RAPID7

SOLUTION BRIEF

CONTINUOUSLY 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

Today's organizations have a wider external attack surface through expanding shadow IT, cloud hosting, and SaaS applications. Attackers are constantly scanning the attack surface to breach defenses, making it critical for organizations to gain visibility into weak entry points from their external attack surfaces.

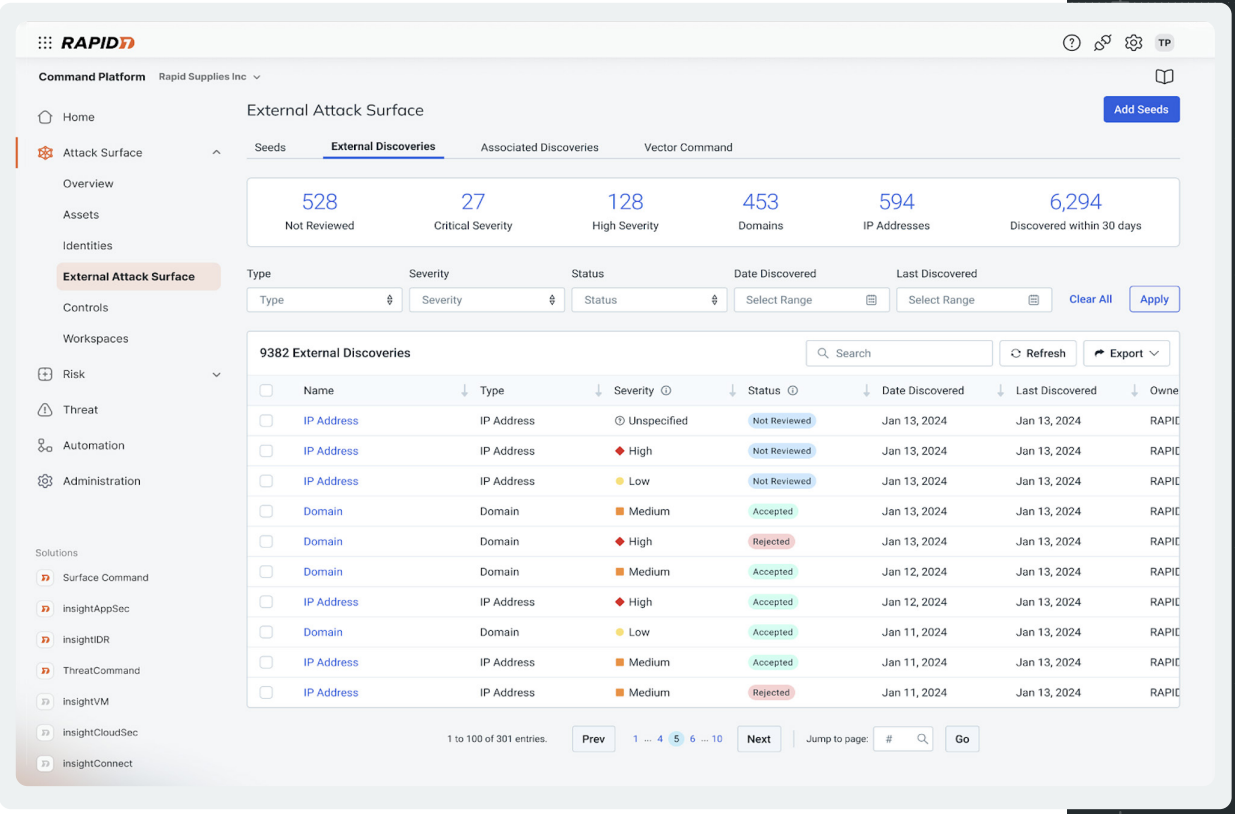
Vector Command - powered by Rapid7's expert Red Team and technology - enables security teams to proactively assess their external attack surfaces and identify gaps in defenses by providing an attacker's view of the internet-facing assets and validating exposures with continuous Red Team operations.

Vector Command cuts through the noise of External Attack Surface Management (EASM)-only tools and latency of point-in-time security testing exercises that risk exploitation by being laser focused on continuously discovering, exploiting, and prioritizing critical external exposures. Vector Command goes beyond vulnerabilities to assess the overall state of an organization's IT security posture and surface critical vulnerabilities, misconfigurations, or missing security controls.

76% of organizations experienced a cyberattack due to unknown, unmanaged, or poorly managed internet-facing assets.

(Source - TechTarget)

KEY VECTOR COMMAND OUTCOMES FOR CUSTOMERS



Know your external attack surface better than the attackers

Get the attacker's perspective on your external attack surface with persistent reconnaissance of your known and unknown internet-facing assets and exposures. Vector Command leverages intuitive External Attack Surface Management capabilities, powered by the Command Platform. Get visibility into previously unknown risks like exposed web services, remote admin services, services with unencrypted communication standards, assets which expose outdated services with known vulnerabilities, expired certificates, and more.

