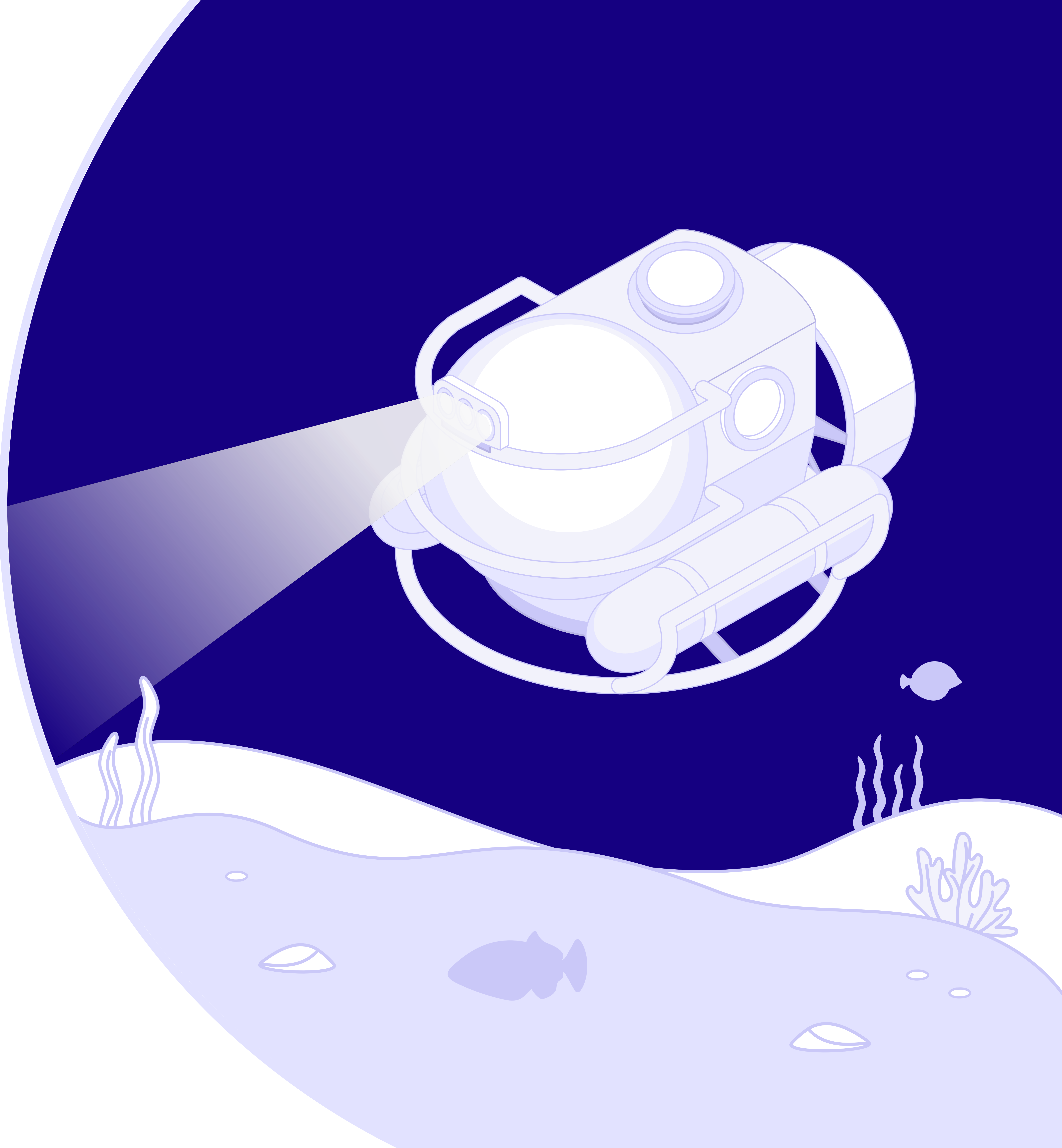
cymulate

10 Cybersecurity Exposures You Can’t Afford to Ignore

Lessons from Real-World
Cybersecurity Exposure Validation



Real Stories from the Front Lines of Cyber Resilience

Assumptions about security controls can be dangerous. Organizations invest millions in layered defenses, believing they are well-protected against cyber threats, but the world's headlines often tell a different story.

