Cymulate

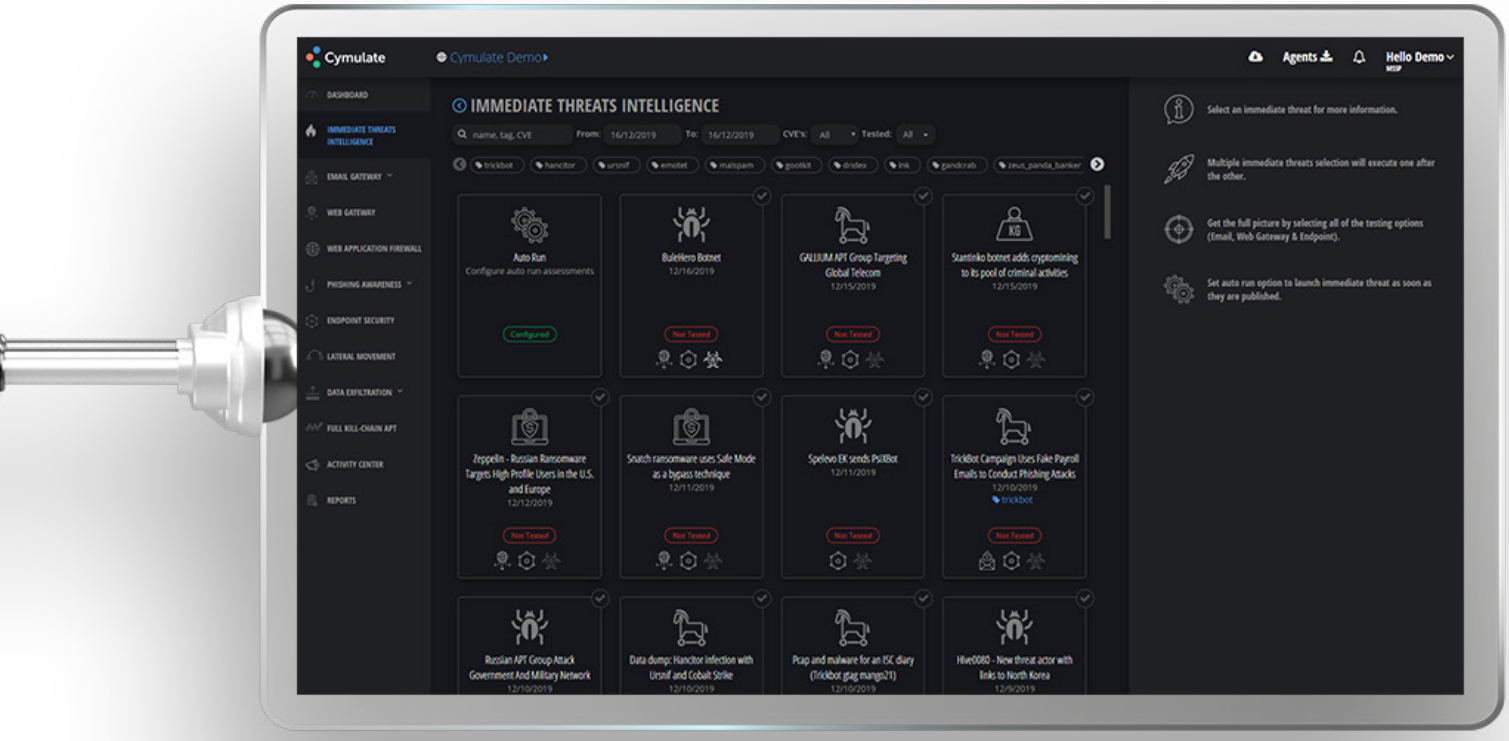
Now is the Time

Proactively Defending Against Immediate Threats

01 Are We or Aren't We?

When a WannaCry, Robbinhood, or Petya makes the headlines, expect a call from your CEO asking if the organization is protected.
Even when you've scrupulously patched systems, increased user awareness efforts, and have state-of-the-art controls in place, there's always that nagging fear that a threat you never heard of has evaded your defenses. How can you really know?

