Cybersecurity Risk Validation & Exposure Management

Enter

EXCLUSIVE NETWORKS | Cymulate

Table of Contents

Introduction

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the gold standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end-to-end.

Trusted by hundreds of companies worldwide

Cymulate continuously enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defences, and assure operational effectiveness. Measuring your cybersecurity performance is fundamental towards creating a more secure organization.

There is no downtime for cybersecurity. Security professionals must constantly protect their organization against a wide variety of threats and answer on-demand:

- Are we secured?
- Where are controls performing strongly, and where do gaps exist?
- Do we have too many tools, or too few?
- Are my information security teams overwhelmed, or able to stay ahead of threat activity?
- Will our Incident Response protocols work as expected?
- Can I clearly report to senior leadership and the board on all of this?
- What will all these answers look like next week, next month, next quarter, next year?
- Will our cybersecurity programs scale adequately over time as the business grows and the threat landscape changes?

The Cymulate platform automatically validates that security programs are effective, continuously optimizes remediation efforts and admissible risk levels, and rationalizes requests for additional budget or headcount.

Named 2022 FROST RADAR™ Breach and Attack Simulation Report Innovation Leader, Cymulate's quantified risk evaluation bridges the communication gap between business leaders and technology teams that too often results from the lack of real, reliable, and accurate cybersecurity performance metrics.

WHY CYMULATE

EASY TO USE
with "click through testing" and automation.

EXTENSIVE
attack surface coverage, attack scenarios, and attack campaigns.

COMPREHENSIVE
platform with validation & exposure risk assessment.

MODULAR
to address a growing business's requirements.

The Cymulate Vision

A WORLD WHERE CYBERSECURITY PROFESSIONALS HAVE CONFIDENCE IN THEIR SECURITY POSTURE.

Where they can make better decisions, faster. When they can easily monitor performance and communicate success to business leadership. When they turn the attackers paradigm upside down by being one step head by proactively minimizing threat exposure in advance.

HOW IT WORKS

Products, Solutions & Services

SECURITY POSTURE VALIDATION PLATFORM USE CASES

The Cymulate Platform is designed by defensive testing professionals and is built to scale and grow with the expertise and needs of the various security teams using it. The platform provides easy-to-use and extensive Breach and Attack Simulation (BAS). Unlike traditional Attack Simulation (AS) solutions, the platform also allows for expansion into extended control sets and the use of custom attack scripting and binaries for advanced validation programs.

BREACH AND ATTACK SIMULATION (BAS)

Leverages simulated cyberattacks for security control validation, SIEM/SOAR optimisation, security validation of cloud environments and SOC & Incident Response optimisation.

THREAT EXPOSURE ASSESSMENT

Includes External Attack Surface Management, Full Kill Chain attack mapping and validation of access and segmentation security policies.

ATTACK-BASED VULNERABILITY PRIORITIZATION

Identifies exploitable vulnerabilities and makes staff patching efforts more effective.

Products, Solutions & Services

CYMULATE SECURITY POSTURE ASSESSMENT CAPABILITIES

The Cymulate platform is designed by offensive testing professionals and is built to scale and grow with the expertise and needs of the various security teams using it. The platform provides easy-to-use and extensive Breach and Attack Simulation (BAS). Unlike traditional BAS solutions, the platform also allows for expansion into extended control sets and the use of custom attack scripting and binaries for advanced validation programs.

CORE SECURITY VALIDATION

Allows for any technology staffer from an IT Administrator to a Red-Teamer to perform broad-spectrum, non-disruptive and non-destructive assessments of Email Gateways, Web Gateways, and Endpoint Security, and validates the resilience to immediate threats. Through automation and continuous updates, the organization gains the benefits of BAS, without overwhelming cybersecurity employees.

EXTENDED SECURITY VALIDATION

Brings the idea of simulated attacks to areas of a cybersecurity practice not typically included in BAS solutions. This includes Attack-Based Vulnerability Management (ABVM), which brings together Cymulate assessment results with information from Vulnerability Managers to help understand and prioritize patching. Additionally, lateral movement and various propagation assessments (using Cymulate's Hopper) challenge Network Detection and Response platforms and network segmentation. Data exfiltration defences like Data Loss Prevention tools also be fully assessed for efficacy. Lastly, Cymulate External Attack Surface Management technology emulates an attacker reconnaissance phase, allowing the organization to minimize digital exposure and prioritize patching of true risk.