This e-book highlights 10 real exposures uncovered by the Cymulate Exposure Validation platform across multiple industries. These are not theoretical risks; they are actual findings from organizations that took a proactive stance, validating their defenses before an adversary could exploit them. Some of these exposures may seem minor at first glance, but left unchecked, even small gaps can lead to major breaches, financial loss or operational disruption.

Thanks to their proactive mindset, these Cymulate customers caught the gaps in time to fix them, proving that continuous validation is essential. These stories prove that with the right tools and mindset, cyber resilience is within reach.

Table of Contents

CUSTOMER 1:
Caught, But Not Contained: The Email Gateway Flaw

Industry:
Insurance

Employees:
201-500

Cymulate Rep:

Daniel Porat

Customer Success Lead

The exposure:
This security team configured its email gateway to prevent ransomware, but Cymulate assessments showed that ransomware was still getting through. The security team discovered that if only one of the seven antiviruses detected ransomware in its email gateway, the email could still get through.

The exposure's potential impact:
Since ransomware could bypass the email gateway, the organization would have been vulnerable to widespread infections. For example, if employees unknowingly opened malicious attachments or clicked on phishing links, ransomware could have encrypted critical business data. This would inevitably lead to business disruption, loss of data, reputational damage and financial and legal consequences.

Cymulate remediation guidance:
Cymulate guided the security team in reconfiguring its email gateway to quarantine an email even if only one antivirus detects ransomware. The email gateway risk score decreased from 30 to 5, and ransomware no longer penetrated its defenses.

Time to remediation:
One hour

CUSTOMER 2:
Weak Segmentation, Wide Access

Industry:
Shipping

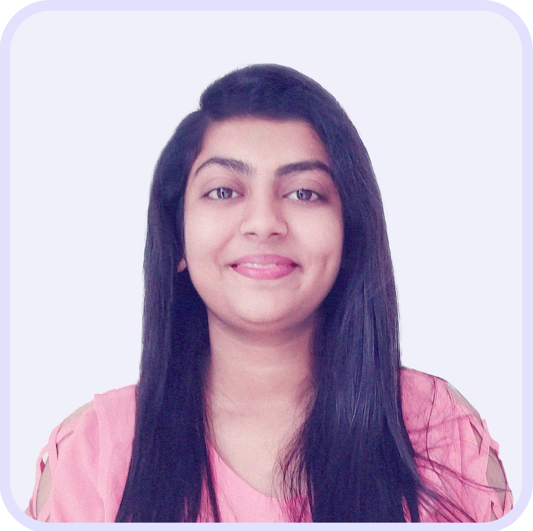
Employees:
251-500

The exposure:
This security team assessed its network segmentation with Cymulate and discovered that an attacker could move from a high-privilege user to 11 domain admin machines, eventually reaching an air-gapped environment. The reason the Cymulate agent was able to move laterally was that the company's local admin credentials were similar.

