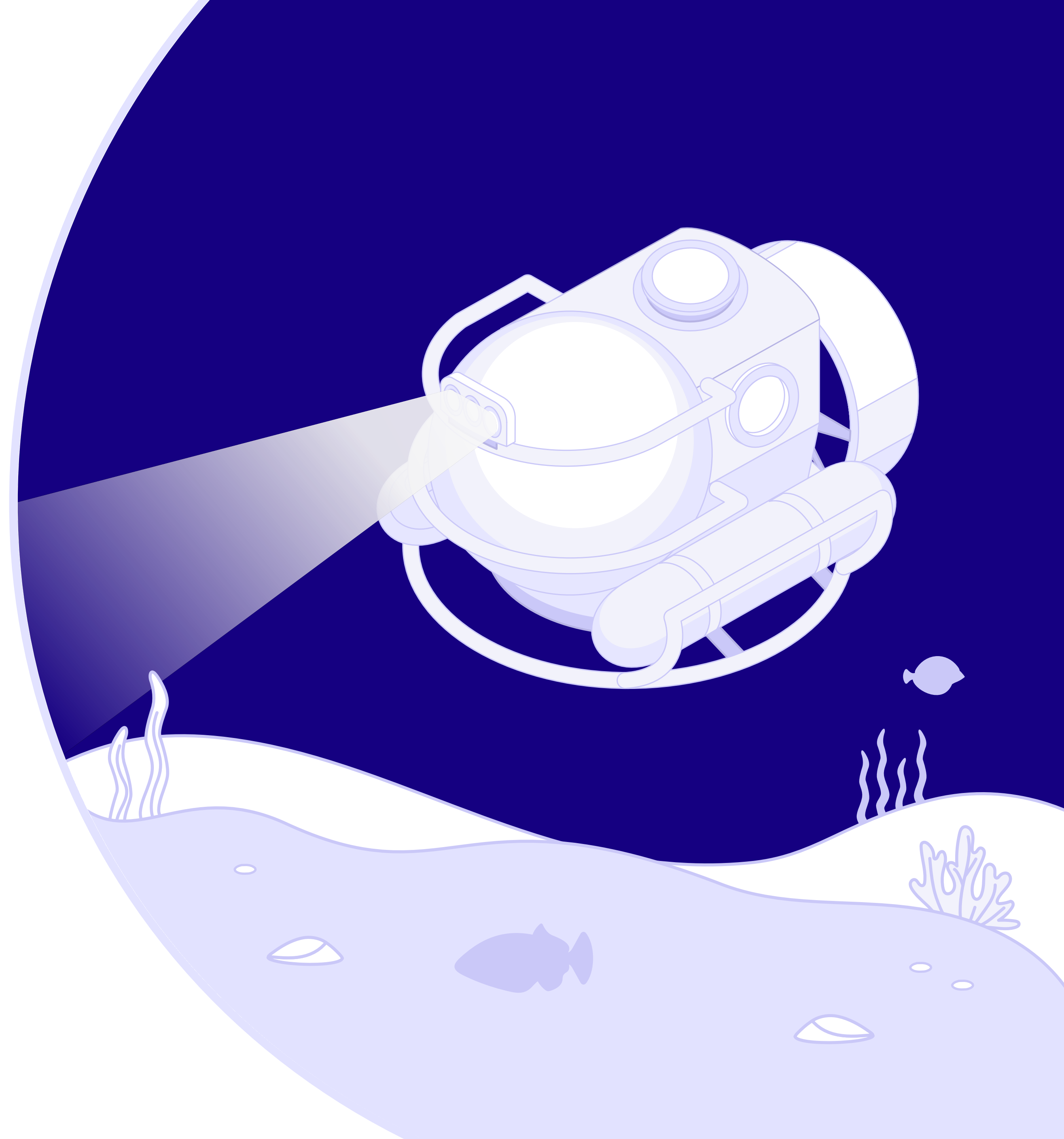




10 Cybersecurity Exposures You Can't Afford to Ignore

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 Cymulate Exposure Validation 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	4
Customer 2: Weak Segmentation, Wide Access	5
Customer 3: The Exposure Behind Vendor-Assured Security	6
Customer 4: Partially Deployed Policy, Fully Exposed Servers	7
Customer 5: The Script That Slipped Through	8
Customer 6: A Single User Exception Becomes a Company-Wide Risk	9
Customer 7: Hardcoded and Headed for Trouble	10
Customer 8: Execs Wanted Speed, Security Demanded a WAF	11
Customer 9: The Nesting Trick That Bypassed the Gateway	12
Customer 10: Open Ports, Open Doors: When Segmentation Fails	13

CUSTOMER 1:

Caught, But Not Contained: The Email Gateway Flaw

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.



