

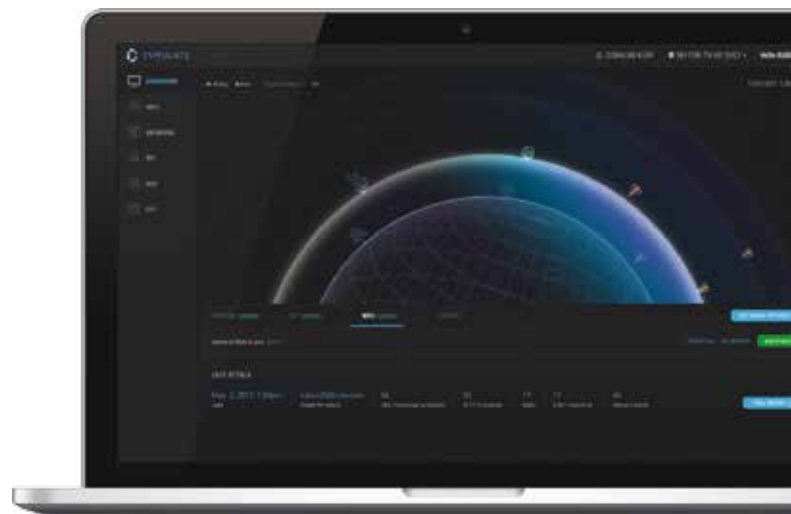


## BREACH & ATTACK SIMULATION

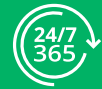
# THE EFFECTIVE APPROACH TO CYBER SECURITY VALIDATION

Cymulate's cyber simulation platform allows you to test your security assumptions, identify possible security gaps and receive actionable insights to improve your security posture.

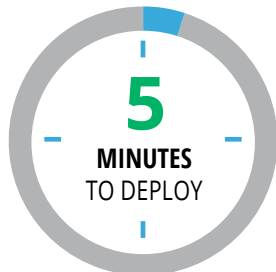
It works by simulating a multi-vector, internal or external attack - which includes the very latest vulnerabilities derived from Cymulate's research unit. The result is a comprehensive validation of your organization's current security posture status - delivered on-demand and with a zero false positive.



## KNOW YOUR REAL SECURITY POSTURE



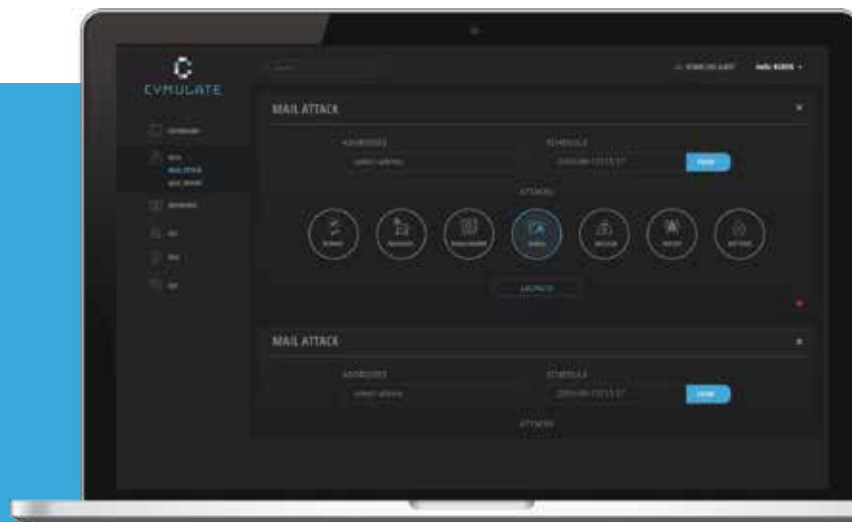
YOU ARE 7 MINUTES AWAY FROM KNOWING IF YOU ARE SECURE!



Organizations now have the power to verify their security posture, on-demand through a unique breach and attack simulation platform. Cymulate's advanced technology provides organizations with the capability to launch simulations of cyber-attacks against themselves, immediately exposing vulnerabilities and providing procedures to mitigate them. Fully-automated and diversified attacks allow for complete security testing anytime, providing organizations with a better understanding of their security posture and allowing them to improve it, continuously. By eliminating false positive, Cymulate delivers only accurate and actionable results.