The best way to know how well your controls are working is to conduct regular or (even better) continuous simulation testing for the latest threats. Traditional methods of manually checking Indicators of Compromise (IOCs), running threat binaries on copies of your network—or even creating your own simulation tool—can no longer keep pace with hyperactive threat actors.
This document will explore the nature of immediate threats, a high-level view of how they work, and an assessment of organizations' risk for the five most common latest threats. You'll also see how Breach and Attack Simulation (BAS) can deliver unprecedented visibility into your organization's security controls and vulnerabilities for proactively addressing threats before they address you.



02 Adversaries Use What Works

Every week, cybersecurity researchers identify new threats in the wild. Threat actors range from cybercriminal gangs to individual hackers and nation states—even new hackers with less expertise can hire botnets in the underground to exploit vulnerabilities for fun or profit. But are the latest threats really all that new? The answer is yes and no. Many are new implementations of existing threats. Some use new techniques to uncover and exploit vulnerabilities with proven strains of malware. A growing number of threats target new vulnerabilities in hardware and software. Adversaries are expert at recycling code and threats and adapting them for use with their next target.

Old Techniques, New Vulnerabilities

What's new is adversaries' increasing agility. They're identifying vulnerabilities or security gaps in legitimate application features much faster. In particular, Microsoft Office application vulnerabilities offer adversaries a number of features to abuse. Because Office is so widely used and trusted, adversaries can spread campaigns far, wide, and fast. Features frequently abused include macros, hyperlinks, and OLE embedded objects. Malicious macros can easily launch PowerShell code that flies under the radar of most security solutions, and Microsoft's Object Linking and Embedding (OLE) functionality is often manipulated for nefarious purposes.

Although document exploits have been around for a while, in 2018 adversaries dramatically changed their use. Exploits that were popular in 2016-2017 were replaced with emerging exploits[1]. During the first quarter of 2018:

- 96% of Microsoft Office-based attacks targeted vulnerabilities that were less than a year old.
- 75% of attacks arrived through three new exploit builders, and older tools were abandoned.
- 90%+ of attacks used Rich Text Format documents because they offer powerful obfuscation methods.

Adversaries waste no time in innovating. Criminal groups that previously had no interest in Office exploits began to use them for distributing malware, even adding previously unseen malware families to this threat vector. Within weeks of identifying a vulnerability, they were targeting victims with new exploits.

Updating Old Techniques

Some threats are new strains of older, known malware. GandCrab ransomware is one example.

Originally, adversaries used phishing emails to transmit GandCrab and infect systems.

In the first nine months of 2018, GandCrab was updated five times[2]. Its creators continue to evolve the ransomware, now enabling it to avoid detection, bypass security solutions, and trick victims into installing it onto their systems.

[1] Office bugs on the rise, Virus Bulletin, VB 2018
[2] Old Threats are New Again, Dark Reading, 5/21/2019, https://www.darkreading.com/perimeter/old-threats-are-new-again/a/d-id/1334731

Adversaries Use What Works

What This Means for Defenders

Cyberthreats' agile adaptation means that organizations can't rest assured with traditional security solutions alone.
Simulation testing is emerging as a powerful practice for challenging an organization's defenses to identify potential gaps—before the latest attack or exploit finds them. Increasingly, when organizations don't test for immediate threats, the consequences can be costly. The following examples illustrate how organizations are affected when significant vulnerabilities remain unknown or unremediated:

City of Baltimore Held for Ransom

In April and May 2019, Greenville, NC and Baltimore, MD were attacked by ransomware known as RobbinHood. Both cities were locked out of their computer servers for ransom.
Security experts who studied samples of the ransomware found that Robbinhood had no known ties to existing malware families nor does it contain a self-propagation function, meaning it requires another method to spread from machine to machine[3]. Affected city systems included email, payments, and real estate. It will take months to recover from the attack, costing the city of Baltimore $18 million—$10 million to restore infected systems and $8 million in lost revenue.