Industry:
Insurance



Employees:
201-500

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:

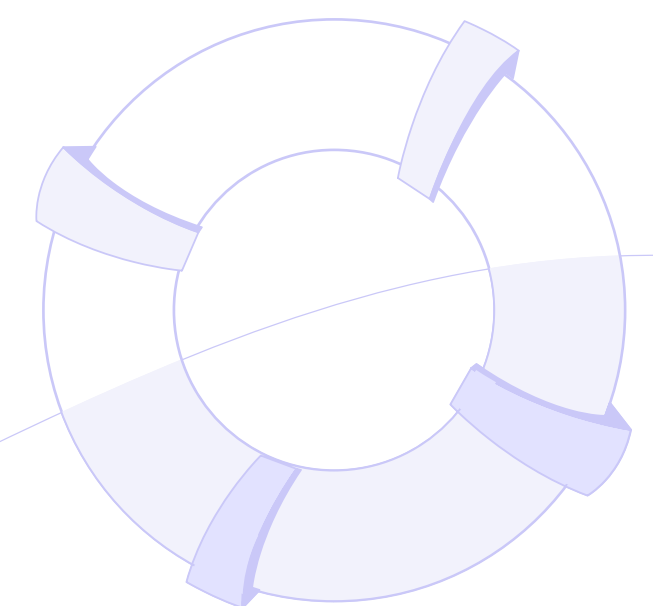
One hour



Cymulate Rep:

Daniel Porat

Customer
Success Lead



CUSTOMER 2:

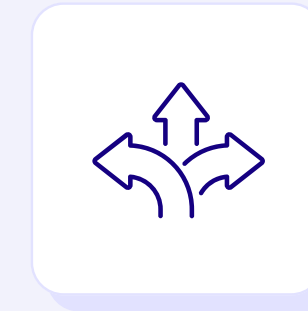
Weak Segmentation, Wide Access

The exposure:

This security team assessed its network segmentation with Cymulate Attack Path Discovery and found 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.



Industry:
Shipping



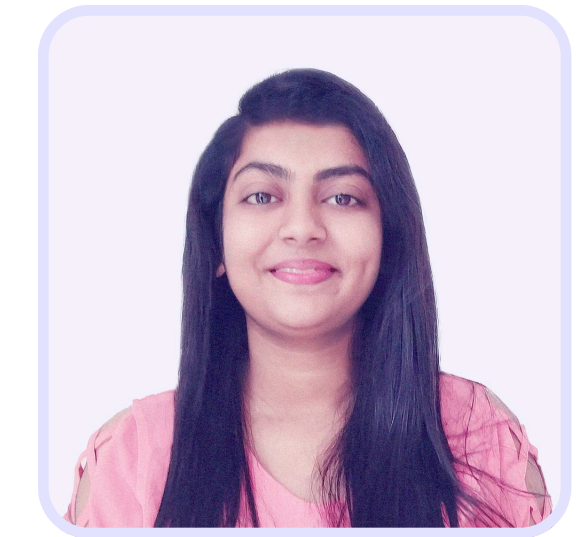
Employees:
251-500

Cymulate remediation guidance:

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

Time to remediation:

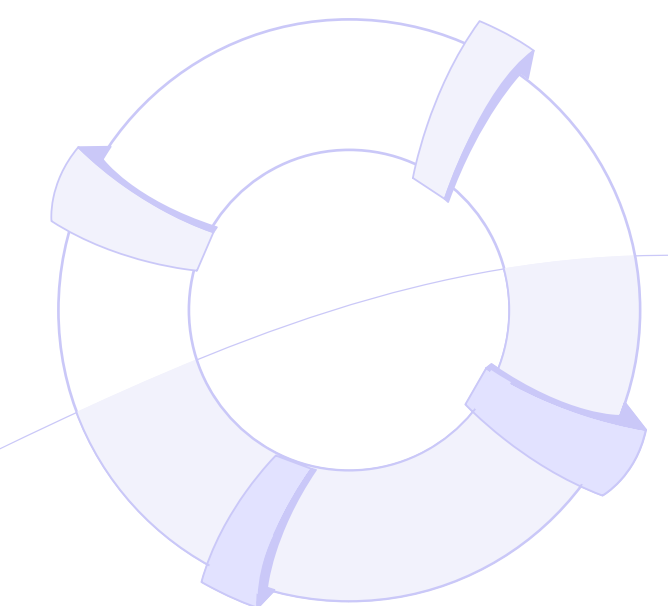
The customer is implementing the remediation in phases, making it an ongoing process.



Cymulate Rep:

Raxita Patel

Customer
Success Lead



CUSTOMER 3:

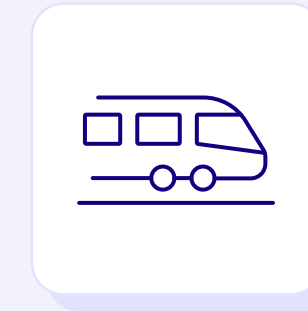
The Exposure Behind Vendor-Assured Security

The exposure:

This customer recently invested in a new XDR, which the vendor helped configure and integrate with his other controls. Once installed and fine-tuned, the vendor assured him it was properly set up. Although the customer was not initially looking for a continuous security validation tool, he decided to run a POC with Cymulate to confirm the XDR's integration and tuning. The Cymulate assessment revealed that the XDR was not detecting or preventing threats as expected. Recognizing the value of continuous validation, the customer immediately purchased Cymulate.

The exposure's potential impact:

If an XDR is not tuned or integrated correctly, malicious activity may bypass detection and prevention entirely, leaving endpoints exposed to ransomware, data theft and lateral movement. This creates a false sense of protection, delays response to real threats and significantly increases the risk of a successful breach.



Industry:
Transportation



Employees:
501-1,000

Cymulate remediation guidance:

Using the platform's remediation guidance, the customer fine-tuned his XDR rules, validated control integrations and continuously tested until the XDR reliably detected and prevented threats as designed.

Time to remediation:

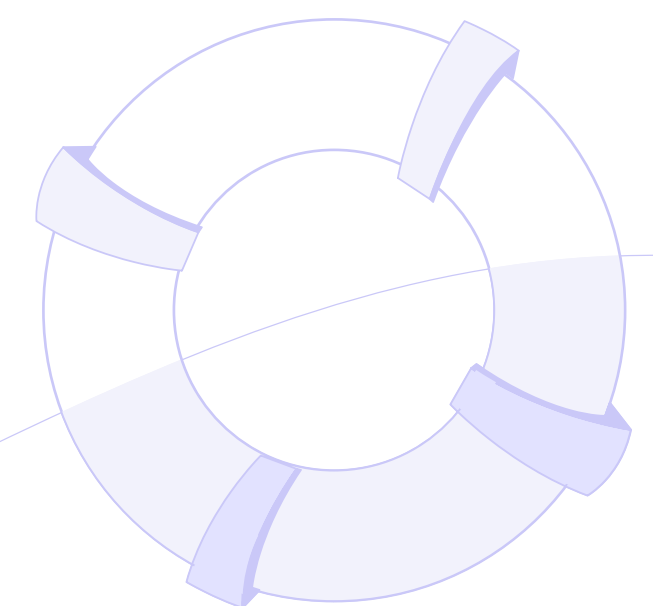
The customer used the Cymulate platform to assess, optimize and validate each security control individually. Within four months, after configuring a new firewall and fine-tuning the web application firewall, XDR, and email gateway, the security team reduced overall cyber risk by 81%.



Cymulate Rep:

Roi Dahan

Customer
Success Engineer



CUSTOMER 4:

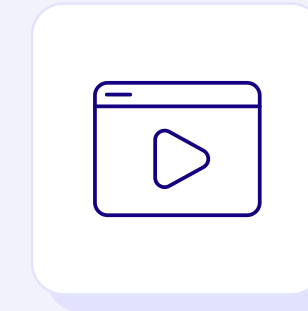
Partially Deployed Policy, Fully Exposed Servers

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.



