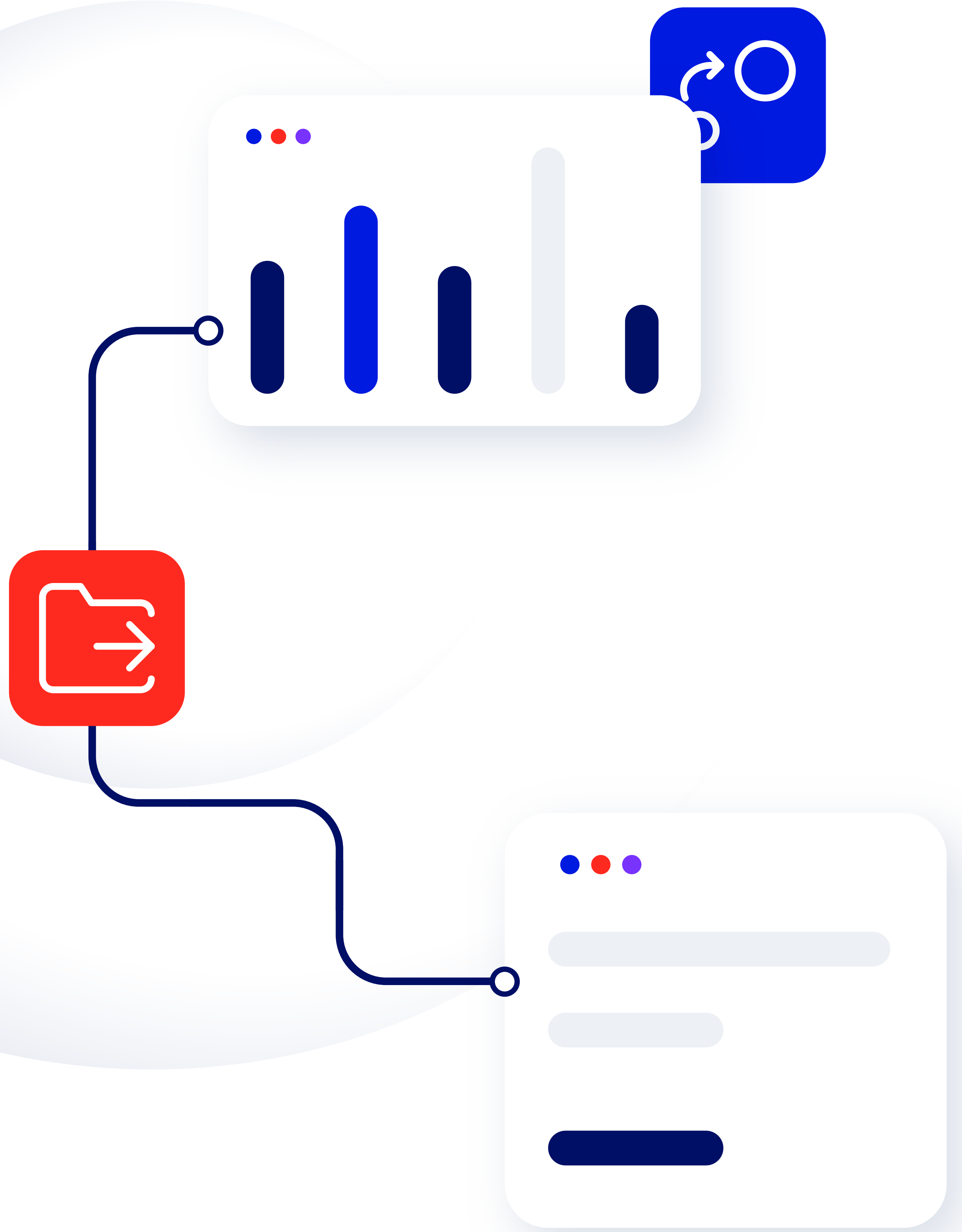
Cymulate

Security Validation Essentials



Like many organizations, you've probably made a massive investment in cybersecurity – both in technology and resources. Global spending on cybersecurity is nearly $200 billion each year, with software and controls accounting for about half. And as this investment continues to grow in parallel with the fast-evolving threat landscape and a complicated, widespread IT environment, so does the scrutiny from executive leadership and the Board. This means you must be able to deliver quantifiable cyber risk results while answering the age-old question, "Are we secure?" with confidence.

The reality is, you're probably running manual penetration tests or investing in internal red teams. While these methods work to identify weaknesses in your controls, they're leaving you with dangerous blind spots. Pen-testing and red teaming are resource-intensive and expensive. Worse, they only reflect a set point-in-time. So, while you're ticking through the list of misconfigurations, malicious payloads and links from your last report, new ones will emerge – and could go undetected for months.

