在更细微的层面上限制这种广泛的访问，需要复杂且昂贵的监督措施。

> **“我们认为，攻击者利用了一个不建议使用的传统虚拟专用网络（VPN）配置文件。”**
>
> *—— 科洛尼尔管道公司 总裁兼首席执行官 Joseph Blount 于 2021 年 6 月 8 日向美国国会作证。[2]*

新的解决方案已经进入市场，例如 IT RPAM 和 CPS 安全远程访问解决方案，但它们支持不同的用例和不同的用户（请见表 1）。

表 1 - 远程访问：满足不同需求的不同工具

	IT RPAM	CPS 安全远程访问
用例	远程访问 IT 设备和应用程序	操作、维护和更新 CPS 设备；培训新工程师和维护人员
主要考虑因素	IT 安全团队管理效率	生产弹性、安全性、生产力或成本控制
访问权限决策者	IT 安全团队	生产工程师、资产保管者、维护人员
相似的功能*	会话记录；带有恶意软件扫描的文件传输；MFA；SaaS；RDP、HTTP 和 SSH；加密；审计跟踪；密码保管库；多用户协作；即时（just-in-time, JIT）连接；无代理	

独特的功能*	基于规则；密钥轮换；与 IT 生态系统集成	访问没有凭证的旧版 CPS；工业协议；不依赖防火墙或交换机；无需跳板机；具有会话控制覆盖的实时监察；本地部署；多隧道；访问非 IT Active Directory；战略合作伙伴关系（OEM 和 CPS 保护平台）；数据驻留；多用户操作；用于培训的会话跟踪；在中断、断开、间歇性和低带宽（disrupted, disconnected, intermittent and low-bandwidth, DDIL）环境中工作；支持合规性（例如 NERC CIP）；用于防御或情报——高完整性飞地隐藏或混淆；支持通用访问卡（Common Access Cards, CAC）
* 概括每个类别中的大多数供应商；每个供应商都有其独特的功能。		

来源：Gartner

描述

定义

CPS 安全远程访问解决方案允许员工、承包商和 OEM 远程访问生产或关键任务型资产，以便安全地操作、维护或更新它们。它们提供了一种强大的机制来验证用户的身份，确保安全通信并跟踪所采取行动的完整性。CPS 安全远程访问工具与 IT RPAM 工具具有相似的功能。但是，两者之间也存在很大差异。

由于这两套工具之间存在相似性和差异性，SRM 领导者需要仔细确定自己的需求和解决方案的功能。例如，它们都：

- 无需代理
- 记录会话
- 支持带有恶意软件扫描的文件传输
- 支持 MFA
- 可以作为基于云的 SaaS 解决方案提供
- 支持 RDP、HTTP 和 SSH 协议
- 支持加密
- 提供审计跟踪
- 提供密码保管库
- 支持多用户协作

- 允许 JIT 连接
- 对访问、端点和会话实施最小权限

因此，如果身份和访问管理（identity and access management, IAM）是核心用例，并且不需要其他特定于操作的安全功能，它们都可以使用。但它们也存在很大差异：

- IT RPAM 可以使用代理、基于规则、提供密钥轮换，并旨在与特定 IT 生态系统集成。
- 另一方面，CPS 安全远程访问解决方案可以提供：
- 除了基于云的部署，还可以进行本地或混合部署。
- 由非 IT 人员进行管理，这些人员通常是全天候工作的生产工程师和资产所有者，他们决定谁可以访问什么。
- 由生产工程师进行实时监察并控制会话。
- 支持工业协议（例如 Profinet、Modbus、BACnet、Telnet）。
- 虚拟网络计算（VNC）连接。
- 特定于设备的细粒度访问。
- 如果某个地点失去互联网连接，请将凭证存储在现场。
- 适用于多站点企业的分布式架构。
- 通用的或多隧道，因为必须在同一会话中访问多个接口。
- 访问非 IT Active Directory，或无需 Active Directory 即可操作。
- 多用户操作，能够共享屏幕，并将控制权交给多名团队成员。
- 用于培训目的的会话跟踪。
- 虚拟控制或操作中心功能，具有多监视器视图。
- 可疑登录尝试的警报。
- 访问 DDIL 环境。
- 支持 CPS 特定的合规环境（例如 NERC CIP）。
- 符合 CPS 特定的标准和规定，例如 NIST SP 800-82 修订版 3、ISA/IEC 62443 或 TSA 指令。