Citrix Breach Results in Class-Action Lawsuit

Between October 2018 and March 2019, adversaries breached the network of Citrix Systems, the multinational software company.
In the Notice
of Data Breach, the company said "cyber criminals had intermittent access to our network between October 13, 2018 and March 8, 2019, and that they removed files from our systems, which may have included files containing information about our current and former employees and, in limited cases, information about beneficiaries and/or dependents.[4]

University of Washington Medicine Compromised Again

In February 2019, the University of Washington Medicine notified 974,000 individuals that some of their patient data was exposed on the internet for three weeks due to a misconfigured server. The cost just to mail notifications to affected individuals will reach $1 million. There is no estimate yet available for recovery costs.
However, this is the organization's second breach in six years[5].
In October 2013, Social Security numbers and medical data of 90,000 patients were compromised when an employee opened a phishing email attachment. Malware took over the computer, which stored patient data.
After that breach, the US Department of Health and Human Services found University of Washington Medicine lacked effective risk assessment that would sufficiently address patient data risks and vulnerabilities, and it finally settled with the organization for $750,000.

[3] Robbinhood: Inside the Ransomware That Slammed Baltimore, Dark Reading, 6/4/19
[4] Breaching News, May 31, 2019 https://breachingnews.com/citrix-sued-for-not-securing-employee-info-before-data-breach/
[5] UW Medicine mistakenly exposed information on nearly 1 million patients, The Seattle Times, Feb. 22, 2019
https://www.seattletimes.com/seattle-news/health/uw-medicine-mistakenly-exposed-information-on-nearly-1-million-patients/

03 When Patches Aren't Enough

Keeping security systems current is the obvious first place to start. Security vendors have dozens of researchers and malware analysts on their teams dedicated to finding the latest threats so protection can be included in product updates and new solutions. But that's just a start. The vendor's lab might not be up to date or the team simply hasn't discovered a new strain yet. Once they do, it still takes time to analyze the threat and create the product update. Add more time to deliver the updates and time for customers to deploy it. Days, weeks, or even months can pass between identifying the latest threat and ensuring that the customer environment is protected.

Assuming that you have diligently kept security defenses current, when a new "Robbinhood" type of threat hits the headlines, what would you do? Traditionally, there have been three options:

01 | Manually check to ensure updated IoCs across security controls

Antivirus companies typically detect new malware binaries first and publish their IOCs. You would check security controls, such as your email gateway, web gateway, and endpoint security solutions, to ensure that they are updated with the latest IOCs.

02 | Create a 'carbon copy' of your network and run the threat binary on that copy

You could create a carbon copy of your network and simulate an attack using the threat binary. Although this is a safe option, your "ideal" carbon copy might not be identical with the real network. Real networks are prone to unintentional variations from the ideal—a firewall might be running in monitoring mode instead of blocking.
Or, certain patches were installed behind schedule. If IT and security teams are unaware of the variations, the simulation results might not be trustworthy.

03 | Build a homegrown simulation

If you have dedicated threat or vulnerability assessment teams, building your own simulations is a possibility. Even so, they are costly to develop and difficult to keep current.
They must be able to adequately simulate across threat vectors and multivendor security controls. Even if you have the resources, the turnaround time required for creating a live, safe simulation for every new threat might not be feasible.

04 Identifying Immediate Threats with BAS

In the first three months of 2019, there were 281 breaches exposing more than 4.53 billion records[6]. Clearly, organizations of all types are at risk from the latest threats. The Cymulate Research Lab has identified five high-profile threats that pose the most risk to organizations, as described in Table 1.

