

## CASE STUDY

# Credit Union Boosts Threat Prevention & Detection with Cymulate

### Proving Security Effectiveness: The Real Challenge

A large North American credit union with more than 1,500 employees and a widely distributed branch network understood that cybersecurity was critical, but proving that its defenses actually worked was increasingly difficult. Manual testing and periodic assessments consumed valuable analyst time while delivering only point-in-time visibility into risk.

The urgency escalated after a U.S. peer credit union suffered a devastating ransomware attack, exposing a critical gap. While backups and business continuity plans were regularly tested, security controls were not being validated against real-world attack techniques.

Key challenges included:

- Limited visibility into control effectiveness between annual assessments
- A reactive security posture focused on theoretical risk rather than exploitable exposure
- Difficulty prioritizing vulnerabilities based on real-world attack paths
- Increased pressure from regulators, executives and the board to demonstrate measurable security effectiveness
- A complex, distributed environment spanning headquarters and dozens of remote branch locations

Security leadership needed a way to continuously validate defenses, reduce operational overhead, and clearly communicate security posture and progress to executive stakeholders.

### The Cymulate Solution

Following a competitive evaluation of exposure validation platforms, the organization selected Cymulate for its clear, customizable executive reporting, rapid time-to-value, and ability to scale continuous validation across a distributed environment—without the complexity of competing solutions.

With Cymulate, the credit union shifted from periodic, manual testing to continuous, production-safe validation, enabling the security team to measure control effectiveness in real time without disrupting business operations.

#### Overview

Industry: Banking

HQ: Florida, USA

Company Size: 1K–5K employees

#### Results

**50%** increase in threat detection rates

**20%** increase in threat prevention rates

**20+ hours/month** saved validating defenses against emerging threats

**40%** more efficient vulnerability prioritization through exposure validation

**4X** more environments assessed compared to manual testing

**40 hours/quarter** saved on control effectiveness and compliance reporting

**\$20,000** annual cost savings by replacing manual compliance testing



I've been using Cymulate for a while now, and the platform has truly impressed me with its comprehensive capabilities. The production-safe and data-driven approach is just icing on the cake!

– SVP Information Security Officer

## Automation and continuous validation

"We've automated security control testing with Cymulate to ensure that changes in our environment do not introduce unintended gaps. That level of continuous, automated validation has been a game changer for us."

– SVP Information Security Officer

## Scalable validation across distributed environments

"We deploy Cymulate agents across headquarters and remote branch locations, and the ability to break down results by environment gives us precise visibility into where controls are working and where they're not."

– SVP Information Security Officer

## Continuous testing against emerging threats

"Cymulate continuously pulls real indicators of compromise from trusted sources, tests them immediately and shows us which threats can actually penetrate our defenses. That visibility allows us to act before those threats become incidents."

– SVP Information Security Officer

## Exposure-based vulnerability prioritization

"Our organization is heavily focused on risk and compliance, and Cymulate immediately shows us the level of risk for each exposure. That clarity helps us focus on what truly matters, rather than chasing theoretical vulnerabilities."

– SVP Information Security Officer

## Executive-ready reporting and board communication

"I am required to report security metrics to the Board, which is critical for effectively communicating risk. Cymulate provides clear visibility into the effectiveness of our security controls, enabling informed governance and oversight."

– SVP Information Security Officer

## Benefits

With continuous security validation in place, the credit union improved cyber resilience by adopting a measurable, proactive approach to security effectiveness.

- Reduced reliance on assumptions and point-in-time assessments in favor of ongoing confidence in security posture
- Enabled the security team to shift focus from manual testing tasks to meaningful risk reduction
- Improved decision-making by aligning remediation priorities with real-world attack paths and business risk
- Strengthened resilience by identifying and addressing security gaps before they could be exploited
- Built executive trust through clear, evidence-based communication of security effectiveness and program maturity

## About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience, accelerate detection engineering, drive continuous threat exposure management, and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit [www.cymulate.com](https://www.cymulate.com).

[Get a Demo](#)