DATA SHEET

Cymulate

# Cymulate Breach and Attack Simulation

## Validate, Measure & Optimize Security Controls

Cymulate Breach and Attack Simulation (BAS) validates cybersecurity controls by safely conducting threat activities, tactics, techniques, and procedures in production environments. With automation and a library of realistic attack scenarios and simulations, Cymulate BAS gives security teams an easy-to-use interface to test security architecture, people, and processes for continuous assessment of cyber resilience.

Cymulate BAS applies the latest threat intel and primary research from the Cymulate Threat Research Group with daily updates on emerging threats and new simulations – all mapped to the MITRE ATT&CK framework. On-demand and scheduling systems allow for both ad hoc checks and automated testing to validate security controls against emergent threat activity, confirm remediation, or prepare for audits and penetration tests.

## How it Works

Cymulate BAS enables customers to securely simulate real-world cyber attacks, thoroughly testing their organization's resilience against known and emerging threats. Cymulate BAS is cloud based and easily deployed with minimal installation and maintenance efforts.

Customers only need to install one lightweight agent per environment to run assessments. The agent facilitates seamless communication between customer devices and the Cymulate platform, ensuring timely updates and efficient transfer of operational data.

## Validate Security Controls

Security is built upon a layered defense that needs continuous testing to assess if controls are working effectively. Cymulate BAS tests for detection and alerting on threats to confirm that controls are functioning correctly or if threats can evade them.

Each vector is scored independently and aggregated for an overall risk score based on industry-standard frameworks. Cymulate BAS integrates with many SIEM, SOAR, GRC, EDR, firewall, and ticketing systems via API to validate and improve security tool detection and response capabilities

## Cymulate BAS Benefits

**REALISTIC CONTROL TESTING**
Offensive testing based on threat actor techniques & tactics, simulated safely

**MITIGATION GUIDANCE**
Clear steps to remediate, close gaps & reduce exposure

**CONTINUOUS VALIDATION**
Repeat assessments to validate mitigations & identify drift

**RISK SCORING**
Benchmarking against peers & continuous improvement with tracked & trending risk scores

**AUTOMATION**
Scheduled & automated assessments for testing on demand or upon threat updates

## Cymulate Dashboard


*The Cymulate dashboard presents an at-a-glance view of threat vectors, their scores, and the overall Cymulate risk score.*

### Test Email Security Controls

The **email gateway capability** challenges email security controls (both native and third-party) by sending emails with attachments containing ransomware, worms, trojans, or links to malicious websites to explicitly defined email addresses within the organization. Cymulate BAS validates control effectiveness for each threat and escalates the email threats that bypass the first line of defense and reach inboxes without being altered or removed.

### Assess Web Gateway Protection

The **web gateway capability** tests employee access to malicious websites through coercion or purposely performing dangerous activities. Cymulate BAS includes tests for both inbound protection against thousands of simulated malicious files and exploits and outbound protection against a daily feed of comprised URLs.

### Challenge Web Application Firewall (WAF) Configurations

The **WAF capability** simulates attacks against web applications that the WAF protects to discover exploitable vulnerabilities in web applications and infrastructure, preventing potentially sensitive information from being stolen. This capability uses payloads such as command injection, XML injection, SQL injection, NSQL injection, and file inclusion. The results of the simulations are mapped to MITRE ATT&CK tactics, techniques, and procedures (TTPs) and Open Web Application Security Project (OWASP) security risks.

### Confirm Endpoint Security Tools

The **endpoint security capability** tests endpoint security platforms and native tools against behavioral and signature-based attacks, lateral movement, and MITRE ATT&CK methods and commands to discover security gaps and misconfigurations.

### Analyze Data Loss Prevention (DLP) Controls

The **data exfiltration capability** tests the effectiveness of DLP security controls and native controls with exfiltration methods such as HTTP & HTTPS, DNS, DNS tunneling, ICMP tunneling, Telnet, email, removable hardware, cloud services, and more. Cymulate BAS packages the data into different file types, including images and office files, and attempts to exfiltrate them using multiple exfiltration methods.