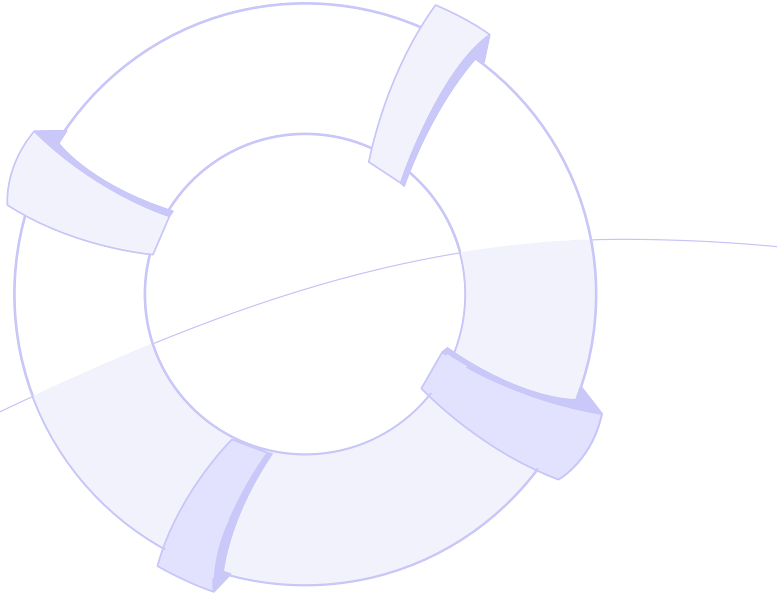
The exposure's potential impact:
An attacker who uses lateral movement techniques to escalate privileges and gain access to 11 domain admin machines can deploy ransomware across the entire network, modify Active Directory (AD) policies, create backdoors for persistence, or disable security tools, including SIEM, EDR and firewalls. Additionally, if an attacker reaches an air-gapped environment, they could sabotage industrial control systems (ICS), exfiltrate sensitive or classified data, or inject malware (e.g., Stuxnet-style attack) to manipulate critical infrastructure.

Cymulate remediation guidance:
Cymulate instructed the customer to create different passwords for all local admin and create internal network segmentation.

Time to remediation:
The customer is implementing the remediation in phases, making it an ongoing process.



Cymulate Rep:
Raxita Patel
Customer Success Lead



CUSTOMER 3:
Legacy Servers Make Easy Targets

Industry:
Government

Employees:
501-1,000

Cymulate Rep:

Marcel Sokolovsky

Customer Success Manager

The exposure:
This security team ran a routine Cymulate attack surface management scan against its domain and found several old IIS web servers running Windows 2008, which should have been retired.

The exposure's potential impact:
An unpatched, End-Of-Life Windows server exposed to the internet left the organization susceptible to known and newly discovered vulnerabilities, like EternalBlue (MS-17-010). Attackers often target outdated systems because they are easier to compromise, and this exposure poses a considerable risk to the customer's infrastructure.

Cymulate remediation guidance:
Cymulate provided a detailed list of affected servers and recommendations for decommissioning them.

Time to remediation:
2 weeks

CUSTOMER 4:
Partially Deployed Policy, Fully Exposed Servers

Industry:
Sports Media

Employees:
1,001-5,000

The exposure:
This security team had configured a CrowdStrike security policy to detect and block malicious Microsoft HTML Application (MSHTA) activity across its environment, believing the policy would be uniformly applied to all its assets. After running Cymulate endpoint assessments, the security team noticed that its production servers failed to trigger the same detection mechanisms as its workstations. The policy had not been properly pushed to all assets in the environment, leaving critical servers exposed to potential attacks that could exploit MSHTA vulnerabilities.

The exposure's potential impact:
MSHTA is a common vector for delivering malicious payloads, particularly in fileless malware attacks. Its detection is crucial for preventing cyberattacks involving PowerShell, script-based exploits, or other advanced persistent threats (APTs). This exposure left these servers vulnerable to attacks leveraging MSHTA exploits, potentially allowing an attacker to execute arbitrary code on the affected servers undetected.

Cymulate remediation guidance:
Cymulate guided the security team to reconfigure its CrowdStrike policies, ensuring that all endpoints, including production servers, were fully covered against MSHTA-based attacks.
The security team also implemented a process for verifying that all security policies were consistently applied to the organization's assets, reducing the risk of similar issues occurring in the future.

