





工业网络安全展望（2023-2030）

Fortinet

 2023
Innovator
OT Visibility & Threat
Management
Fortinet


 2023
Leader
IT/OT Network Protection
Platforms
Fortinet


OT网络安全投资的宏观趋势依旧强劲

得益于数字化转型、机构监管和风险管理三大助推因素，即便全球经济形势充满挑战，OT网络安全支出依然呈现稳步增长趋势。

OT设备、系统和流程之间的日益互联互通，持续推动工业运营加速数字化转型，企业云计算服务、数据分析、数字孪生和机器学习等技术需求日益增长。此外，IT和OT环境的持续融合，使以往相互隔离的两大环境实现无缝集成和数据交换。全新数字资产所有者得以具备更高水平的协同和协作能力，实现流程优化和生产力提升。然而，数字化转型是一把双刃剑，优势往往与风险并存，资产所有者需有效管理不断激增的IT和OT环境漏洞，最大限度发挥数字化转型的众多优势。鉴于此，企业亟需部署全新网络安全策略、流程和步骤，积极打造适应未来网络环境的弹性运营模式。

此外，机构监管对采购决策的影响持续加深。随着执法力度的不断加强，机构监管范畴覆盖更多行业领域和供应链，构建更高水平弹性运营的需求日益高涨。美国相关案例包括：CISA（美国网络安全和基础设施安全局）发布的约束性运营指令 23-01、2023 年生效的 TSA 指令 SD1580/82-2022-01，以及旨在联邦运营基础设施中构建零信任架构的OMB M-22-09指令。NIS 2指令将于2024年起在欧盟国家全面生效，目前所保护的关键制造业领域已将欧盟经济基础设施覆盖率从21% 提升至36%，而关键实体弹性法案（CERA）则重点覆盖关键基础设施。近期，澳大利亚、印度、日本和加拿大均已出台新法规或开展现状审查以制定相应法规。

推动OT安全投资持续增长的最后一大驱动因素，源于广泛报道的勒索软件事件令业内同行深受触动。行业高管对OT风险的认识也因此逐渐提高，有利于改善网络治理水平并专注构建弹性安全网络。据Orange Cyberdefense研究显示，制造业跃居 2022 年遭受威胁攻击最严重的行业。部分归因于该行业规模庞大，于攻击者而言，诱惑力相对更高（制造业 CVSS（通用漏洞评分系统）漏洞评分比全球平均水平高 33%）。此外，该调查机构还强调，58% 的安全事件源于内部违规行为和错误配置。资产所有者在有效抵御外部威胁的同时，仍需密切监控内部流程。

网络安全要求持续升级

OT网络安全管理权归属因组织而异，可能由运营团队、工程总监负责，也可能由首席信息安全官（CISO）负责。为便于描述，下文将负责OT网络安全的团队统称为OT安全管理者。

OT安全管理者的主要目标是确保将影响运营可靠性、可用性和安全性的网络安全事件风险降至最低。鉴于此，需准确识别和管理漏洞，并部署一层控制策略以防止威胁参与者非法访问网络。因此首先应对所有资产进行识别和分类，尽管任务繁重但势在必行。例如，尽管有的工厂可能已运营长达30年之久，但从未正式建立资产登记清单，基础设施的安全防护往往依赖于不同OEM系统和传感器的叠加拼凑。安全管理者需全面了解组织内部应管理的所有资产、资产固件和补丁状态及其端点连接情况。

