Cymulate
Continuous Security Validation

# Enhance Supply Chain Security with Continuous Security Validation

## You're Only as Strong as Your Weakest Link

# 01 | Introduction

## Risks of an interconnected business world increase with the benefits

The value of the global internet has brought incalculable benefits to both businesses and consumers. As network connectivity and reach expands, tighter connections with suppliers, partners, and customers have increased business efficiency for all parties. The explosion of the cloud, as-a-service delivery models, and third-party hosted applications have made connecting with both suppliers and customers more manageable than ever before. Interconnected supply chains have now become a requirement of doing business.

With each additional link, however, your network's effective size grows, bringing risks that are often hard to quantify and operationalize.
In an attempt to measure the security risk of a possible new partner, companies have emerged to evaluate and "score" the security level of potential suppliers and partners. Unfortunately, as recent supply-chain attacks have shown, numbers don't always tell the whole story. Any new supplier can open a hidden door into your network, from software suppliers to IoT device manufacturers.

The number of supply-chain attacks has increased steadily as more and more partners link their networks. According to a survey conducted in June 2020 by Opinion Matters, 80% of organizations had a breach in the previous 12 months traced to one of their vendors[1]. Infamous attacks such as the 2013 breach of Target began with an attack on Target's HVAC supplier. After breaching the vendor's network, cybercriminals moved laterally through the Target network, eventually reaching the point-of-sale database and stealing details on more than 70M customer credit and debit cards.

The widely analyzed SolarWinds breach of late 2020 provides a valuable lesson on the lengths cybercriminals will go to steal information. SolarWinds is a trusted network monitoring partner to many large US Government agencies and Fortune 500 companies. The attackers reportedly gained their initial foothold by installing a "malicious backdoor" in the SolarWinds software release management system[2]. When customers updated SolarWinds software, criminals then opened the backdoor, created a covert command and control channel, and moved laterally through the network to locate valuable data. This pattern is typical for large-scale criminal attacks. Once attackers find their target, they pull the trigger, either stealing the data (as in the case with the SolarWinds attack) or encrypting it for ransom, or both. These attackers also cover their tracks as they move—making detection more difficult—until they can gain access to the target's core assets, using credentials and privileges stolen along the way[2].

[1] Opinion Matters, BlueVoyant Global Insights 2020, "Supply Chain Cyber Risk," https://www.bluevoyant.com/ciso-report-download-form

[2] The Hacker News, "New Evidence Suggest SolarWinds' Codebase Was Hacked to Inject Backdoor," December 16, 2020, https://thehackernews.com/2020/12/new-evidence-suggests-solarwinds.html

### Know if you can stop attacks before data assets are removed

Many companies have implemented security assurance programs to reduce the risk of attack in an environment of constant change.
Security assurance programs are designed to verify that your security infrastructure, people, and processes protect your network as intended. Such programs are particularly beneficial in complex, multi-partner organizations.

Today's standard practice for security validation consists of four well-defined processes: Security Audits, Vulnerability Scans, Pen Tests, and Red Team Exercises. While valuable and necessary, these tests are not sufficient in confronting threats and business-driven changes at the same pace as they occur.

They cannot provide the real-time visibility, validation, and assurance required to know if your security infrastructure is at its optimal state at any given moment. If testing frequency can't keep up with the rate of change (internal or external), your network is vulnerable during the "gaps" between tests. These "gaps" create real threat opportunities for cybercriminals.

According to a 2020 study by the Ponemon Institute[3], while 60% of companies reported making daily or weekly changes to their security controls, only 22% perform weekly tests to validate these changes, and 53% perform security testing less than once a year or don't have a regular testing program in place.

## 02 | Solution

### Expand current security assurance program to include automated security validation

The most practical and effective way for a security team to test their network's security against supply chain attacks is to use automated simulations that mimic the criminals' behavior. These are known as Breach and Attack Simulations (BAS).
By simulating cybercriminal attacks, BAS assessments validate the efficacy of not only your security equipment and policies but your internal procedures as well. Given the fluid nature of any security network, and especially given the complexity of large, interconnected supply chains, attack simulations also give your security team valuable knowledge and experience in dealing with supply chain attacks.

In the event of an actual attack, your team will be better prepared and respond quicker and more effectively by being tested against genuine cybercriminal tools and methods. This experience will help reduce any impact of an actual attack and strengthen your attack-response procedures, allowing the organization to recover more quickly and gracefully. And because BAS assessments are automated, security teams can perform them at any time, providing the coverage and frequency of testing required to stay ahead of cybercriminals in the continually shifting threat landscape of a multi-partner organization.

