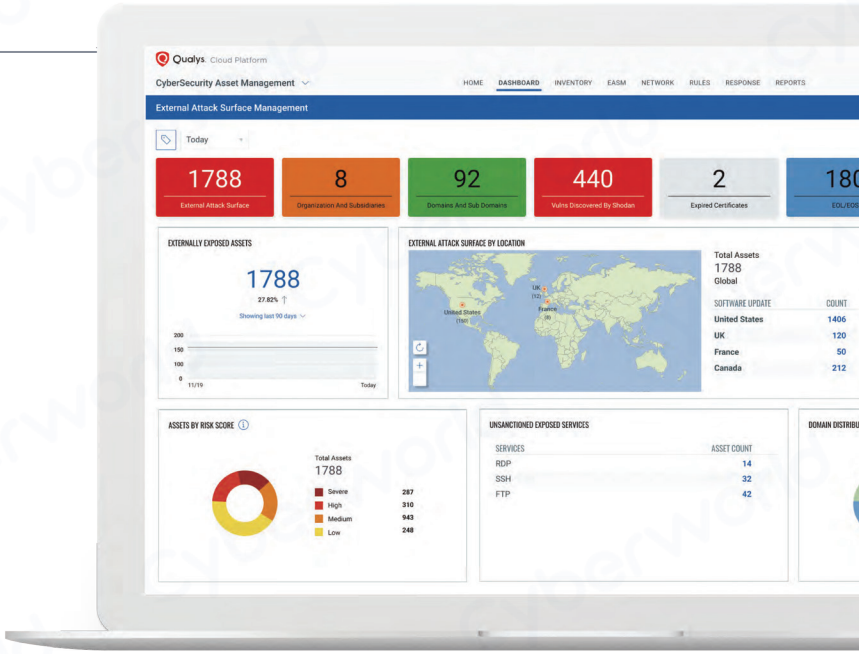
Qualys

Cyberworld

网络安全资产管理 (CSAM) 2.0

具有外部攻击面管理功能

CSAM



以攻击者的视角
看待自己的攻击面

攻击面正在以指数级速度扩大，为攻击者提供了新的攻击目标。超过30%的本地和云端的资产、服务没有清点。对于网络安全而言，这是一个巨大的可视化差距。

CSAM是一项云服务。它能在攻击者行动之前，持续地发现、分类、修复、显著改善其内部和外部 IT 资产的网络安全状况，并且使用与攻击者相同的可行性情报。它可以发现所有已知和以前未知的面向互联网的资产，实现 100% 可视化并改进网络风险管理。

Qualys CSAM 2.0 具有外部攻击面管理功能，它增加了"纵深防御"，以更新企业网络安全态势。它通过红队式资产和漏洞管理解决方案，实现 360 度全方位覆盖，持续地发现和分类以前未知的资产。

主要特点

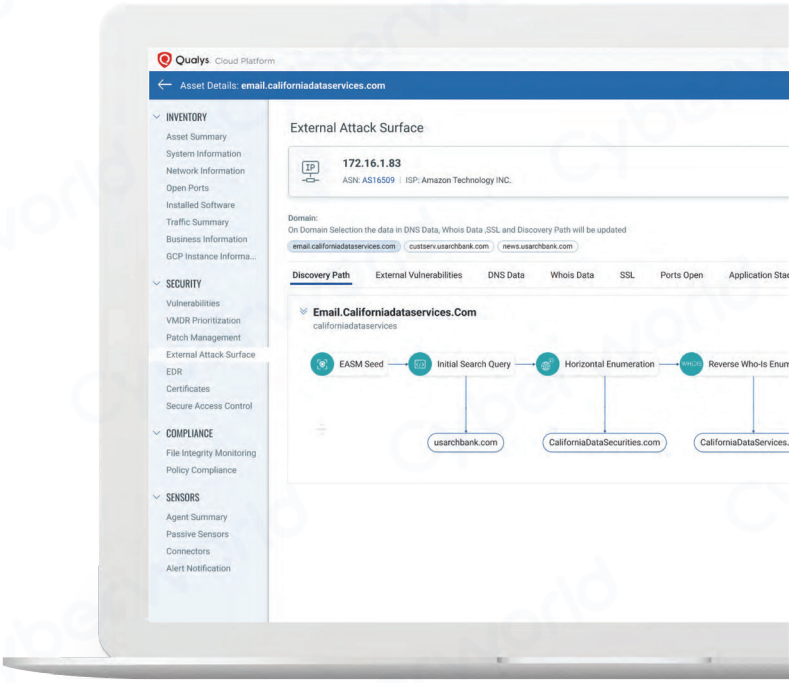
专为安全而构建并与 IT 集成的资产管理

360 度全方位了解整个 IT 生态系统

通过持续发现本地、云端、OT 和 IoT 的所有资产，了解攻击者对您的生态系统的看法。CSAM使用先进的凭证和非凭证扫描技术，持续且快速地发现漏洞，对其进行分类和修复。它会自动查找已知和以前未知的资产，范围从实例和容器到存储库和设备以及域和子域、连接的子公司和业务合作伙伴，以全面了解潜在的风险向量。