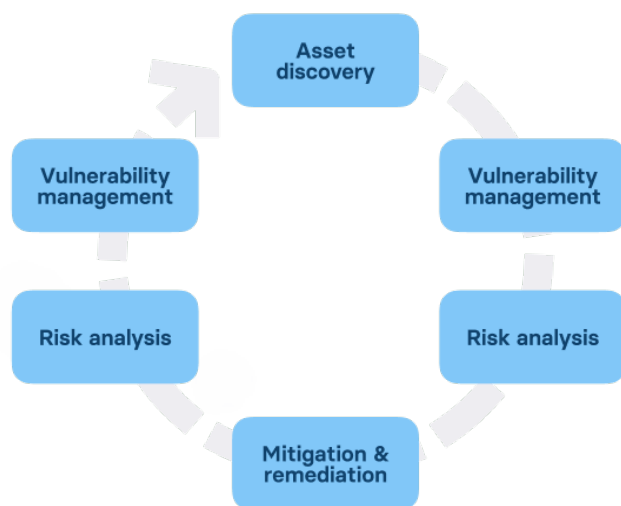


一旦所有资产被准确识别并记录在册，OT安全管理者应立即探查所有已知漏洞，并执行相应流程对其进行持续监控和管理，包括更改默认密码、进行补丁管理和监控访问控制。

作为一套面向 OT 环境的传统分层安全模型，纵深防御（DiD）体系囊括了一系列安全技术和
管理控制策略，可全方位保护数据、应用程序、端点和网络，令不法分子难以横向入侵网络，
从而有效阻断漏洞利用行为。技术控制策略涵盖部署于 IT/OT 网络边界和不同区域之间的防火
墙，以提供适当的网络分段、端点防护和访问控制功能。OT网络监控功能则提供额外防御
层，高效检测异常事件并自动响应威胁。

然而，随着OT与IT网络的持续融合以及工厂车间和云之间数据交换规模的不断扩大，攻击面也
随之持续扩大。仅构建纵深防御（DiD）体系远不足以全方位保护OT运营。现代化组织亟需部
署跨数字基础设施、实体和物理资产组成的复杂网络，统一执行策略、监控和编排功能的安全
解决方案。

攻击面管理（ASM）解决方案，有助于解决识别、评估和缓解位于组织内部数字和物理基础设
施、供应链和 OEM 合作伙伴等外部实体中存在的漏洞挑战。



攻击面管理（ASM）解决方案旨在采用主动安全管理方法识别和管理风险，而DiD则主要采用
分层控制机制防范威胁。如NIST 800-53指南中所述，这些解决方案互为补充，该指南将攻击
面减少描述为“与威胁和漏洞分析及系统架构和设计保持一致，减少攻击面是一种降低组织风
险的有效方法，可令攻击者减少利用系统、系统组件和系统服务中的薄弱环节或缺陷（即潜在
漏洞）的机会。”鉴于此，建议将分层防御机制作为组织整体安全架构的组成部分，同时采
用“最低权限”方法管理网络访问。

攻击面管理（ASM）日渐受到OT安全管理者的欢迎，其功能包括资产发现、风险评估和威胁修复。此外，还应基于不法分子针对工业领域独有战术、技术和程序（TTP）的深入研究，部署特定于 OT环境的响应方案。

构建牢不可破的 OT 安全态势，要求技术控制解决方案具备联动能力。部署在 DiD 框架中的防火墙、入侵检测系统（IDS）、防病毒和访问控制解决方案应支持无缝集成和数据交换，从而实现安全流程和工作流的协同联动，以加速威胁检测和事件响应。此外，还应具备支持ASM的组件，赋能OT安全管理者实现统一的自动化安全运营。

