

# Technology Alliances

An organization's security posture is affected by many different variables— both known and unknown—that are constantly changing. Together with Cymulate's technology ecosystem partners, the platform empowers security leaders to maximize operational efficiency while minimizing risk exposure.

These integrations enable organizations to:



Validate and improve security tool detection and response capabilities



Prioritize efforts by correlating attacks to the findings of vulnerability management systems



Integrate Cymulate remediation guidance into automated workflows
















Streamline security task management with IT and then track, monitor, and assure that security gaps are being closed

## SIEM Systems

Verify and optimize the effectiveness of SIEM solutions in the complex landscape of modern cybersecurity. Cymulate correlates logging and incident generation with assessments to produce a more complete picture of the efficacy of SIEM operations. Cymulate also provides SIGMA rule output and supports the use of custom queries to further assist in SIEM tuning and troubleshooting.

Cymulate integrations are available with the following solutions:

 Splunk	 IBM QRadar	 Falcon LogScale	 Rapid7 InsightIDR
 LogRhythm	 Microfocus ArcSight	 Microsoft Azure Sentinel	 RSA NetWitness
 Sumo Logic	 Trellix	 Securonix	 Google Chronicle
 McAfee			

## SOAR and GRC Systems

With the Cymulate integration, organizations leverage assessment data within other platforms and workflows which permits higher levels of automation and streamlined compliance operations.

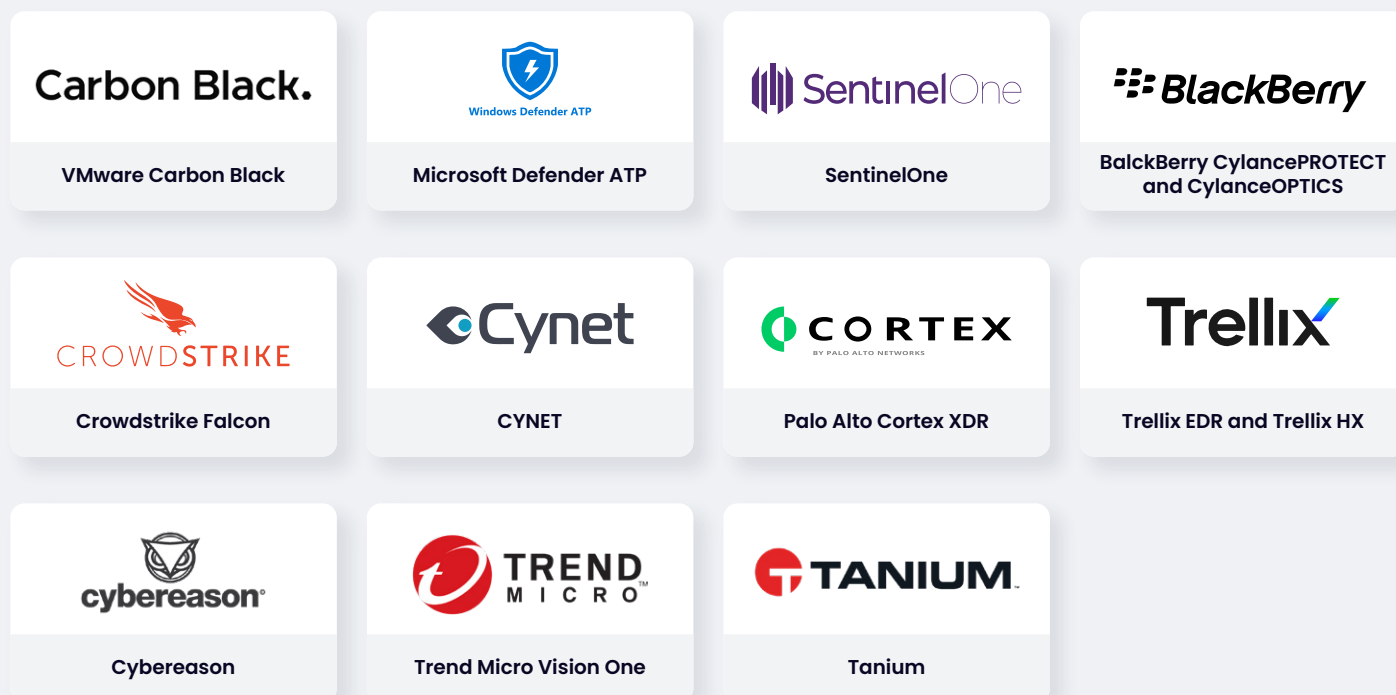
Cymulate integrations are available with the following solutions:



## EDR and Anti-Malware Systems

Cymulate ingests data from EDR/XDR/Anti-Malware solutions and correlates that data with the actions taken during assessments. With this information, organizations confirm the efficacy of endpoint defenses or determine remediation paths and streamline troubleshooting.

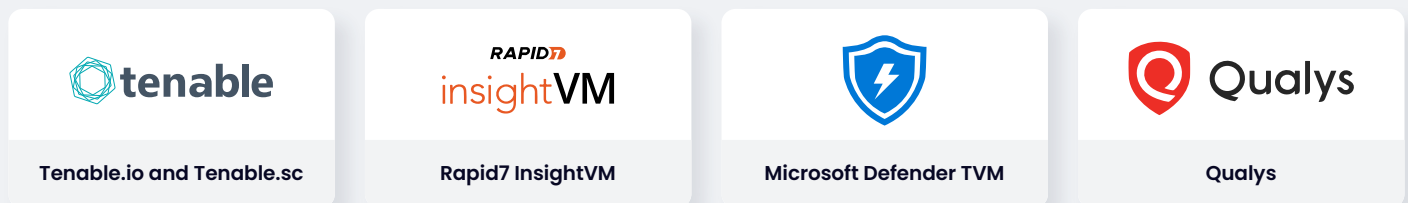
Cymulate integrations are available with the following solutions:



## Vulnerability Management Systems

Cymulate compares information gathered through assessments against data produced by Vulnerability Management Systems (VMS) to provide a more complete picture of the risk associated with known exploit activity. By correlating the existence of the vulnerability (the VMS) and the ability of compensating controls to block exploitation (Cymulate), determining and rationalizing priority in patching becomes significantly easier.

Cymulate integrations are available with the following solutions:



## Firewall Systems

Cymulate challenges an organization's network firewall against a comprehensive set of attacks to validate inbound and outbound communication's configuration settings and policies. This integration enables the results to appear directly in Cymulate's reports so organizations can respond to threats faster and streamline remediation.

Cymulate integrations are available with the following solution:



## Ticketing Systems

Integration with ticketing systems enables security teams to manage security tasks from within the Cymulate platform. This integration streamlines security ticket management so security and IT teams respond to threats faster, more efficiently, and stay focused on what is most critical to the organization.

Cymulate integrations are available with the following ticketing solution:



Contact us for a live demo

[Start Your Live Demo](#)