FULL KILL-CHAIN VALIDATION

By creating entire attack flows from building blocks provided by Cymulate, blue-teamers and others who are less experienced in offensive testing can safely and accurately determine the efficacy of the security stack in its entirety – from infiltration to execution to potential impacts of any gaps that can be leveraged.

ADVANCED SCENARIO VALIDATION

Extends the platform to meet the needs of experienced offensive testing staff and red teams. With the ability to use custom code, scripting, binaries, and other objects; Advanced Scenarios deliver the flexibility necessary for more targeted and intrusive testing under the watchful eye of highly skilled professionals.

Products, Solutions & Services

BENEFITS

AUTOMATION

Is woven into every aspect of the Cymulate platform. The Core Security and Security Validation capabilities provide repeated assessments both on-demand and on set schedules for assessing exposures, confirming remediation, and closure of security gaps. With Advanced Scenarios automation the offensive testing staff can complete more testing, in more areas, more often. The automation will replace manual processes and discovery tasks to reduce employee burnout and enable employee productivity.

MULTI-LEVEL REPORTING

Is native to the Cymulate platform. In-depth technical reporting is available within the User Interfaces of the Cymulate Dashboard. It is also available offline in multiple formats for ease of use by technology professionals. This reporting also provides detailed remediation guidance so that corrective action can be taken quickly and effectively. Executive Reporting is available for every assessment and lays out the business rationale and provides straightforward data for the decision-making by technology teams and those in other business practice areas (Finance, Board Members, etc.).

INTEGRATIONS

Sharing data from Cymulate allows it to be used in other process systems and for security controls to feed data into Cymulate for correlation. Integrations allow technology teams to tune and troubleshoot security controls by seeing both the witnessed results of the actions Cymulate has taken, and the details of what that control saw and did – without violating Separation of Duty more quickly and effectively. API access allows the ticketing system and other orchestration tools to ingest data from Cymulate to power workflows, advise staff, and provide business intelligence.

