Cymulate
Continuous Security Validation

Security Validation Became Continuous and Reduces Risk

2020 Platform Usage Report

01 | Introduction

Security Validation is a recognized cyber best-practice that is gaining broad acceptance by companies in many industries, fast becoming a must-have element in every enterprise security stack. In this, our 2021 report, we share 2020 customer usage patterns, outcomes, and insights of the Cymulate Continuous Security Validation platform, to help you decide on the priority of continuous validation for your organization.

This market category has also attracted attention from the analyst community, including Gartner and Frost & Sullivan. In the latest report of the Frost Radar™: Global Breach and Attack Simulation (BAS) Market, 2020, Cymulate received the highest score on the innovation index of the Frost Radar™ and the second highest score on the growth axis, recognizing that "Cymulate has rapidly become one of the leaders in the Global BAS market."

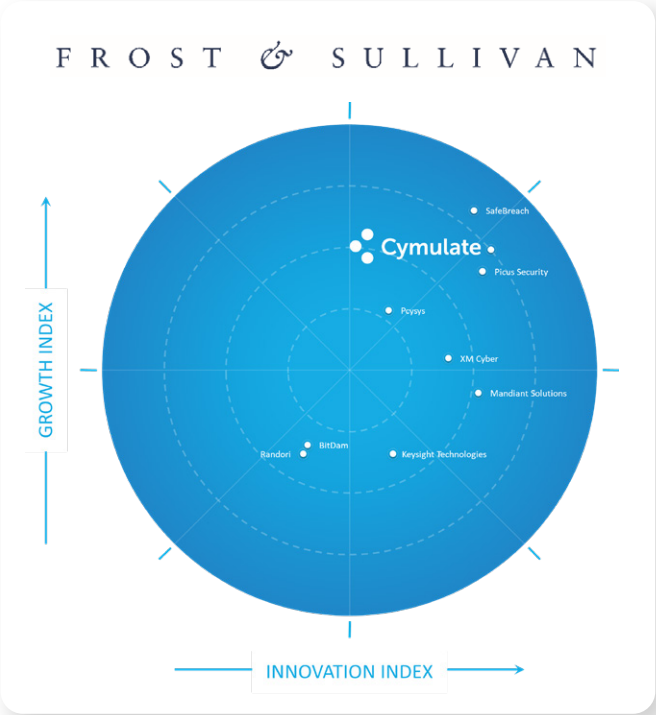
One thing is sure, customers have added "continuous" to their security validation programs. **Platform usage grew by 50% from 43,000 assessments in 2019 to almost 65,000 in 2020**. The average customer subscribes to four or five of the platform's vectors and just over 20% of customers subscribe to over 75% of the available vectors in the platform.
During 2020 our customers performed on average 54 assessments for each vector they subscribe to.
For example, a customer with 4 vectors ran 208 assessments, on average slightly more than once a week for each vector.

While Cymulate has customers across most industry sectors, **39% of the assessments were launched by companies from the banking and financial sector.** Known to be a sector with a high level of security matureness, it is not surprising that this sector represents the largest proportion of customers using the Cymulate platform, it is also the sector with the lowest risk score.

While use cases vary, the main usage of our platform is to **validate security control efficacy** and improve our customer's capabilities to detect and prevent breaches from existing and new threats, and threat actor techniques. By focusing the validation process on attack vectors, security practitioners gain the added benefit of improving their cyber security skillset, as one CISO stated, **"It helps my team to think like the adversary and become better defenders, effectively doubling the productivity of my security team."**

The second primary use case is to identify infrastructure and security weaknesses, and attackable vulnerabilities that may arise from misconfigurations or technology failures and software errors. Essentially, enabling a **risked based approach to vulnerability management.** Enabling companies to move their focus from what they think they need to purchase, to optimizing what they have and continuously improve the security posture of their enterprise infrastructure.

Another use case is **red team automation** and exercising incident response playbooks.
While this was an existing capability it has been greatly improved by the release of the new Purple Team module. This module scales red team and pen testing skills and makes security exercises accessible and achievable for all enterprises, regardless of initial skill set and size. Released towards the end of the year we have limited usage data, but if you want to read about it, click here.