Percentage of Organizations at Risk	Threat	Notes
40%	Dridex trojan	This threat typically is delivered through massive spam email campaigns that include malicious links, macros, or attachments in Microsoft Office documents. Dridex spam campaigns are often disguised as financial emails, such as invoices, receipts, and orders with the objective of stealing banking credentials.
38%	Hidden Cobra	Hidden Cobra is a North Korean group that commonly targets systems running older, unsupported versions of Microsoft operating systems, as well as Adobe Flash player vulnerabilities. They use DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. The malware implements a custom protocol that allows traffic to be tunneled between source and destination IP addresses.
33%	Ryuk ransomware	This strain of ransomware has been used in targeted, high profile attacks with ransom demands in the six figures. It is typically preceded by malware infections involving Emotet and/or TrickBot trojans, which lay the groundwork for network-wide compromise and the encryption of critical network assets.
26%	Emotet	Emotet is an advanced, modular malware that downloads or drops banking trojans. It can be delivered through malicious download links or attachments, such as PDF or macro-enabled Word documents. Recently, a new module appeared that exfiltrates email content. It evades signature-based detection and has several ways of maintaining persistence—even in virtual environments.
26%	Trickbot	Emotet drops this modular banking trojan. It targets user financial information and acts as a dropper for other malware. It uses man-in-the-browser attacks to steal financial information, such as login credentials for online banking sessions. When spread by malspam campaigns, it arrives in emails with Word or Excel attachments and in branding that is familiar to the recipient.

Table 1. Organizations at risk based on simulations of high-profile threats, starting in January 2019. Sources: Cymulate Research Lab; Top 10 Malware April 2019, Center for Internet Security

[6] A deeper look: How the 281 data breaches in Q1 2019 will impact companies, Help Net Security, May 10, 2019 https://www.helpnetsecurity.com/2019/05/10/data-breaches-q1-2019-impact/

04 Identifying Immediate Threats with BAS

Automated Breach & Attack Simulation: A Better Way

You can double-check for updated IoCs across security controls, which is never a bad thing to do. You also can carbon copy your network and run threat binaries. You might be less likely to build your own simulations, but it's an option. However, when threats morph almost weekly, adapt to the environment in which they find themselves, and can disable controls—traditional testing approaches simply can't keep up.

Breach & Attack Simulation (BAS) solutions are up to what seems like an overwhelming task. They operate from an attacker's perspective, challenging your defenses in order to measure their effectiveness. Anyone on your security team can simulate attacks on any—and all—of your existing controls, across vectors, with up-to-the-minute knowledge of immediate threats and tactics. Use BAS to test email gateways, web gateways, and endpoints for effectiveness against the latest threats. With just a few clicks, a BAS solution can initiate thousands of simulations to challenge both internal and external defenses.

Email Gateways:

BAS can check detection and response tools, content disarm and reconstruction (CDR) tools that remove suspicious macros and links, and sandboxes that detain suspicious emails or attachments for analysis. A simulated attack will send emails with weaponized attachments that contain different malicious behaviors, but are harmless to the target system. An agent sitting on top of the email client handles incoming emails and deletes them immediately after the simulation. A BAS solution also can simulate threats in nested files—such as an executable inside a Word file inside a PowerPoint presentation—which many email gateways cannot detect.

Web Gateways:

BAS tests across the web gateway, IPS/IDS solutions, EDR solutio ns, and policies to uncover vulnerabilities. In testing for command-and-control (C2) communications, a simulation will attempt to establish a connection over HTTP/S, with an agent installed on the endpoint serving as a proxy to block any malicious requests sent. It drops the connection at the end of the test.

Endpoint Security:

Use BAS to know how well your endpoints catch signatures and suspicious behaviors. It can test EDRs, endpoint protection platforms (EPPs), antivirus, next-gen antivirus, and IPS/IDS solutions to ensure that they detect and stop threats. When testing endpoint security controls, rather than executing a real payload, one simulation technique drops a malware sample to see if security controls can detect and delete it. BAS will test settings to ensure that endpoint solutions are actually blocking or quarantining files rather than just monitoring. In addition, BAS can extract malware's behavioral information—such as activities or commands executed—and then generate a simulation based on identified MITRE ATT&CK techniques to create a safe replica, which is executed on a target machine. Simulation results are the outputs from each command.

If you run BAS on a dedicated golden image of a standard workstation or server, you can continuously simulate attacks even in a production network. This way, real users' data is not jeopardized, and you can check the latest threats' abilities to bypass security controls. Ongoing or daily simulations of the newest menaces across your network, you can determine how well your controls catch IoCs such as command-and-control (C2) URLs and malicious file hashes.