Industry:

Sports Media



Employees:

1,001-5,000

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:

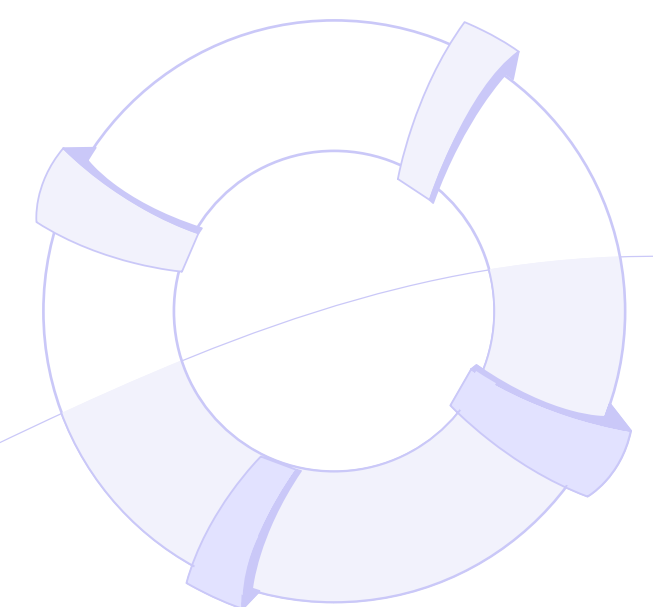
Under 24 hours



Cymulate Rep:

Gio Macias

Senior Technical
Account Manager



CUSTOMER 5:

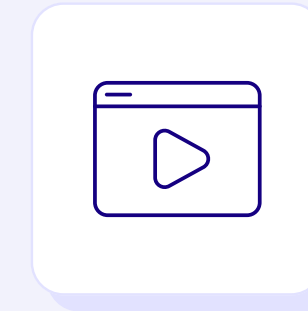
The Script That Slipped Through

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.



Industry:
Media



Employees:
2,501-5,000

Cymulate remediation guidance:

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

Time to remediation:

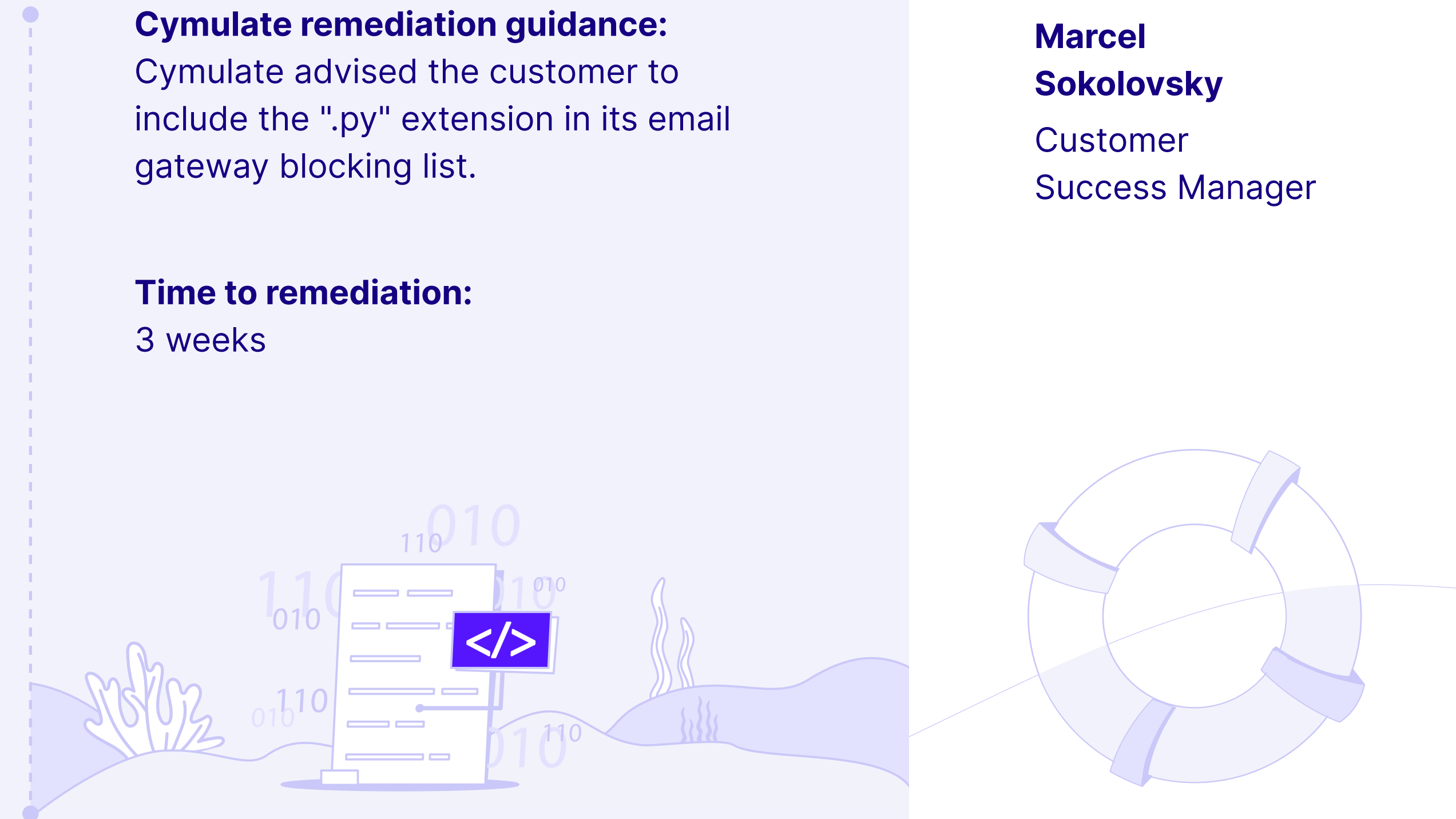
3 weeks



Cymulate Rep:

Marcel Sokolovsky

Customer
Success Manager



CUSTOMER 6:

A Single User Exception Becomes a Company-Wide Risk

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.



Industry:

Airlines & Aviation



Employees:

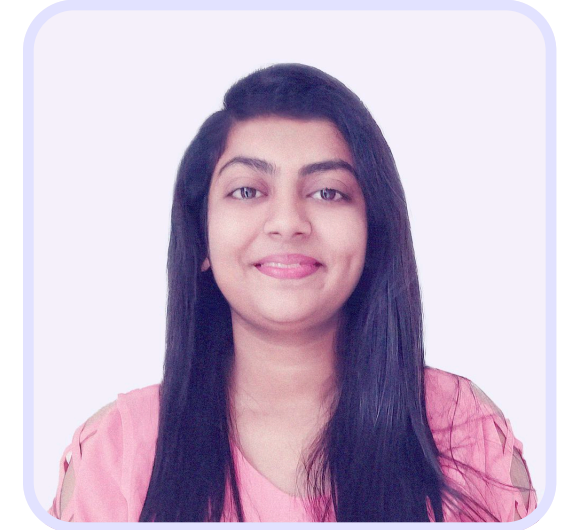
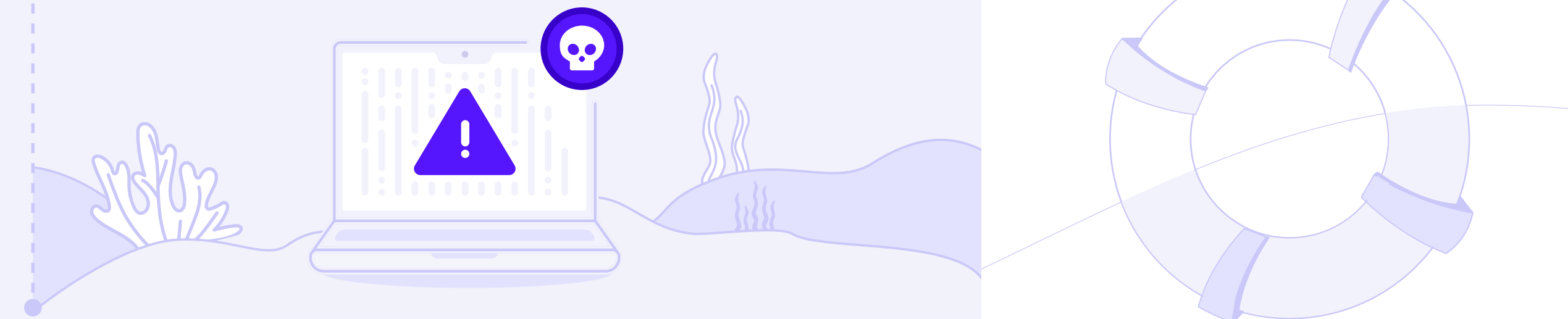
10,001+

