Cymulate
Breach & Attack Simulation

Security Validation for Remote Workers

01 | Introduction

Over the past 20 years working from home (WFH) has become commonplace, but even as the trend grew, the percentage of permanent WFH employees remained significantly low. This changed with the Covid-19 pandemic that led to broad geographic shutdowns, quadrupling the overall number of people working from home, with some companies shutting offices for 100% of their workforce. This introduced significant changes in many company's IT and cybersecurity architectures.
In a recent survey of security professionals YL Ventures found that 51% of those surveyed acquired new security solutions to accommodate remote workforces.
These included technologies such as multifactor authentication, virtual desktop security, endpoint security in remote environments and Zero Trust / Secure Access Service Edge (SASE) services.

Another interesting finding was that 21% had to relax security policies to accommodate remote workers, these included technical attributes such as extending the time-out period of VPNs, to workflow changes such as contract printing and signing.
All these changes were performed within accelerated timeframes and under the shadow of spiraling cyber threats that attempted to exploit an expanding remote workforce.
This paper will describe some of the security challenges created due to the rapid growth of a remote workforce. And how the Cymulate SaaS-based Breach and Attack Simulation Platform can be used to validate the effectiveness of new or modified security controls introduced to accommodate the remote workforce.

02 | Concerns for securing a remote workforce

Best practice dictates that remote users should be considered "untrusted" whether you implement a zero trust security policy or not. Zero-trust is not a policy that can be implemented overnight, so most organizations had to face the individual challenges and concerns with the expansion in remote workers on a case-by-case basis. These include:

Expanded use of personal devices reduces overall visibility.

An increase in data accessed remotely increase the threat of data exfiltration.

New security controls and their configuration require validation of their operational effectiveness.

Changes to the security policy and their implementation can inadvertently introduce new security gaps.

Threat actors leverage the pandemic to target employees working from home.

VPNs enable a remote asset to connect simultaneously to corporate assets and the internet.

YL Ventures CISO survey
https://cyber.ylventures.com/hubfs/CISO%20Current%20Reports/2020/Q%202%202020/CISO%20Current%20Q2%202020%20Report%20Final.pdf

03 | Security validation

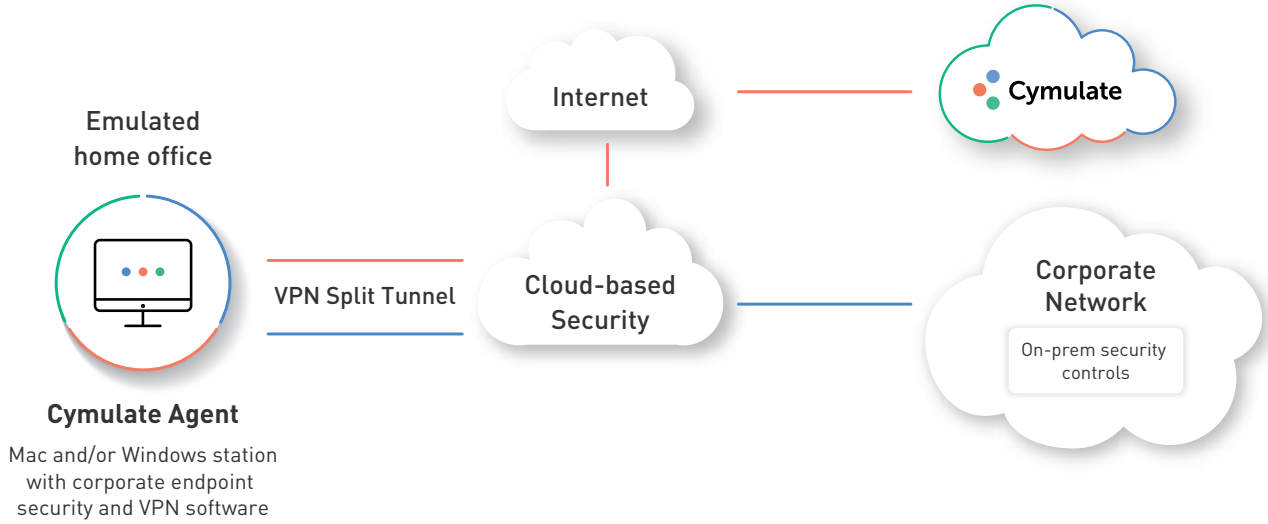
In a classic deployment of Cymulate, one agent is installed on a standard corporate machine and deployed in the corporate network. The agent participates in a broad spectrum of simulated attacks that validate the effectiveness of the corporate security controls. The agent can serve as the target of the attacks, for example to measure the effectiveness of email security controls that are protecting the agent. Or it can source the attack simulations, for example to validate the effectiveness of network segmentation policy enforcement and to discover infrastructure weaknesses and misconfigurations that are used by hackers to propagate within a network. Cymulate currently supports eight vectors and two multi-vector modules, that perform security validation across the full attack kill chain. For more information please refer to cymulate.com.

