

CASE STUDY

Investment Firm Evaluates all Angles of its Security Posture with Cymulate

Challenge

The cybersecurity team of an Abu Dhabi investment firm must protect the organization's exclusively cloud infrastructure. The investment firm's cybersecurity function is divided into security architecture, IT governance and risk. The firm's small in-house security team has one person leading each function and works with third-party partners to outsource operational and monitoring activities.

With limited resources, the security team faced three main challenges:

- No real-time visibility of the organization's security posture**
 The security team would conduct manual third-party security assessments every six months to validate its security program, but these were expensive and provided point-in-time snapshots that were quickly outdated. The team wanted a way to validate its security controls in real time.
- Difficult to immediately assess against emerging threats**
 When a new emerging threat was announced, the team had to research the indicators of compromise and manually create assessments to validate if the organization was protected on Windows, Mac, and Linux machines.
- Unable to prioritize vulnerability patching**
 The security team couldn't keep up with each new vulnerability being released. However, the team didn't have the context to understand which vulnerabilities needed to be prioritized because they could be exploited.

The Cymulate Solution

The security team decided that breach and attack simulation (BAS) would provide the necessary automation to improve its security posture and increase productivity. After evaluating various BAS tools in the market, the investment firm decided that Cymulate BAS and Cymulate BAS Advanced Scenarios were the best fit for its organization because they allow for extensive customization and provide the most detailed assessments.

The investment firm's Vice President and Head of Cybersecurity reflected on his choice: **"If I run an endpoint assessment, Cymulate doesn't just stick to validating the endpoint. Unlike the other vendors, Cymulate tries to connect the dots and also checks the web and the application layers to see where the risk and vulnerabilities are."**

Overview

Industry	Venture Capital
HQ	UAE
Company Size	51-200 employees



Cymulate is a trusted platform that tells me anything I need to know about my organization's security posture.

Vice President and Head of Cybersecurity

Solution

- Breach and attack simulation (BAS)
- BAS advanced scenarios

Results

- Emerging threats evaluated in 1-2 hours
- 360-degree cloud security posture visibility
- Continuous automated assessments

After a smooth and easy implementation process, the Vice President and Head of Cybersecurity says that his team uses Cymulate BAS to:

Run continuous assessments

“Instead of bringing in a vendor to run assessments every six months, we run automated assessments every week. We know how secure we are at any given moment.”

Comprehensively evaluate its security posture

“Cymulate gives us 360-degree visibility of our entire security posture, something we never had before.”

Immediately assess against emerging threats

“Before Cymulate, it took us 2 to 3 days to evaluate a threat — now it takes us one to two hours because all we need to do is run the assessment that Cymulate prepares for us.”

Prioritize vulnerability patching

“Cymulate shows us our security gaps so we know what to focus on, where to prioritize our patching, and discover where we should invest most of our efforts.”

Customize chained assessments

“Cymulate BAS Advanced Scenarios provides a chained scenario-based approach which enables us to evaluate all the angles of our security posture, instead of just testing security controls one by one.”

Outcomes

The security team has embedded Cymulate into many of its security processes:

- **Measurement of security performance** — Cymulate provides a security baseline for continuous improvement to measure and track the third-party SOC's performance.
- **Major OS updates** — Each time a major OS update is deployed in the firm's user environment, the team runs a Cymulate assessment to ensure the deployment doesn't raise the organization's risk score.
- **Tabletop exercises** — The security team evaluates its SOC's readiness for an attack with Cymulate assessments. The team has plans to expand these exercises into the business user environment to evaluate employee preparedness in case of an attack.
- **Security reporting** — The team integrated Cymulate with its power BI tool so all the information and data that flows from Cymulate appears on the investment firm's centralized reporting platform and impacts decision-making.

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.