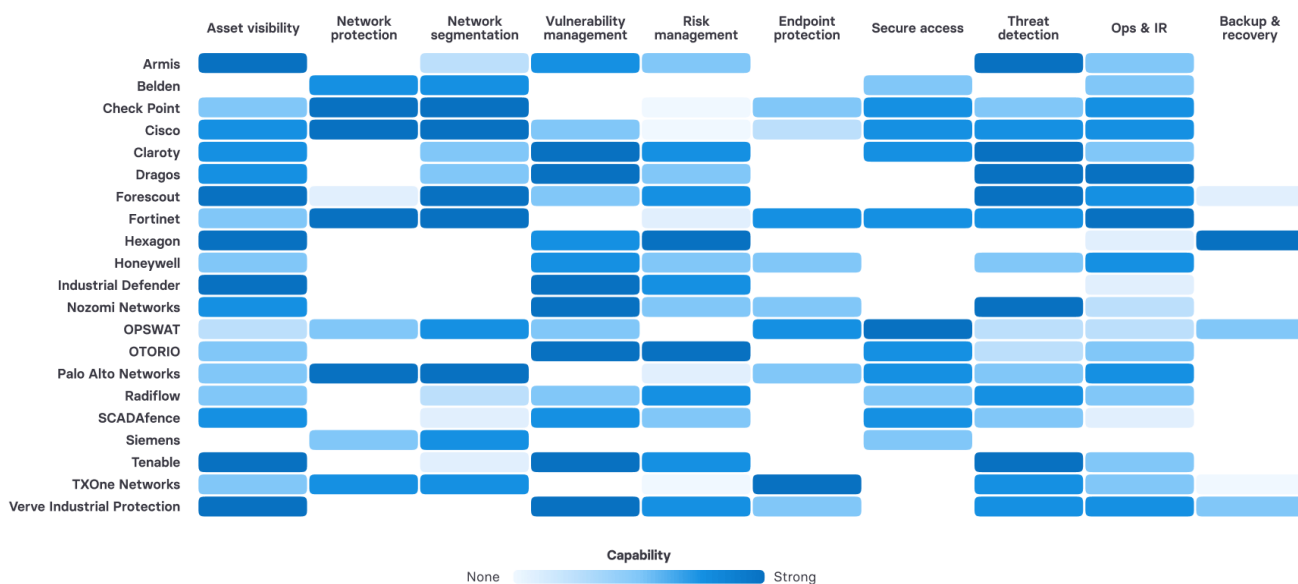
安全供应商筛选

当前，市面上没有一家供应商可提供涵盖所有安全控制技术的原生功能。因此，计划开展全新安全计划、整合供应商或更新安全计划的 OT 安全管理者，应首先寻求集成式平台方法，确保不同供应商解决方案之间实现无缝集成。采用单一平台的一大优势在于，可将集成负担转移至平台供应商。平台供应商负责确保其产品支持互操作性，从而减轻资产所有者的技术设计压力。

网络生态系统通常由两大类供应商组成。OT网络保护供应商通常提供防火墙产品，涵盖众多工业协议，以及从端点防护解决方案到安全运营中心即服务（SOCaaS）等一系列附加服务或功能。主要用例包括网络保护、网络分段和访问管理，部分厂商还可提供可见性解决方案。多数供应商还拥有强大的IT安全平台，使工业企业具备单独管理IT和OT安全运营的能力，或将二者合而为一，采用单一操作系统进行统一管理。

资产可见性和威胁管理供应商则提供由 OT 特定威胁情报支持的可见性、漏洞管理和威胁检测功能。这些供应商通常为OT环境中的 ASM提供安全产品。而且不同供应商往往拥有独特的产品优势，如部署类型、托管服务或功能（远程访问管理和事件响应等）。

OT安全行业分析和战略公司威士兰咨询（Westlands Advisory，下文简称WA）针对OT网络安全行业开展的最新分析显示，以下供应商均支持平台解决方案和集成功能。该调查结果为安全管理者筛选安全供应商提供了可靠参考。



筛选供应商时，OT安全管理者还应考虑其战略发展动向。WA分析师指出，过去18个月间，随着安全行业的竞争加剧，业内厂商争先发布重大创新，一些供应商的技术路线图无疑具备强劲竞争优势，包括平台可用性优化、全新集成功能、风险分析优化及全新OT用例支持。

简介：Fortinet



Fortinet 是一家总部位于美国加利福尼亚州桑尼维尔市的上市企业。作为业内领先的网络安全和组网供应商，旗下拥有50 多种支持广泛集成的企业级产品组合，可满足多种安全和组网用例需求。Fortinet 目前增长势头强劲，全球用户数超 66万，2022财年账单收入达 56亿美元（约合402亿元人民币）。

摘要

Fortinet始终秉持锐意创新理念，持续保持高比例研发投入，目前专利持有数量多达1,285项。得益于全球研发中心和卓越中心网络的支持，以及近期在日本相关领域的投资，Fortinet持续稳居工业和关键基础设施领域IT和OT网络安全解决方案领先提供商，全球用户群庞大且遍及所有工业垂直领域。

2023 年，Fortinet 的首要任务是力争成为网络防火墙、SD-WAN 和 OT 安全领域首屈一指的安全厂商。鉴于Fortinet 对其产品、员工及销售和营销业务的持续投资，OT业务超市场平均增长水平，增长势头强劲。

Fortinet OT Aware Security Fabric 无缝整合安全组网、零信任访问和自动化安全运营等一系列广泛的安全组件，并由囊括OT 专用 FortiGuard 威胁情报共享服务、超 3,000 个 OT 应用程序签名以及超 600 条 OT 威胁签名的安全服务提供强劲支持。