Security validation in a remote access network configuration

In a work from home scenario the agent is deployed in an emulated home, and it is connected to the internet to access the corporate network via security controls setup for remote access. Network configurations will vary between companies, a typical implementation will include the following security layers:

- Client-side security and remote access software.
- Cloud-based security services that provide, for example, DLP, web security and remote access aggregation.
- Corporate on-prem controls that handle remote access security and policy enforcement.

Depending on the configuration the client can access the internet directly from home, via the cloud security providers or hairpin via the corporate on-prem security controls. Typical network configurations will be similar to the following diagram:



Remote access typical network configuration and Cymulate deployment

For companies that enable the use of personal devices the endpoints will vary but this will have little impact on the validation of the security controls deployed to protect them. We recommend using both Mac and Windows versions of the agent to validate the effectiveness and implementation of OS specific security controls.

Remote access security validation

Just as corporate controls require continuous security validation, so do the controls protecting remote workers. The requirement for security validation increases where new technologies or services were implemented to support the immediate expansion in remote workers and where security policies were modified to accommodate them.

Security validation will answer two primary questions,

1. how well are remote endpoints protected? and

2. what damage can a compromised endpoint potentially incur? The findings enable security teams to optimize remote access protections and configure infrastructure and segmentation policies to limit malicious network propagation.

Simulated attacks on the home-office endpoint validate the security controls protecting the endpoint such as client-side software and cloud-based protections. These include:

- Endpoint security
- Web security
- Email security
- Immediate threats
- Phishing awareness

Simulated attacks from the endpoint validate client security software and cloud-based and on-prem security controls. These include:

- Lateral movement
- Data Exfiltration

Following is a breakdown of the vectors, the priority and objective of remote access security control validation.

"**Case in point:** By validating their remote access security controls with Cymulate, a large Insurance company found and rapidly rectified an SSL inspection misconfiguration in their cloud-based web security service that otherwise would have gone unnoticed, leaving their remote workforce unprotected."

Vector	Priority	Validation objective
Web Security	High	Endpoint and cloud-based web security effectiveness.
Endpoint security	High	Endpoint software detection and prevention of attacks, to and from the endpoint.
Email Security	Low	Email security controls typically do not differ between on-prem and remote workers.
Immediate threats	High	Test email, endpoint and web security control effectiveness against the latest threats that are updated daily in the platform.
Lateral Movement	High	Validate VPN access policy enforcement. Identify and protect corporate assets that a compromised VPN connected endpoint can access by applying hacking techniques.
Data Exfiltration	High	Validate corporate, endpoint and/or cloud based DLP effectiveness.
Phishing awareness	High	Internal phishing campaigns should be tailored to scenarios targeting remote workers (Covid-19 themed) in order to measure and improve employee awareness.
WAF	Low	Web application security controls are not applicable to this use case.

In addition to the above the Cymulate platform can emulate the full kill chain APT to evaluate the effectiveness of the end-to-end security architecture and operational effectiveness of interdependent security controls and procedures.

04 | Summary

Automated security validation enables rapid and objective evaluation of new security controls, changes to the IT and cybersecurity architecture and continuous validation after deployment to new threats and hacking tactics and techniques.

Cymulate enables security operations to match the pace of changes in the IT architecture and of the evolving threat landscape, even in extreme conditions such as those that the pandemic created.

Who we are

Cymulate SaaS-based continuous security validation makes it simple to measure and improve your security posture across the full attack kill-chain.
Every assessment is scored and includes actionable remediation guidance to mitigate risk and optimize security control effectiveness. Cymulate enables you to take data-driven decisions and manage your security resources efficiently.

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