04 Identifying Immediate Threats with BAS

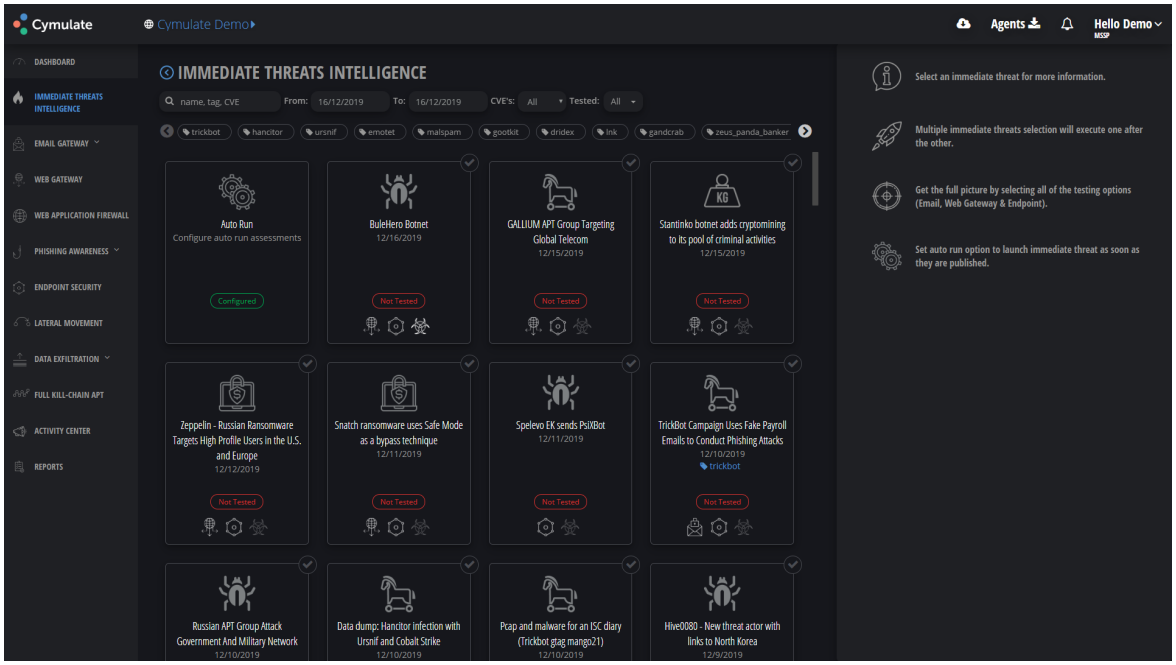


Figure 1. Immediate Threats Available for Simulation

Continuous Threat Updates

The BAS tool continuously receives new threat simulations. This data comes from the research lab, which analyzes threat data received from public feeds, proprietary research, honeypots, and other sources. In addition, expert security analysts and researchers actively hunt threats. New threats are captured, analyzed, and a simulation created for customers to run within one to two days.

Automated Testing

Automated BAS enables you to test controls in the actual environment, instead of on a network carbon copy, to ensure nothing is overlooked. In this way, you can more easily uncover vulnerabilities due to human error, such as a web gateway set to "monitor" instead of "block." Schedule immediate threat simulations to run automatically across email gateways, web gateways, and endpoints or search and simulate by threat type. BAS tests for multiple threats in each vector, providing detailed data about vulnerabilities, including remediation suggestions.