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



Cymulate Rep:

Raxita Patel

Customer
Success Lead

CUSTOMER 7:

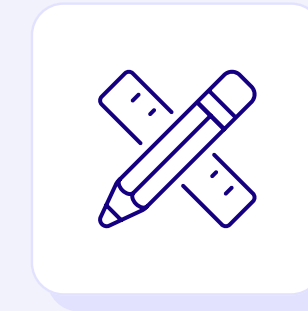
Hardcoded and Headed for Trouble

The exposure:

Using Cymulate Attack Path Discovery, this security team ran a 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).



Industry:

Manufacturing



Employees:

10,001+

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:

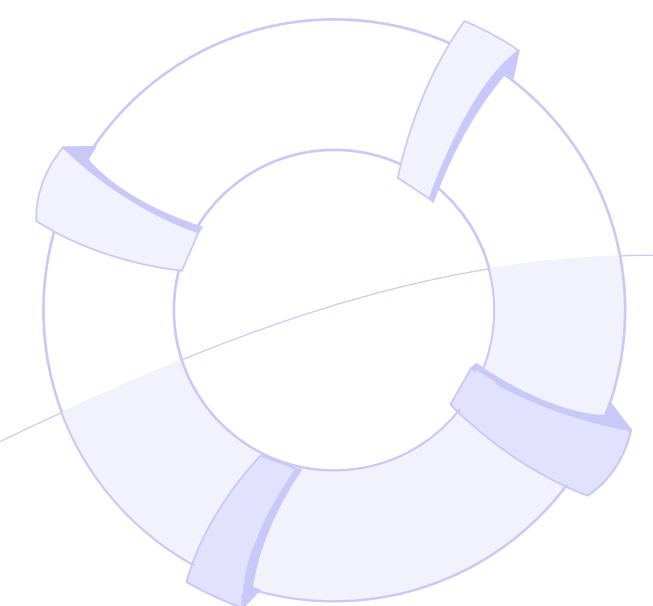
6 weeks



Cymulate Rep:

Marcel Sokolovsky

Customer Success Manager



CUSTOMER 8:

Execs Wanted Speed, Security Demanded a WAF

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.



Industry:
Retail



Employees:
10,001+

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:

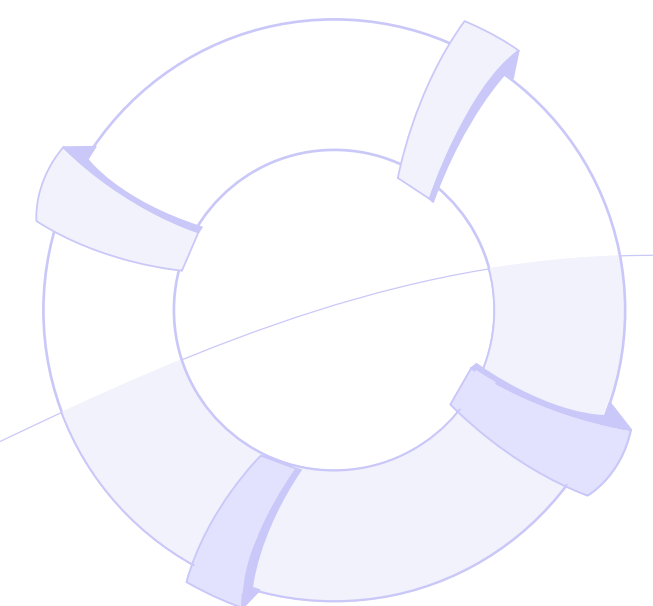
It took two days to implement the web rules and put the server behind a WAF. Since this incident, every time the organization wants to push a website to production, the security team must run a Cymulate WAF assessment to ensure its security.



Cymulate Rep:

Lucas Veiga

Customer
Success Lead



CUSTOMER 9:

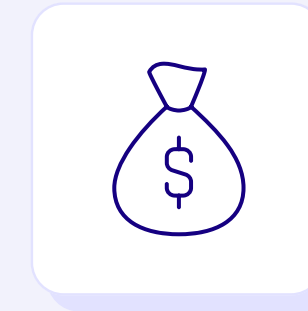
The Nesting Trick That Bypassed the Gateway

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.



