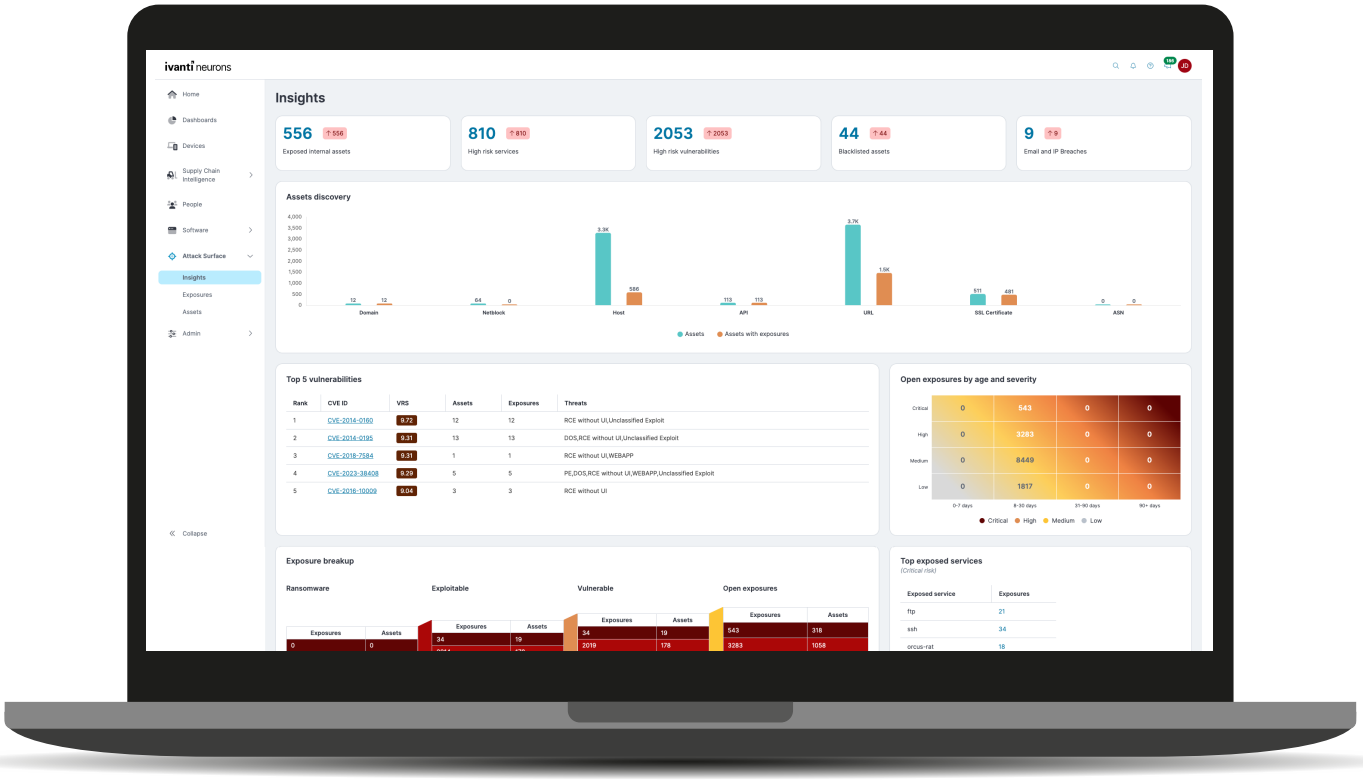
Ivanti Neurons for EASM

通过全面掌握面向外部的资产和实用的风险情报来应对攻击面的扩大

Everywhere Work 的日益普及和持续的数字化转型导致攻击面不受控制地扩大。Ivanti Neurons for External Attack Surface Management (EASM) 让您能全面持续洞察攻击面上针对互联网的资产及相关暴露风险。凭借这些情报，您就可以消除高风险漏洞，主动防御网络攻击。