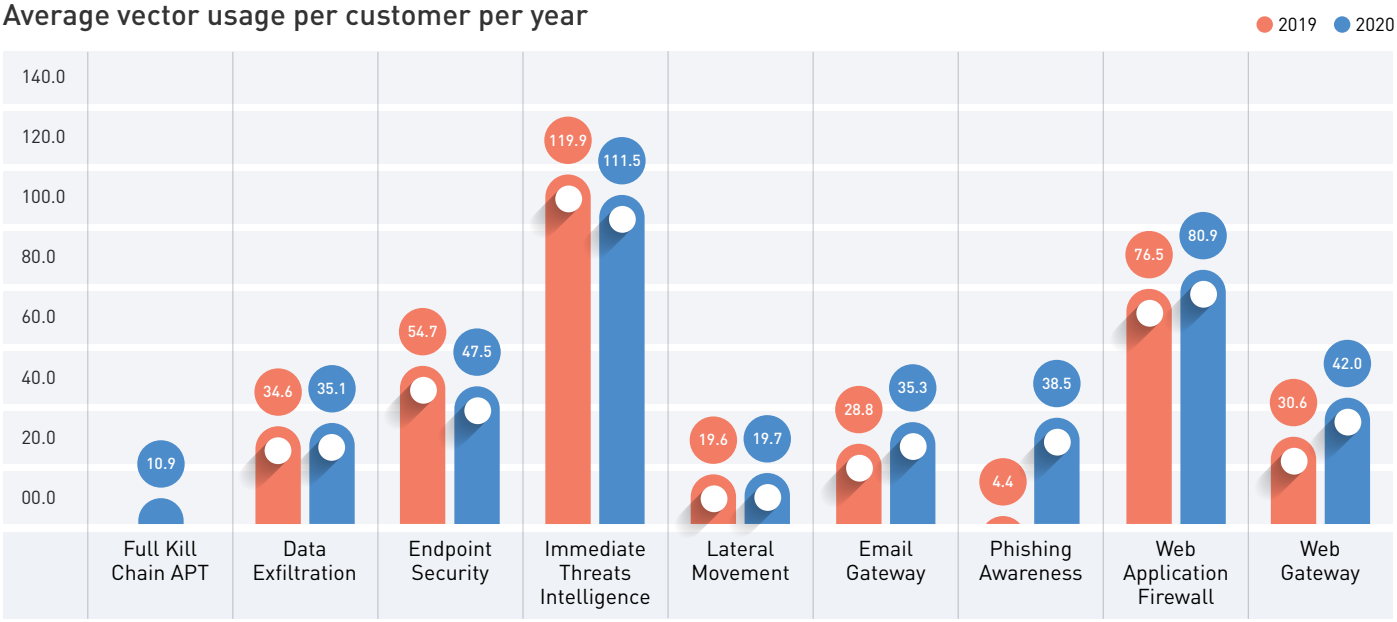
Source: Frost Radar™: Global Breach and Attack Simulation (BAS) Market, 2020

02 | Usage

Driven by the reality of working from home, and the surge in COVID related phishing campaigns, companies were faced with the challenge of rapidly securing remote workers and adapting security policies to enable business continuity.
This reflected in the platform with **phishing awareness usage increasing by a factor of nine,** Web vector utilization and validation grew by 37% and Email by 23%. The Immediate Threats Intelligence module remained the most popular type of assessment, since it answers a concerning question "are we vulnerable to the latest attack?"
Unsurprisingly the SolarWinds attack simulation was the most popular, tested by all the customers subscribed to this module. Furthermore, COVID theme related threats were also among the most popular Immediate Threats assessments.

The APT Full Kill Chain module released end of 2019 was not included in last year's report and has gained traction. This is an advanced module that mimics APT groups and their tactics and techniques in a sequenced attack flow scenario and was used almost once a month by customers.
Recon and Purple team, released late 2020 are also ramping up, and will be included in our next report.

Average vector usage per customer per year



Measure to improve

The Cymulate risk score provides a quantifiable metric that enables customers to prioritize their mitigation activity, track performance and benchmark themselves over time.
The score is calculated based on risk determination factors taken from NIST, CVSSv3 and DREAD in addition to the MITRE ATT&CK® framework.
The risk score ranges between zero to a hundred where a low score equates to low risk.
A consistent methodology is applied to risk scoring across all the vectors and assessments, making them comparable. Following is a comparison of the average 2019 and 2020 yearly scores, by vector.