Time to remediation:
Under 24 hours

Cymulate Rep:

Gio Macias

Senior Technical Account Manager

CUSTOMER 5:
The Script That Slipped Through

Industry:
Media

Employees:
2,501-5,000

Cymulate Rep:

Marcel Sokolovsky

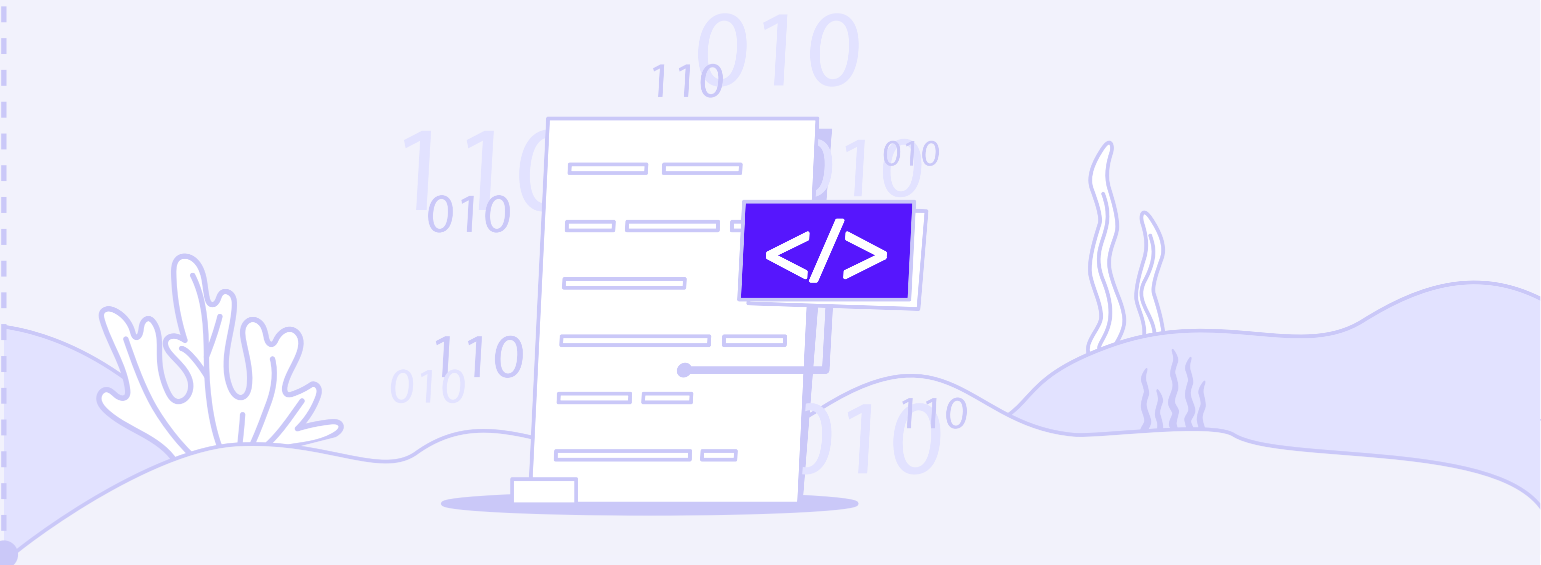
Customer Success Manager

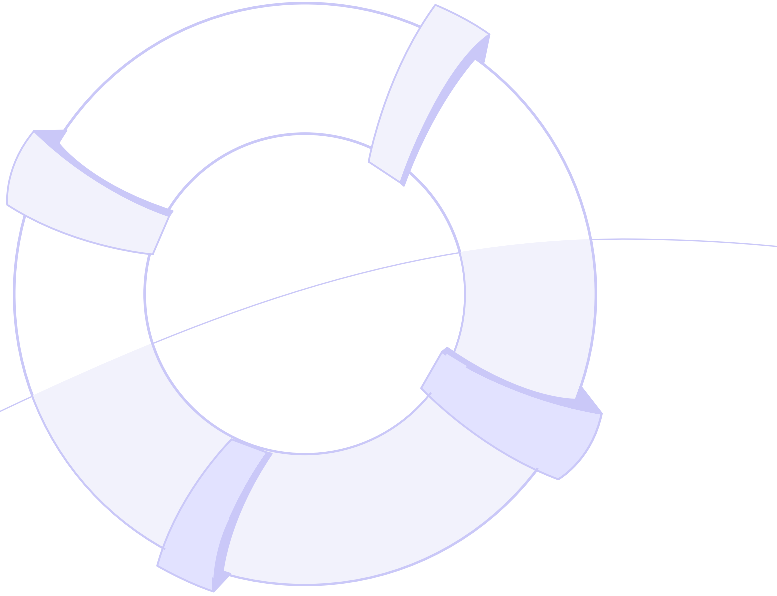
The exposure:
This security team ran routine email gateway assessments and discovered that the organization wasn't blocking ".py" Python scripts as email attachments.