## STAY ONE STEP AHEAD OF HACKERS

Cyber-attacks today are more sophisticated and dynamic than ever before, as hackers work around the clock to breach networks, steal intellectual property, and disrupt operations. Organizations worldwide invested more than \$80 billion last year to protect their data, block malware, and safeguard critical business processes. Yet despite all the time, money, and effort invested in cybersecurity solutions, many CISOs still can't answer an essential question: **Is my organization safe right now?** Cymulate provides the answer to this question and empowers organizations to validate their cyber defenses more frequently and comprehensively.



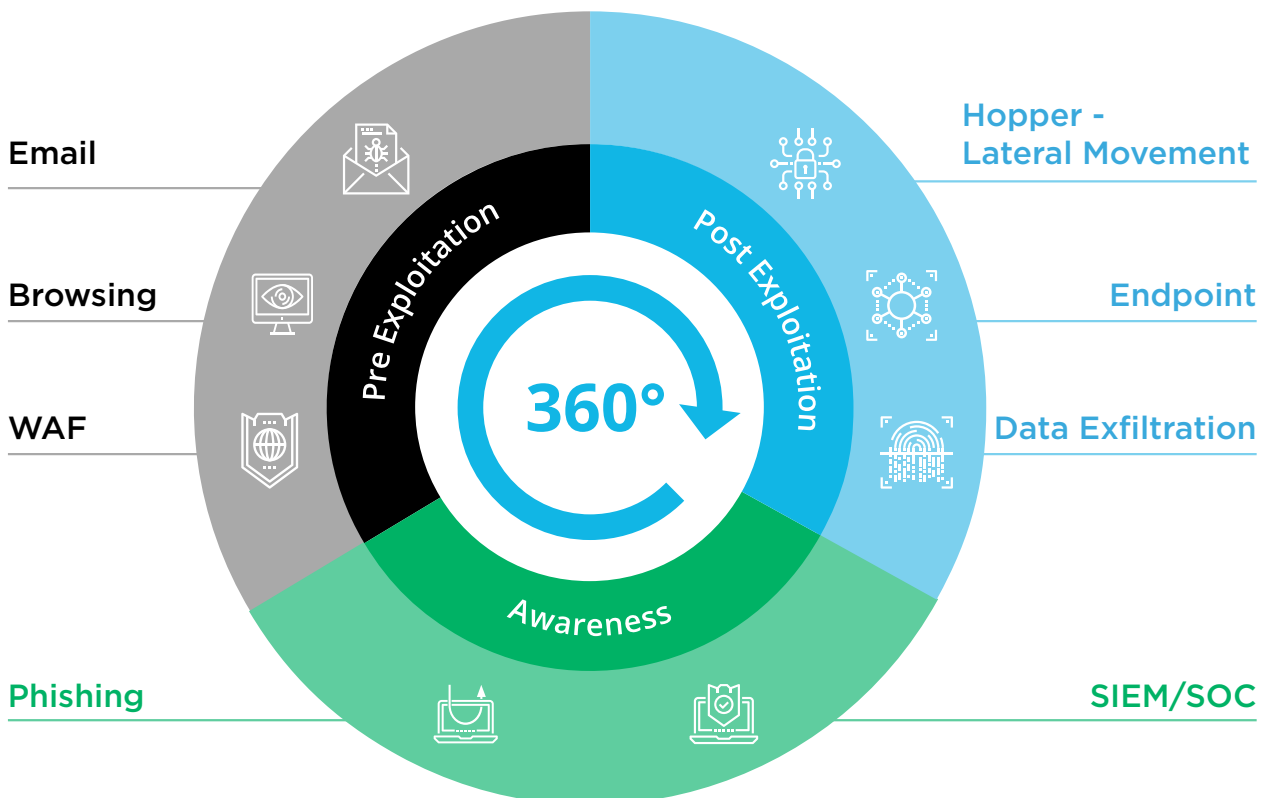
Mail Attack



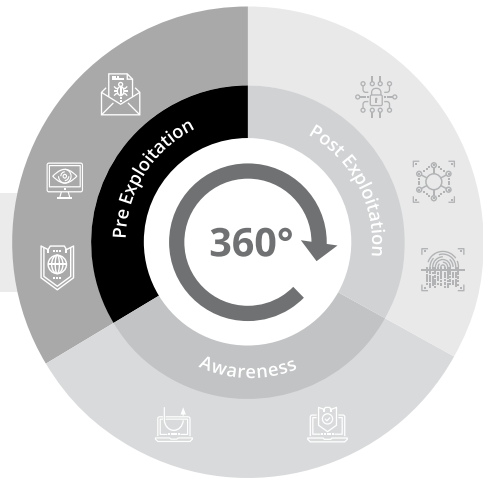
## OUR SOLUTIONS

Cymulate's platform comprehensively exercises your defenses with the industry's widest range of attack vectors, providing an Advanced Persistent Threat (APT) simulation of your security posture at all times. Test your network's ability to cope with pre-exploitation-stage threats in Email, Browsing, and WAF. Analyze your ability to respond to real incidents with our post-exploitation solutions as the Hopper, Endpoint and Data Exfiltration and improve awareness among employees against phishing, ransomware and other attacks.

Gain a clear picture of your vulnerabilities from every point of exposure and anticipate what will really happen prior to the attack.



## PRE EXPLOITATION



### E-MAIL ASSESSMENT

#### Test Your Entire E-Mail Security with Our Vast & Diverse Email Assessment

Despite the widespread use of mail filters, email gateway security and sandboxes, the majority of attacks still originate via email. Poor configuration or implementation of security products might lead to the false assumption that you are safe. Cymulate's Email Assessment module enables organizations to challenge this significant attack vector and test your assumptions.