不受控制的攻击面扩大

向 Everywhere Work 的过渡以及数字化转型的持续推进加速了影子 IT 和云端工具的使用。与此同时，组织越来越多地采用物联网设备，并且供应链的联网程度也越来越高。

安全团队越来越难以掌控自身攻击面上那些面向外部的资产。他们也因此缺乏对与这些资产相关的风险漏洞的了解。

未知、未经审查、未经管理和未打补丁的资产使组织面临数据泄露、罚款和停机的风险。安全团队需要持续了解整个攻击面，以妥善地保护其组织。

Ivanti Neurons for EASM

借助 Ivanti Neurons for EASM，获得并维护组织攻击面中每个面向外部的资产的可见性。利用基于风险的实用情报来了解影响这些资产的风险，主动防范数据泄露、罚款和停机。

主要功能

实现全面可见性

洞见每个面向互联网的资产以及整个组织攻击面的相关风险漏洞。代理监控可以发现传统发现工具检测不到的资产，以及通常不被安全团队监控的资产——例如配置错误的 Amazon S3 存储桶、被忽视的 QA 和开发环境、运行在大家都认为已退役的服务器上的那些被遗忘的营销网站以及 Java 应用。

持续监控可确保这些资产的近实时可见性，因此您可以立即知道现有资产何时存在暴露风险，或新资产何时部署，并可以做出相应对策。

工作区功能允许按类别（例如部门和子公司）对资产和风险漏洞进行分组。事实证明 Ivanti Neurons for EASM 也有助于监控第三方组织（例如供应链合作伙伴）存在的外部攻击面。

EASM 发现的资产类型	EASM 发现的漏洞攻击向量
■ API	■ 应用安全性
■ 域	■ 数据泄露
■ 主机	■ DNS 状况
■ 网区	■ 电子邮件安全性
■ SSL 证书	■ 网络安全性
■ 网址	■ 补丁节奏
	■ 社会工程

对高风险漏洞进行排序

利用有关外部攻击面风险漏洞情况的实用情报来确定在何处开展修复工作。情报包括 Ivanti Neurons for EASM 发现的每个 CVE 的漏洞风险评分 (VRS)。

VRS 使安全团队能够量化漏洞带来的风险并了解其威胁背景，从而制定明智的决策。它考量来自国家漏洞数据库 (NVD) 的 CVSS 分数以及反映既定环境下漏洞影响力的一系列其他属性。