### Identify Exposure to the Latest Active Threats

The **immediate threat intelligence capability** tests security controls against new and emerging threats observed in the wild. The Cymulate Threat Research Group updates Cymulate BAS daily with attack simulations of these latest threats that require urgent attention and action. Threat and simulation updates include insights into threat actors, attack vectors, techniques mapped to MITRE ATT&CK, and indicators of compromise.

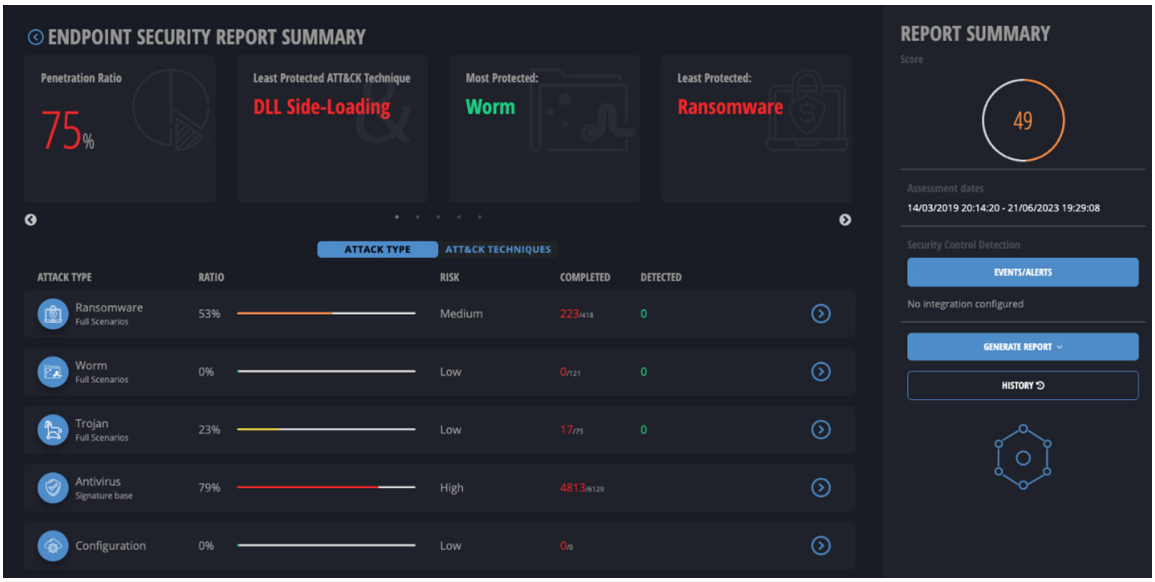
### Validate Security Architecture Against APT Attacks

The **full kill-chain scenarios capability** simulates end-to-end attack scenarios of known advanced persistent threat (APT) groups. These attack simulations deliver and execute production-safe ransomware, trojan, worm, or custom payload via web or email attack vectors. In addition to challenging each attack vector separately, Cymulate BAS tests the effectiveness of various security controls across the entire cyber kill-chain—from attack delivery to exploitation and post-exploitation.

