

1CONTINUOUSLY ASSESS YOUR ATTACK SURFACE WITH VECTOR COMMAND

A continuous Red Team managed service to proactively assess your external attack surface and identify any security gaps.

SOLUTION BRIEF

Vector Command is a continuous red teaming service designed to help organizations understand and validate exposures/ It combines Rapid7's robust attack surface management (ASM) technology with the expertise of its elite red teamers. The service continuously discovers internet-facing assets, both known and unknown, and then proactively subjects them to real-world attack scenarios, emulating current threat actor tactics, techniques, and procedures (TTPs).

Vector Command goes beyond traditional vulnerability scanning or point-in-time penetration tests, but delivers against Gartner's vision for adversarial exposure validation, focusing on truly exploitable attack paths and high-risk assets.

The service also now includes the full internal and external attack surface management capabilities of Surface Command, and has expanded to help security teams to meet specific compliance requirements with added internal pen-testing and reporting as part of Vector Command Advanced.

By providing clear visualizations of validated attack chains and expert-guided remediation, this "always-on" red team approach allows organizations to continuously test their defenses, prioritize actual risks, and build resilience against ever-evolving threats.76% of

organizations experienced a cyberattack due to unknown, unmanaged, or poorly managed internet-facing assets.

TECHTARGET

Key Vector Command outcomes for customers

2Know your attack surface better than the attackers

Persistent recon of your internet-facing assets, constantly looking for new assets and exposures and providing you with the attacker's perspective. Leverage the full capabilities of Surface Command to the external attack surface with full internal context on business criticality.

Continuously validate your most critical external exposures with hands-on Red Team experts

Rapid7's expert operators leverage the latest tactics, techniques, and procedures (TTPs) to safely e the external exposures and test your security controls with Red Team exercises like:

- Opportunistic phishing - Our experts will design and conduct phishing campaigns using the latest TTPs with focus on demonstrating the impact of credential capture and payload execution.
- External network assessment - Continuously assess vulnerabilities exposed in the external network, with focus on obtaining access to your organization and its sensitive systems.
- Post-compromise breach simulation - Upon breach, our experts will safely emulate the latest tactics to obtain command and control over the compromised system. Post-exploitation activities emulate adversary behavior to assess privilege escalation, lateral movement, and persistence.
- Emergent threat validation - Assess your network perimeter's susceptibility against the latest Rapid7 emergent threat vulnerabilities so you can validate patching and security configurations.

Visualize vetted attack paths to drive prioritization
Move beyond isolated vulnerabilities to see and understand multi-vector attack chains through clear visualizations provided by Rapid7's expert red team operators. This enables rapid, targeted remediation and effective communication of risk to stakeholders.

Optimize risk reduction with actionable prioritization:

Focus remediation efforts on the most critical exposures and high-value assets identified through Rapid7 real-time simulated attacks. Receive prescriptive, expert guidance to efficiently reduce your organization's risk profile.

Vector Command Advanced

Streamline compliance requirements with integrated offensive security

Fulfill diverse compliance requirements through a unified service offering continuous, human-led red teaming, annual internal penetration testing, and comprehensive documentation for simplified audits.

How Vector Command works

Powered by intelligence

from Rapid7 Labs,

persistently recon the

external attack surface

for internet-facing

assets. Prescriptive guidance

from Customer

Advisors on how to best

remediate exposures. Regular cadence of

expert Red-Team

emulating real-world

attacks to validate

exposures and monitor

security controls. Prioritize critical

exposures - vetted

by experts - that

are most likely to be

exploited by attackers.

Discover Exploit Prioritize Remediate Vector Command

A continuous Red Team managed service

Ongoing Red Team operations to validate external exposures

- Opportunistic phishing.
- External network assessment.
- Post-compromise breach simulation.

- Vetted attack paths.
- Emergent threat validation.
- Asset attractiveness index.

RAPID7 VECTOR

COMMANDRAPID7 VECTOR

COMMAND ADVANCEDEXTERNAL

ATTACK SURFACE

MANAGEMENTTRADITIONAL ONE-TIME

PENTESTTRADITIONAL RED

TEAM ENGAGEMENT

Core Use CaseContinuous external

discovery and ongoing

exploit validation

through the lens of an

adversaryContinuous attack

surface management

technology and

internal network

testingVisibility into public

exposure of known

and unknown assetsOften compliance-

focused, in-depth

evaluation for a very

specific, defined

scopeDeep 1:1 engagement

over a defined period

of time (typically 1

month) with a set

objective

KEY CAPABILITIES

Automated external

scanningScope-dependent Targeted external

scanning; not

automated

Ongoing Red Team

operations

Point in time; not

continuous

Emergent threat

response reviewPoint in time; not

continuousPoint in time; not

continuous

Vetted attack paths

Prioritized exposuresPoint in time; not

continuousPoint in time; not

continuous

Expert remediation

guidance

Same-day findings

and reporting
Ongoing as findings
are uncovered
Not applicableOne-time; Post-
engagementOne-time; Post-
engagement
Annual internal
penetration and
segmentation testNot applicable
Not applicableNot applicable Not applicable