### BROWSING ASSESSMENT

#### Test Your HTTP/HTTPS Outbound Exposure to Malicious Websites

The vast majority of web malware encounters occur via legitimate browsing of mainstream websites. A significant amount of malware is delivered through browser add-ons – malicious scripts that use Flash, Java and Microsoft Silverlight plug-ins on webpages make up a quarter of malware attacks. Cymulate's Browsing Assessment solution enables you to assess your outbound exposure to malicious websites using common HTTP/HTTPS protocols. Browsing-security tests are performed against a large and ever-growing database of malicious websites.

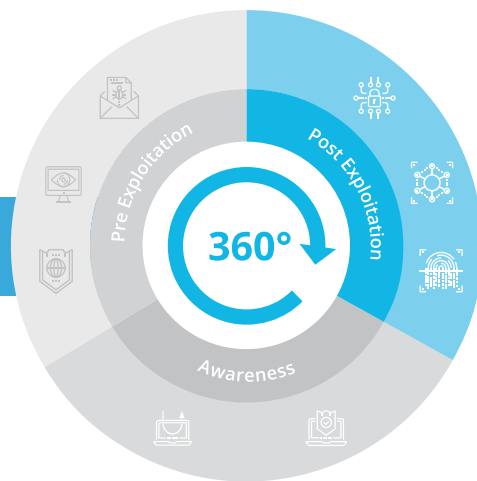


### WEB APPLICATION FIREWALL ASSESSMENT (WAF)

#### Test Your WAF security resilience to web payloads for better protection of your web apps

Web applications have become a central business component; huge amounts of money and effort are spent protecting them. Whereas in the past, IT security teams were tasked with defending just a few enterprise web apps, now they must protect a multitude of web backends of mobile apps, SaaS apps and other cloud-delivered solutions. Cymulate WAF tests your WAF configuration, implementation and features, ensuring that it can block payloads.

## POST EXPLOITATION



### HOPPER - LATERAL MOVEMENT

#### Test Your Windows Domain Network Configuration Using Our Sophisticated Algorithm

Lateral movement inside a Windows Domain Network is a common penetration scenario. As threat actors move deeper into the network, their movements and methods become difficult to detect, especially when they utilize Windows features and tools typically used by IT administrators. Cymulate Hopper's sophisticated and efficient algorithm gathers all the common and clever techniques used by the most sophisticated hackers to move laterally inside the network to reveal the breach spots of your Windows Domain Network.