[3] https://cymulate.com/resources/collateral/ponemon-report/

By incorporating automated security validation, companies can increase the cadence and scope of their assurance programs to include:

**Policy Enforcement Validation:** Policies and configurations frequently change in response to changes in your internal network, as well as to changes in partner networks that may impact access to your network. This form of validation can verify policy enforcement across the entire partner ecosystem, examining access controls, the configuration of new devices or software, or any unexpected effects of network maintenance. For example, to validate that the correct network segmentation policies are consistently in place to prevent unwanted crossover between internal and partner networks or between classified and unclassified networks.

**Threat Intelligence-Based Assessments:** Cybercriminals never sleep. This test allows you to stay abreast of the latest attack vectors, methods, and malware unleashed anywhere in the world, preventing new attacks and exposing any vulnerabilities caused by these threats. Threat Intelligence-Based Testing gives you real-time visibility into the state of your security against cybercriminals, optimizing your security controls against new threats, and letting you stay ahead of the latest malware before criminals deploy it against you.

**Security Control Validation:** As the physical network changes with new partners, new endpoints, and new devices, the nature of the attack surface changes. This test subjects your security infrastructure to a broad spectrum of attacks and threats to ensure that they are optimally configured and accurately detecting and preventing malicious activity. Security Control Validation validates, for example, data loss prevention (DLP) controls, infrastructure resilience to lateral movement and provides a risk-based approach to vulnerability management. Whether installing new software, new endpoints, or new partner equipment, this test validates security control efficacy against potential supply chain attacks.

**Purple Team Automation:** Purple Team testing enables security teams to craft and launch attack flows proactively to exercise threat hunting and incident response playbooks. By using automated, out-of-the-box attack scenarios, resource constrained security teams can launch Purple Team exercises at any time with minimal adversarial skills. Sophisticated customizability allows companies with existing red team or pen tester experience to scale these valuable resources and increase productivity by leveraging automation, without limiting their creativity. Automated Purple Team testing recreate "real-life" scenarios, for example to simulate a supply chain attack.

The following table lists the primary security assessment objectives in preventing supply-chain attacks.Meeting these objectives tightens overall security while maintaining the efficiencies of your multi-partner infrastructure.

| Assessment Objectives | Value |
|---|---|
| Strengthen endpoint security. | • Validate endpoint protection is intact.<br>• Ensure controls preventing lateral movement are working effectively.<br>• Identify anomalous command and control (C2) behaviors. |
| Stop unauthorized lateral movement. | • Identify infrastructure misconfigurations that allow unauthorized lateral movement.<br>• Validate authorization, password, and access policies working correctly.<br>• Verify proper network segmentation. |
| Prevent data exfiltration. | • Verify that DLP security controls are functioning correctly.<br>• Ensure regulatory compliance. |
| Improve detection capabilities. | • Simulate supply chain attack scenarios to exercise incident response and threat hunting playbooks.<br>• Use "real-life" attack scenarios to remediate SOC/SIEM and EDR technology and process deficiencies.<br>• Facilitate frequent and cost-effective automated purple team exercises |
| Improve institutional knowledge. | • Increase team effectiveness and skill level when responding to attacks.<br>• Maintain ongoing education of your team on the latest attack vectors<br>• Improve defensive procedures by identifying potential weaknesses in your network. |

**Figure 1 -** Validating Protection Against Supply Chain Attack Vectors

## Conclusion: constant vigilance required to maintain security

When defining a security assurance program, the guiding principle must be one of constant vigilance. To ensure you are getting the best protection you can from your security infrastructure, security teams should use automated tests that mimic real-life attack scenarios and run them in response to the rate of change in the internal or external environment. Automated and continuous security validation represents a practical and achievable way of keeping pace with today's rate of change as well as the growth of supply-chain cybercrime.

