Randori™

RANDORI OFFENSIVE SECURITY PLATFORM

- Attack Surface Management (ASM)
- Continuous Automated Red Team (CART)

KNOW YOUR UNKNOWNS

Most organizations are only aware of 60 percent of the scope of their external attack surface. Ever wonder what's lurking in the other 40 percent? Find out with Randori.

Our automated Attack Surface Management platform discovers what you can't see, but hackers could be targeting. Leveraging the hacker's perspective to find the assets your existing tools are missing, Randori shows you how your organization really appears to a world full of bad actors:

- Emulates discovery techniques used by nation-state adversaries and ransomware attackers.
- Finds exposed assets that attackers can target but you might miss, including Shadow IT, exploitable software, and unpatched, misconfigured, and decommissioned systems.
- Discovers IPv6 and cloud assets others miss.

PRIORITIZE TARGETS, MANAGE RISK

By showing you what hacker's see and where they might attack, Randori gets you on the fast track to protecting your company's most important assets:

- Provides a real-time inventory of exposed and attackable software.
- Automatically prioritizes vulnerabilities that hackers are most likely to attack.
- Contextualizes risk, providing a "temptation" score for every exposed asset.

GET AHEAD, STAY AHEAD

Dynamic IPs, mergers and acquisitions, new vulnerabilities, botched configurations, rotating cloud infrastructures, and more. Your attack surface is a moving target. Randori helps you validate your security posture and stay on top of it:

- Continuously monitors and analyzes ever-changing attack surfaces.
- Delivers risk assessments in real time so you can focus on those that matter most.
- Provides insightful metrics and status workflows to track performance and fortify your security posture.

KEY BENEFITS

- Hacker's perspective provides a full-spectrum view of the external attack surface.
- Prioritization of potential exploits allows security teams to proactively protect mission-critical assets.
- Real-time monitoring, actionable intel, and automated red teaming enables or ganizations to test, validate, and continuously improve their defenses.
- Cloud-native, no-agent platform means there's no downloads; friction-free ser vice works quietly in the background.
- Seamless integration with existing asset and vulnerability management systems.
- Easy to get started — all it takes is an email address.

Gartner COOL VENDOR 2021

IDC Innovator

EVOLVIN AWARDS GOLD

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2021

BOOST YOUR DEFENSES, BE RESILIENT

Randori's Continuous Automated Red Team provides real-time insights into the effectiveness of your security program, enabling ongoing improvements:

- Goes beyond simple penetration testing.
- Tests your defenses under real-world conditions.
- Identifies issues that need immediate attention and helps prioritize security investments and assess risk.

PROVE IT!

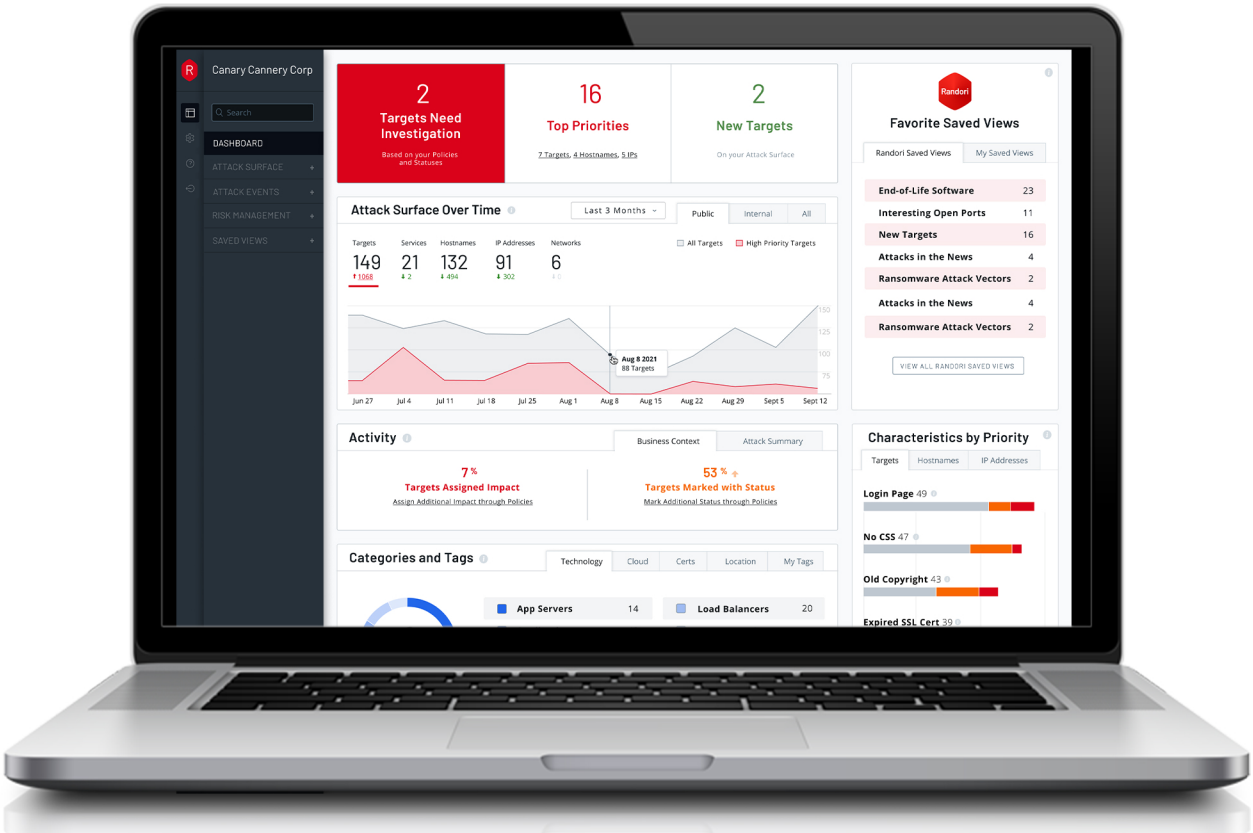
Test the resiliency of your security program by sparring with a nation-state caliber red-team. Put your SOC, MDR, MSSP, and incident response capabilities to the test under real-world conditions. Just give us the go ahead and authorize our automated red team. Then sit back and wait for your results.

COMPLEMENTARY USE CASES

Ransomware Prevention
Get instant visibility into your most tempting ransomware targets with "Target Temptation" scoring

Shadow IT Discovery
Find forgotten assets, blind spots, and process failures that allow attackers to bypass your defenses

Secure Cloud Migration
Get an attacker's view as your network shifts to the cloud and integrate it into existing workflows with robust APIs and integrations



ABOUT RANDORI

At Randori, We Attack to Protect. Recognized by Gartner & IDC as a leader in Offensive Security, the Randori Platform unifies Attack Surface Management (ASM) and Continuous Automated Red Teaming (CART) to provide enterprises the visibility, actionable insights and validation they need to proactively prevent breaches. Customers like VMWare, Greenhill Inc, FirstBank, NOV, Lionbridge and many more, trust the Randori platform, which was designed by the world's foremost offensive security practitioners at nation-state levels. Discover what's exposed on your attack surface today at randori.com and get the latest insights by following Randori on Twitter and Linkedin.

Randori™