Risk score by attack vector

Vector/ Module	Average risk score 2020 (*)	Average risk score 2019 (*)
Phishing Awareness	18.4	66.3
Lateral Movement	12.9	17.2
Data Exfiltration	30.5	23.1
Web Application Firewall	39.6	35.8
Email Gateway	16.5	18.6
Web Gateway	33.9	31.5
Endpoint Security	21.1	17.2
Immediate Threats Intelligence	31.2	31.9

(*) A risk score of zero indicates the lowest exposure to an attack vector. Scores range between zero and a hundred

Most impressive is the significant reduction in the phishing risk score across most industries.
As mentioned above 2020 saw significant increase in usage of this vector to evaluate employee security awareness, by a factor of nine. On average the phishing risk score across all industries decreased by a factor of almost four from 66.3 to 18.4. The Technology sector was the best performing with the lowest risk score of 17, with healthcare the worst performing sector with a risk score of 52. Comparative to 2019 The Banking and Financial Services sector improved significantly from 2019 reducing the risk score from 70 to 18.
This was also the sector that registered the highest average usage of the Phishing module per-customer.

Phishing awareness by industry

Industry	Risk Score
Technology	17
Banking & Financial Services	18
Other	19
Insurance	31
Health Care	52

*The lower the score, the lower the risk

Threat intelligence-led validation

Fulfilling the need to validate security efficacy to threat evolutions is apparent in the usage of the Immediate Threats Intelligence module.
This module is updated daily with new threats, engineered to be launched safely in production environments by Cymulate Labs cyber-researchers.
During 2020 our customers ran over 24,000 assessments of 600 unique threats.
By far the most popular assessments were related to the **SolarWinds supply chain attack,** COVID themed attacks and Ransomware in general, as can be seen in the following table of the top 15 most popular Immediate Threats assessments.

Top 15, most popular threat assessments

Immediate Threats	Proportion of customers that assessed at least once	Average risk score (*)
SUNBURST backdoor - SolarWinds supply chain attack	96%	23
Shirbit BlackShadow attack additional indicators	90%	34
New APT uses DLL side-loads to "KilllSomeOne"	87%	42
Data Breach at Shirbit - BlackShadow attack	80%	24
Invisimole: The Hidden Part	73%	15
Pfizer COVID 19 vaccine documents accessed in EMA cyberattack	70%	25
Fake COVID-19 survey hides ransomware in Canadian university attack	65%	20
Kraken - Windows Error Reporting Service Abuse	63%	22
GravityRAT Comes Back to Earth	60%	34
New Kimsuky Module Makes North Korean Spyware More Powerful	59%	27
T-RAT 2.0 - Telegram Used to Issue Commands	59%	43
BazarLoader deploys Ryuk ransomware	59%	41
CERT IL Urgent warning - malicious email campaign	59%	32
MountLocker ransomware gets slimmer	58%	35
TA551 (shathak) Word docs push IcedID	57%	22

(*) A risk score of zero indicates the lowest exposure to an attack vector.

The following table lists the top 15 assessments that resulted in the highest average risk score.

Noticeable are threats targeting Google Chrome, MacOS and Linux.

Top 15, highest risk score threat assessments

Immediate Threats	Proportion of customers that assessed at least once	Average risk score (*)
CSP Bypass Vulnerability in Google Chrome Discovered	45%	87
Discord Turned Into an Account Stealer by Updated Malware	31%	80
Jigsaw Ransomware dropped by Lokibot	33%	72
Malware authors trick Apple into trusting malicious Shlayer apps	22%	68
Doki Infecting Docker Servers in the Cloud	34%	62
InterPlanetary Storm cross-platform P2P botnet	45%	61
Shlayer Trojan attacks one in ten MacOS users	23%	60
Gstaticapi Credit Card Stealing Malware	51%	59
Microsoft warns about attacks with the PonyFinal ransomware	50%	56
North Korean hackers infect real 2FA app to compromise Macs	32%	54
HHS.gov Open Redirect Used by Coronavirus Phishing to Spread Malware	38%	54
TrickBot Updates Propagation Module	38%	54
New Mac malware spreads disguised as Flash Player installer	30%	53
Dridex infection	32%	53
Fox Kitten - Widespread Iranian Espionage-Offensive Campaign	34%	50

(*) A risk score of zero indicates the lowest exposure to an attack vector.

An indication of security matureness

Current adoption of BAS is high among companies with high security matureness, with the banking and financial services sector leading the way. This is also reflected in the industry breakdown of Cymulate customers. During 2020 almost 65,000 assessments were performed, 39% of these were launched by companies from within the financial sector.