## Analyze Assessment Results & Generate Insights

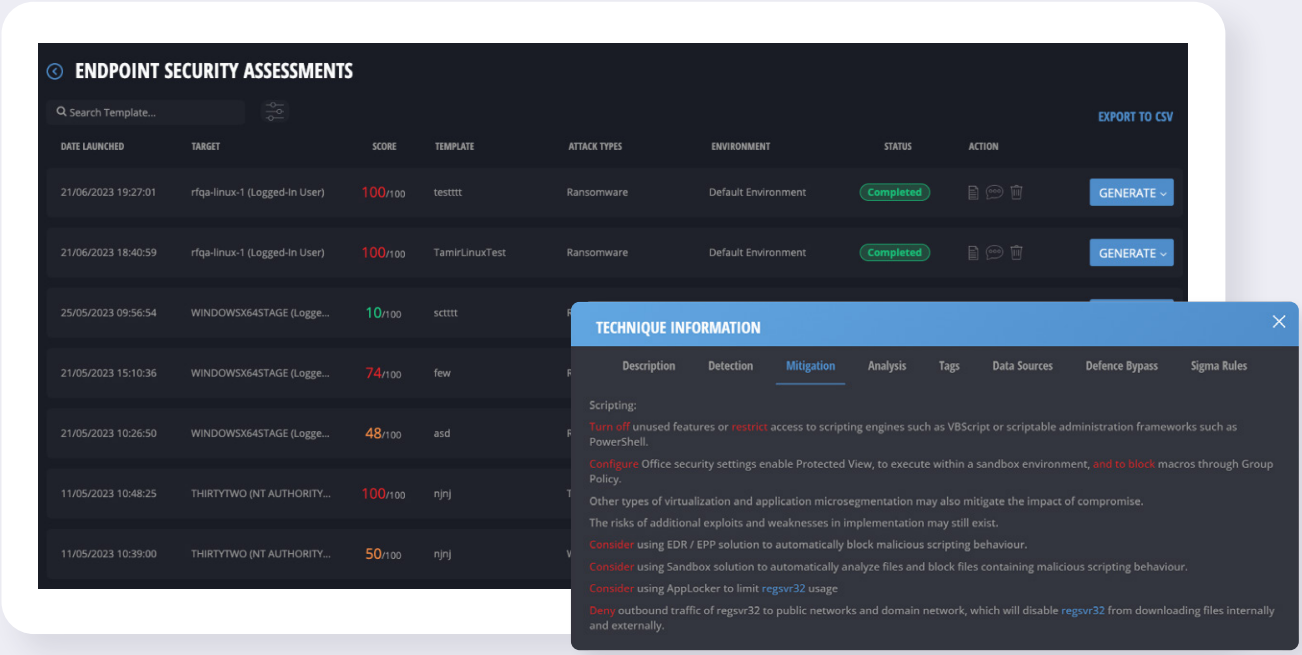
### Control Validation Dashboards

Dashboards and detailed reports summarize results for each Cymulate BAS Scenarios capability and threat vector with both at-a-glance metrics and details (payload/URL/site) from recent tests.



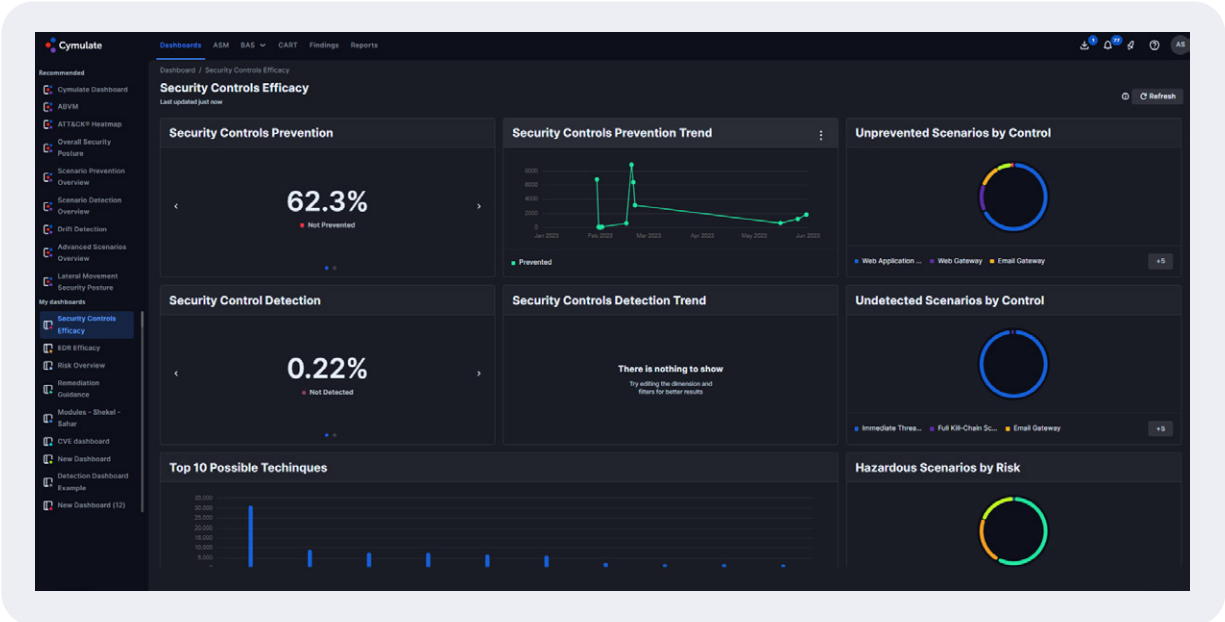
## Assessment History & Mitigation Guidance