Fortinet 原生产品通过技术联盟生态系统合作伙伴提供增值解决方案，有力支持多数 OT 网络安全用例，为用户提供端到端网络安全平台，全方位满足IEC-62443、NIST CSF、针对工业控制系统的ATT&CK知识库（ATT&CK for ICS）及其他相关标准要求。

定位

OT战略旨在有效应对不断增加的云连接保护、确保远程安全访问、实现IT/OT融合安全运营，以及有效管理威胁和漏洞等快速兴起的用户挑战。凭借全面囊括威胁和漏洞管理供应商、Fabric-Ready OEM合作伙伴以及业内领先系统集成商的OT Aware Security Fabric架构，Fortinet助力用户轻松应对上述挑战。

Fortinet 产品的突出优势在于，能够从传感器至云端跨整个普渡模型为用户提供安全解决方案。Fortinet 解决方案易于部署、使用和扩展等优势，已获得众多行业合作伙伴和用户的普遍认可。

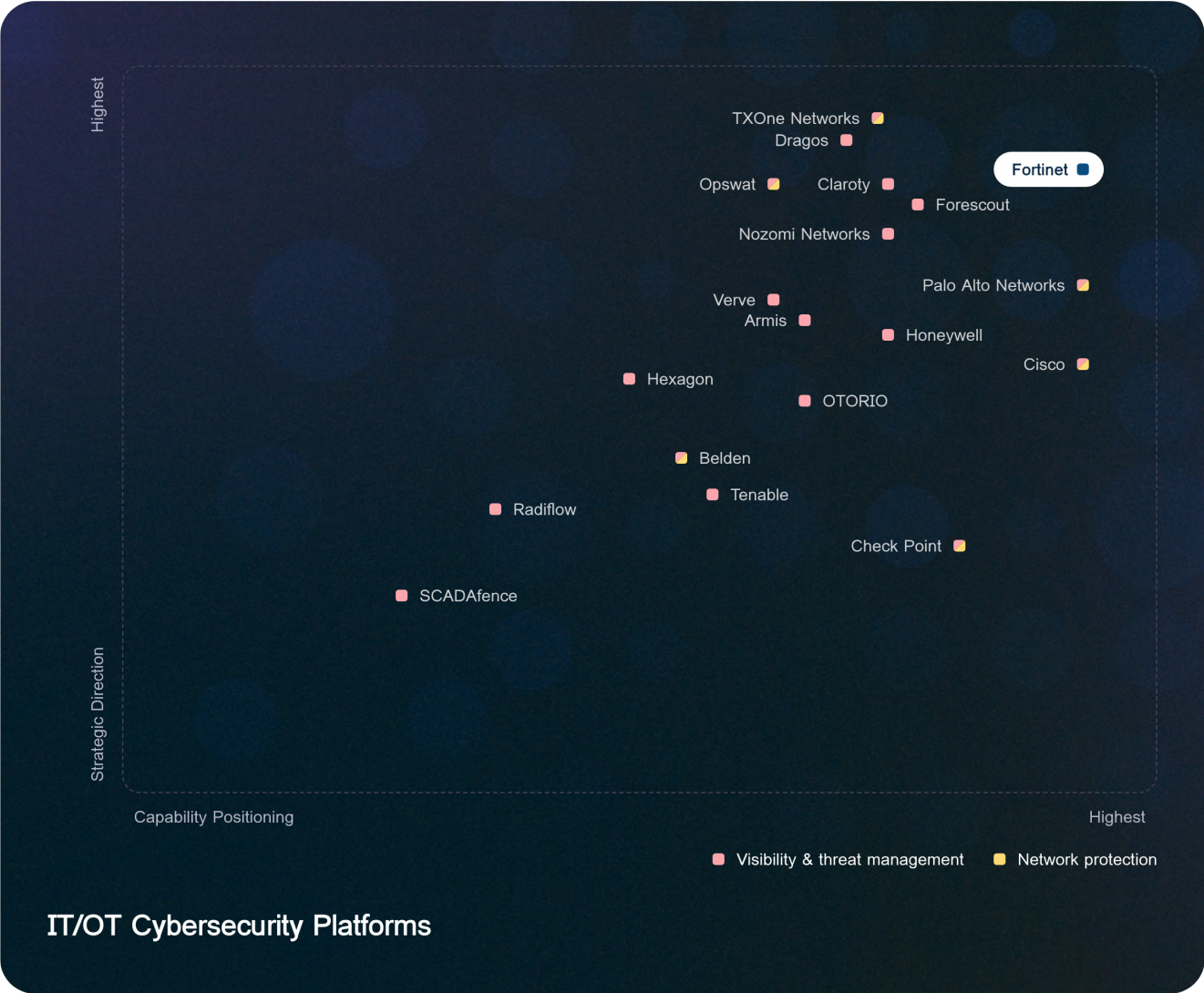
Fortinet 始终践行 OT 网络安全承诺，持续投资旗下安全产品。过去 3 年间，旗下产品组合数量显著增长，近期发布了安全远程访问管理（FortiPAM）、资产和网络可见性解决方案 FortiOS OT View 等支持全新用例的新产品及服务。其他新增功能和服务还包括经优化的可视化和报告功能，以及一些有效应对MITRE ATT&CK for ICS各阶段战术和策略的关键产品和服务。

