Randori

Randori Recon - Attack Surface Management

Randori Recon provides a continuous view of your external perimeter to reduce the risks of blindspots, misconfigurations, and process failures.

Great security starts by understanding what you need to protect. The rise of cloud computing and the proliferation of SaaS solutions has made knowing what to protect more challenging than ever. As a result, many organizations have begun to lose control of their attack surface and 2019 is on track to the worst year on record for data breaches.

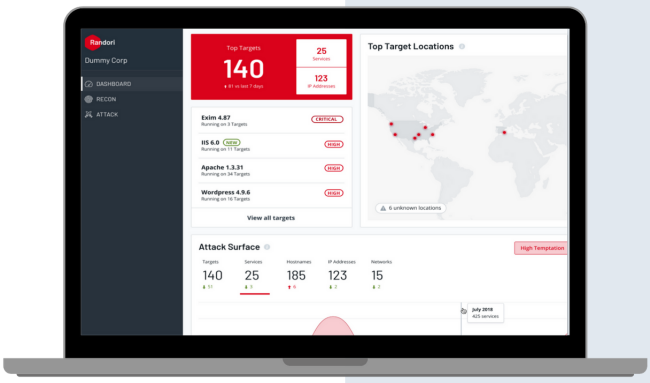
The processes organizations have traditionally relied upon to track and manage their externally exposed assets have proven ineffective, and organizations are increasingly looking for new ways to monitor their attack surface and manage risk.

Designed by some of the best minds in offensive security, the Randori Attack Platform is an authentic, automated adversary that enables organizations to practice, test, and assess their security program. The Randori Platform begins with reconnaissance, and leverages the same tactics and techniques used by advanced threat actors, to build a comprehensive view of an organization's attack surface.

Randori Recon provides a continuous view of all internet-connected assets that belong to an organization. IT and Security teams use this insight to gain control of their attack surface and to reduce the risks associated with blindspots, misconfigurations, and process failures.

"Randori Recon helped us discover that our attack surface was 10% larger than what we originally thought"

Houghton Mifflin Harcourt



Key Benefits

Reduce risk of unknown assets (blind spots / shadow IT)

Locate and remediate exposures faster & more effectively

Better prioritize patch and remediation efforts

Identify misconfigurations & process failures

- Find compromised domains
- Find externally facing login pages
- Find outdated applications
- Find assets leaking internal data or information
- Find unintentionally exposed services

RANDORI RECON

Real time insight into your greatest security risks.

Learn more at
Randori.com

Randori

Key Capabilities

1. Blackbox Discovery

Starting with just an email address, Randori Recon, a SAAS based platform, automatically creates a baseline of your organization's attack surface - no configuration and no software or hardware deployment required. Once activated, Randori Recon continuously monitors the internet for evidence of your external systems and alerts you as changes or new discoveries are detected.

2. Authentic Collection

Randori Recon uses the same techniques and procedures used by sophisticated threat actors. Therefore, unlike other solutions in the market, Randori Recon is designed to be difficult to detect or block using existing defenses. Randori leverages multiple cloud providers, across multiple countries, regions and zones for data collection. This allows Randori to provide a more complete view of your attack surface than providers that leverage high-speed scanning or conduct all activity from a single point of origin that may get blocked or throttled. Randori Recon is a fully integrated component of the Randori Attack Platform, and after authorization by the organization, provides the ability to launch authentic attacks against the discovered assets in order to validate existing defenses.

3. Prioritized Analytics Randori

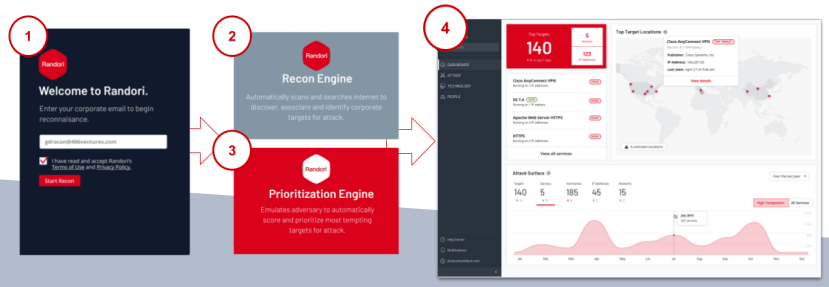
Randori Recon highlights assets most likely to be interesting to an adversary. The platform performs continuous analysis of numerous factors, such as known exploits and ease of discovery, to focus users on assets likely to be first targets.

4. Actionable Findings

Randori Recon provides the context and information needed to take steps to reduce an organization's risk by hardening or reducing the organization's attack surface. Findings are easy to search and automatically classify characteristics that are likely to be of interest to an organization.

5. Easy to Integrate

Randori Recon includes a robust API that makes it easy to integrate data from Randori into your security program's existing workflows. This API includes the ability to support integration with third party security solutions (SIEMs, ticketing systems, and orchestration platforms).



Key Use Cases

- Attack Surface Monitoring
- Continuous Asset Discovery (CIS #1 and CIS #2)
- PCI Compliance (PCI DSS Reqs 10 & 11)
- M&A and divestiture diligence
- Threat modeling validation
- Rapid baselining for a new CISO
- Risk-based vulnerability management

Key Features

- Blackbox Recon
- Continuous Monitoring
- Real time alerting
- Change notifications
- Artifact & Screenshot Collection
- Path of Discovery
- Target Temptation
- Alerting and Notifications
- Trending and Reporting
- Asset Tagging
- Open APIs
- Workflow Integration
- Multi-Factor Authentication
- Role Based Access Control

REQUEST A DEMO

Contact us today to schedule a demonstration.

Sales@Randori.com

About Randori

Randori is the attack platform CISOs rely upon to stay ahead of the next attack. Our nation-state caliber platform combines continuous reconnaissance, real-time target analysis, and the ability to safely execute attacks on-demand to provide an attacker's perspective of where and how threat actors will strike you next.