Customers can view the history of all assessments and drill down further per assessment to view results and mitigation guidance mapped to the MITRE ATT&CK framework.




## Dynamic Dashboards & Reports

Dynamic dashboards and reports provide organizations with the ability to gather insights based on findings from across the Cymulate platform. Organizations can choose from out-of-the-box templates or create customized dashboards and reports tailored to meet their specific needs and goals. Included in the dynamic reports is an up-to-date view of the latest critical and high-risk security gaps across security controls and policies in the organization Customers use this report as a base for discussion with IT and security engineering teams to prioritize remediation efforts and further investigate the best course of action.



Cymulate

## Map Assessments to the MITRE ATT&CK® Framework

**The MITRE ATT&CK® Heatmap** provides a detailed view of the current state of cyber resilience by visualizing the exposure to each technique. The heatmap correlates all findings from across the Cymulate platform, including filtering and drill-downs into the assessment details for test results and recommended mitigations.


## Validate and Improve Detection and Response with Security Control Integrations

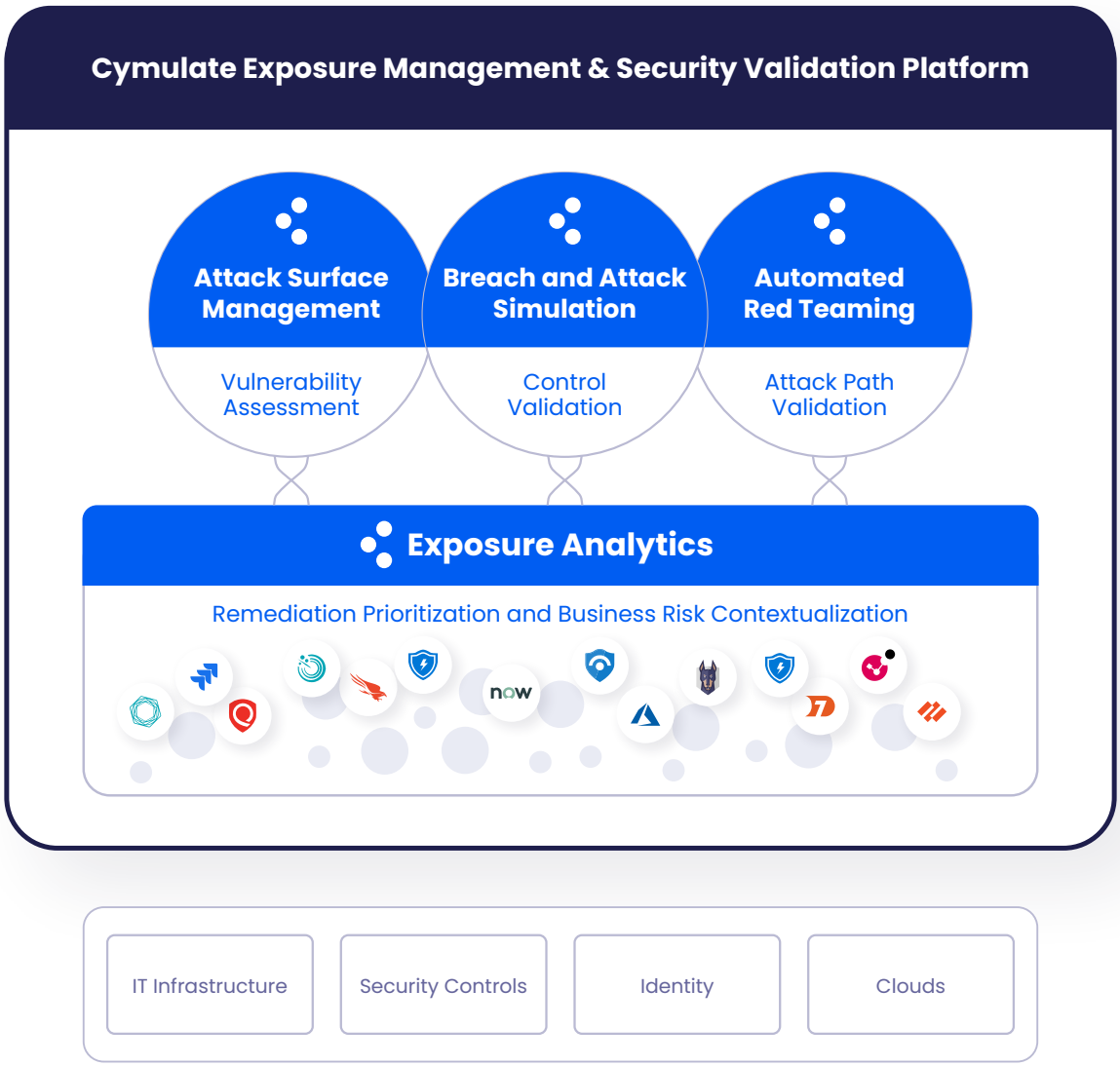
Cymulate BAS integrates with many SIEM, SOAR, GRC, EDR, and other tools via API to augment and benefit existing security solutions. With the API integrations, Cymulate identifies the specific policies that need to be tuned to improve security posture and mitigate control gaps. Cymulate remediation guidance integrates with IT service management to streamline workflows and security task management. Here is just a small sample of the available integrations.