未来，Fortinet将持续扩展产品组合，如将FortiNDR集成至OT Aware Security Fabric以优化合规性管理，还包括近期发布的全新产品和服务：FortiPolicy（网络微分段产品）和 FortiRecon（数字风险保护服务）。此外，Fortinet 专注于成为 OT 安全领域首屈一指的供应商，持续扩展专家支持团队、加强体验中心建设并广泛推广网络安全意识培训课程，以提高用户投资价值，提升产品体验。

显著优势

- 全球领先的网络安全企业
- 广泛、集成的安全解决方案组合
- 网络安全和组网创新技术
- 大型合作伙伴生态系统
- 不断增长的OT网络安全市场占有率

IT/OT 网络安全平台



IT/OT网络安全平台均搭载多款原生产品组件，且支持与其他产品或平台无缝集成，为用户提供支持单一控制台的全局运营视图。

定义

目前该领域市场主要涉及两类供应商：一类供应商提供可见性和威胁管理功能，另一类提供功能强大的网络防护产品组合。安全管理者通常为每个应用类别至少选择一个供应商。然而行业竞争异常激烈，各大厂商均不断扩展其产品功能，可同时提供可见性和威胁管理及网络保护解决方案的厂商日益增加。

详情请参阅 WA 洞察报告《工业网络安全行业分析》，了解更多该市场和行业趋势深入洞察。

评估

IT/OT 网络安全平台评估主要涉及以下技术：

- 资产可见性
- 网络保护
- 网络分段
- 漏洞管理
- 风险管理
- 端点防护
- 安全访问
- 威胁检测
- 安全运营与事件响应
- 容灾备份与恢复

资格

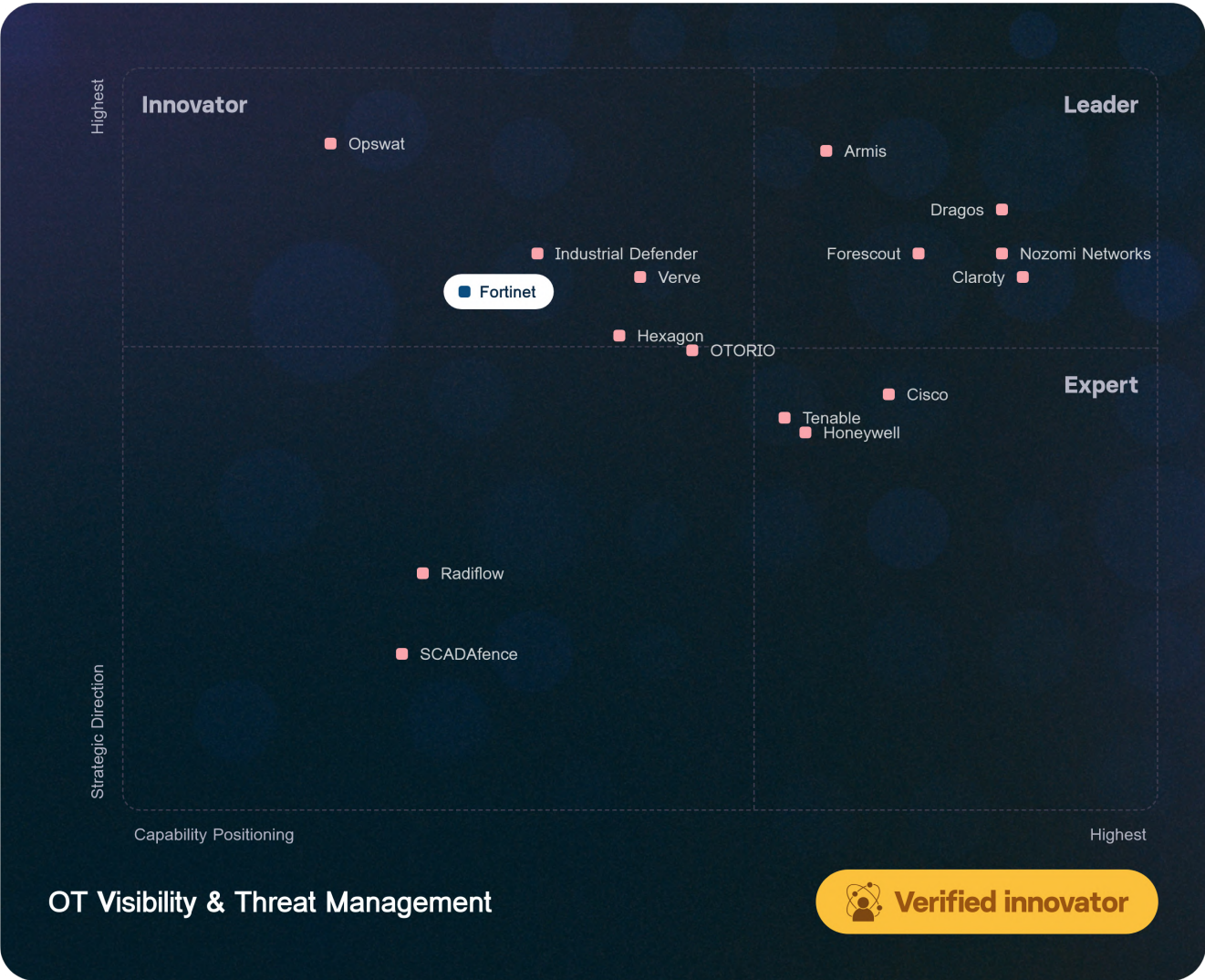