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

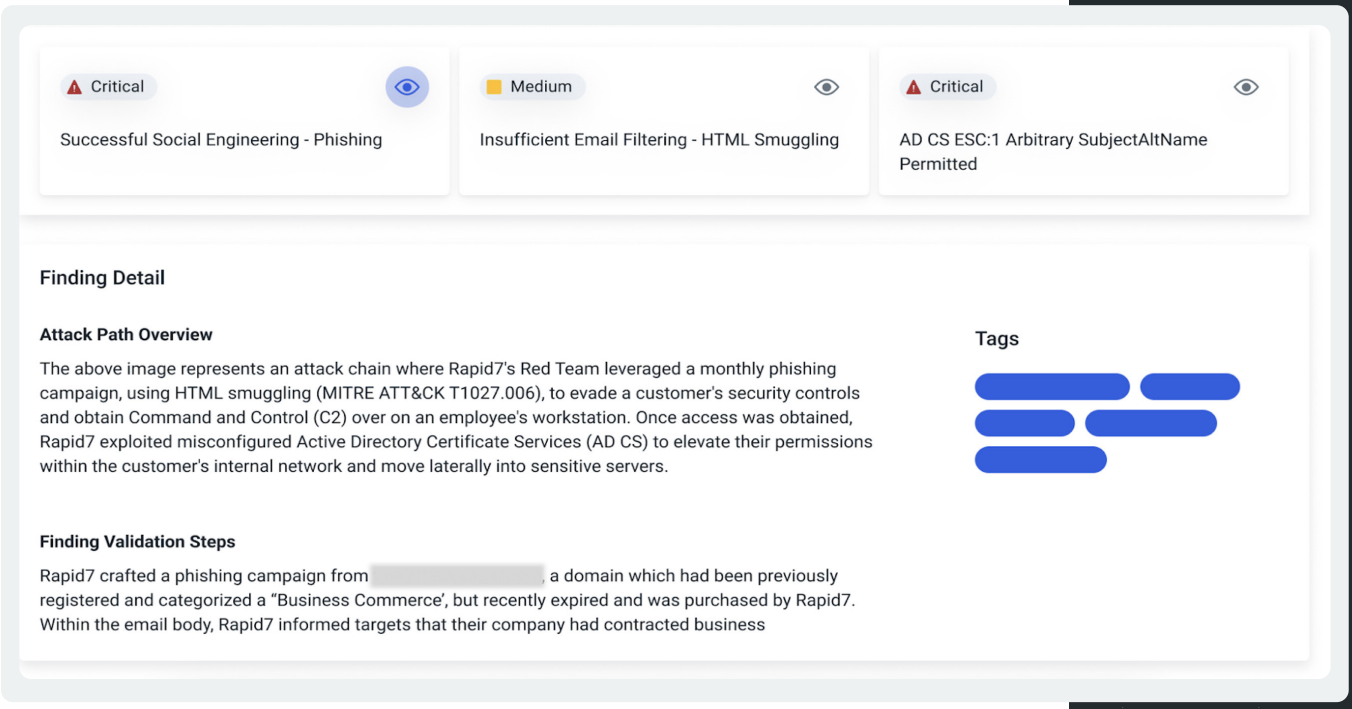
Rapid7's expert operators leverage the latest tactics, techniques, and procedures (TTPs) to safely exploit the external exposures and test your security controls with Red Team exercises like:

- **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 perimiter's susceptibility against the latest Rapid7 emergent threat vulnerabilities so you can validate patching and security configurations.

Visualize vetted attack paths to drive prioritization

Our expert team of attackers will safely exploit vulnerabilities and attempt to move laterally in your environment, demonstrating risks and providing visualization of multi-vector attack chains. Get an expert-curated list of assets most likely to attract a malicious actor; this includes assets using legacy frameworks, web admin exposures, websites, or APIs which expose excessive functionality without authentication. Understand the attack methodology and share expert-vetted critical exposures with relevant stakeholders to drive prioritization.



Prioritize remediation with expert guidance and findings from simulated attacks

Address critical issues right away by leveraging same-day findings from successful Red Team exploitations. Get prescriptive guidance from our advisors on how to best remediate critical exposures and strengthen your overall security posture against successful attack chains. Go beyond patch management with recommendations to improve your network segmentation, identity and access management, social engineering resilience, external attack surface reduction, and more.

HOW VECTOR COMMAND WORKS

Vector Command

A continuous Red Team managed service

Discover	Exploit	Prioritize	Remediate
Powered by intelligence from Rapid7 Labs, persistently recon the external attack surface for internet-facing assets.	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.	Prescriptive guidance from Customer Advisors on how to best remediate exposures.

\+

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

Experience the Rapid7 Vector Command Difference

	Rapid7 Vector Command	External Attack Surface Management	Traditional One-Time Pentest	Traditional Red Team Engagement
Core Use Case	Continuous external discovery and ongoing exploit validation through the lens of an adversary	Visibility into public exposure of known and unknown assets	Often compliance-focused, in-depth evaluation for a very specific, defined scope	Deep 1:1 engagement over a defined period of time (typically 1 month) with a set objective
Key Capabilities				
Automated External Scanning	✓	✓	Scope-dependent	Targeted external scanning; not automated
Ongoing Red Team Operations	✓	✗	✗	✗ Point in time; not continuous
Emergent Threat Response Review	✓	✗	✗ Point in time; not continuous	✗ Point in time; not continuous
Vetted Attack Paths	✓	✗	✓	✓
Prioritized Exposures	✓	✗	✗ Point in time; not continuous	✗ Point in time; not continuous
Expert Remediation Guidance	✓	✗	✓	✓
Same-day Findings & Reporting	✓ Ongoing as findings are uncovered	✗ Not applicable	✗ One-time; Post-engagement	✗ One-time; Post-engagement

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight