



Cymulate Research

# 2024 State of Exposure Management & Security Validation



# Table of Contents

<b>01</b>	Executive Summary & Key Findings	3
<b>02</b>	Methodology & Sources	4
<b>03</b>	Exposure Management	5
<b>04</b>	Threat Validation	11
<b>05</b>	MITRE ATT&CK Techniques	18
<b>06</b>	Control Validation	20
<b>07</b>	Key Takeaways for Adopting Exposure Management	28

# Executive Summary & Key Findings



## 5% decrease in Control Effectiveness

Based on the average Cymulate score of controls/vectors (endpoint, email gateway, WAF & data exfiltration)



## 63% of organizations found at least one instance of Publicly Exposed Management Services



## Data Exfiltration risk score increased from 33 to 46 since 2021

## The Year of Exposure Management

Security leaders recognize that the pattern of buying new tech and the frantic state of find-fix vulnerability management is not working. Rather than waiting for the next big cyberattack and hoping they have the right defenses in place, security leaders are now more than ever implementing a proactive approach to cybersecurity by taking action to identify and address security gaps before attackers find and exploit them.

This 2024 State of Exposure Management & Security Validation report from Cymulate highlights the accelerated adoption of exposure management to redefine security operations by:

- Taking an attacker's view to understand weaknesses and gaps
- Profiling the networks, systems, clouds, applications, data, SaaS and controls that make the organization vulnerable to attack – and knowing the downstream impact if each was attacked
- Testing and validating security controls, defenses and incident response

# Methodology & Sources

## Cymulate Scoring Legend & Color Chart

Secure	0-10
Low	11-33
Medium	34-67
High	68-100

This report aggregates anonymized data from attack surface assessments, simulated attack scenarios and campaigns and automated red teaming performed with the Cymulate Exposure Management and Security Validation Platform across a global user base of more than 500 customers.

For reported exposures and vulnerabilities, this report anonymizes data from attack surface management customers and their assessments. The threats-related section of this report is based on customer results from the immediate threats module. When analyzing the top attack techniques, the report analyzes customer findings from both breach and attack simulation and continuous automated red teaming. For benchmarking control effectiveness, the results are aggregated from breach and attack simulation customers.

To benchmark security posture and control effectiveness, Cymulate uses a proprietary scoring method based on known industry standards, including the MITRE® ATT&CK® Framework, NIST Special Publication 800-50 and other benchmarks. The weighted averages used in this report compensate for the divergence in the relative usage of specific vectors. The results are presented on a scale of 0 to 100 (with 0 indicating the least risk); and further divided into four risk categories: Secure for the top performers, Low Risk for systems which may require tuning, Medium Risk for areas that require definite attention and High Risk indicating little to no security control or ineffective security controls.

# Exposure Management

Security operations are evolving the traditional practice of vulnerability management to continuously monitor the attack surface, validate risk and focus on the biggest weaknesses.

## Vulnerabilities vs. Exposure Risks

Traditional vulnerability management aims to strengthen your security posture with an internal focus to identify and remediate Common Vulnerabilities and Exposures (CVEs) – the industry-reported weakness that an attacker can potentially exploit. In contrast, exposure management adopts the attacker's view of your organization to focus on the most potentially damaging security gaps.

### Vulnerabilities

A vulnerability is defined by the MITRE organization as “a set of one or more related weaknesses within a specific software product or protocol that allows an actor to access resources or behaviors that are outside of that actor's control sphere.” Vulnerabilities arise when software, services, or platforms develop a weakness which is then discovered by threat researchers or threat actors and indicates only the potential for an exposure event.

### Exposures

An exposure event is when either a vulnerability or some other set of circumstances is not balanced by security controls, leaving the organization with a path for a threat actor to gain access to systems and data that they would not otherwise have access to. Such circumstances could include misconfigurations, lax defensive protocols, outdated software that cannot be upgraded any longer or a host of other operational issues that stretch far beyond vulnerabilities alone. Exposures can also be mitigated in multiple ways – by patching, when possible, but also by implementing and/or strengthening security controls, processes, and personnel actions, correcting misconfigurations, strengthening identity and access management, etc.

### Attack surface management

The Cymulate platform includes attack surface management to continuously monitor an organization's cyber presence – both known and unknown. This attack surface includes traditional CVEs as well as misconfigurations, deviation from best practices, and control gaps. It also includes the dark web and the likely availability of organization data and secrets available – and outside their control.

The following section explores interesting observations from attack surface management scans and provides easy-to-implement recommendations on how to better protect your organization's attack surface from exposures.

## External Attack Surface & Vulnerable Websites

Public-facing websites and web apps present an organization to its prospects, partners, users and the market at large. While code libraries enable integrations and efficient use of existing tech, these same code libraries often include software vulnerabilities that create the opportunity for unauthorized access to sensitive data, malware distribution and more. Attack surface management continuously scans websites to present the attacker's view of the attack surface.

As part of these scans in 2023, Cymulate identified vulnerable code libraries with at least one high severity CVE in 76 percent of all scans; 91 percent of scans identified a code library with at least one medium severity CVE. Code libraries with at least one low-severity CVE were found in 83 percent of all scans.

### Vulnerability management best practices

Library maintenance and updates should be a priority for organizations. Application security teams should leverage available platforms that track libraries in use while monitoring for known vulnerabilities.

### Role of exposure management

The high prevalence of vulnerabilities in a website's code libraries is NOT a simple binary indicator of weak security. In fact, the high number points to the need for exposure management, where vulnerabilities are analyzed based on the full context of the affected asset/system, business impact and validated attack paths. These factors verify both how an attacker could exploit the vulnerability and the following ramifications of lateral movement, escalated privilege, access to crown jewels, etc. Organizations can have very valid reasons for leaving these vulnerabilities unpatched, such as end-of-life systems that do not have patches and are protected with mitigating controls like web application firewalls.

### Customers with at least one vulnerable library identified on a website

76%

High Severity CVE

91%

Medium Severity CVE

83%

Low Severity CVE

CVSS Ratings: Low 0.1-3.9, Medium 4.0-6.9, High 7.0-8.9, Critical 9.0-10

## Top Exposures: Misconfigurations & Weaknesses Across the Attack Surface

Attack surface management continuously monitors external-facing digital assets and the dark web to present the attacker's view of the organization. Results highlight common misconfigurations, vulnerable applications in use and other security gaps. Results from dark web monitoring highlight an organization's sensitive information available – likely the result of a data breach.

### Top-10 Exposure Types

Exposure Types	Scans with findings	Security Value
DNSSEC is Not Configured	91%	Low
Domain without SPF Records Configured	90%	Medium
Possible Phishing Domains	86%	Varies
Publicly Exposed Management Services	63%	High
SSL Certificate Host Mismatch	56%	Medium
Sensitive Account Information Found in Data Leak or Breach	53%	Low
Account Credentials Found in Data Leak or Breach	48%	High
Publicly Exposed Email Service	47%	Medium
No DMARC Record Configured for Domain	37%	Medium
Company Mentioned on the Darknet	36%	Low

### Top-10 Critical and Severe Exposure Types

Exposure Types	Scans with findings	Security Value
Publicly Exposed Management Services	63%	High
Account Credentials Found in Data Leak or Breach	48%	High
Publicly Exposed Database Service	10%	High
Application with Exploitable Vulnerability CVE-2022-45362 (Server-Side Request Forgery vulnerability in Paytm Payment Gateway)	5%	High
Application with Exploitable Vulnerability CVE-2021-43421 (File Upload vulnerability in Studio-42/elFinder)	5%	Critical
Nginx Information Disclosure Vulnerability (version pre-1.21.1)	2%	High
Nginx 1-byte Memory Overwrite Vulnerability (version 0.6.18 - 1.20.0)	2%	High
WordPress Contact Form 7 - Unrestricted File Upload	1%	Critical
Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux	1%	High
Operating System (OS) End of Life (EOL) Detection	1%	High

## Exposure Analysis: Management Services

Management services play a crucial role in the efficient operation and maintenance of systems, networks and applications – and should rarely be exposed externally. Publicly exposing management services greatly expands the attack surface by creating initial access points to a malicious actor.

Attack surface management identified publicly exposed management services in 63 percent of all scans. This exposure of sensitive services to the public internet is a critical security lapse, potentially allowing unauthorized access to sensitive areas of an organization's network.

While CVEs can create the opportunity for exposing management services, this is a preventable misconfiguration for most organizations.

### Recommended action

- Limit access to management services to a dedicated management network or use a jump server
- Restrict access to management interfaces based on IP whitelisting
- Implement strong authentication mechanisms (e.g., multi-factor authentication)
- Regularly update and patch management software
- Monitor and log activities on management interfaces for suspicious behavior
- Using network security measures such as firewalls and intrusion detection/prevention systems

**63%** Publicly Exposed  
Management Services

**47%** Publicly Exposed Email  
Services

**10%** Publicly Exposed  
Database Services

### Common Exposed Administration Panels

NetScaler AAA Login Panel	6%
WordPress Login Panel	5%
Citrix ADC Gateway Login Panel	4%
Palo Alto Networks GlobalProtect Login Panel	4%
Cisco ASA VPN Panel	4%

Results show the share of scans across all Cymulate customers with this finding.



## Exposure Analysis: Phishing Domains

Phishing domains are websites created with the intent to deceive users by mimicking legitimate websites in order to steal sensitive information. These fraudulent websites often imitate the look and feel of trusted entities, such as banks, social media platforms, or email services, with the goal of tricking users into providing their confidential information, such as login credentials, personal details, or financial information.

The high occurrence of possible phishing domains underscores a prevalent risk. Cymulate results show 86 percent of all scans identified possible phishing domains. This suggests that organizations might be failing to monitor and secure their web domains effectively, leaving them open to being mimicked by malicious actors.

When Cymulate identifies potential phishing domains, the risk score is determined by specific finding details such as:

- Informational – Domains registered but inactive
- Low risk – Domains associated with a specific IP address or nameserver
- Medium risk – Domains include MX records (signifying email capability)
- High risk – Indicators of recent phishing or blacklist evasion (recent registration, visually similar)

### 86% Possible Phishing Domains\*

#### Recommended action

- Report to hosting providers
- Submit to anti-phishing organizations
- Report to domain registrars
- Contact CERT (computer emergency response team)
- Notify web browsers and security software
- Cooperate with law enforcement
- Educate users and community

\*Share of all Cymulate scans with this finding

## Exposure Analysis: SSL/TLS Weaknesses

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) provide the essential cryptographic protocols for provide secure transfer of sensitive information such as login credentials, personal data and financial transactions. Cymulate results show 56 percent of Cymulate scans identified an SSL certificate hostname mismatch where the hostname in the certificate does not match the hostname configured in NAT settings.

As technology advances and new vulnerabilities are discovered, older cipher suites may become deprecated or considered insecure. Cymulate results show 31 percent of Cymulate scans identified vulnerable cipher suites for HTTPS.

Insufficient DH Group Strength is a security issue that occurs when the SSL/TLS service uses Diffie-Hellman groups with key sizes less than 2048 bits. Cymulate results show 25 percent of Cymulate scans identified weak encryption keys that are easier to break.

These misconfigurations can lead to weakened encryption and increased susceptibility to man-in-the-middle attacks. The frequency of these issues suggests that SSL/TLS configurations are not being regularly reviewed or updated in line with best practices.

In many cases, these security weaknesses are unavoidable as older web applications rely on legacy code libraries that cannot be updated. In this case, mitigation is critical. Web application firewalls should be properly deployed and routinely validated to block attacks that exploit these configurations and alert to suspicious activity indicative of man-in-the-middle attacks.

**56%** Organization domains have SSL certificate host mismatch

**31%** Organization domains report vulnerable cipher suites for HTTPS

**25%** Organization domains have insufficient DH Group Strength

### Recommended action

- Manage and update SSL certificates to only include hostnames of supported domains
- Disable vulnerable cipher suites to ensure the security of HTTPS connections
- Use a 2048-bit Diffie-Hellman group in the key exchange process
- Deploy, tune and validate web application firewall capabilities to block exploits and alert suspicious activity

\*Share of all Cymulate scans with these findings

# Threat Validation

Exposure management includes critical steps to validate threats with offensive testing that measures cyber resilience to active threats.

## Control Effectiveness vs. Immediate Threats

Too often, security teams are driven by the external threat environment with the daily announcements of new vulnerabilities (CVEs) as well as the constant evolution of threat actors, their campaigns and successful techniques for breaching defenses. Exposure management brings together threat intel with offensive security testing to validate threats. The Cymulate Platform includes the immediate threats module with daily updates for continuous automated threat validation by measuring the effectiveness of controls to block or detect emergent threats.

To highlight the difference between vulnerability management and exposure management, this report highlights the top vulnerabilities or CVEs and the aggregate threats that may or may not include an associated CVE.

## Threats Exploiting Vulnerabilities (CVEs)

In the daily updates of new threat assessments, Cymulate tags all associated vulnerabilities related to the threat. When analyzing the threats associated with CVEs, the top 10 most frequently assessed threats include eight critical and two high severity vulnerabilities as scored by CVSS with the average control effectiveness ranging from 66 to 89 percent. Other threats targeting CVEs have control effectiveness as low as 34 percent as seen with CVE-2021-21974 – a VMware ESXi vulnerability exploited by malware known as ESXiArgs.

## Threats without Targeted CVEs

Threats are not limited to vulnerability exploitation. Targeted campaigns and common attacks can exploit misconfigurations, control gaps and especially human errors or poor judgment. When analyzing the Cymulate immediate threats that are most likely to penetrate defenses, only one of the top threats had an associated CVE.

The immediate threats assessment data and control effectiveness represent the ability of security controls to block or detect indicators of compromise (IoCs) of the associated threat. Other modules of BAS do assess the effectiveness of behavioral detection and monitoring solutions in stopping executions in progress. In the case of threats targeting CVEs, the results do not indicate the presence of the vulnerability.

## Mitigation of Threats Targeting CVEs: Most Assessed

Targeted CVE	Avg. Control Effectiveness	CVSS Score	Affected Systems	Summary	Sample Threat Actors & Associated Malware
CVE-2021-44228	66%	<b>10 Critical</b>	Apache Log4j	Remote Code Execution	2023 Threat Actors <ul style="list-style-type: none"> <li>Lazurus (aka APT38)</li> <li>MuddyWater</li> <li>Gold Melody</li> </ul>
CVE-2017-11882	74%	<b>7.8 High</b>	Microsoft Office	Memory Corruption	2023 Active Malware <ul style="list-style-type: none"> <li>Agent Tesla</li> <li>ModiLoader</li> <li>Poison Ivy</li> </ul>
CVE-2023-27350	69%	<b>9.8 Critical</b>	PaperCut	Bypass Authentication	2023 Active Malware <ul style="list-style-type: none"> <li>China-sponsored threat actors</li> <li>MuddyWater</li> <li>Blacktail</li> </ul>
CVE-2023-2868	88%	<b>9.8 Critical</b>	Barracuda Email Security Gateway	Remote Command Injection	2023 Active Malware <ul style="list-style-type: none"> <li>SeaSide</li> <li>SeaSpray</li> <li>SSLShell</li> </ul>
CVE-2017-0199	84%	<b>7.8 High</b>	Microsoft Office	Remote Code Execution	2023 Threat Actors <ul style="list-style-type: none"> <li>Gamaredon</li> <li>APT37</li> </ul>
CVE-2020-1472	80%	<b>10 Critical</b>	Windows Netlogon	Domain Controller Administrator Access	2023 Active Malware <ul style="list-style-type: none"> <li>Rhysida ransomware</li> </ul>
CVE-2023-3519	64%	<b>9.8 Critical</b>	Windows	Remote Code Execution	2023 Active Malware <ul style="list-style-type: none"> <li>AsyncRAT</li> </ul>
CVE-2023-34362	68%	<b>9.8 Critical</b>	MOVEit	Unauthenticated Access	2023 Active Malware <ul style="list-style-type: none"> <li>Rhysida ransomware</li> <li>TrueBot</li> </ul>
CVE-2021-34523	89%	<b>9.8 Critical</b>	Microsoft Exchange	Privilege Elevation	2023 Threat Actors <ul style="list-style-type: none"> <li>AvosLocker</li> </ul>
CVE-2021-26855	76%	<b>9.8 Critical</b>	Microsoft Exchange	Remote Code Execution	2023 Threat Actors <ul style="list-style-type: none"> <li>PikaBot</li> <li>APT35</li> </ul>

**Recognizing that security teams do not have the capacity to immediately remediate and patch every vulnerability, exposure management draws upon the concept of threat validation. While new threats and CVEs emerge daily, security controls can serve as effective mitigation and validate the cyber resilience to these threats.**

The average control effectiveness rate reported is based on the security controls' ability to recognize known Indicators of Compromise (IoCs). The immediate threats module does not run active code like other BAS modules. The other modules in BAS do assess the effectiveness of behavioral detection and monitoring solutions in stopping executions in progress. In the case of threats with CVEs, the results do not indicate the presence of the vulnerability.