竞争企业需满足以下标准，才有资格被纳入WA的IT/OT Cybersecurity Platform Navigator 进行评估：

- 该公司拥有至少 4 项技术类别的原生解决方案。
- 相关产品支持集成至单一集中式管理平台。
- 该平台可从其他平台或源汇集并整合威胁信息以丰富事件数据。
- 该平台具备复杂的集中管理功能，可为分析师提供全面的分析和报告，以监控和管理安全运营。
- 该平台具备安全信息和事件管理（SIEM）功能或支持与安全编排自动化与响应（SOAR）平台无缝集成。
- 该公司在全球范围内覆盖多个地理区域，覆盖范围广阔

方法论

登录WA官网 <https://navigator.westlandsadvisory.com>，了解更多WA方法论信息。

OT 可见性与威胁管理



可见性和威胁管理平台涵盖资产和网络发现、威胁情境化、漏洞管理和威胁检测等功能。该平台通常支持与其他安全平台或安全信息和事件管理（SIEM）解决方案集成。

定义

该领域市场主要由一系列采用不同解决方案的供应商组成，如使用基于代理发现的单一可见性和资产管理企业，使用被动扫描等技术的威胁检测公司，以及通过防火墙或嵌入式交换机提供可见性和威胁检测功能的网络供应商。详情请参阅WA 洞察报告《工业网络安全行业分析》，了解更多该市场和行业趋势深入洞察。

评估

可见性和威胁管理平台评估主要涉及以下技术：

- 资产可见性，包括主动扫描和基于代理的资产发现。
- 漏洞管理。
- 风险管理，包括风险量化、配置管理和合规性管理。
- 威胁检测，包括机器学习、用户和实体行为分析（UEBA）及威胁签名。