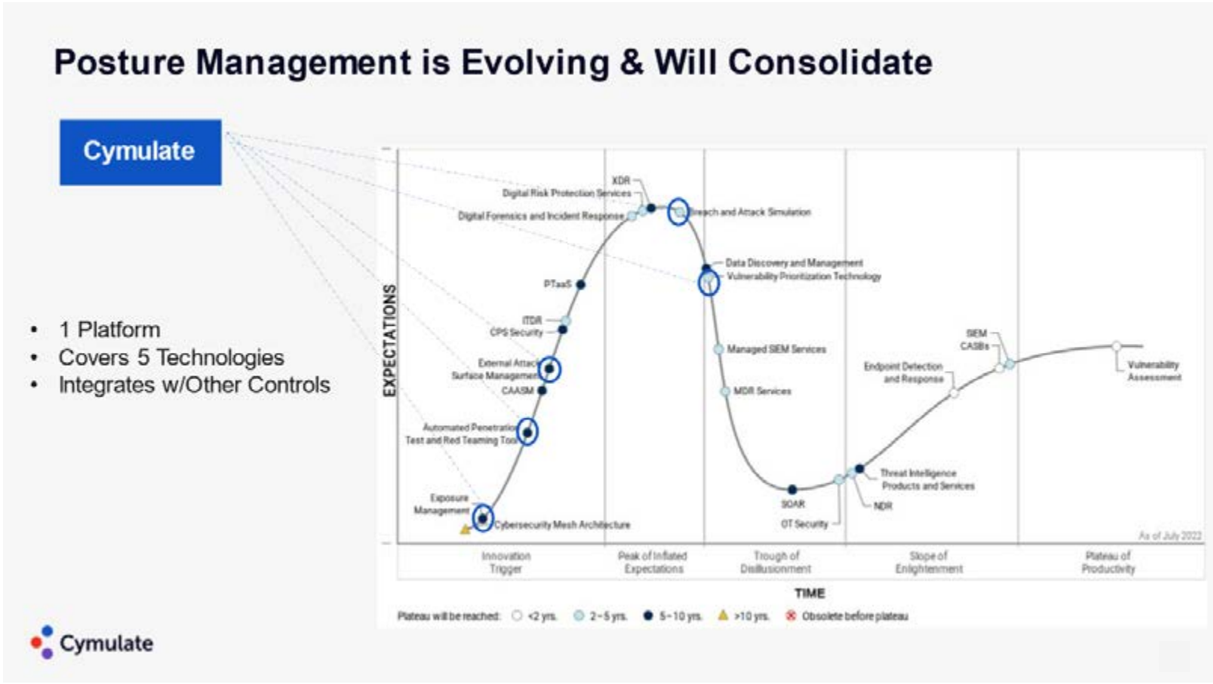
Products, Solutions & Services

INDUSTRY RECOGNITION

NAMED 2022 FROST RADAR™ BREACH AND ATTACK SIMULATION REPORT INNOVATION LEADER

CYMULATE'S QUANTIFIED RISK EVALUATION BRIDGES THE COMMUNICATION GAP BETWEEN BUSINESS LEADERS AND TECH TEAMS THAT TOO OFTEN RESULTS FROM THE LACK OF REAL, RELIABLE, AND ACCURATE CYBERSECURITY PERFORMANCE METRICS.

The Cymulate solution is recognized as the industry's most innovative security validation technology by multiple analysts and awards programs. It has achieved these accolades because the platform goes beyond BAS to provide a flexible and expandable platform for security control validation that meets the organization's technical, and business needs not only for today but also over time as cybersecurity resilience and maturity needs evolve. Integrations allow Cymulate to "pull in" data from other security controls and tools to further enhance and enrich reporting after assessments are complete. Complete reporting for both technical teams and business decision-makers provides the rationalization of both remediation efforts and cybersecurity spending where one or more controls do need to be upgraded or replaced.



Products, Solutions & Services

CUSTOMER VALUE MATRIX

	CYMULATE	ATTACKIQ	MANDIANT	PENTERA	SAFE BREACH
SECURITY CONTROL VALIDATION	✓	✓	✓		✓
IMMEDIATE THREAT READINESS	✓	✓	✓		✓
SIEM & SOC VALIDATION	✓		✓		✓
ATTACK SURFACE MANAGEMENT	✓		✓	✓	
RED TEAM AUTOMATION	✓	✓		✓	
ATTACK-BASED VULNERABILITY MANAGEMENT	✓				✓
NETWORK SEGMENTATION & LATERAL MOVEMENT	✓	✓	✓	✓	
CLOUD SECURITY VALIDATION	✓		✓	✓	

Competition

COMPETITORS INCLUDE:

XM Cyber

ATTACKIQ

PICUS

CALDERA

SafeBreach

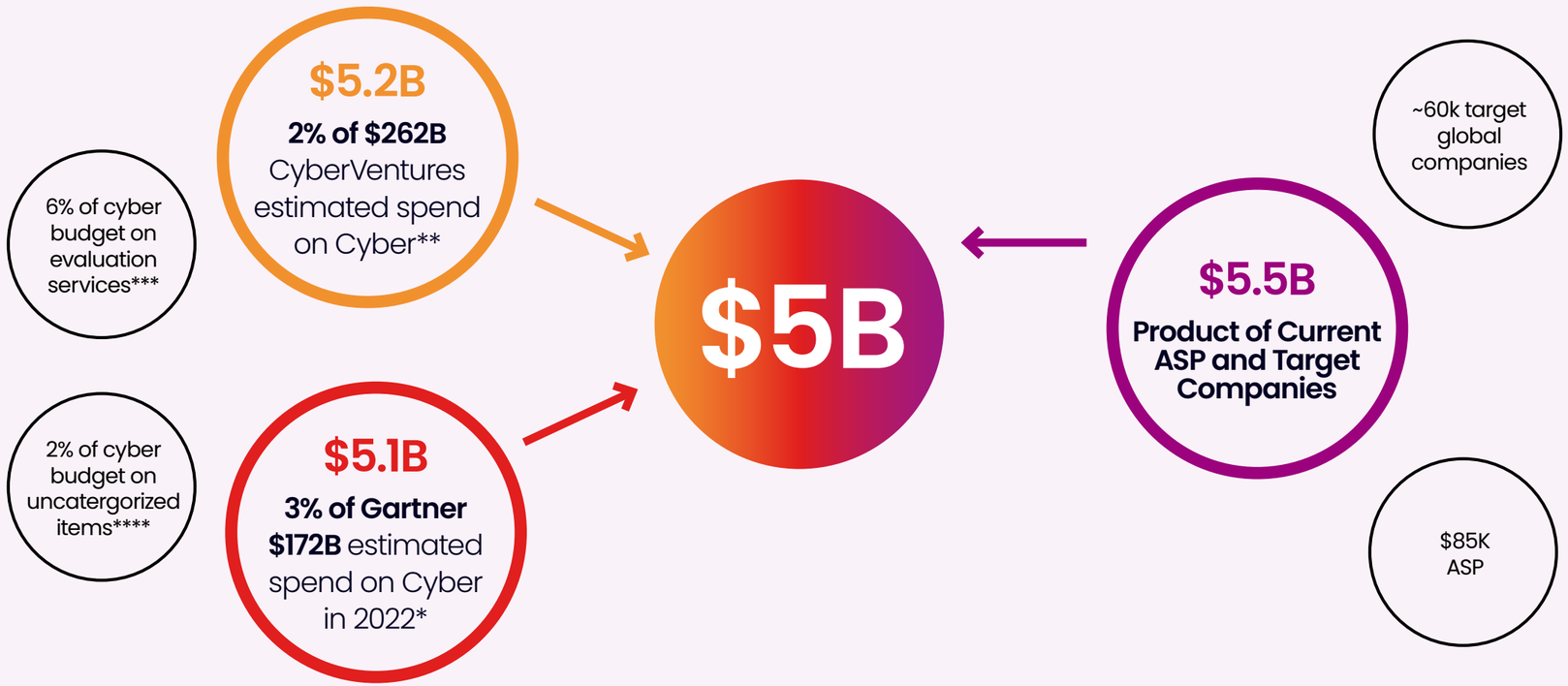
MANDIANT

PENTERA

SNAPATTACK

The Market Opportunity

CYMULATE ADDRESSABLE MARKET



*https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html
**https://cybersecurityventures.com/cybersecurity-spending-2021-2025/
***https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html
****https://www2.deloitte.com/content/dam/insights/us/articles/6507_Cybersecurity-FS-ISAC/DI_2020-FS-ISAC-Cybersecurity.pdf

The Market Opportunity

TARGET AUDIENCES

EXECUTIVE & LEADERSHIP

- Risk Management
- Security Performance Baselining
- Cyber Security Posture Measurement
- "Can I stop the latest attack?"
- Demonstrate ROI on security technologies & services
- Mergers & Acquisitions

RISK & COMPLIANCE

- Continuous monitoring of controls
- Demonstrateadherence to compliance frameworks (NIST, MITRE ATT&CK, etc)
- Third Party Risk Management
- Consistentautomatable, measurement of risk

SECURITY OPERATIONS

- Detection Engineering improvement for Security Operations
- Alert and correlation rule content development & tuning
- Validate log collection and accurate categorization
- Security Analyst training
- Process testing and improvement

SECURITY INFRASTRUCTURE

- Defensive control testing and improvement
- Gap analysis
- Prevent, Detect, Respond validation
- Configuration drift prevention
- Technology analysis
- Multi-environment, multi-cloud posture comparison

THREAT & VULN MANAGEMENT

- Operationalize Threat Intelligence
- Adversarial Simulation
- Attack Surface Discovery & Analysis
- Attack based vulnerability prioritization
- MITRE ATT&CK mapping to known APT groups and their TTPs

RED/PEN TEAM

- Ability to scale and improve efficiency of small teams
- Ability to replay and automate manual activities
- Improve effectiveness of offensive activities through remediation and mitigation guidance

