Discover unknowns, prioritize your findings and reduce your attack surface

Manage your cyber risks with a comprehensive solution

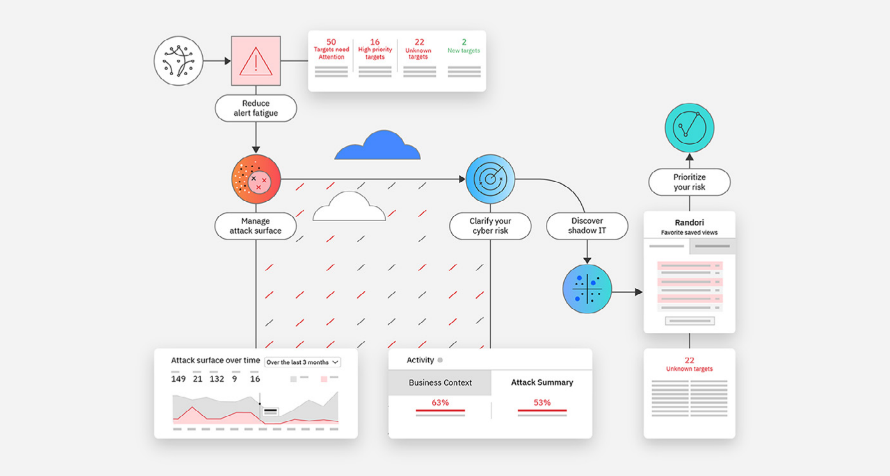
Highlights
Clarify your cyber risk

Drive program efficiencies

Streamline operations

The expanding digital landscape creates a growing attack surface for enterprises. The explosion of hybrid cloud environments and remote workforces makes comprehensive attack surface management a challenge. Plus, mergers and acquisitions add further complexity by introducing unknown attack vectors. As a result, traditional security patching known vulnerabilities is not enough to protect managed assets. To stay ahead of cyber threats, organizations need proactive visibility into their entire attack surface.

IBM Security® Randori® Recon is an attack surface management (ASM) software as a service (SaaS) that gives your SecOps team a continuous, attacker-centric view of your organization's external attack surface. Randori Recon continuously discovers assets and prioritizes risks based on their interest to attackers (adversarial temptation). That helps your team focus on the most critical vulnerabilities first. Randori Recon seamlessly integrates with your existing security tools so you can strengthen your overall cybersecurity posture without adding complexity.



Clarify your cyber risk

With continuous asset discovery and risk-based prioritization, you get an accurate view of your current attack surface and make better-informed decisions. IBM Security Randori Recon can reduce the time an asset remains exposed to potential external attacks by as much as 50%[1]:

- **External discovery**
  Identify your organizational exposures, including IPv6 assets, accurately and non-intrusively while reducing false positives to keep your signal-to-noise ratio under control.

- **Risk-based prioritization**
  Optimize risk prioritization with our patent-pending algorithm that accounts for adversarial temptation, business context, and common vulnerability scoring system (CVSS) severity.

Drive program efficiencies

Reduce the amount of time and effort your security team spends on vulnerability scanning and attack surface exposure analysis. With Randori Recon for SecOps you can accelerate exposure response speed by 10%:[1]

- **Discovery path**
  Act on newly identified assets without additional research by showing how a particular asset was located on the perimeter.

- **Security testing**
  Validate defenses through dynamic control checks, on-device MITRE ATT&CK testing, and targeted vulnerability exploitation to enable continuous assessment of your organization’s defenses against internal and external threats

- **Remediation guidance.**
  Improve your cyber resilience by implementing remediation best practices across your infrastructure with adversarial insights.

Streamline operations

Eliminate data silos and improve the effectiveness of your security tools by validating vulnerabilities and using bidirectional integrations with your existing security stack:

- **Vulnerability validation**
  Confirm whether common vulnerabilities and exposures (CVEs) exist on your attack surface and if they are exploitable.

- **Enterprise integrations**
  Create bidirectional integrations with other security solutions such as security information and event management (SIEM); security orchestration, automation and response (SOAR); vulnerability management and ticketing systems, to enhance your security ecosystem.

Stay ahead of attackers and proactively address external attack surface risks with Randori Recon. Choose the tier that best fits your needs from our flexible options.

	Essentials	Standard	Premium
External discovery	√	√	√
Discovery path	√	√	√
Risk-based prioritization	√	√	√
Remediation guidance	√	√	√
Policies and reports	√	√	√
Enterprise integrations		√	√
Vulnerability validation			√
Security testing			√

Note: Internal discovery can only be enabled in the Standard and Premium tiers.
The above outlines the external discovery.

Why IBM?

Using the attacker's point of view to discover exposures is an optimal way to regain control and help close the advantage that attackers have over defenders. IBM offers a rich combination of human intelligence, machine-based visibility, and automation to accurately map your organization's attack surface and prioritize your risk exposure. IBM can help continuously manage attack surfaces as part of an overall security program while applying your existing ecosystem of security tools.

For more information

Learn more here or contact your IBM representative or IBM Business Partner.

[1] The Total Economic Impact of IBM Security Randori, Forrester Consulting, commissioned by IBM, June 2023.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
April 2024

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.

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.