## Log4J: 2 Years Later and Still an Immediate Threat

Initially disclosed in December 2021, the infamous Log4j vulnerability known as Log4Shell (CVE: 2021-44228) wrecked the holidays for many security and IT teams – and remains an exposure risk more than two years later. This easily exploitable vulnerability in a widely used Apache utility instantly put millions of Java-based applications and services at risk of remote code execution.

Threat actors were quick to exploit this vulnerability and continue to target organizations that have yet to patch and remediate the issue. In 2023, Cymulate released four new threat assessments associated with this vulnerability – on top of the 11 published in 2021 and 2022.

To validate control effectiveness to mitigate threats targeting Log4Shell, Cymulate simulates both exploitations against web application firewalls and post-exploitation threat activity against endpoint and web gateway controls.

### **CVE: 2021-44228**

Affected Systems:  
Apache Log4j versions  
2.0-beta9 to 2.14.1

### **75%**

Average web application  
firewall effectiveness  
against Log4J

### **2023 Immediate Threat Assessments**

### **Post- Exploitation Protection**

### **Avg. Control Effectiveness**

Gold Melody: Profile of an  
Initial Access Broker

- Web Gateway
- Endpoint

62%

Lazarus: Operation  
Blacksmith Campaign Uses  
DLang Malware

- Web Gateway
- Endpoint

63%

US Cert: Ransomware  
Attacks on Critical  
Infrastructure Fund DPRK  
Malicious Cyber Activities

- Web Gateway
- Endpoint

69%

MuddyWater: Israel  
Campaign (March 2023)

- Web Gateway
- Endpoint

89%

## Mitigation of Threats Targeting CVEs: Most Assessed

Targeted CVE	Avg. Control Effectiveness	CVSS Score	Affected Systems	Summary	Sample Threat Actors & Associated Malware
CVE-2021-21974	34%	<b>8.8 High</b>	VMware ESXi	Heap-overflow Resulting In Remote Code Execution	2023 Active Malware: • ESXiArgs
CVE-2023-21716	41%	<b>9.8 Critical</b>	Microsoft Word	Remote Code Execution	Proof of Concept Malware published by security researchers
CVE-2017-0213	48%	<b>4.7 Medium</b>	Microsoft Windows	Privilege Elevation	2023 Threat Actors: • Space Pirates
CVE-2017-17215	49%	<b>8.8 High</b>	Huawei HG532	Remote Code Execution	2023 Active Malware: • Mirai malware variant
CVE-2023-23397	50%	<b>9.8 Critical</b>	Microsoft Outlook	Privilege Elevation	2023 Threat Actors: • APT28
CVE-2023-36884	52%	<b>8.8 High</b>	Microsoft Windows	Remote Code Execution	2023 Threat Actor: • Storm-0978 (aka RomCom Group)
CVE-2022-37969	53%	<b>7.8 High</b>	Microsoft Windows	Privilege Elevation	2023 Threat Actor: • Nokoyawa ransomware group Note: these three CVEs were included in the same immediate threat assessment
CVE-2023-23376	53%	<b>7.8 High</b>	Microsoft Windows	Privilege Elevation	
CVE-2023-28252	53%	<b>7.8 High</b>	Microsoft Windows	Privilege Elevation	
CVE-2019-17232	54%	<b>7.8 High</b>	WordPress	Unauthenticated Options Import	2023 Active Malware: • Linux.BackDoor.WordPressExploit.1

### Control Effectiveness

When analyzing the CVE-based threats for the most successful threats, it's important to note there was less active threat activity as compared to the most assessed CVE threats. None of the most assessed CVEs make the list. Seven of the top 10 most penetrated CVE-based threats are associated with Microsoft products – Outlook, Windows and Word. Two of the top 10 have CVSS scores that fall into the most severe “Critical” category while seven of these CVE-based threats have “High” CVSS scores.

The average control effectiveness rate reported is based on the security controls' ability to recognize known Indicators of Compromise (IoCs). The immediate threats module does not run active code like other BAS modules. The other modules in BAS do assess the effectiveness of behavioral detection and monitoring solutions in stopping executions in progress. In the case of threats with CVEs, the results do not indicate the presence of the vulnerability.

## Immediate Threats: Most Frequently Assessed

Immediate Threat	Avg. Control Effectiveness	Targeted CVE	MITRE ATT&CK Tactics
Malware: Possible Pikabot	47%	CVE-2021-26855	Execution, Defense Evasion, Credential Access, Discovery, Collection
Muddywater in Israel	89%	CVE-2021-44228	Reconnaissance, Resource Development Initial Access, Execution, Persistence Privilege Escalation, Defense Evasion, Credential Access, Discovery, Collection, Command and Control, Exfiltration
Spear Phishing: Malicious Control Panel File Used To Drop Agent Tesla	49%	N/A	Execution, Privilege Escalation
Fake Web Site: Novel Malware Campaign Targets LetsVPN Users	63%	N/A	Credential Access, Collection
Ransomware: Novel Cylance Ransomware Windows & Linux Systems	61%	N/A	Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Discovery, Lateral Movement, Impact
Malware: AceCryptor And Its Operation	63%	N/A	Execution, Privilege Escalation, Defense Evasion
Ransomware: Rorschach	50%	N/A	Execution, Persistence, Privilege Escalation, Defense Evasion, Discovery, Command and Control, Impact
NIS and NCSC: DPRK State-linked Software Supply Chain Attacks	86%	N/A	Initial Access, Persistence, Privilege Escalation, Defense Evasion, Discovery, Exfiltration, Impact
CISA: Russian Foreign Intelligence Service SVR Exploiting JetBrains TeamCity CVE	51%	CVE-2023-42793	Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Command and Control, Exfiltration, Impact
Malware: New Version of Mirai	54%	N/A	Execution, Persistence, Privilege Escalation, Defense Evasion, Discovery, Command and Control

The average control effectiveness rate reported is based on the security controls' ability to recognize known Indicators of Compromise (IoCs). The immediate threats module does not run active code like other BAS modules. The other modules in BAS do assess the effectiveness of behavioral detection and monitoring solutions in stopping executions in progress.

