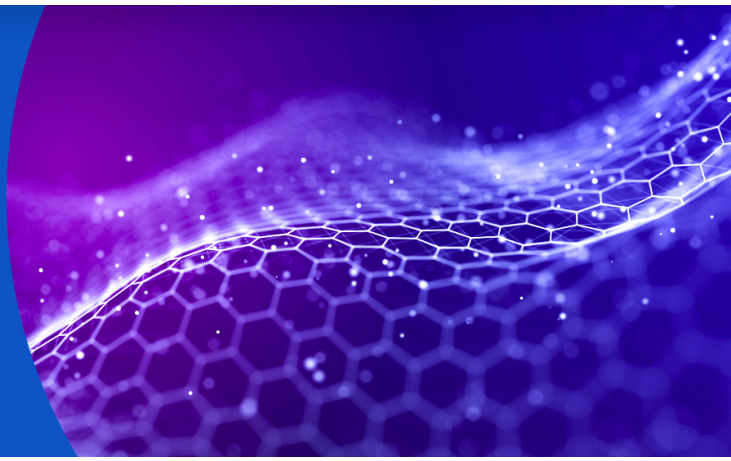
Cymulate and Rapid7

Solution Brief



The Challenge: Disjointed Data Collection

As organizations evolve their security programs, data generated by multiple security controls is difficult to quickly translate into coordinated workflows and incident response. Data from SIEM, UBA, EDR, vulnerability management (VM), cloud application security, incident detection and response tools, and breach and attack simulation (BAS) tools, such as Cymulate, must be integrated and interpreted to be actionable. Only then can security, IT, DevOps, and DevSecOps teams quickly prioritize and coordinate their efforts to reduce the organization's attack surface.

The Solution: One-Click Visibility

Rapid7, a leading provider of security analytics and automation, and Cymulate, an award- winning SaaS-based breach and attack simulation platform, have joined forces to give security teams, IT DevOps, and DevSecOps teams single-click security visibility. The Cymulate-Rapid7 integration enables security practitioners to:

- Identify machines that can potentially be exploited alonga simulated lateral movement route
- Prioritize and accelerate remediation of vulnerable systemsaccording to various parameters, such as asset type, user privileges, and proximity to the organization's most critical digital assets (crown jewels)

Integration Benefits

The joint Cymulate-Rapid7 partnership offers multiple organizational efficiencies, including:

- Data enrichment of attack simulation results with Rapid7-sourced data to provide exploitability and risk scores, mitigation guidelines, and indication if a CVE is currently being exploited by variants found in the wild
- Seamless, automated integration via API
- Automated association of systems along a potential lateralmovement path with CVEs relevant to those specific IP addresses, hostnames, and other relevant details
- Mitigation prioritization based on user privileges andassets most likely to be exploited during lateral movement, such as domain controllers, databases, servers, and workstations
- Fast mitigation of critical paths to organizational crownjewels with comprehensive remediation guidelines and mapping to the MITRE ATT&CK™ framework

Key Integration Benefits

- Accelerated identification, prioritizationand remediation of security gaps
- Discovery of vulnerable systems alonga potential lateral movement path
- Seamless automated integration via API

Mapping Lateral Movement to Unpatched Vulnerabilities

Cymulate integrates with Rapid7 Vulnerability Management to map attackers' potential lateral movement paths. It highlights exploitable operating system and software vulnerabilities that enable an attacker to hop between systems and network segments. Challenging the effectiveness of security controls against the ability to move laterally, Cymulate's Lateral Movement (Hopper) vector uses a sophisticated algorithm to identify potential attack routes. It continues 'hopping' from one system to another until there are no more hops to move towards, your predefined crown jewels have been reached, or when you decide to end the attack simulation.

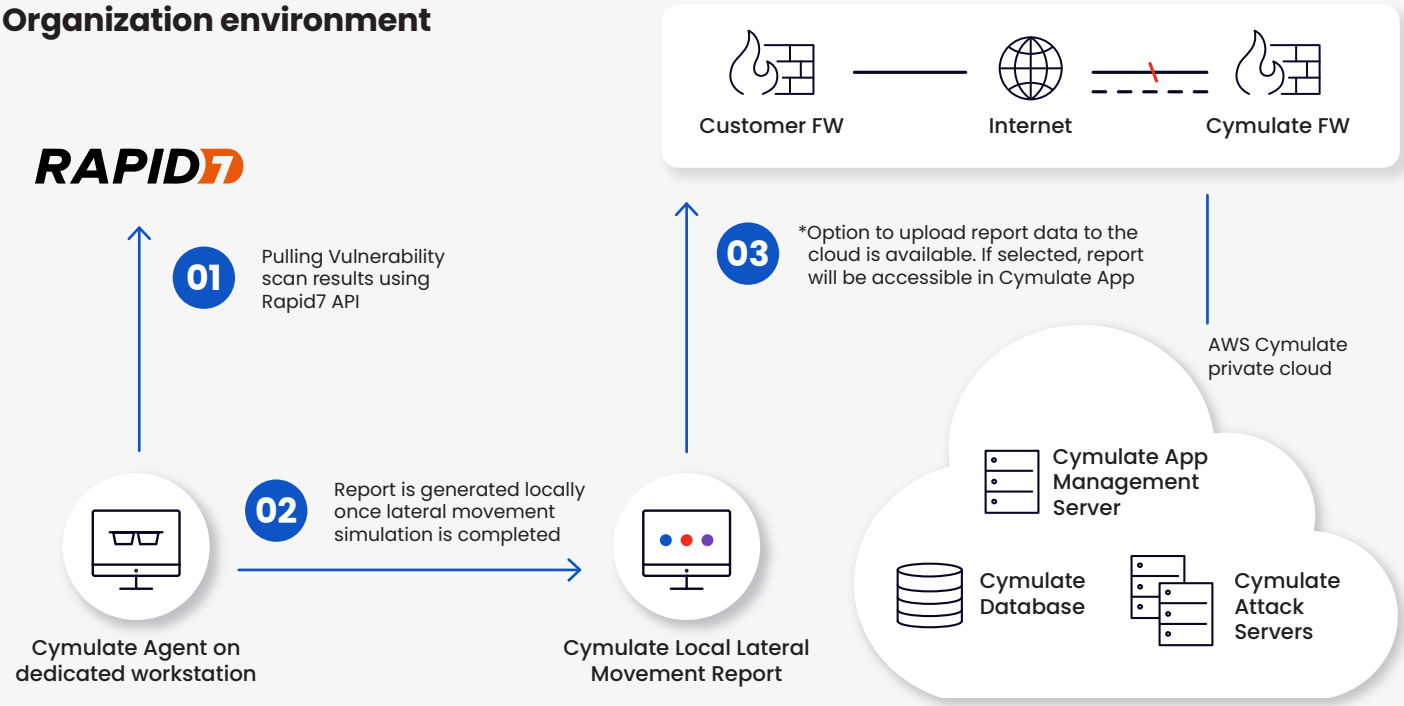
How It Works

01 Organization regularly runs vulnerability assessments using Rapid7.

02 Organization regularly runs lateral movement attack simulations using Cymulate.

03 Cymulate Agent pulls data from Rapid7 via API. Cymulate Agent combines Cymulate results with Rapid7 data to create a single-pane view. The combined report is generated locally and can be uploaded to the cloud.

Organization environment



About Rapid7

Rapid7 is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Its solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 7,800 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. Rapid7 Nexpose is an on-premises option for vulnerability management software. It monitors exposures in real-time and adapts to new threats with fresh data, ensuring security teams can always act at the moment of impact.

About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632