CORTEX XSOAR BY PALO ALTO NETWORKS · CROWDSTRIKE · cybereason · IBM Radar · LogRhythm · SentinelOne · splunk > · sumo logic · Trellix

Cymulate

## The Cymulate Platform

Cymulate BAS is available both as a standalone SaaS offering and as an integrated offering within the Cymulate Exposure Management and Security Validation Platform. The Cymulate platform provides a comprehensive and scalable solution for security leaders, regardless of their security posture maturity, to drive their continuous threat exposure management program and support both the technical and business requirements of scoping, discovery, prioritization, validation, and mobilization.




## About Cymulate

Cymulate, the leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience against emergent threats, evolving environments, and digital transformations. The solution has a quantifiable impact across all five continuous threat exposure management (CTEM) program pillars and on a business's ability to reduce risk by understanding, tracking, and improving its security posture. Customers can choose from its Attack Surface Management (ASM) product for risk-based asset profiling and attack path validation, Breach and Attack Simulation (BAS) for simulated threat testing and security control validation, Continuous Automate Red Teaming (CART) for vulnerability assessment, scenario-based and custom testing, and Exposure Analytics for ingesting Cymulate and 3rd-party data to understand and prioritize exposures in the context of business initiatives and cyber resilience communications to executives, boards, and stakeholders. For more information, visit www.cymulate.com.

Contact us for a live demo

**Start Your Live Demo**

info@cymulate.com | www.cymulate.com