## Threat Analysis: Pikabot

In 2023, Cymulate customers ran the Possible Pikabot threat assessment more than any other immediate threat. PikaBot is an emerging malicious backdoor compromising systems since early 2023 by providing access to other attackers for ransomware, crypto-mining, data theft and remote control.

A sophisticated phishing campaign that was first detected in September, Pikabot has demonstrated a remarkable evolution in its tactics. Initially focused on disseminating DarkGate malware, this campaign has now incorporated more complex and elusive strategies. These advanced techniques are not only aimed at evading detection but also include anti-analysis measures, which enables the continued spread of the DarkGate malware.

Cymulate Threat Research Group identified a sample in the wild that is highly likely to this campaign. The identified sample shares certain characteristics with the recent PikaBot cases, including defense evasion tactics like data encoding using XOR and base64 and discovery methods that suggest phishing as a probable distribution method – although web-based spreading cannot be ruled out. The sample also exhibits features not previously associated with PikaBot, such as input capture, data collection, the ability to impersonate access tokens and the ability to check for a debugger presence. Researchers within the cyber community have also drawn connections between this file and PikaBot.

### Immediate Threat:

Possible PikaBot

### Threat Summary:

Malware drops backdoors and often leads to ransomware attacks

### Penetration Rate:

53 percent

### Security Controls:

- Email gateway
- Web gateway
- Endpoint

### Threat Actors:

Water Curupira

### Ransomware family:

Black Bastia

### ATT&CK™ MATRIX

Collection	Credential Access	Defense Evasion	Execution	Discovery
Input Capture	Input Capture	Scripting Rundll32 Virtualization/ Sandbox Evasion Disable or Modify Tools	Scripting	System Information Discovery Virtualization/ Sandbox Evasion



## Immediate Threats: Most Successful Threats

Immediate Threat	Avg. Control Effectiveness	Targeted CVE	MITRE ATT&CK Tactics
Malware Dropped Through A Zpaq Archive	13%	N/A	Initial Access, Defense Evasion
CISA: Daixin Team	17%	N/A	Reconnaissance, Initial Access, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Lateral Movement, Exfiltration, Impact
ParaSiteSnatcher: How Malicious Chrome Extensions Target Brazil	29%	N/A	Execution, Persistence, Defense Evasion, Discovery, Command and Control,
Terminator antivirus killer: vulnerable Windows driver in disguise	30%	N/A	Execution, Defense Evasion, Discovery
Cert IL Alert: Iranian Muddy Water Phishing campaign	33%	N/A	Initial Access, Persistence, Privilege Escalation, Defense Evasion, Lateral Movement
Editbot Stealer Spreads Via Social Media Messages	34%	N/A	Initial Access, Execution, Persistence, Privilege Escalation, Discovery, Collection, Command and Control, Exfiltration
CISA: Snatch Ransomware	35%	N/A	Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Impact
ANSSI: APT28 Breaches French Critical Networks	36%	CVE-2023-38831 CVE-2023-23397 CVE-2022-30190 CVE-2020-12641 CVE-2020-35730 CVE-2021-44026	Initial Access, Persistence, Exfiltration
MS-SQL Servers Attacked With Proxyware	37%	N/A	Execution, Privilege Escalation, Defense Evasion
Malware: BiBi-Linux Wiper	37%	N/A	Initial Access, Persistence, Privilege Escalation, Defense Evasion, Discovery, Exfiltration, Impact

The average control effectiveness rate is calculated as the number payloads arrived divided by the number of payloads sent. This reported penetration rate is based on IoCs in the immediate threats module and not active code. Other BAS modules can highlight the effectiveness of behavioral detection and monitoring solutions in stopping executions in progress.

# The MITRE ATT&CK® Framework

Share a common language to streamline and enhance your organization's defenses.



Exposure management requires taking the attacker's view of your security posture, and the MITRE ATT&CK® framework helps visualize strengths, deficiencies and blind spots. The framework of tactics and techniques provides a common taxonomy and reference framework of the cyber attack kill-chain.

Cymulate assessments imitate MITRE ATT&CK tactics and techniques to simulate how real-world adversaries operate. By simulating these techniques, security teams gain insight into how attacks are structured so they can better protect their organizations. Additionally, because Cymulate aligns with industry standards it provides immediately interpretable results.

Within the MITRE ATT&CK framework, some techniques represent legitimate actions that can be part of normal user activity, which makes them difficult to detect as malicious without context or a pattern of behavior. These techniques further illustrate the nuanced challenge in cybersecurity: **Distinguishing between benign actions performed as part of normal operations and those same actions being leveraged for malicious purposes.** Effective security measures often rely on advanced detection tools, anomaly detection and understanding the context of each action within the broader scope of network behavior and user activity patterns.