In addition to being the largest adopter of continuous security validation this sector is also the most secure. In the table below we highlight the yearly usage per industry and average risk score, in addition to the high-risk vectors and scores per industry which are Data Exfiltration and Web Application Firewall.

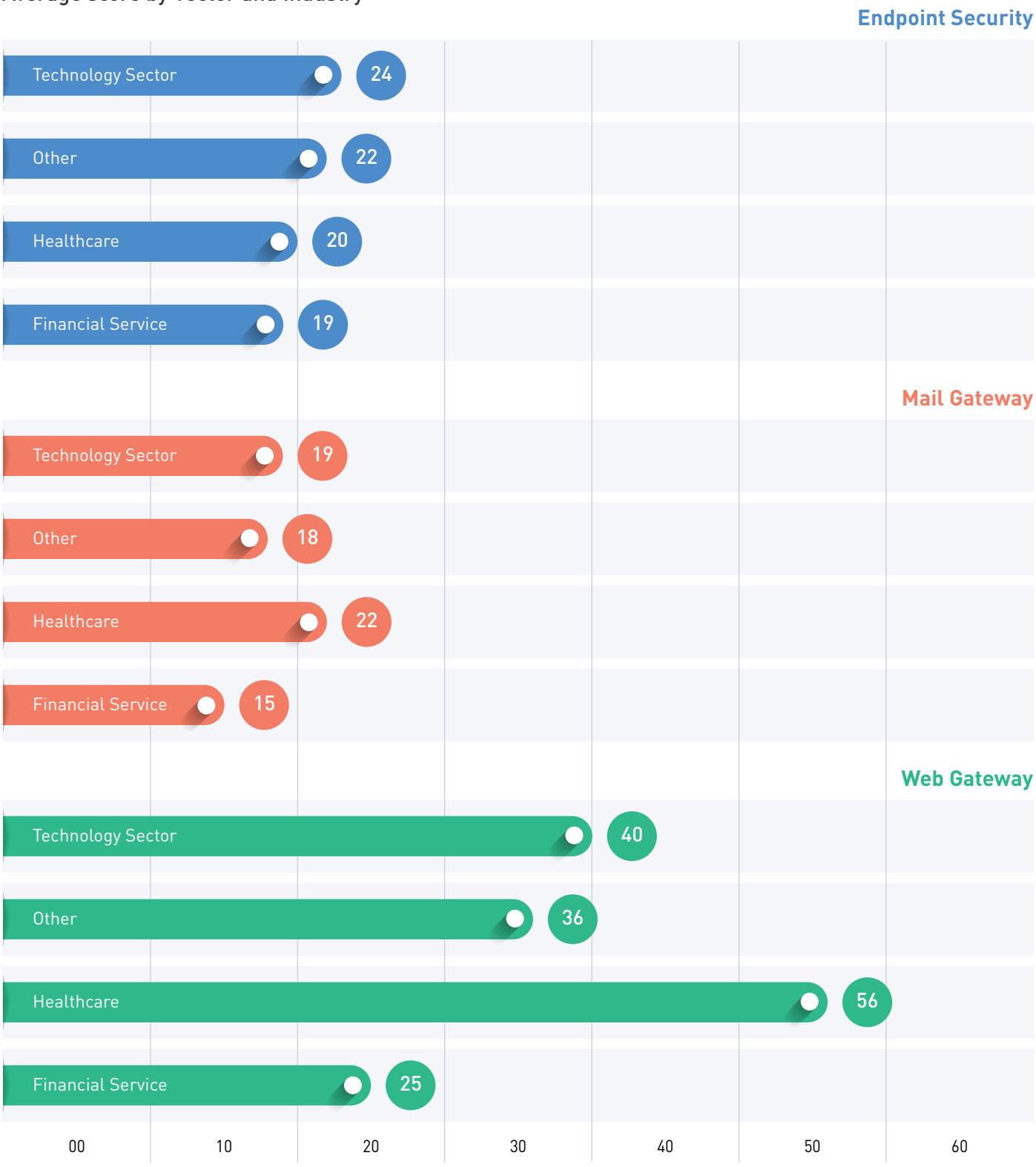
Usage and average score by industry

Sector	Yearly Usage	Average Score (*)	Highest Risk Vector	High-risk vector score(*)
Banking and Financial Services	39%	25	Web Application Firewall	32
Technology	12%	34	Web Application Firewall	80
Health Care	8%	36	Data Exfiltration	71
Insurance	8%	25	Data Exfiltration	36
Manufacturing	6%	29	Data Exfiltration	46
Transportation	6%	30	Web Application Firewall	48
Telco	4%	32	Web Application Firewall	60
Other	16%	31	Data Exfiltration	41

(*) A risk score of zero indicates the lowest exposure to an attack vector.