The exposure's potential impact:
A malicious Python script could be delivered as part of a phishing campaign targeting specific users and tricking them into running code from unknown sources to distribute malware, ransomware, or other malicious payloads. Additionally, Python scripts are highly versatile, allowing attackers to include logic that detects virtualized environments, evades antivirus systems, or adapts behavior based on the target.

Cymulate remediation guidance:
Cymulate advised the customer to include the ".py" extension in its email gateway blocking list.

Time to remediation:
3 weeks





CUSTOMER 6:
Leaked Credentials Lead to a Security Wake-Up Call

Industry:
Government

Employees:
2,501-5,000

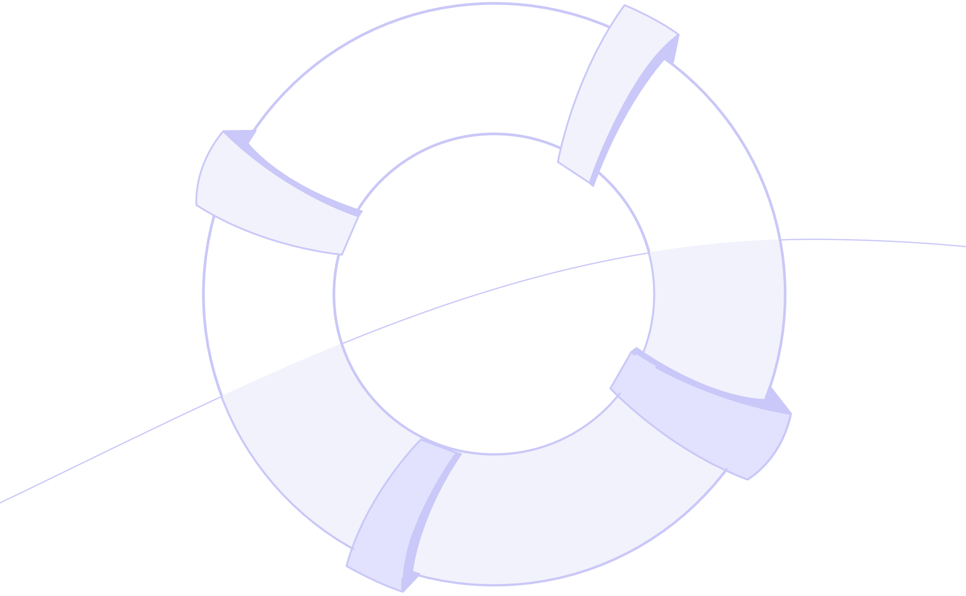
Cymulate Rep:
Marco Sasso
Customer
Success Manager

The exposure:
After a breach, this security team wanted to understand where its employees' credentials were leaked, so they ran a Cymulate attack surface management scan. The scan discovered that many employees were using their work credentials and passwords on e-commerce websites, where they were easy for hackers to steal.

The exposure’s potential impact:
Employees’ exposed credentials could lead to an account takeover and additional large-scale breaches.

Cymulate remediation guidance:
Once the exposure was discovered, the company immediately pushed the impacted user to change his credentials and elevated the password complexity and rotation policy. The organization created an emergency advisory to its employees not to use work credentials outside of the workplace. Additionally, the organization prioritized educating its employees on security hygiene practices.

