

SOLUTION BRIEF

Cymulate for MSSPs

Challenge

Enterprises and SMBs rely on their trusted partners for expertise in accelerating the deployment of Endpoint Detection and Response (EDR) solutions, designing and maintaining proper configuration and responding to threats. MSSPs seek to be a trusted partner but often struggle with:

- **Manually intensive onboarding to tune to specific customer environments**
- **Communicating the value of services to customers**
- **Poor alignment with clients on shared responsibilities**
- **Adapting to changes in the customer environment**
- **Analyzing new threats and updating EDR for proper prevention or detection**

Differentiate Your Security Service with EDR Validation

Cymulate offers MSSPs an easy way to optimize their services with automated validation of EDR technologies. With integrations with all the leading endpoint solutions, Cymulate security validation helps MSSPs understand their customer's security posture, confirm proper EDR configuration, automate IoCs for the latest threats and optimize EDR with custom behavior rules for better detection and prevention of unknown attacks. By adding automation, MSSPs save time and resources while differentiating their services with validated protection.

Optimize EDR Protection and Detection

MSSPs can easily validate and optimize their customers' EDRs while proving security effectiveness and threat coverage with this simple process:

1. Painless deployment of a single Cymulate agent for EDR configuration.
2. Run attack scenarios mapped to the MITRE ATT&CK® framework on a customer's endpoints to test EDR policies and validate that they are tuned correctly.
3. Apply Cymulate-recommended EDR mitigation rules to guide the detection, prevention and mitigation of threats identified during the assessments. To save time and ensure correct tuning, Cymulate translates the rules so they can easily be adapted to fit any EDR system.
4. Apply vendor-specific mitigation rules suggested by Cymulate to mitigate identified gaps and improve EDR detection and prevention.
5. Validate mitigated policies and schedule continuous automated assessments to monitor drift and maintain an optimized policy baseline.
6. Visualize threat coverage with MITRE ATT&CK heatmaps.
7. Measure and baseline security resilience based on the evidence security resilience to real-world threats.

Solution Benefits



Accelerate onboarding

Configure and tune EDR deployments across different environments with ease.



Validate threat coverage

Prove that EDRs are protecting customers against threats before an event occurs.



Deliver transparency

Demonstrate true state of cyber resilience and improve alignment with clients.



Baseline and benchmark

Drive continuous improvement with metrics and analytics.



Improve retention

Visualize and measure the value of threat coverage and security resilience.



Create upsell opportunity

Identify gaps in cyber protection not covered by current services.

Security and Control Validation Built for MSSPs

Multi-tenancy: Cymulate enables MSSPs to manage customer tenancies from an MSSP parent tenant. With this management model, each tenant is scored individually with separate metrics for a holistic and focused view of customer security posture. MSSPs can also run assessments on multiple clients simultaneously from their parent tenant.

MITRE ATT&CK® Heatmap: Cymulate leverages the MITRE ATT&CK® framework to standardize adversarial tactics, techniques and procedures (TTPs). The MITRE ATT&CK® Heatmap dashboard visualizes simulated attack data, color-coded by risk, to provide an instant visual cue to MSSPs on a client's susceptibility to various attack types.

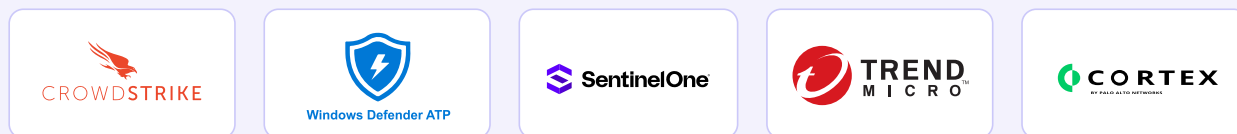


Immediate Threats: Daily updates that apply the latest threat intel to automatically validate controls against ongoing threat campaigns, new exploits and advanced attacks.

Automated IoC updates: Cymulate automatically detects, uploads and mitigates potential threats identified by IOCs without manual intervention. This capability enables MSSPs to enhance their defense mechanisms while reducing the time and effort required for manual IOC management.

Custom dashboards and reports: MSSPs can customize dashboards and reports for each customer based on their priorities and preferences. MSSPs can also aggregate all customer data into one view for better tracking.

Integrations



About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.

Get a Demo