Digging further into the results by looking at the average risk scores by industry of the most common attack vectors, Email, Web and Endpoint, the financial sector leads with the lowest risk scores for all three vectors, and across all industries the Web Gateway vector is the riskiest of the three.

Average score by Vector and Industry



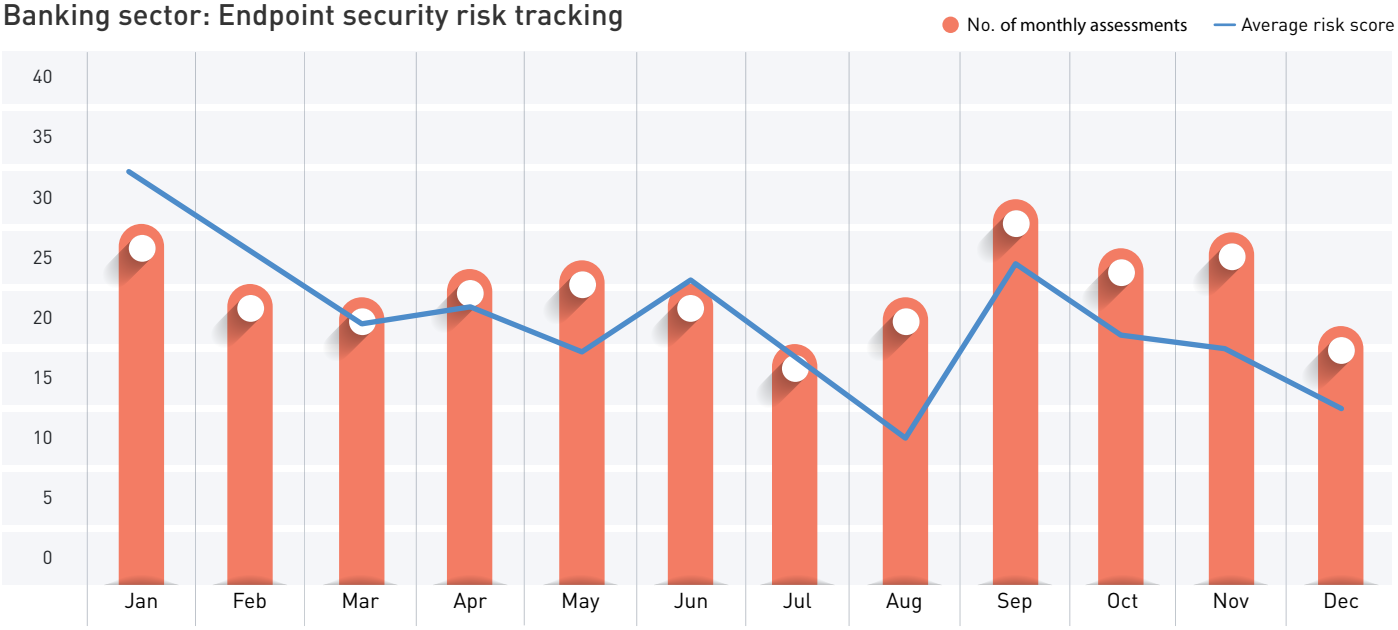
(*) A risk score of zero indicates the lowest exposure to an attack vector.