TARGET TITLES:

- CISO
- Security Management teams
- Cyber Security teams
- Security Architects
- Network Security
- Vulnerability Managers
- Pen Testers
- Data protection officers
- CIO
- Head of Risk and/or Compliance
- Blue Teams
- Red Teams
- Ethical Hackers

(based on Exclusive's solution list)

Cymulate Partner Program

PROGRAM OVERVIEW

As a Cymulate Partner, partners can provide continuous security assurance with security posture management to their customers. The Cymulate platform provides our partner community with a powerful business development tool that not only makes sure their client's network security posture is effective, but the reporting generated from Cymulate's platform can help our partners to identify further sales and services opportunities within their customer environments.

Cymulate's Partner Program is the cornerstone to our channel strategy and consists of **three partner levels.**

AUTHORIZED

This is the entry partner level into the Cymulate Partner Program. It contains minimum requirements and partners can be promoted to higher classification levels based on accomplishing designated requirements and capabilities.

ADVANCED

This level is offered to both resale and managed services partners who have made a commitment to revenue goals with Cymulate and a joint business development plan with the regional Cymulate channel team.

ELITE

This is the highest level of the Cymulate Partner Program and this level is offered to both resale and managed services who are committed to growing their business and partnership with Cymulate. There is an annual business level commitment, and a joint business and marketing plan will be developed with the partner and the regional Cymulate channel team.

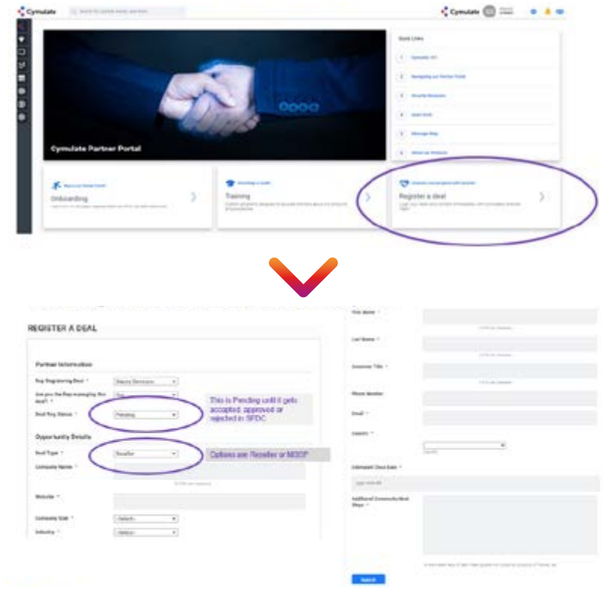
Cymulate Partner Portal

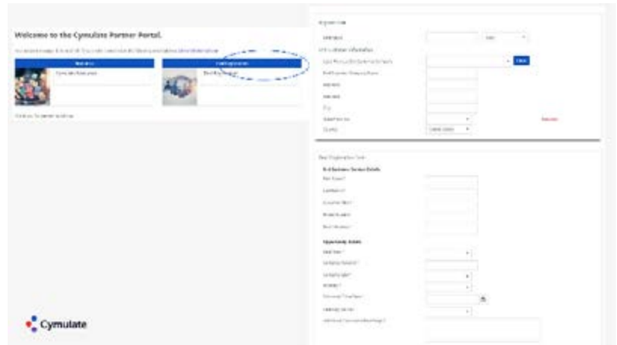
Cymulate has made a significant investment in its partner infrastructure, including the partner portal which will provide Cymulate partners with:

- Access to deal registration
- Role-based partner onboarding
- Content relevant to specific job roles
- Content related to Rapid Response to Immediate Threats
- Demand generation campaigns
- Co-marketing capabilities of Cymulate assets

DEAL REGISTRATION THROUGH PARTNER PORTAL

Partner generated leads should be submitted through Cymulate Partner Portal, https://partner.cymulate.com





Screenshots are taken from the new Cymulate partner portal launching in mid February 2023

Alliances & Integration

INTEGRATING CONTINUOUS VALIDATION INTO YOUR SECURITY ECOSYSTEM

The Cymulate Security Posture Management Platform is a SaaS solution which makes it simple to measure and improve security posture across the full attack kill-chain. Cymulate integrates with various technology partners to validate, augment and benefit existing security solutions, automating and simplifying security control validation.

