Cymulate

AMPLIFY Jumpstart

Begin your security validation journey the easy way

What is AMPLIFY Jumpstart?

Cyberattacks are increasingly making headlines and the likelihood that every organization, big or small, will become a victim of an attack is rising. Even knowing the high costs associated with attacks, companies do not continuously test and validate their defenses due to limited resources, among other reasons. With the shortage of cybersecurity professionals, many lack the skills or the time to think and act like threat actors or perform advanced resilience assessments.

With AMPLIFY Jumpstart, you will have an expert-led security validation program at your disposal to begin building your validation efforts. With our experts, you will be able to immediately challenge, validate, and manage **email, web, and endpoint security**, including the **latest threats**. A Cymulate license is included with AMPLIFY Jumpstart.

Who Benefits From AMPLIFY Jumpstart?

AMPLIFY Jumpstart is designed for organizations that understand the importance of ensuring they are protected against daily emerging threats and continuously validating their security controls, but for whatever reason are unable to do so on their own. Our experts will run the assessments and provide actionable reports, so your team can focus on remediation efforts and reducing risk.

Program Benefits

Optimize resources
Instead of running simulations and analyzing the results, focus your team's efforts on remediation

Protect against immediate threats
Know if you are protected against the latest emerging threats and if you are not, receive easy to digest remediation guidance

Prevent security drift
Continuously validate your controls to stay on top of the constantly changing threat landscape and prevent security drift

Quick time to value
Utilize Cymulate's reports to instantly begin improving your security posture and reducing risk, without training or hiring additional labor

What is Included?

Immediate Threat Intelligence

Updated daily with new threat assessments, Immediate Threat Intelligence tests and validates if you are effectively protected against the latest threats found in the wild and provides actionable remediation guidance to close security gaps. Immediate Threat Intelligence runs its assessments through three attack vectors: Email Gateway, Web Gateway, and Endpoint Security.

Email Gateway

Cymulate's Email Gateway vector tests and optimizes your email security posture. This vector challenges your security controls against a comprehensive set of attacks and together with the results, provides actionable remediation guidelines.

Endpoint Security

Cymulate Endpoint Security assessment vector tests and optimizes your endpoint security posture. This vector challenges your endpoint security controls against a comprehensive set of attacks and together with the results, provides actionable remediation guidelines.

Web Gateway

Cymulate's Web Gateway vector validates your organization's web security controls. This vector challenges the controls that protect employees from both accessing and downloading malware from malicious and compromised websites.

How Often are the Assessments Executed?

Immediate Threat Intelligence will execute every time a new emerging threat is uncovered and technical and executive reports will be automatically generated following each assessment. Once a month, the prior month's Immediate Threats will be aggregated into a single assessment and executed again to provide visibility into mitigation actions.

Best practice assessments for **Email Gateway, Web Gateway**, and **Endpoint Security** will be executed on a monthly schedule. Prioritized mitigation guidance, as well as technical and executive reports, will be automatically generated each time an assessment is executed.

Expert-Led Service Benefits

Limited resources and staff are no longer a barrier to accessing the Cymulate platform. Cymulate with assign an expert to work with your security team to provide:

Operations

You and your advisor will create the ideal assessment schedule to maintain a consistent testing cadence. Attend quarterly meetings to review the schedule and modify as needed.

Monitoring

Your advisor will monitor the Cymulate platform's performance to ensure assessments are being properly executed according to the schedule.

Reporting

Technical reports and prioritized mitigation guidance will be provided following each assessment, as well as executive reports to enhance communication with leadership.

About Cymulate

Cymulate Extended Security Posture Management solutions enable companies to challenge, assess and optimize their cybersecurity posture against evolving threats, simply and continuously.

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

Start Your Free Trial