### ENDPOINT ASSESSMENT

#### Test if your Endpoint solutions are tuned properly and if they are protecting you against the latest attack vectors

Endpoints have become the target of choice by hackers. Organizations reinforce their endpoints with layers of protection such as anti-virus, anti-spyware and behavioral detection. They often deploy highly sophisticated deception systems to lead attackers away from the real endpoints and information to honeypots and traps. Cymulate's Endpoint Assessment simulation shows you which of your products are really protecting your endpoints and which are not working properly, exposing your organization to breach. This Assessment allows you to understand the actual security state of your endpoints by comprehensively testing: Automated behavioral detection (EDR), signature-based detection (Anti-Virus), known vulnerabilities including Windows patches and your 3rd-party software, Hardening of your endpoints according to Proven methodologies. The results will provide you a unified report of all endpoint security aspects in an easy-to-understand format that lets you take specific actions to upgrade the security state of each of your endpoints.



### DATA EXFILTRATION ASSESSMENT

#### Test Your Outbound Critical Data Safely Before Real Data is Exposed

Laws and regulations are increasingly putting the onus on companies to fully safeguard their data. Breaches create huge financial impact and damage a victim company's reputation. Data Loss Prevention products are designed to protect against data exfiltration. Precious digital assets depend almost entirely on DLP implementation, methodology and configuration. Cymulate's Data Exfiltration assessment allows you to test your outbound flows to validate that information assets stay indoors.

## AWARENESS



### PHISHING & AWARENESS

#### Test Your Employees' Awareness of Phishing Campaigns

Designed to reduce the risk of spear-phishing, ransomware or CEO fraud, Cymulate Phishing solution minimizes malware-related downtime and saves money on incident response. Focused on raising organization's employees' security awareness by creating and executing simulated phishing campaigns, it finds weak links in your organization, helping you build tailored training programs that improve and reinforce proper employee cyber-security behavior.



### SIEM/SOC SIMULATION ASSESSMENT

#### Test Your SIEM/SOC Alert Configuration and Team Competence

SOC teams are built to react, and can sometimes get a little rusty. To adapt cyber defenses to the current threat landscape, a proactive security approach is needed. Rather than reacting to the last attack, organizations need to continuously monitor their networks, hunt attackers and create strategic intelligence. SIEM/SOC Simulation Assessment allows organizations to test the SIEM events correlation and to validate the SIEM alerts. Furthermore, it enables the CISO to test the SOC Team Incident Response procedures.





## KEY BENEFITS

### KEY BENEFITS

Mitigate attacks before they happen



Eliminate false positives



Remote test your entire Security



Audit your security products - Maximize your ROI



Plug & Play solution  
Easy to deploy and use



SaaS solution  
No hardware required



Immediate results:  
24/7/365



Fully Automated -  
Continuous testing  
& improvement

## CYMULATE RESEARCH UNIT

Comprising top Reverse Engineers, Penetration Testers & Programmers, Cymulate's distinguished Cyber Support Unit is what sets us apart. Our primary role is to uncover flaws across a variety of vectors, and continuously search for new vulnerabilities and exploits.

With diverse backgrounds encompassing private security, military and intelligence experience, and combined with the understanding of how your business works, our highly experienced security

experts can deliver the visibility into threats and the actors behind them that you need to protect your organization.

We monitor the cyber threat landscape to provide a globalized view of emerging threats, zero-day vulnerabilities, and the tactics, techniques, and procedures (TTP) of advanced threat actors. Our researchers proactively identify new and one-of-a-kind breach methods through emulation of hacker's tactics and strategies.

Results Dashboard



## ABOUT CYMULATE

Cymulate was founded by an elite team of former Israel Defense Forces intelligence officers and leading cyber researchers with world-class experience in offensive cyber solutions. Combining vast expertise in cyber simulation technology with extensive field experience to mimic the latest and most sophisticated cyber-attacks. Cymulate employs software-as-a-service applications to simulate the myriad tactics and strategies employed by hackers to attack network and endpoint security infrastructures.

Cymulate helps companies stay one step ahead of cyber attackers with a unique breach and attack simulation platform that empower organizations with complex security solutions made easy to safeguard their digital assets and maintain business continuity. With Cymulate, organizations can assess their true readiness to handle cyber security threats effectively.

For more information, visit [www.cymulate.com](http://www.cymulate.com)