Industry:
Banking



Employees:
10,001+

Cymulate remediation guidance:

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

Time to remediation:

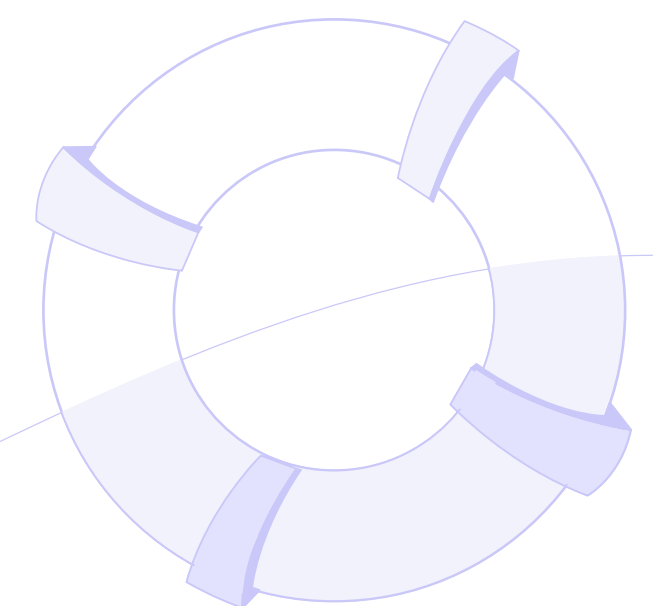
After multiple rounds of fine-tuning, it took the team about 4 weeks to close this gap.



Cymulate Rep:

Raxita Patel

Customer
Success Lead



CUSTOMER 10:

Open Ports, Open Doors: When Segmentation Fails

The exposure:

This customer was unaware that its network segmentation gaps were putting the organization at risk. A standard Cymulate Attack Path Discovery assessment revealed numerous open ports across the network.

The exposure's potential impact:

If network segmentation is misconfigured and open ports remain exposed, adversaries can exploit these weaknesses to gain unauthorized access, move laterally across the environment and escalate privileges. This undermines the purpose of segmentation, leaving the organization vulnerable to widespread compromise from a single entry point



Industry:

Financial Services



Employees:

10,001+

Cymulate remediation guidance:

Using Cymulate's remediation guidance, the customer addressed the segmentation gaps by upgrading its Active Directory environment, blocking unnecessary ports, and tightening internal access controls. The security team systematically re-ran assessments between each change to confirm progress and validate improvements.

Time to remediation:

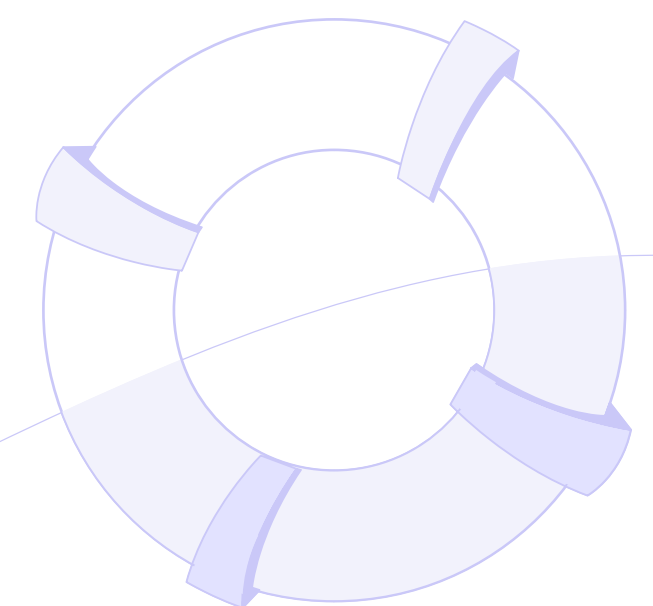
Within a month, the organization significantly strengthened its segmentation posture and reduced its cyber risk by 98%.



Cymulate Rep:

**Abhijeet Kumar
Chandan**

Customer
Success Manager



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



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 is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience; accelerate detection engineering; drive continuous threat exposure management; and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit www.cymulate.com.