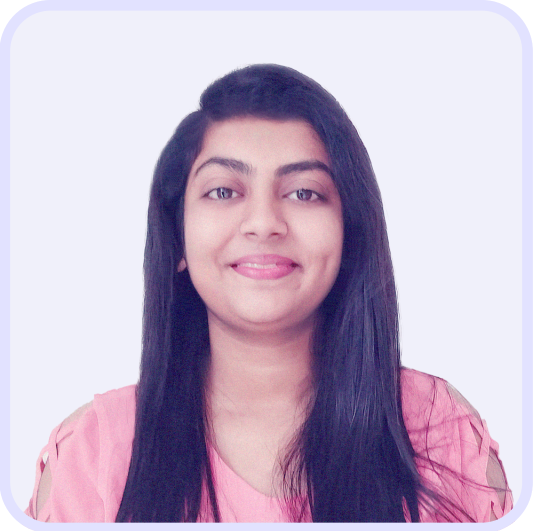
Time to remediation:
A few hours



CUSTOMER 7:
A Single User Exception Becomes a Company-Wide Risk

Industry:
Airlines & Aviation

Employees:
10,001+



Cymulate Rep:

Raxita Patel

Customer Success Lead

The exposure:
This organization’s CSO prioritized web application security because he was confident that his additional security controls prevented downloading from the internet. To prove his assumption, the CSO ran a few web gateway assessments and was shocked to discover that he was wrong; employees could download executables, scripts and other high-risk files directly from the internet. The CSO reached out to the proxy team with the assessment results. After some investigating, the proxy team discovered that when it had configured a web gateway exception for one specific user to download these files from the internet, it had actually implemented this policy for all its 40,000 employees.

The exposure’s potential impact:
Employees could download malware, ransomware or trojans directly from the internet, exposing the entire organization to ransomware, phishing and data breaches.

Cymulate remediation guidance:
The proxy team reconfigured the policy to prevent all employees from being able to download malicious files from the web.

Time to remediation:
2 minutes

CUSTOMER 8:
Hardcoded and Headed for Trouble

Industry:
Manufacturing

Employees:
10,001+

The exposure:
This security team ran a Cymulate lateral movement assessment to validate network resilience in its corporate environment. The results showed hundreds of servers using the same local administrator passwords, which were hardcoded in its golden image. It also discovered additional passwords in the CompanyNameYear! format.

The exposure's potential impact:
These weak passwords could be easily guessed or cracked using custom password lists and leaked credentials. If an attacker had captured one of these local administrator passwords, the attacker could move laterally across the corporate environment, collecting critical information and escalating privileges to reach the organization's domain controller. Additionally, if an attacker gains initial access, it increases the risk of an advanced persistent threat (APT).

Cymulate remediation guidance:
Cymulate shared the list of hosts accessed with the same password and recommended implementing Microsoft LAPS to manage and rotate local administrator account passwords. Cymulate also recommended reviewing the weak passwords and implementing a password vault solution.

Time to remediation:
6 weeks

Cymulate Rep:

Marcel Sokolovsky

Customer Success Manager

CUSTOMER 9:
Execs Wanted Speed, Security Demanded a WAF

Industry:
Retail

Employees:
10,001+

Cymulate Rep:

Lucas Veiga

Customer Success Lead

The exposure:
This retail company suffered a significant cyberattack and continued losing money because the affected server was down. The executive team wanted to get the server back into production immediately. However, the security team knew it needed to strengthen its web application firewall (WAF) defenses before reestablishing the affected server and contacted Cymulate to help make the case. The security team ran a Cymulate assessment, resulting in 96% of web-based attacks getting through the organization's defenses and proving to the executive team the importance of strengthening its WAF.

The exposure's potential impact:
Without a WAF, the previously attacked server could have been attacked again, causing more downtime, additional costs, and further loss of customer trust.

Cymulate remediation guidance:
Cymulate guided the customer in putting the server behind a WAF and helped them fine-tune the new configurations.

Time to remediation:
It took two days to implement the web rules and put the server behind a WAF. Since this incident, every time the organization wants to push a website to production, the security team must run a Cymulate WAF assessment to ensure its security.