Delivering life-cycle value with continuous validation

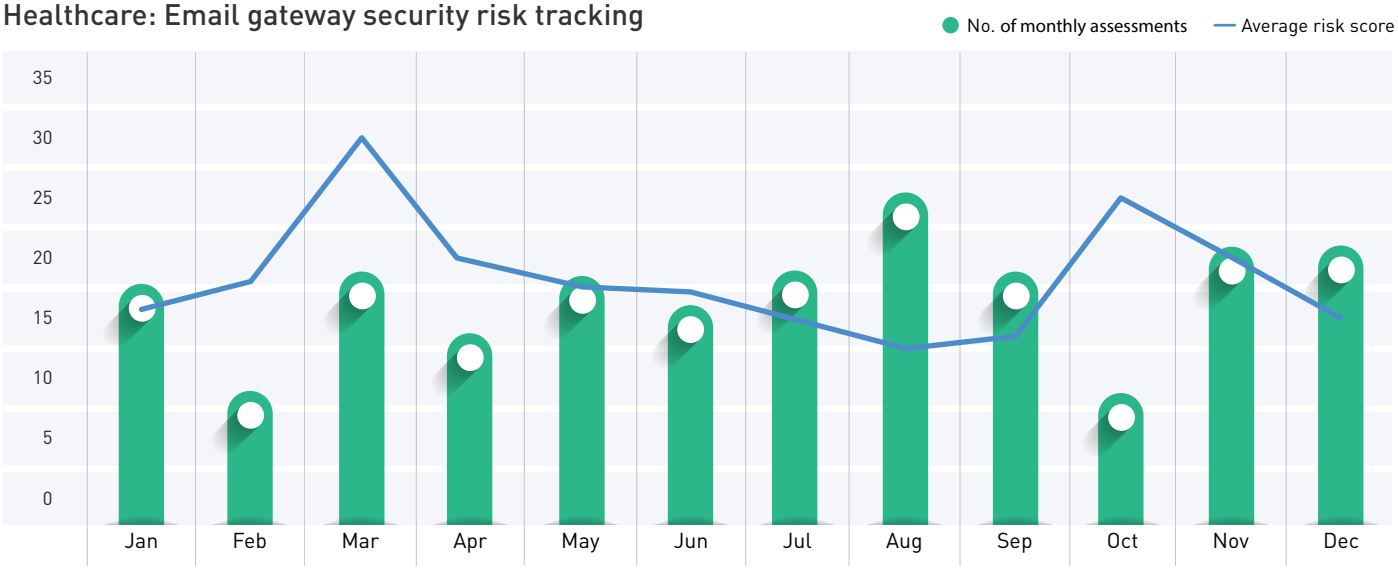
The threat landscape does not stand still, driving the need for continuously updated assessments. Meeting that need, Cymulate Labs constantly update the platform with new threats, tactics and techniques so that customers can achieve constant improvement of their security controls.

Organizations that adopt a daily or weekly cadence of security validation are able to confront threat evolutions more effectively, they are able to assure that changes in their IT and security architectures do not create new, unintended vulnerabilities and through the practice gain priceless cybersecurity skillsets. In the following two cases, a bank that performs endpoint security validation and a healthcare organization that validates email security, both almost once a day. The average monthly risk score varies, due to many parameters including changes in the security configuration and policies and as new threats and techniques are added to the platform.

Banking sector: Endpoint security risk tracking



Healthcare: Email gateway security risk tracking



(*) A risk score of zero indicates the lowest exposure to an attack vector.

Attack Surface Management

During mid Q4 2020 we released the Recon module that performs outside-in reconnaissance.
It identifies externally accessible digital assets and analyses them for misconfigurations and vulnerabilities. The Recon module also looks for intelligence that can serve a threat actor for different types of attacks, including social engineering attacks. Overall adoption is growing, and findings are impressive and surprising customers.

The most common use case is increased Cyber and IT hygiene. Due to the timing of the release, we do not have enough usage data to identify patterns or common exposures, but we have three examples to share. We expect to have more insightful data for the next report.

