

持续地评估、确定优先级并修复混合攻击面的暴露情况

获得更深入的见解

- + 聚合安全技术、数字资产和基础设施的数据，以获得完整可视化。
- + 动态安全模型提供攻击面视图，评估安全控制。
- + 了解暴露风险，确定漏洞的优先级并采取最佳的修复措施。

做出更明智的决定

- + 随时拥有最新的漏洞和威胁暴露整体视图。
- + 无与伦比的威胁情报为行动提供依据。
- + 自动地修复漏洞，提高安全效率。

增强业务弹性

- + 在错误发生之前验证变更。
- + 在暴露成为威胁之前了解它们。
- + 随着新法规的颁布，不断满足合规性。

最大限度地利用资源

- + 根据优先级，首先降低最大的风险
- + 提高决策的速度和准确性。
- + 将稀缺的技术资源集中在处理对业务构成最大风险的漏洞上。

Skybox 持续性暴露管理平台

Skybox持续地评估、确定优先级并修复混合攻击面中最大的网络暴露风险。Skybox持续性暴露管理平台由攻击面管理、漏洞管理和安全策略管理解决方案组成。这三个解决方案都构建在单一动态安全模型上，可全面地了解您的攻击面。

使用Skybox，您可以创建一致的、企业范围内的暴露管理计划。Skybox持续地映射出所有攻击面，将结果置于上下文中，评估漏洞，确定其优先级，自动地采取修复措施来应对威胁。

- + 提供包含威胁情报和风险数据的 360 度混合攻击面视图。
- + Skybox应对动态变化攻击面的能力始终处于业界领先地位。
- + 获取您所需要的上下文，从而更好更快地解决网络安全问题。
- + 优先处理最大的暴露风险，实现安全效率最大化。
- + 微调网络安全策略，确定防御的优先级。
- + 简化并自动化跨混合攻击面的合规性评估。

Skybox 使企业能够实现持续威胁暴露管理。



在一个平台中，统一且持续地管理威胁暴露

攻击面管理

提供攻击面视图，发现和厘清所有资产，包括网络设备、应用程序和用户身份等。

- + 识别可通过互联网访问的资产，帮助检测风险、确定其优先级和对抗有针对性的攻击。
- + 使用攻击路径分析和模拟功能，发现潜在攻击者可能利用危害整个网络中暴露资产的精确路径。
- + 分析路径上的每个步骤，包括漏洞、防火墙设备、配置和可能导致攻击的规则，从而在攻击发生之前预测和抵御攻击。

漏洞管理

利用一系列第三方威胁情报源和Skybox威胁情报来丰富您的攻击面视图，并提供漏洞和威胁暴露的整体视图。

- + 根据严重性、重要性、可利用性和网络暴露等多种因素评估暴露风险，并确定其优先级，使您能够将资源集中在风险最高的漏洞上。
- + 除了识别和评估漏洞，还为每个漏洞提供主动的、自动的修复建议和控制。
- + 通过ITSM系统集成来自动响应。即使没有立即打补丁，Skybox也能提供有效的风险缓解替代方案。

安全策略管理

利用集中式安全策略管理，深入了解您的网络，分析配置、路径和访问。在保持合规性的同时，增强网络安全性。

- + 确保严格遵守正确的网络分区，弥合官方网络分段策略与混合网络中实际实施之间可能存在的任何差距。
- + 识别和消除隐藏的或冗余的防火墙规则，集中式界面管理众多防火墙，从而优化性能。
- + 自动执行防火墙变更，并在配置新规则之前进行风险评估。轻松地重新认证防火墙规则，并生成对合规审计至关重要的报告。

使用 Skybox 持续性暴露管理平台，可增强网络安全性，能应对不断变化的威胁。并且，体验无与伦比的可视化、主动漏洞管理以及精简的网络安全策略管理。让您对关键资产的保护之旅充满信心。

关于 Skybox Security

全球500多家注重网络安全的大型企业依靠Skybox获得所需的见解和保障，以降低风险。Skybox 应对动态变化攻击面的能力始终处于业界领先地位。

Cyberworld
广州科明大同科技有限公司

**中国区
总代理**

官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

 **SKYBOX**
SECURITY