CUSTOMER 10:
The Nesting Trick That Bypassed the Gateway

Industry:
Banking

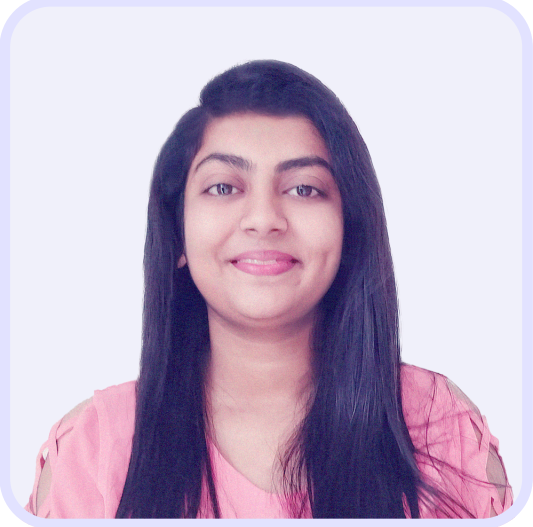
Employees:
10,001+

The exposure:
This security team configured its email gateway and was confident that it didn't allow email attachments outside of the organization. To validate the configuration, the security team ran a Cymulate email gateway assessment. The assessment found that when sending emails with singular attachments without a nesting structure, the control blocked the email, but if the email included a zip file with an exe, the email was not blocked.

The exposure's potential impact:
This gap in the organization's email gateway control could easily be exploited by attackers to deliver ransomware, steal credentials and exfiltrate sensitive data.

Cymulate remediation guidance:
Cymulate assisted the team in fine-tuning its CDR (content disarm and reconstruction) and sandbox policies.

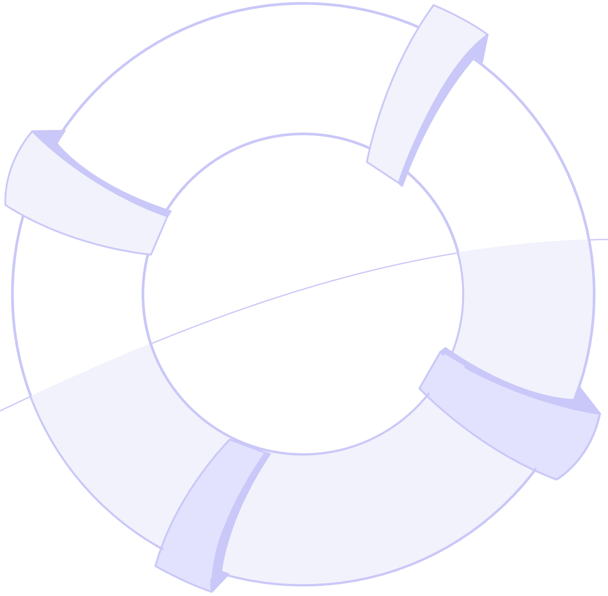
Time to remediation:
After multiple rounds of fine-tuning, it took the team about 4 weeks to close this gap.



Cymulate Rep:

Raxita Patel

Customer
Success Lead



Don’t Wait for a Breach to Discover Your Gaps

These 10 stories highlight a crucial truth: even the most well-funded, well-intentioned security programs can leave dangerous exposures unchecked. From outdated servers and misconfigured policies to overlooked exceptions and unexpected gateway gaps, every organization is vulnerable to something.

What sets these customers apart isn’t perfection; it’s vigilance. They chose to validate, not assume. Because they acted early, they avoided what could have become major security incidents.

Here are examples of real Cymulate customer outcomes:

Hertz
TRANSPORTATION

↓ 81%
Reduction in security risk score in 4 months

BANCO PAN
FINANCE

↓ 25%
Reduction in manual SecOps tasks

Persistent
IT SERVICES

↓ 70%
Reduction of vulnerabilities from previous pen test

cymulate

Schedule a Demo

Request a Cymulate demo today and see how exposure validation can uncover your hidden gaps before an attacker does.

Request a Demo

About Cymulate

Cymulate, the leader in security and exposure validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 1,000 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.