Ransomware Resilience Assessment

Solution Brief

Cymulate

Challenges

All companies are susceptible to ransomware attacks, regardless of the organization's size or industry. IBM reports[1] that the average cost of a ransomware attack in 2022 was $4.54 million. It is important to note that following a ransomware attack, an insurer may deny the claim if the policyholder fails to comply with the policy requirements[2]. For example, if the policyholder does not have adequate documentation to support the loss or if the insurer suspects that the policyholder may have been complicit in the attack.

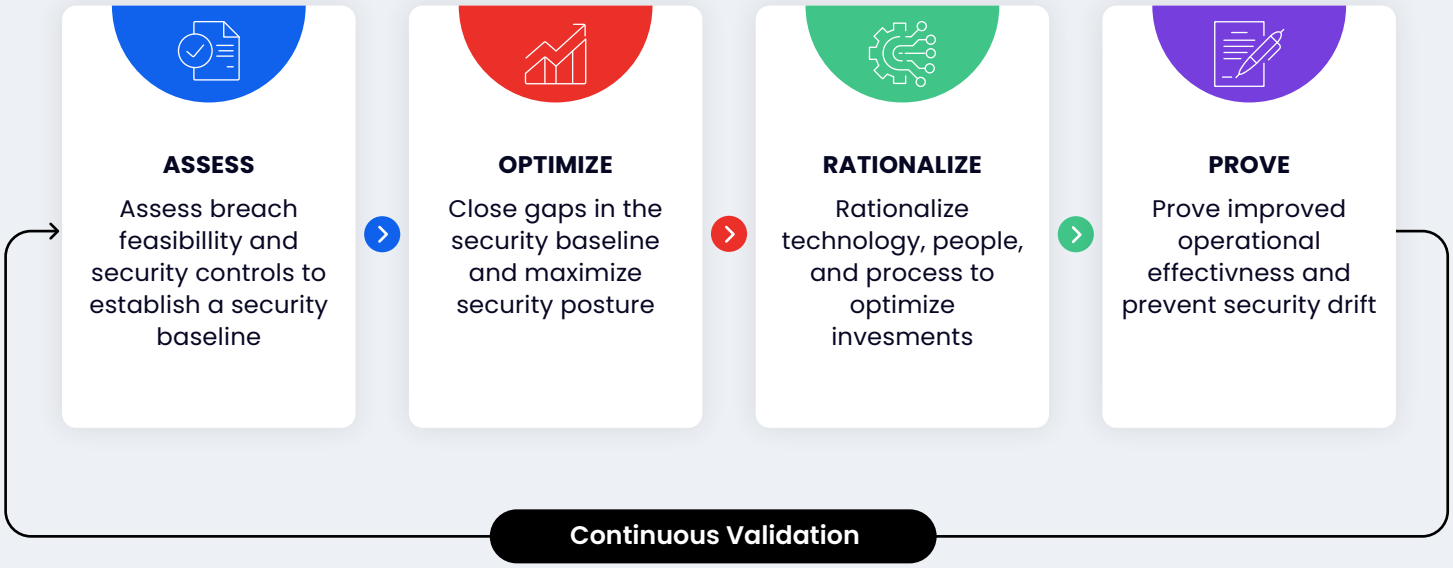
To mitigate the risk of a ransomware attack, companies implement security controls, keep software and systems up to date, use strong passwords and multi-factor authentication, train employees on how to identify and avoid phishing scams, and have a response plan in place. These precautions are vital to mitigate and reduce risk, but it is impossible to know if these measures work until an attack occurs.

Overview

Organizations utilize Cymulate's Ransomware Resilience Assessment to ensure they are prepared before an attack occurs. The platform's broad range of assessments test for breach feasibility, as well as what would occur if a ransomware attack successfully penetrated an organization. Additionally, attack simulations of new and emerging ransomware payloads are added daily to the platform so organizations can immediately assess their security against the latest threats.

The results of each assessment are used to identify any weak points in the organization's cyber security posture. The platform also provides remediation guidance so organizations can close gaps and optimize protection against ransomware attacks.

Assess Ransomware Resilience with Cymulate



1 https://www.ibm.com/reports/data-breach
2 https://www.jdsupra.com/legalnews/cyber-insurance-carriers-increasingly-3361129/

Main Features

Attack-based analytics assess security controls for block and detection rates, determining if the current controls are effective against ransomware.

Threat intelligence-led assessments of new and emerging ransomware payloads are added daily to the platform so organizations can immediately assess their security against the latest threats.

Technical and executive reports provide a comprehensive overview of an organization's security posture and generate insights into where security is strong and where more resources are needed.

Case Studies and Customer Success Stories

Hedge Fund Optimizes Testing Against Emerging Threats with Cymulate

A global hedge fund with a few hundred employees has offices in the US, Hong Kong, and London.

Challenge
Continuously validating the hedge fund's security controls and testing them against emerging threats and ransomware was too difficult and time-consuming to accomplish manually with a small security team.

Solution
Implement Cymulate's easy-to-use platform to automate security control validation, test immediate threats, and increase team efficiency by scaling adversarial skills.

Benefit
With Cymulate, the small security team can perform more tests, focus their remediation efforts, and continuously validate its security posture.

Read more

Private Equity Firm and Media Giant Reduces Risk with Cymulate

Daily Mail and General Trust (DMGT) is a British multinational media company, the owner of the Daily Mail and several other titles.

Challenge
Securing a highly dynamic environment with lots of M&A activity and overseeing a diverse portfolio of companies. Major concern over ransomware attacks while running lean with only the CISO overseeing all security activities.

Solution
Use Cymulate to measure risk reduction, optimize security control configurations, and convey measurable improvement to company executives and the Audit & Risk Committee of the Board.

Benefit
Fast. Easy. Automated. Cymulate brings confidence through continuous security validation.

Read more

> At any given time, Cymulate provides us insights into attacks that can penetrate us and how to mitigate the attack. I can check my remediation efforts, know that I am protected and that all my controls are working as they should
>
> **Yoav Gefen, CISO, Maman Group**

Additional Resources

Cymulate

Outsmart Ransomware with Security Controls Validation

Read More

Backed by the Industry

Awards and Accolades

About Cymulate

Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. This modular solution addresses a wide variety of business and technical use cases and scales from out-of-the-box simulations to full customization for advanced attack simulations. With Cymulate, companies assess, optimize, rationalize, and prove their security program with minimal resource investment. Security professionals and business stakeholders leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to executive leadership, and gain evidence for compliance and regulatory purposes.

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

Start Your Free Trial

info@cymulate.com | www.cymulate.com