All of this means that you may not be as secure today as you were six months ago. And just because you've invested in security controls doesn't mean your security is under control.

It’s Time to Automate Your Control Testing

You’ve made a significant investment in security controls from the endpoint to cloud, and it’s time to make sure they’re working as expected and can stop a breach. This starts with automation.

Security Control Validation is the answer to manual, point-in-time pen-testing. It’s automated and ensures key security controls in your environment are tested and validated on a continuous basis while optimizing the controls for better protection. It allows you to:

Optimize what you have

Security Control Validation enables you to make the most of the tools you already have in place while continuing to make improvements on a consistent basis by implementing new detection rules for the latest threats. This also applies to your MSPs.

Measure continuous improvements

Know where you are from a security standpoint and know where you need to improve. Set a baseline of how secure you are today and measure changes and improvements over time. This can be impacted by things like the efficacy of your tools and impacts of the changing threat landscape.

Manage Drift

Your IT environment, which includes your controls, doesn’t remain still, especially in the cloud. And the threat landscape is constantly changing. Without the right visibility, unknown changes to policies, controls and applications could cause a ripple effect if left undetected.

Breach and Attack Simulation

There are two ways to know if your security controls are working: You can suffer an attack or you can simulate one.

By simulating an attack, you're testing whether the controls are set up and working properly in an environment that is dynamic and constantly changing, as the threat landscape ebbs and flows, and as threat actors become more sophisticated with new techniques.

The right Security Control Validation solution will give you the ability to conduct attack simulations and probe these primary controls:

Email controls

Are your email servers capable of detecting a phishing, malware or social engineering attack?

Network controls

Can you confirm that your firewalls are optimally designed to guard against a malicious actor? This might include validating that detection systems are robust enough to guard against intrusive activity.

Web controls

Are your web gateways and proxies up to the task of preventing or detecting malicious links and payloads?

Cloud controls

Does your cloud architecture contain security gaps and redundancies that could provide a portal for malicious actors to steal or exploit your vital assets?

Endpoint controls

Will your endpoints survive a targeted attack from a sophisticated threat actor?

SIEM observability

Can your security operations team detect and respond to malicious activity in your environment?

Data exfiltration

Are you confident that your critical and sensitive data is protected from unauthorized access?

6 Security Validation Essentials

Having the confidence and insight into whether your security tools can keep pace with the breadth and volume of persistent, emerging and immediate threats doesn't have to be complicated and unmanageable – if you have the right tools in place.

Here are **six essentials** to help you identify weaknesses in your security controls, address threats to your valuable IT assets, and improve the overall resilience of your security operations:

Validation of threats

Active testing for the latest persistent, emerging and immediate threats discovered by the threat intelligence community and validated daily.

Validation of security controls

Confirmation that the security controls put in place, such as email gateways, web gateways and firewalls, endpoint, and cloud security and access controls are effectively implemented and function as expected.

Simulation and modeling of attacks

Simulate and enact various breach and attack scenarios within a safe, controlled environment with an attacker's approach of the latest threat tactics and techniques that will better prepare your defenses.

Validation of operational response

Evaluation of security operations team to respond to alerts and recover from security incidents. This includes running purple teaming simulations and drills to assess the effectiveness of security operations and incident response plans.

Compliance verification

Ensuring that the security measures adhere to relevant industry standards, regulations and best practices. Compliance validation often involves audits and assessments against standards such as ISO 27001, NIST, PCI DSS, GDPR, DORA and more.

Continuous improvement

Security Validation is an ongoing improvement process that begins by benchmarking your risk level against industry peers, then measures the performance of controls, threats and responses over time with frequent assessments.

The Bottom Line

Even if you've deployed the most expensive endpoint and cloud solutions that money can buy, if you're not continuously testing and validating your security controls and running breach-and-attack simulations, you're leaving your organization susceptible to things like financial loss, operational impact and downtime, brand erosion, data leakage and exploitation, and more.

If you're going to invest millions of dollars a year on security, don't be left wondering if you're actually secure. Security Validation should be part of every modern cybersecurity toolkit and top-of-mind for practitioners, like you. Find a solution that integrates seamlessly and quickly into your existing infrastructure, and gives you the confidence – and results – you need to answer these questions:

01 **Am I secure?**

02 **How exposed am I?**

03 **What's my risk score?**

To learn more, read this blog: Continuous Security Validation: The Key to Proactive Cybersecurity.
info@cymulate.com | www.cymulate.com

About Cymulate

Cymulate is the leader in exposure management and security validation. More than 500 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization, and guided remediation of security gaps before attackers can exploit them. For more information, visit www.cymulate.com.