与 ServiceNow 集成

CSAM 提供丰富的 ServiceNow CMDB 双向集成，可持续更新资产视图。它通过 Service Graph Connector Program 认证，利用 CMDB 业务上下文数据（如资产重要性和数据所有者）丰富了 Qualys 资产。



检测和监察安全漏洞

CSAM 可轻松识别有风险的资产。它会自动将资产重要性评分分配给标签以及具有上下文扩充数据的相应资产。此上下文可以实时分析威胁和错误配置，准确度为六西格玛。该服务持续检测全局混合环境中可远程利用的漏洞和严重错误配置，例如EOL、EOS、未经授权或缺失的Title。CSAM 还可以发现缺少的所需软件，并提供有关零日漏洞、受损资产和网络异常的实时警报。

使用 VMDR 2.0 进行编排

自动部署最相关、正确且可替代的补丁，从而快速修复任何规模环境中的漏洞和威胁。CSAM 会自动隔离可疑设备，直到可以对其进行调查为止。作为 Qualys TruRisk 企业平台的一部分，该服务持续提供集成的端点检测和响应、漏洞和补丁管理以及策略合规性。

优点

从攻击者的角度看待整个 IT 生态系统

- 获得对整个内部和外部攻击面的可行性情报、可视化和见解。
- 发现企业、子公司和业务合作伙伴中的域、子域和证书，全面了解可远程利用的漏洞，包括通过归属发现以前未知的设备。
- 暴露"影子IT"和基准差异，包括虚拟机、容器、FaaS 和 IoT，其运行速度比 IT 使用传统工具跟踪的速度快。
- 从外到内了解面向互联网的资产，以发现安全端点盲点。
- 通过符合 CISA 标准的 EOL 和 EOS 软件跟踪以及 Ling 软件版本控制来跟踪操作系统状态和相关漏洞，减少技术债务。

通过量化风险管理寻找安全漏洞

- 标记资产以便轻松分组。
- 启用风险管理。
- 以攻击者的方式执行任务。
- 启用业务影响分析（BIA）。

通过 ServiceNow 集成接收所有资产的完整上下文

- 与 ServiceNow 持续同步。
- 添加上下文，实现以安全为中心的资产可视化。
- 将安全上下文和业务上下文添加到资产清单中。

按业务和技术上下文将风险状况分配给资产

- 用户可选地选择标签上的重要性分数，然后将其应用于一个或多个资产。
- 资产属性在分配的资产标签中，被分配最高的重要性分数。
- 如果从 CMDB 提提取数据，资产重要性分数就会自动分配给标签和相应的资产。

快速识别盲点

- 主动跟踪授权和未授权的软件。
- 根据资产类型、位置、重要性和使用情况，自动管理多个软件列表。
- 跟踪详细的资产信息，以标记配置问题、安全风险、IT 策略违规和不合规情况。

使用 VMDR 协调自动警报、报告和响应

- 对已识别的安全风险发出警报、报告和响应。
- 自动记录 PCI DSS、FedRAMP、NIST、ISO 和其他政策的合规性。
- 利用集成的 Qualys TruRisk 企业平台，超越传统的外部攻击面管理。

由 **Qualys TruRisk 企业平台**提供支持
为 Qualys IT 安全性和合规性云服务提供支持的创新架构

单一管理平台界面

只需几秒钟即可在一处查看结果。安全与合规专业人员或经理使用AssetView，可以从单个仪表板界面获得完整且持续更新的 IT 资产视图。它是完全可自定义的，能让您了解全局，深入了解细节，并为安全团队成员或审核员生成报告。直观且易于构建的动态仪表板将来自所有 Qualys Cloud App 的全部 IT 安全性和合规性数据聚合，并关联到一处。借助其强大的弹性搜索集群，您只需花2秒时间，即可搜索到任何资产，包括在本地、端点、公有云和私有云的资产。

集中化和定制化

集中发现主机资产以进行多种类型的评估。组织主机资产组以匹配您的业务结构。Qualys 端到端加密和强大的访问控制可以确保安全数据的机密性。您可以通过企业单点登录 (SSO) 集中管理用户对其 Qualys 帐户的访问。Qualys 支持基于 SAML 2.0 的身份服务提供商。

轻松部署

从公有云或私有云进行部署，由Qualys完全管理。使用 Qualys，无需配置服务器，无需安装软件，也无需维护数据库。您始终可以通过浏览器使用最新的Qualys功能，无需设置特殊的客户端软件或 VPN 连接。

可规模化和可扩展

按需在全局范围内扩展。通过基于XML的可扩展API与其他系统集成。您可以将Qualys与广泛的安全性、合规性系统结合使用，例如 GRC、工单管理系统、SIEM、ERM 和 IDS。