资格

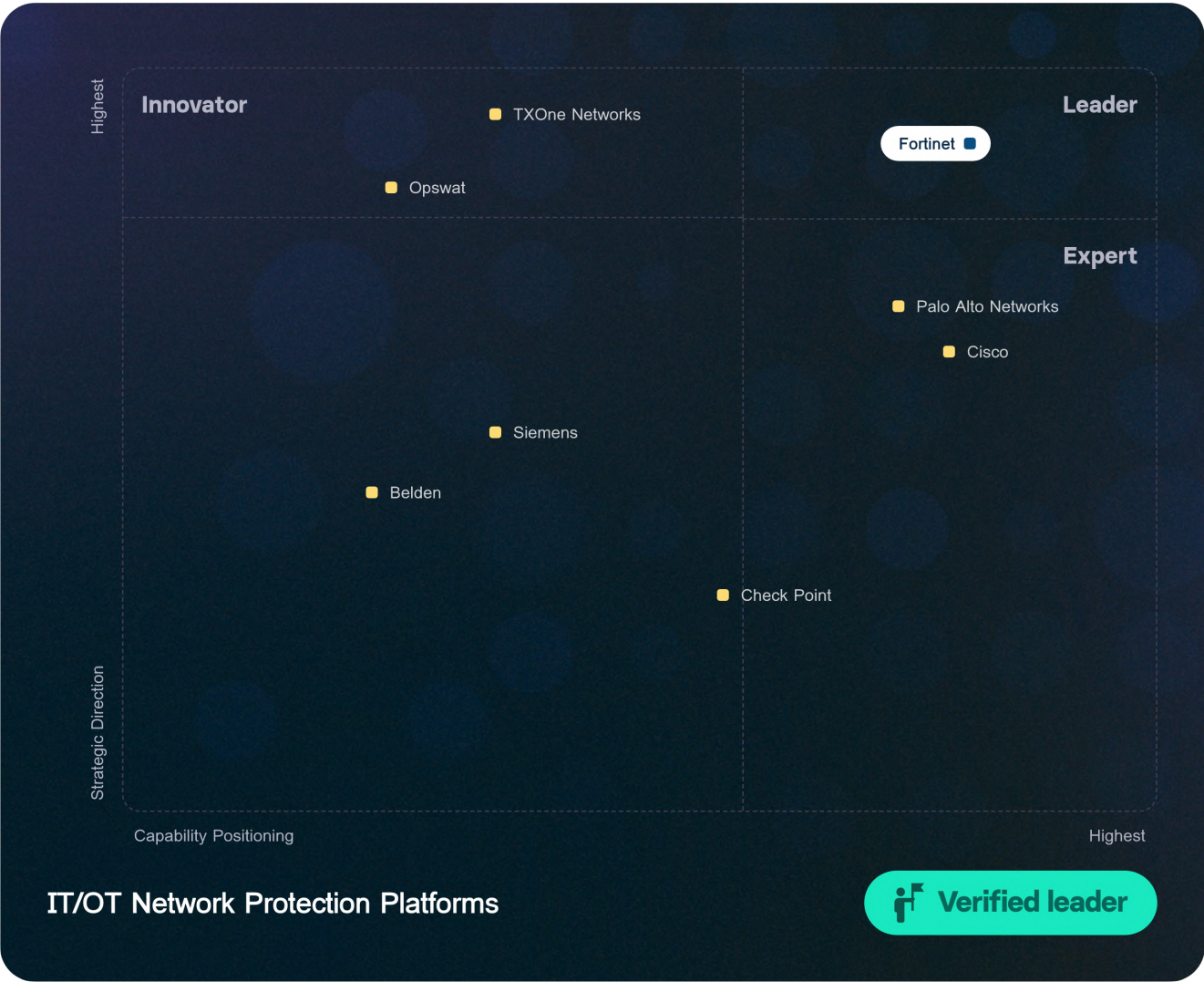
竞争企业需满足以下标准，才有资格被纳入WA的 IT/OT Visibility & Threat Management Navigator 中进行评估：

- 该企业应能提供支持资产可见性和威胁检测的原生解决方案。
- 相关产品支持集成至单一集中式管理平台。
- 该平台支持从其他平台或源汇集并整合威胁信息，以丰富数据并提供威胁上下文。
- 该平台具备复杂的集中管理功能，可为分析师提供全面的分析和报告，以监控和管理安全运营。
- 该平台具备安全信息和事件管理（SIEM）功能或支持与安全编排自动化与响应（SOAR）平台无缝集成。
- 该公司在全球范围内覆盖多个地理区域，覆盖范围广阔