有些解决方案还可以为防御或情报环境提供独特的功能，例如访问高完整性飞地隐藏或混淆，以及支持 CAC。

值得注意的是，未来的新兴进展包括：

- 下一代防火墙正在增加与 CPS 环境用例相适应的功能。

- 基于生物识别的 MFA。

好处和用途

CPS 安全远程访问解决方案越来越需要处理以下问题：

- **安全考虑**：一些 CPS 部署在恶劣的环境中或处理可能对人体有害的材料。因此，远程管理可以是部署人员的首选方案。
- **合同义务**：随着 OEM 出售设备，他们无法在每个地点都安排支持团队待命。通常，他们会在销售合同中规定远程访问以支持服务级别协议（service-level agreement, SLA）。这些 OEM 还需要确保他们自己的员工只能访问他们应该访问的内容。
- **成本或生产力压力**：通过同一劳动力资源来支持多种操作环境的能力，是成本控制和生产力计划的核心。
- **竞争压力**：竞争压力正在推动自动化的发展，提高产量和质量。远程管理资产的能力已成为一个差异化因素。
- **生产正常运行时间，设备维护或升级**：保持生产和关键任务环境不中断地正常运行的能力，是保持竞争力的关键因素。
- **技术员工短缺的压力**：在全球范围内，生产工程师和工业维护专业人员短缺。由于缺乏当地专业人员或当地专业人员的成本较高，通常需要进行远程操作。
- **新工程师和维护人员的培训**：为了应对技术员工短缺的压力，企业不得不培训新员工，CPS 安全远程访问解决方案越来越多地用于此目的。

CPS 安全远程访问解决方案：

- 提供传统 VPN 的替代方案。传统 VPN 越来越不安全，并且充满了已披露和被利用的漏洞。
- 通过为远程用户启用时间限制、特定会话、JIT 访问，确保只有合适的人员才能访问适当的系统，从而减少攻击风险。
- 允许访问无需凭证即可运行的旧版 CPS。
- 无需依赖防火墙或交换机。
- 无需使用可能需要复杂身份验证管理的跳板机。
- 通过支持本地部署，支持某些司法管辖区的数据驻留要求。
- 隔离多供应商供应链。
- 使用已与 OEM 建立战略合作伙伴关系的供应商来：
  - 了解其特有的设置、配置和协议。

  - 将安全远程访问连接器作为组件嵌入到新设备中。
  - 与西门子的完全集成自动化（Totally Integrated Automation, TIA）门户等工具进行交互。
- 使用与 CPS 保护平台建立战略合作伙伴关系的供应商，以利用其资产发现功能。
- 支持特定于生产或关键任务环境的非 IT Active Directory。

风险

虽然 CPS 安全远程访问工具比传统方法提供了许多好处，但 SRM 领导者应注意以下风险：

- 没有意识到：在整个运营网络中，尤其是在现场，可能已经存在未经正式记录或未经授权的远程访问。
- 部署新的 CPS 安全远程访问解决方案，但没有移除过时或不受支持的 VPN 等旧技术。
- 有些供应商进入市场还不到三年，随着数字化转型工作推出更多自动化，并实现更多远程操作，这些功能将保持旺盛需求。因此，可能会发生并购活动。
- 对远程用户实施接入、管理和访问控制之前，请使用 CPS 安全远程访问工具启用远程访问。
- MFA 是一种有效的保护控制措施，可防止帐户接管（account takeover, ATO）威胁，但静态 MFA 方法不像自适应 MFA 方法那样考虑外部上下文和风险信号。大多数 CPS 安全远程访问工具都提供静态 MFA 机制，这比没有 MFA 有所改善，但它们无法提供自适应 MFA 所提供的一系列上下文和风险信号。

建议

- 在选择适用于远程用户的临时和有时限的访问解决方案之前，请先确定企业的需求和用例。在某些情况下，IT RPAM 工具可用于轻度触及权限的 CPS 访问，但如果需要手动操作、维护或升级设备，则需要 CPS 安全远程访问解决方案。
- 与资产所有者（例如生产工程师或维护人员）密切合作，制定平衡安全最佳实践（例如 MFA）与运营或生产需求的策略。
- 对企业的所有远程连接进行全面盘点。未经正式记录或未经授权的远程访问可能存在于整个运营网络中，特别是在现场。
- 在部署新的 CPS 安全远程访问解决方案时，请移除旧的 VPN。通常，企业在部署新解决方案时，没有注意遗留的问题。因此，被利用的 VPN 漏洞数量不断增加，这是一个重大盲点。

供应商代表

下面列出的供应商并非详尽无遗。本节旨在帮助您更好地了解市场及其产品。

- Blue Ridge Networks
- BlastWave
- Claroty
- Cyolo
- Dispel
- Honeywell Forge
- OTORIO
- WALLIX
- Xage Security
- XONA Systems

参考来源

本分析基于分析师在与 Gartner 客户和其他创新企业合作时的经验，也基于分析师的讨论以及与主要行业参与者的众多对话。

[1] 来源于 U.S. CISA 发布的紧急指令《ED 24-01：缓解 Ivanti Connect Secure 和 Ivanti Policy Secure 漏洞》

[2] 来源于证词文件《美国参议院听证会 国土安全与政府事务委员会 2021 年 6 月 8 日 科洛尼尔管道公司总裁兼首席执行官 Joseph Blount 的证词》

缩略词和术语词汇表

IACS	industrial automation and control systems 工业自动化和控制系统
ICS	industrial control system 工业控制系统
IoT	Internet of Things 物联网
IIoT	Industrial Internet of things 工业物联网
OT	operational technology 运营技术
SCADA	supervisory control and data acquisition 监察控制和数据采集