Zero Trust Validation

Solution Brief

Challenges

The zero-trust security model operates under the assumption that no user, device, or system can be trusted by default, necessitating continuous verification of identities, devices, communications, and transactions. It cannot function as a "set it and forget it" type of system.

Integration of legacy systems and infrastructure, maintaining a balance between security and user experience and productivity, overcoming organizational resistance and cultural shifts, and ensuring scalability and flexibility to accommodate growth and change all demand frequent adjustments. In complex systems (like most applications and platforms), any adjustment can produce unexpected consequences, and validation ensures that new security gaps do not emerge undetected.

Yet, validating the efficacy of zero trust implementation is fraught with challenges. Those range from mapping users, devices, and resources; including their interactions and dependencies to balancing security with user experience and productivity. As any new deployment, alterations, changes to users and permissions, or change in the threat landscape can introduce gaps in compartmentalization; maintaining zero trust requires continuously testing the efficacy of access policies, definition, and enforcement to avoid unexpected breaking of micro-segmentation.

Overview

The Cymulate security validation platform's simulates thousands upon thousands of cyber-attacks to verify that zero trust segmentation functions as intended. Its continuous assessments validate segmentation from various perspectives, including user access control, attack path mapping, and data protection. The platform offers off-the-shelf attack simulation templates that can be customized to suit unique security needs and environments.

Creating or customizing attacks to produce environment-specific validation is easily achieved through a wizard that includes an extensive repository of executions, templates, sigma rules, and more.

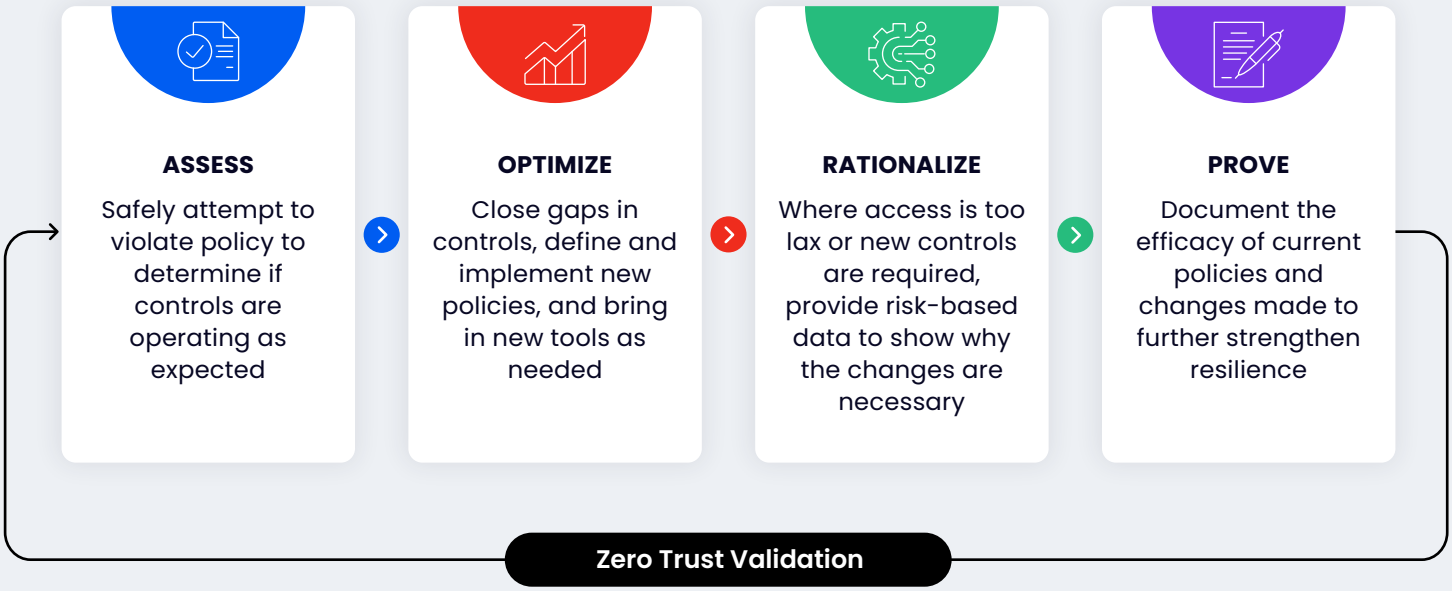
The platform automatically generates detailed reports that provide in-depth analysis of each uncovered identified weakness or gap; complemented by actionable mitigation guidance. This enables the swift identification of security gaps and accelerates the remediation processes.

Attack templates – both out-of-the-box and custom built for the environment - are schedulable and repeatable. This can accelerate implementation of a continuous zero trust validation process capable of identifying emerging gaps as they appear.

Benefits

- Simple to deploy
- 360° security posture visibility
- Continuous threat exposure monitoring
- Increases operational efficiency
- Improved security posture
- Security drift detection and prevention
- Reduced costs

Capabilities of Zero Trust



Main Features

Comprehensive set of automated attack simulations
120 000 out-of-the-box production-safe attack simulations, easily customizable with a drag-and-drop wizard as needed.

Validate that any administrative
Activity in these platforms generates alerts for proper checks and balances.

Assess the effectiveness of the detection
Of unauthorized and unauthenticated attempts to access sensitive data; and abnormal behaviors that do not match roles and permissions.

Automatic report generation
Out-of-the-box and customizable executive and technical reports facilitate communication across departments, auditors, and stakeholders. Technical reporting also accelerates mitigation with actionable guidance and integrated ticketing for streamlined mitigation management.

Case Studies and Customer Success Stories

Using Cymulate, I was able to find out that several of my security products were not configured as I wanted them to be, I discovered had several vulnerabilities based on the misconfigured products. Once everything was configured correctly, I tested the system again using Cymulate. And the security hole within my network was eliminated.

Tamir Ronen
CISO, Assuta

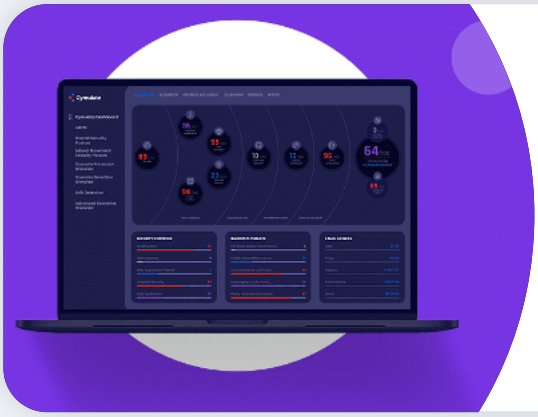
We chose Cymulate because we saw right away that it would require much less effort and time on our part to get immediate and effective insight into a security program and the solution could easily be leveraged globally.

Itzik Menashe
VP Global IT & Information Security , Telit

We chose Cymulate because we saw right away that it would require much less effort and time on our part to get immediate and effective insight into a security program and the solution could easily be leveraged globally.

Itzik Menashe
VP Global IT & Information Security , Telit

Additional Resources



Cymulate

Demo Recording
Lateral Movement: Breaking Down & Identifying

Watch Now

Cymulate

Webinar
Making SecOps & Security Leaders More Successful

Watch Now

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