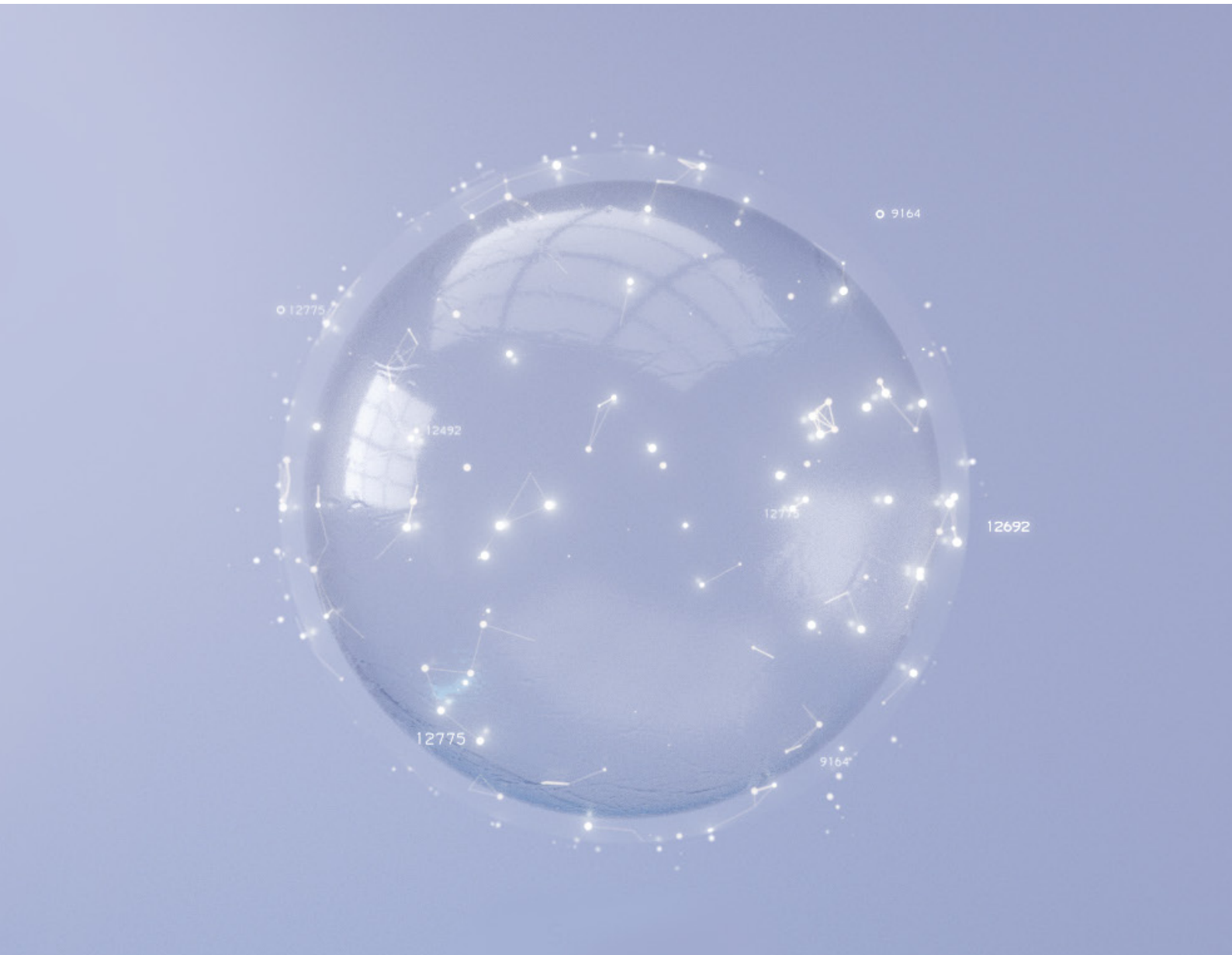
As the SolarWinds breach demonstrates, even the most secure networks cannot guarantee 100% protection from attack.

In a world of continuous change, new services, devices, and access points create a shifting threat landscape that is by nature dynamic and unpredictable. Securing any global network is a complicated and costly endeavor. As cybercrime becomes more organized and sophisticated, large, multi-partner organizations face an ongoing challenge to protect themselves and their customers.
By implementing a security assurance program that includes automated assessments based on attack simulations at regular and frequent intervals, you are giving your organization the most straightforward, most effective, and most impactful toolkit available, as well as providing skills that can prevent even the strongest cybercriminal organizations from achieving their goals.

# 03 | About Cymulate

For companies that need to assure their security against the evolving threat landscape.
Cymulate SaaS-based Continuous Security Validation deploys within an hour, enabling them to challenge, assess and optimize their cyber-security posture simply and continuously end-to-end, across the MITRE ATT&CK® framework.
The platform provides out-of-the-box, expert and threat-intelligence led risk assessments that are simple to use for all skill levels and constantly updated. It also provides an open framework for ethical hackers to create and automate red and purple team exercises and security assurance programs tailored to their unique environment and security policies. Cymulate: for security professionals who want to know and control their dynamic environment.

For more information, visit Cymulate




**Contact us for a demo or get started with a free trial**

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com
US Office: +1 212 6522632