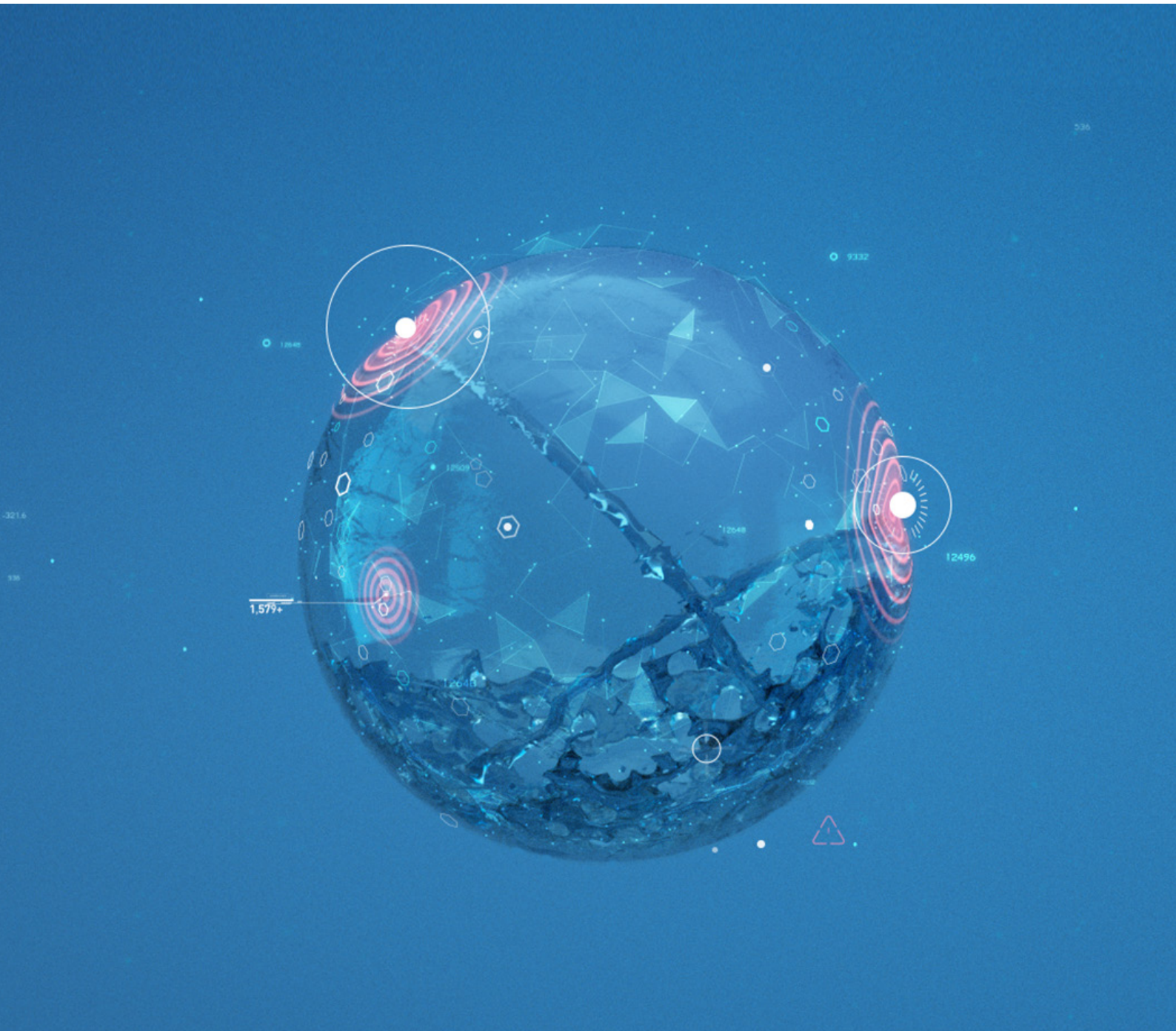
The New Normal

Cyberthreat agility and innovation are only increasing. Automated BAS testing now gives you more equal footing. Continuous testing enables you to identify gaps before they can be exploited. With the power to expand and refine simulations across your environment and drill down to deep levels of technical detail, your organization can significantly reduce the risk of making the headlines. Which in this case, is always a good thing.

05 About Cymulate

Cymulate helps companies to stay one step ahead of cyber adversaries with a unique breach and attack simulation platform that empowers organizations with complex security solutions to safeguard their business-critical assets.

By mimicking the myriad of strategies hackers deploy, the system allows businesses to assess their true preparedness to handle cyber security threats effectively. Cymulate is privately held and headquartered in Israel.



Ready to Cymulate? Get started with a free trial

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com
US Office: 31W 34th Street, 8th floor, New York, New York, 10001 | +1 212 6522632