## Most Difficult MITRE Techniques to Prevent

Technique	Tactic	Legitimate Use	Malicious Use
T1560 - Archive Collected Data	Collection	Users or applications may archive data for legitimate reasons, such as backup, organizational purposes, or to save space.	Attackers might archive data before exfiltration to reduce size and evade detection.
T1083 - File and Directory Discovery	Discovery	Users frequently search for files and directories for daily work or file management tasks.	Threat actors scan file systems to find sensitive files or data for exfiltration or further exploitation.
T1140 - Deobfuscate/Decode Files or Information	Defense Evasion	This process is commonly used in software development and data analysis to interpret encoded data or to make software more readable.	Malware often uses obfuscation to hide its code, which it then de-obfuscates during execution to evade antivirus detection.
T1537 - Transfer Data to Cloud Account	Exfiltration	Users and organizations use cloud services for data storage, sharing, and backup as part of normal operations.	Attackers may transfer stolen data to a cloud account they control as part of data exfiltration strategies.
T1071 - Application Layer Protocol	Command & Control	Protocols like HTTP, HTTPS, FTP, and SMTP are used legitimately by applications for communication over the internet.	Malware uses these common protocols to blend in with normal traffic while communicating with command & control servers or exfiltrating data.
T1059 - Command and Scripting Interpreter	Exfiltration	Scripting is a powerful tool for automation, configuration management, and software deployment within IT systems.	Attackers use scripting to execute malicious code, automate movements, and exploit vulnerabilities within the target environment.
T1036 - Masquerading	Defense Evasion	Renaming files and changing file extensions can be part of normal software installation, updates, or maintenance.	Malware may masquerade as legitimate files or applications to evade detection by users and security software.
T1113 - Screen Capture	Collection	Screen capture tools are used for creating tutorials, documenting issues, or capturing information for support purposes.	Threat actors use screen capture functionality to steal sensitive information displayed on the screen, such as login credentials or confidential documents.
T1016 - System Network Configuration Discovery	Discovery	IT professionals often query network configurations for troubleshooting, network setup, and maintenance purposes.	Attackers may gather network configuration information to understand the network topology, find valuable targets, or prepare for lateral movement.
T1057 - Process Discovery	Discovery	Administrators and users may monitor running processes for system management, performance monitoring, or troubleshooting issues.	Malware and attackers use process discovery to identify security mechanisms, find processes to inject into, or identify potential targets for exploitation.
T1082 - System Information Discovery	Discovery	Collecting system information is common for software diagnostics, compatibility checks, and ensuring appropriate updates or configurations are applied.	Attackers collect system information to tailor their attack strategies, identify vulnerabilities, and ensure their malware or tools will work effectively on the target system.
T1049 - System Network Connections Discovery	Discovery	Users and administrators check active network connections to monitor network activity, troubleshoot network problems, or ensure no unauthorized connections exist.	Adversaries examine active connections to map out internal network communications, identify communication between servers and devices, and plan for lateral movement or data exfiltration pathways.

# Control Validation

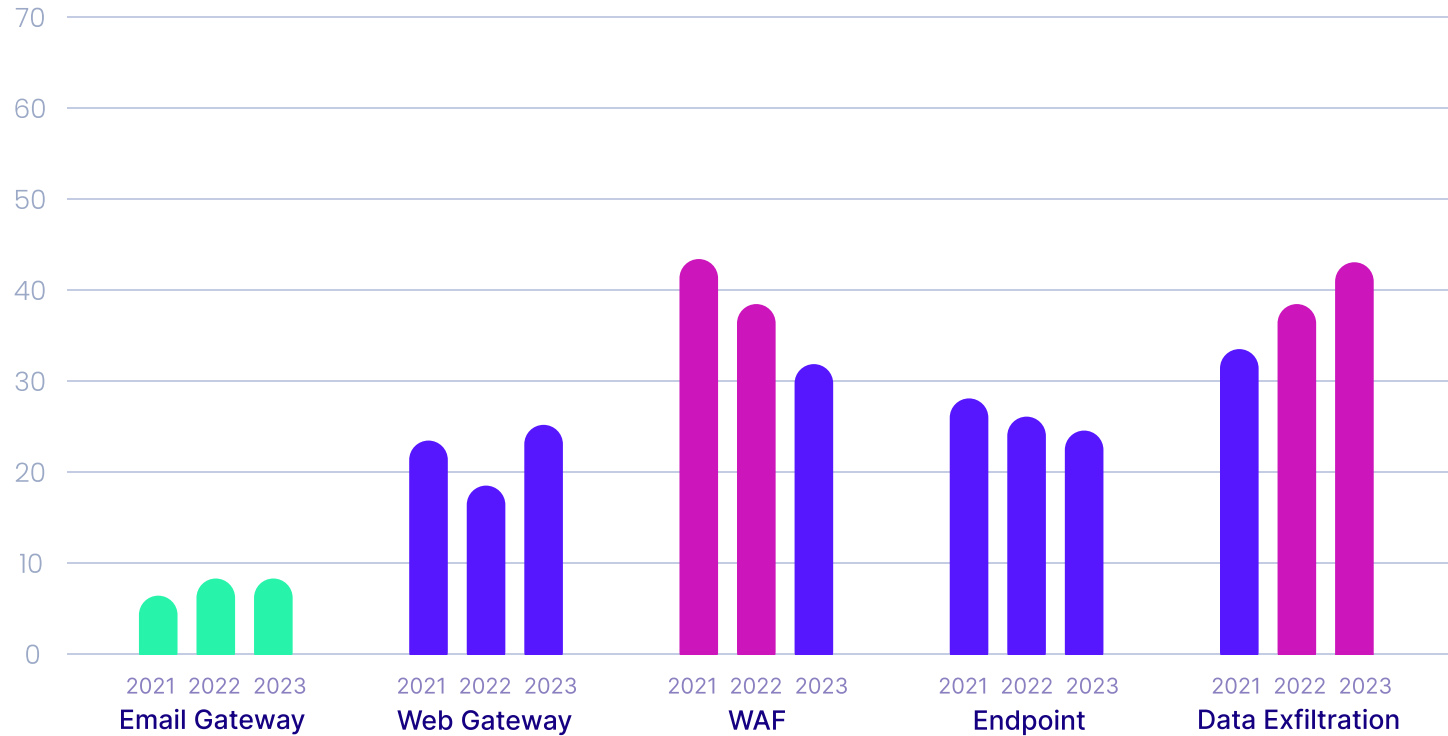
Exposure management takes a proactive approach to measure and improve security posture to cyber resilience.

