

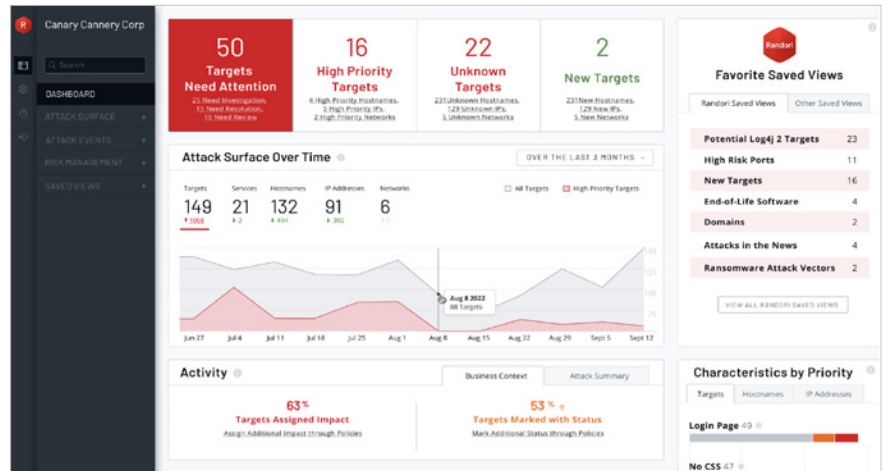
IBM Security Randori Recon: 攻击面管理

像攻击者一样查看攻击面

要想知道攻击者将攻击哪里，您首先需要知道他们如何查看您的攻击面。IBM® Security Randori Recon 从攻击者的视角持续进行资产发现问题和优先级划分。

随着云迁移、影子 IT 和并购 (M&A) 等新态势的出现，企业的外围情况始终在不断变化。这些变化说明这里存在攻击机会的窗口。利用 Randori Recon 发现攻击窗口——无需安装或配置。

Randori Recon 就如同真实攻击者一样持续监视企业的外部攻击面，发现那些容易被遗漏的盲点、错误配置和进程故障。Randori 采用一种类似黑匣子的方法来找到他人未曾发现的互联网协议版本 6 (IPv6) 和云资产。



“Randori 改变了我与执行团队之间的对话。通过对我们的攻击面进行丰富而持续的外部评估，让我能够将攻击面风险纳入公司级别的指标观察机制。”

Douglas Graham

首席信任官

Lionbridge 公司

主要用例

- 发现攻击面
- 影子 IT
- 漏洞优先级划分
- 并购风险
- 新闻中的攻击

主要优点

- **发现未知之处**
像攻击者一样查看企业的外围，以发现配置错误和进程故障。无需安装。
- **划分发现结果的优先级**
采用我们正在申请专利的基于黑客逻辑构建的模型，准确查明攻击者的主要目标。
- **减少攻击面**
比影子 IT、并购和意外事件领先一步。新风险出现时会发出警报。

Randori Recon 如何运作



输入电子邮件：只需一个电子邮件地址，即可开始采用低摩擦设置



发现攻击面：搜索互联网以发现、关联和识别面向互联网的资产



划分发现结果的优先级：模拟攻击者，对易招致攻击的目标进行自动评分并划分优先级

Randori Recon 为何与众不同？

1. 真实的发现

攻击者不会从扫描整个互联网开始，我们也不会。我们采用与攻击者相同的技术，能够找到他人错过的 IPv6 和云资产。

2. 持续的洞察分析

Randori 一直不断地观察，搜寻企业新资产和攻击面的各种变化。采用我们正申请专利的 Target Temptation 模型可快速识别问题，它可根据攻击者的发展趋势和 IBM Security Randori Attack 的数据及时进行更新。

3. 主动采取补救措施

了解已暴露目标、如何发现该目标、相关风险以及应对措施——这一切都在攻击者发动攻击之前完成。需要证据？使用 Randori Attack 验证风险。

为什么选择 IBM？

IBM Security Randori Recon 在单一、统一的平台中进行攻击面管理 (ASM)，以提供持续、前瞻、真实防范攻击的安全体验。[进一步了解](#) Randori Recon，以及它如何助力企业比攻击者领先一步。

© Copyright IBM Corporation 2022

国际商业机器（中国）有限公司
有关详情，欢迎访问我们的官网：
<https://www.ibm.com/cn-zh>

美国出品
2022 年 9 月

IBM 和 IBM 徽标是 International Business Machines Corporation 在美国和/或其他国家/地区的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的最新列表可参见 [ibm.com/trademark](https://www.ibm.com/trademark)。

本文档为最初发布之日起的最新版本，IBM 可能随时对其进行更改。IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。

用户自行负责评估和验证任何其他产品或程序与 IBM 产品和程序搭配运行的情况。本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据的协议条款和条件获得保证。