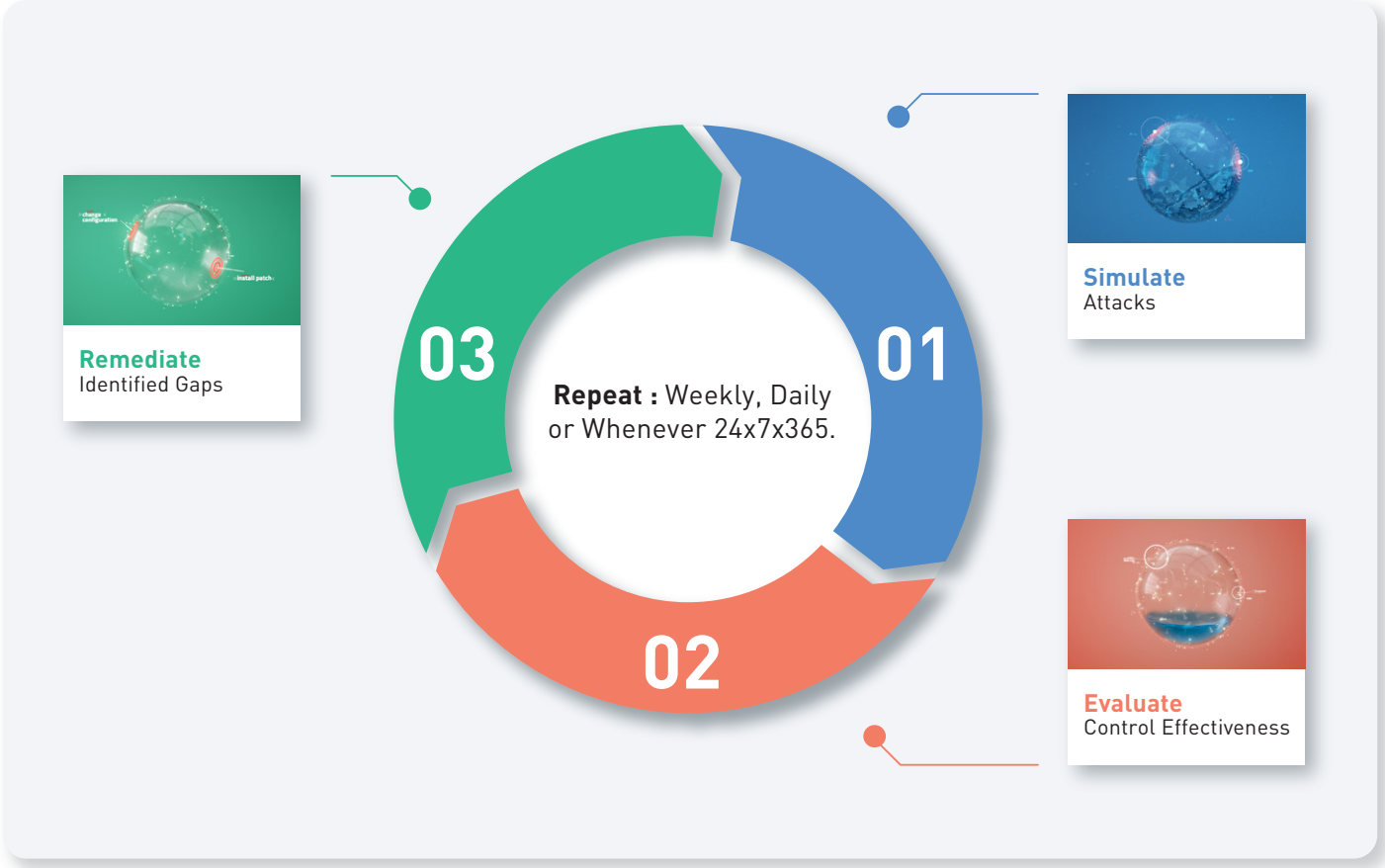
Customer A. Found hacked email accounts of employees that included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and their location. Information valuable for a successful engineering attack.

Customer B. Found corporate email addresses in the wrong A/D domain. An IT hygiene issue that was quickly resolved.

Customer C. Received a list of detected open ports, while many of the ports were legitimate, some were not, and probably a result of shadowIT. Subsequently the security team updated the corporate policy to manage externally accessible open ports, including approval, lifecycle testing and periodic reviews.

04 | Summary

The daily and weekly platform usage prove that companies are achieving Continuous proves Security Validation. They are addressing the dynamics of threat evolutions by validating their security efficacy to threats as they emerge with Immediate Threats Intelligence assessments and performing continuous security control optimization.
The witnessed outcome is that risk scores improve (are lowered) where usage has increased.
2020 was an interesting year to say the least, and needless to say not only from a cybersecurity perspective. Security assessments and validation continued during shutdown, even with security teams working from home. Behind the risk score are concrete examples of security visibility and optimization, for example a large company in the UK finance sector discovered that most of their employee traffic was unprotected, as SSL inspection was mistakenly turned off on their cloud-based web security service. A US based company simulated a compromised endpoint of an employee working from home to evaluate the risk and consequently updated their incident response playbooks.
And a healthcare customer reported that by making one policy change in their endpoint protection tool they prevented 168 exploits from being able to run on their computers. These examples and many others give our customers the conviction that Continuous Security Validation is critical component of an enterprise security architecture.
Click here for our free continuous trial and check it out for yourself, we are sure that you too will be convinced.



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