Manual configuration of security controls is a time-consuming and error-prone process that fails to provide consistent protection. Designed to minimize security risks, security controls are often misconfigured, which prevents them from functioning as intended and might result in a misleading sense of security and in a proliferation of false positive alerts.

The Cymulate Platform safely and efficiently assesses the efficacy of security controls against threat activity across on-premises, cloud and hybrid environments. This leads to more targeted and effective tuning operations, true risk visibility and fewer false-negative alerts.

This report baselines control effectiveness by taking the average Cymulate score for organizations with breakdowns by geography, industry and organization size. The scores reported are a proprietary Cymulate methodology designed to measure control effectiveness and baseline security posture. The 0 to 100 scale considers industry standards, including the MITRE ATT&CK® Framework, NIST Special Publication 800-50 and other benchmarks.

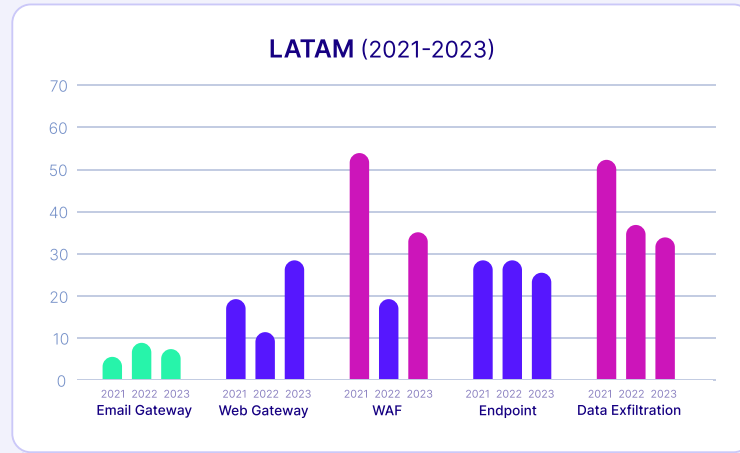
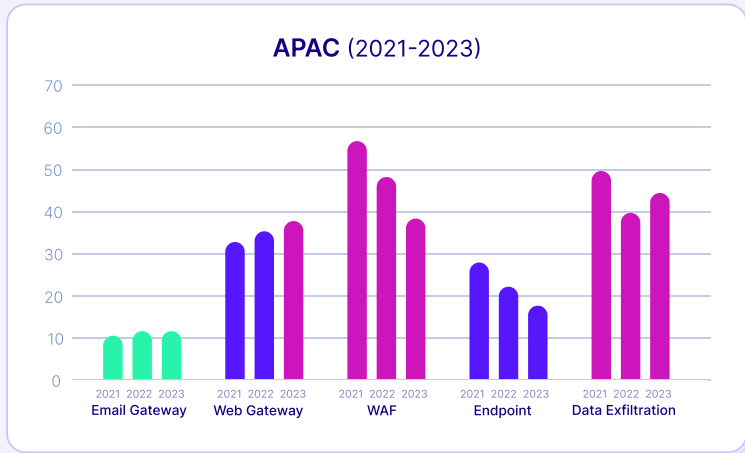
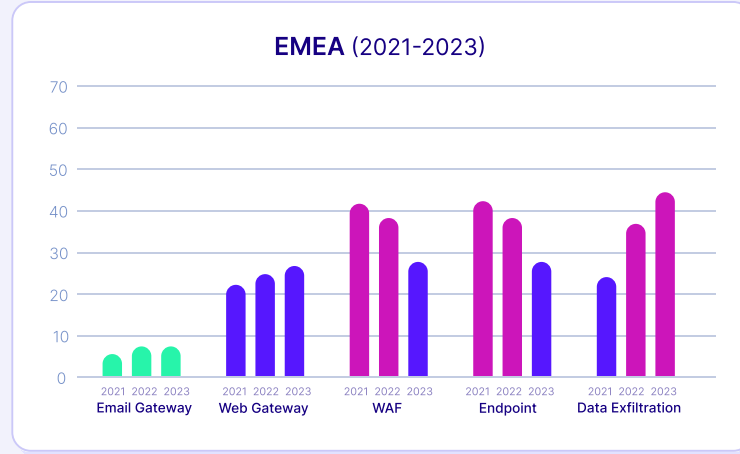
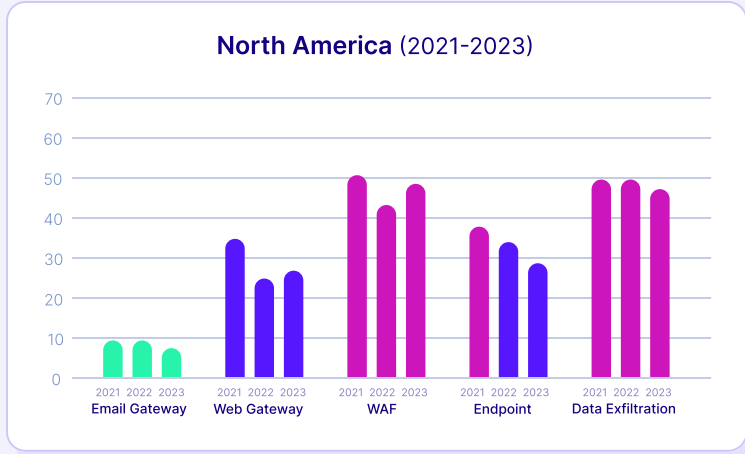
## Average Score per Control Over Time



- Secure
- Low risk
- Medium risk
- High risk

To measure control effectiveness and baseline security posture, Cymulate uses a proprietary 0 to 100 scoring method based on known industry standards, including the MITRE® ATT&CK® Framework, NIST Special Publication 800-50 and other benchmarks.