方法论

登录WA官网 <https://navigator.westlandsadvisory.com>，了解更多WA方法论信息。

IT/OT 网络防护平台



OT 网络防护平台是纵深防御机制不可或缺的重要组成部分，通过网络监控和策略执行提供网络边界安全防护。

定义

网络防护平台应具备多种原生功能，如防火墙和访问控制。支持用例应涵盖网络可见性、网络分段、零信任策略执行和事件响应。多数网络防护平台还支持其他原生技术控制功能（如端点防护）或与第三方工具无缝集成。该平台支持集成组件的协同联动，并提供对OT网络安全操作的集中可见性和控制能力。

详情请参阅 WA 洞察报告《工业网络安全行业分析》，了解更多该市场和行业趋势的深入洞察。

评估

网络防护平台评估主要涉及以下功能：

- 网络防护，包括防火墙、入侵防御系统（IPS）、单向网关和数据二极管。
- 网络分段，包括防火墙、虚拟局域网（VLAN）、访问控制列表（ACL）、软件定义网络（SDN），以及对资产和设备进行识别和逻辑分组的无代理微分段。
- 端防护，包括恶意软件扫描、应用程序白名单和补丁管理以及 USB 防护。
- 安全访问，包括特权账号管理（PAM）、虚拟专用网（VPN）和零信任网络访问（ZTNA）。
- 安全运营和事件响应，包括安全信息和事件管理（SIEM）、安全编排自动化与响应（SOAR）、扩展检测和响应（XDR）、端点检测和响应（EDR）以及Playbook。

资格

竞争企业需满足以下标准，才有资格被纳入 WA 的 IT/OT Network Protection Platform Navigator进行评估：

- 该企业应能提供OT网络防护原生解决方案，且具备下一代防火墙（NGFW）、入侵防御系统（IPS）和数据二极管等全部或其中一项功能。
- 相关产品支持与其他网络防护产品（如访问管理）无缝集成至单一集中式管理平台。
- 该平台支持从其他平台或源汇集并整合威胁信息，以丰富事件数据并提供威胁上下文。
- 该平台具备复杂的集中管理功能，可为分析师提供全面的分析和报告，以监控和管理安全运营。
- 该平台具备 安全信息和事件管理（SIEM）功能或支持与安全编排自动化与响应（SOAR）平台无缝集成。
- 该公司在全球范围内覆盖多个地理区域，覆盖范围广阔

方法论

登录WA官网 <https://navigator.westlandsadvisory.com>，了解更多WA方法论信息。

总结

OT网络通常存在数据丰富和信息匮乏两大特点，深化数据利用无疑将挖掘更多优势和潜能。为实现数字化转型加速，资产所有者应具备资产和网络的全面可见性，同时有效管理海量数据和告警。这一趋势势必推动安全产品的迭代更新，使其能够准确识别资产，同时实现风险和漏洞管理的分类、剖析和自动化。目前，资产发现和漏洞管理属于高增长产品领域，可高效应对众多“已察觉的已知”运营风险。除了防火墙和网络分段、访问管理和端点防护技术外，这些控制功能还可提供强大的保护措施。

法规和标准对“未知风险”防护覆盖的监管作用日益突出，要求企业通过被动或主动扫描进行持续监控，以实时检测风险，一旦偏离基线及时发出告警。为有效防范未知风险，资产所有者应构建基于弹性运营的安全模型，重点关注人员、技术和流程，确保组织能够承受网络事件风险并从事件中快速恢复，并将对运营的负面影响降至最低。部署ASF（Aware Security Fabric）是提前响应威胁的关键，有迹可循的事件响应流程有助于实现协同、及时和有效的威胁响应。

WA 预计到 2030 年，公用事业和大型跨国制造组织的 OT 网络安全成熟度将出现大幅提升。许多组织将构建融合型安全运营体系，具备企业整体可见性，且专门的OT团队均受过流程和程序方面的专业培训。安全性将逐渐通过云平台由资产所有者或托管服务提供商进行管理，无线 5G网络的管理和保护将备受关注。此外，WA还预计供应链网络安全成熟度等级将逐步提升，基于安全设计原则的工业运营基础设施安装数量将持续扩大。安全管理者应择优选择拥有先进解决方案的合作伙伴，以满足当前和未来的行业发展需求。