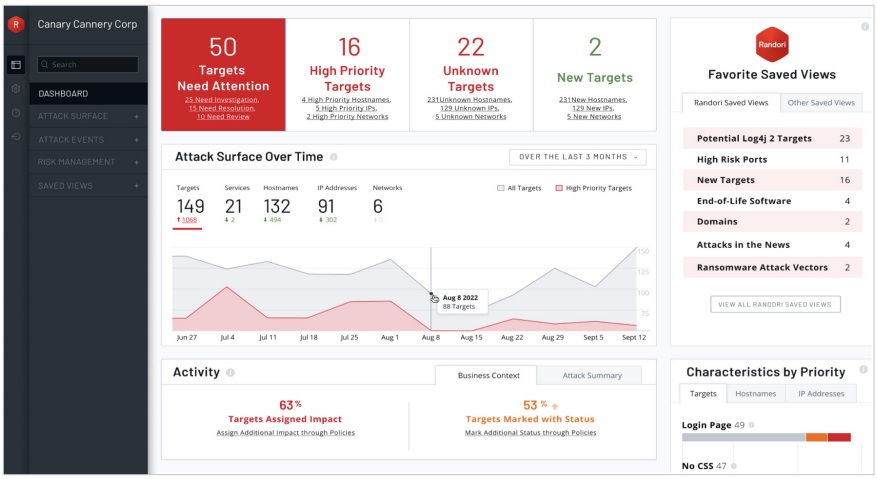
IBM Security Randori Recon: attack surface management

See your attack surface like an attacker

To know where attackers will strike, you first need to know how they view your attack surface. IBM® Security Randori Recon provides continuous asset discovery and issue prioritization from an attacker's perspective.

With cloud migrations, shadow IT, and mergers and acquisitions (M&A), your perimeter is constantly changing. These changes represent windows of opportunities for attackers. Discover them with Randori Recon—no installation or configuration required.

Just like real threat actors, Randori Recon continuously monitors your external attack surface, uncovering blind spots, misconfigurations and process failures that would otherwise be missed. Using a black-box approach, Randori finds the Internet Protocol version 6 (IPv6) and cloud assets that others miss.



IBM

Randori

an IBM Company

“Randori has changed the conversations I am able to have with the executive team. Having a rich and continuous external assessment of our attack surface has enabled me to make attack surface risk a company-level metric.”

Douglas Graham
Chief Trust Officer
Lionbridge

Key use cases

- Attack surface discovery
- Shadow IT
- Vulnerability prioritization
- M&A risk
- Attacks in the news

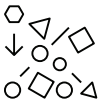
Key benefits

- **Discover your unknowns**
  View your perimeter like an attacker to expose misconfigurations and process failures. No installation required.
- **Prioritize your findings**
  Pinpoint an attacker’s top targets with our patent-pending model built on hacker logic.
- **Reduce your attack surface**
  Stay a step ahead of shadow IT, M&A, and unexpected change. Alerts inform you of new risks as they arise.

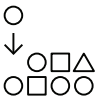
How Randori Recon works



Enter email: Low-friction setup only requires an email address to get started



Discover attack surface: Searches internet to discover, associate and identify internet-facing assets



Prioritize findings: Emulates adversary to automatically score and prioritize the most tempting targets for attack

What sets Randori Recon apart?

1. **Authentic discovery**
   Attackers don't start by scanning the entire internet, and neither do we. We use the same techniques attackers do, allowing us to find the IPv6 and cloud assets that others miss.

2. **Continuous insight**
   Randori is always watching, looking for new assets and changes in your attack surface. Identify issues fast with our patent-pending Target Temptation model, which updates based on attacker trends and IBM Security Randori Attack data.

3. **Proactive remediation**
   Understand what's exposed, how it can be discovered, what the risk is and what you should do—before attackers strike. Need proof? Validate the risk with Randori Attack.

Why IBM?

IBM Security Randori Recon offers attack surface management (ASM) in a single, unified platform to provide a continuous, proactive and authentic offensive security experience. Learn more about Randori Recon and how it can help your organization stay one step ahead of attackers.

To learn more, contact your IBM Business Partner:

Specialist Computer Centres plc
07976 014124 | sarah.hilton@scc.com
scc.com

© Copyright IBM Corporation 2022

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
September 2022

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.