CASE STUDY

Financial Regulatory Authority Strengthens Security and Gains Continuous Visibility with Cymulate

Limited Visibility and Reliance on Point-in-Time Testing

With a lean team of five responsible for securing a complex internal environment, the security team at a financial regulatory authority in Hong Kong managed multiple layers of defense, including email security, web gateways, firewalls and endpoint protection. Yet despite this layered architecture, they lacked visibility into how these controls actually performed against real-world threats.

Security validation relied on periodic penetration tests conducted once or twice per year. Without continuous testing or an internal red team, the team had no efficient way to validate configurations, test changes, or uncover hidden gaps across their security stack. They were also unable to test their defenses against new and emerging threats as they appeared.

As a result, the team operated with limited assurance that their controls were functioning as intended, leaving potential blind spots undetected.

The Cymulate Solution

To gain the visibility they were missing, the team adopted Cymulate to introduce continuous security validation into their environment. Instead of relying on periodic penetration tests, they can now continuously test their controls across email, web gateways, endpoints and network defenses using real-world attack simulations.

The impact was immediate. Early on, Cymulate helped the team discover that default security control settings were blocking less than 70% of known threats. What had appeared to be a well-protected environment was leaving significant exposure to common attack techniques.

The cybersecurity manager reflected, **"Cymulate showed us that relying on default settings wasn't enough. We were able to identify where our controls were underperforming and make targeted improvements based on real validation data."**

With this insight, the team established Cymulate as an ongoing validation layer, continuously testing, identifying gaps and strengthening their security controls over time. As a result, they moved from periodic testing to continuous validation, gaining greater visibility into their environment, improving control effectiveness and strengthening their ability to respond to emerging threats.

Overview

Industry: Financial Services

HQ: Hong Kong

Company Size: 201-500 employees

Use Case

Threat Validation

Control Optimization

Results

Continuous validation of security controls

Improved, data-driven security vendor selection

Faster, automated validation of threats

> Cymulate helped us move from point-in-time testing to continuous validation, giving us much better visibility into our security posture."
>
> – Cybersecurity Manager

Validate security controls continuously

"Cymulate is our trusted platform for continuous testing. It gives us an independent way to test our environment and see how our controls perform, without relying on point-in-time testing or a red team. Vero AI also helps us easily create templates and automate assessments."

– Cybersecurity Manager

Evaluate new security vendors

"We use Cymulate to evaluate new tools before purchase, comparing their performance in our environment and selecting the vendor with the highest Cymulate score. Cymulate is also embedded in our tender process, where vendors are evaluated based on their results."

– Cybersecurity Manager

Test against emerging threats

"Cymulate helps us test new threats and understand how our controls would perform if attacked. The live threat feed provides visibility into how the threat landscape is evolving."

– Cybersecurity Manager

Benefits

- **Continuous visibility into security posture.** Ongoing testing provides clear insight into how security controls perform across the environment.
- **Faster identification of security gaps.** The team can quickly uncover misconfigurations and weaknesses that would otherwise go undetected.
- **Data-backed security investment decisions.** Cymulate enables objective comparison of new tools, helping the team select solutions that perform best in their environment.
- **Stronger readiness against emerging threats.** The team can test new threats as they arise and understand how their environment responds.