These integrations enable you to:

- Validate and improve security posture with detection and response capabilities
- Integrate Cymulate remediation guidance into automated workflows
- Prioritise efforts by correlating attacks to the findings of vulnerability management systems
- Streamline security task management with IT and then track, monitor and ensure that security gaps are being closed.

Alliances & Integration

EDR AND ANTI-MALWARE

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

Cymulate integrations are available with the following solutions:

Carbon Black.
Windows Defender ATP
SentinelOne
BlackBerry
CROWDSTRIKE
Cynet
CORTEX BY PALO ALTO NETWORKS
Trellix
cybereason
TREND MICRO
TANIUM

CYMULATE & PALO ALTO NETWORKS

Palo Alto Networks and Cymulate are committed to an ongoing partnership that provides continuous security control validation and exposure management with zero impact on operability.

CORTEX BY PALO ALTO NETWORKS
CORTEX XSOAR BY PALO ALTO NETWORKS

PALO ALTO NETWORKS CORTEX XDR

Cymulate assessments evaluate the efficiency of deployed security configurations by providing production safe attacks against an endpoint.

Cymulate ingests data from Cortex XDR via API and automatically correlates the attack assessments to the XDR data, which includes actions taken during the assessment and the exact log for further investigation.

With this information, organizations validate the efficiency of endpoint defences per policy deployed, resolve misconfigurations, and streamline troubleshooting.

PALO ALTO NETWORKS CORTEX XSOAR

This integration simplifies and automates the security validation and remediation process.

Cymulate proactively validates security efficacy with threat intelligence led attack simulations and the results of each assessment include data I0Cs, and Sigma rules. To expedite and manage the remediation activity, cases are opened automatically in Cortex XSOAR with all the relevant information.

Additionally, each case and its progress are visible from within the Cymulate platform.

Alliances & Integration

SIEM

Verify and optimise the effectiveness of the 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 training and troubelshooting.

Cymulate integrations are available with the following solutions:

splunk> · IBM QRadar · Humio · Rapid7 insightIDR · LogRhythm · Micro Focus ArcSight · Azure Sentinel · NetWitness An RSA Business · sumologic · McAfee

SOAR AND GRC

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:

Cortex XSOAR by Palo Alto Networks · RSA

Alliances & Integration

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 to compensate controls for blocking exploitation (Cymulate), determining and rationalizing priority in patching becomes significantly easier.

Cymulate integrations are available with the following solutions:

TICKETING SYSTEMS

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

Cymulate integrations are available with the following ticketing solution:

The Exclusive Networks Value

VALUE ADDED SERVICES

As well as bringing experience-first networking to your partners we can further enhance the commercial opportunity with Exclusive Networks value added services.

DEDICATED SALES & MARKETING

Tools and campaigns to help promote Cymulate products to your customers as well as support with business planning, account mapping, marketing execution, lead generation and more.

END TO END PARTNER SUPPORT

From configuring customer solutions to providing post sales implementation and support. 2:1 technical resource. Exclusive Networks align two technical engineers to each sales person to support solution design, configuration, demos and staging.

FINANCING & LEASING

With more and more businesses looking at financing options in order to ease cash flow, Exclusive Networks' Finance & Leasing service provides simple and flexible finance options that put liquidity back into the channel. We offer multiple payment options and multiple contract options with global availability.

Get Started Doing Business

STEP 1 Visit the Exclusive Networks Cymulate landing page **to find out more** https://www.exclusive-networks.com/introducing-cymulate/

STEP 2 Request sales enablement training

STEP 3 Identify customers and prospects for targeting

STEP 4 Engage with marketing and schedule call out days

Contacts

GLOBAL

ANA LOVRIN
Global Business Development Manager
ana.lovrin@exclusive-networks.hr

HARRIET GOUGH
Global Marketing Manager
hgough@exclusive-networks.com

EXCLUSIVE NETWORKS

Cymulate