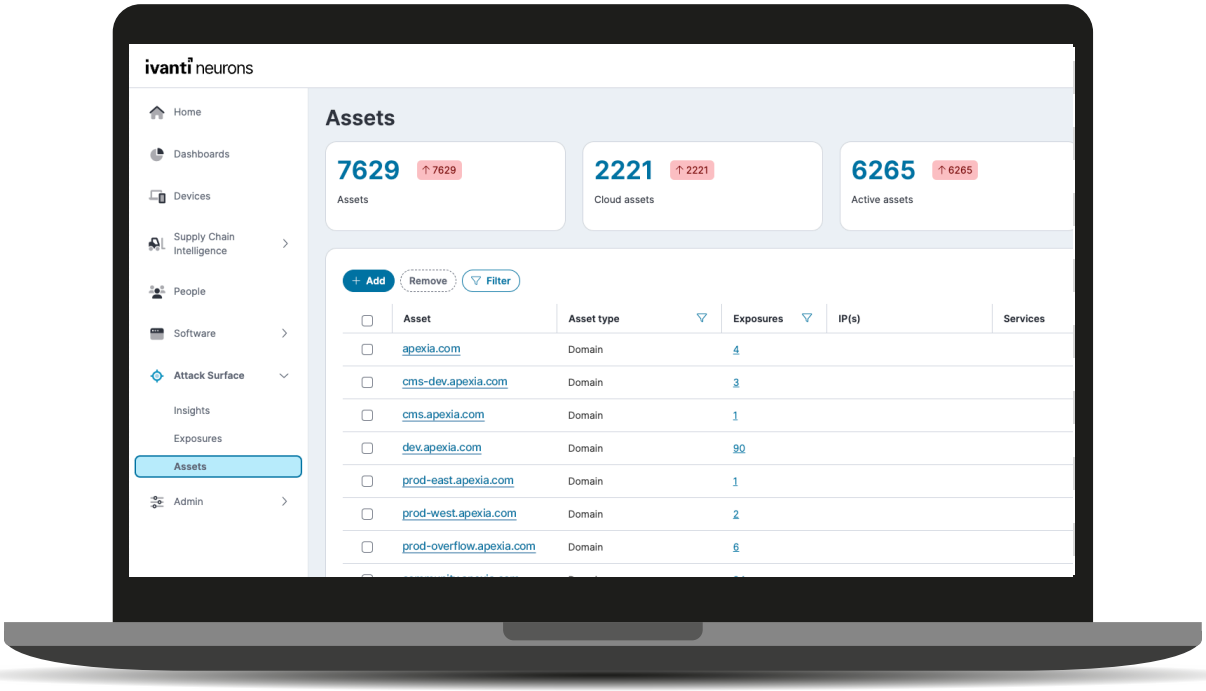
风险报告

满足高级别安全领域利益相关者的报告要求，并通过 PDF 报告帮助对潜在收购、合作伙伴和供应商进行尽职调查。这些可导出的报告全面梳理和盘点与组织外部攻击面相关的风险漏洞。

解决攻击面缺口

利用 Ivanti Neurons 的强大功能来弥补 Ivanti Neurons for EASM 所发现的重大攻击面缺口。将 Ivanti Neurons for EASM 与以下产品结合使用，从而能够最快速地应对那些影响对外资产的问题：

- Ivanti Neurons for ITSM：协调整个团队对问题的响应。
- Ivanti Neurons for UEM：管理和保护端点。
- Ivanti Neurons for Patch Management: 修复漏洞。



广泛的 EASM 用例

EASM 解决了现代企业面临的一系列挑战。

- **发现和清点数字资产:** 在云、IT、物联网和 OT 环境中查找并清点来自网站、IP、域名、SSL 证书和云服务的面向互联网的资产。
- **分析风险并确定其优先级:** 对影响面向外部的资产的风险（从未修补的漏洞到错误配置和开放端口）修复工作进行排序。
- **遏制云蔓延和影子 IT:** 识别各个云提供商的公共资产，包括员工在适当渠道之外创建的云实例。
- **检测数据泄露:** 监控经由内部和第三方使用的协作工具和云应用发生的敏感数据泄漏或暴露风险。
- **执行风险评估以审查子公司、第三方和收购目标:** 在将系统与其他实体集成之前执行全面的安全检查。
- **减少网络钓鱼和社会工程攻击:** 监控网络钓鱼域、识别欺骗网站并检测针对员工和客户的潜在社会工程攻击。
- **遵守监管合规要求**: 遵照 GDPR、HIPAA 和 PCI DSS 等法规的要求开展资产发现和清点工作。

关于 Ivanti

Ivanti 完善并保护 Everywhere Work，从而使员工和公司都能够实现蓬勃发展。我们让技术为人们服务，而不是相反。如今员工使用各类公司和个人设备通过多种网络访问 IT 应用和数据，以便无论他们身在何处以何种方式工作，都能够保持工作效率。Ivanti 是为数不多的能够发现、管理和保护组织中每一处 IT 资产和端点的科技公司之一。有超过 40,000 家客户（包括财富 100 强企业中的 88 家）选择 Ivanti 来帮助他们提供卓越的数字化员工体验，并提高 IT 和安全团队的生产力和效率。在 Ivanti，我们努力营造一个倾听、尊重和重视所有观点的环境，我们致力于为客户、合作伙伴、员工和地球创造更可持续的未来。更多信息请访问www.ivanti.com.cn。

ivanti

如需更多信息或与 Ivanti 取得联系，请访问 ivanti.com.cn

1. Forrester，“The External Attack Surface Management Landscape, Q1 2023”，2023 年 1 月 9 日