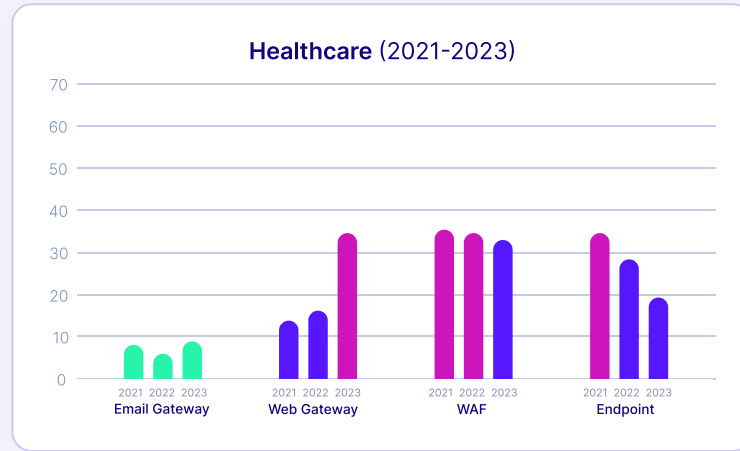
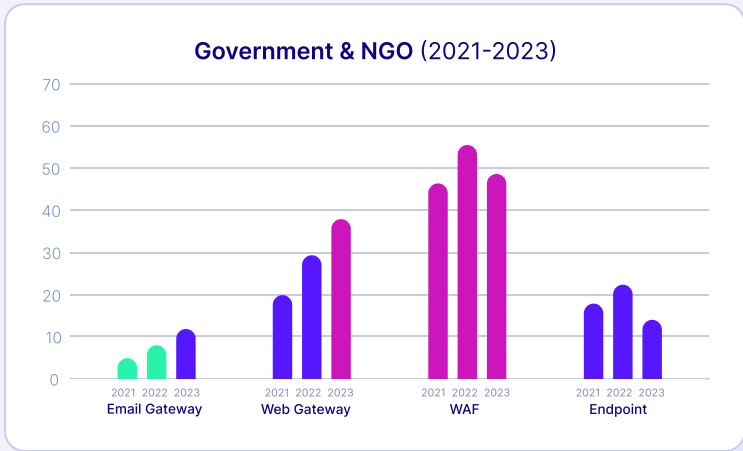
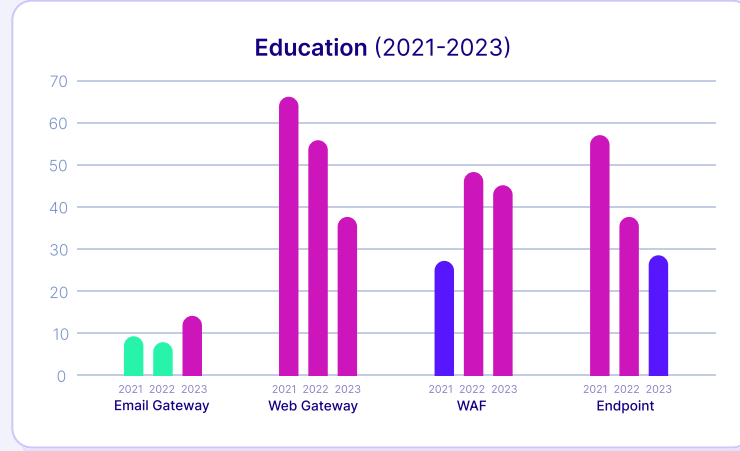
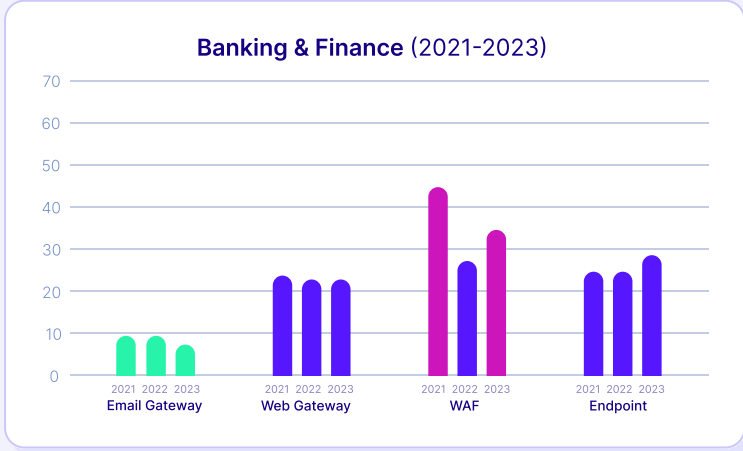
## Average Score per Control Over Time (Region)



- █ Secure
- █ Low risk
- █ Medium risk
- █ High risk

To measure control effectiveness and baseline security posture, Cymulate uses a proprietary 0 to 100 scoring method based on known industry standards, including the MITRE® ATT&CK® Framework, NIST Special Publication 800-50 and other benchmarks.

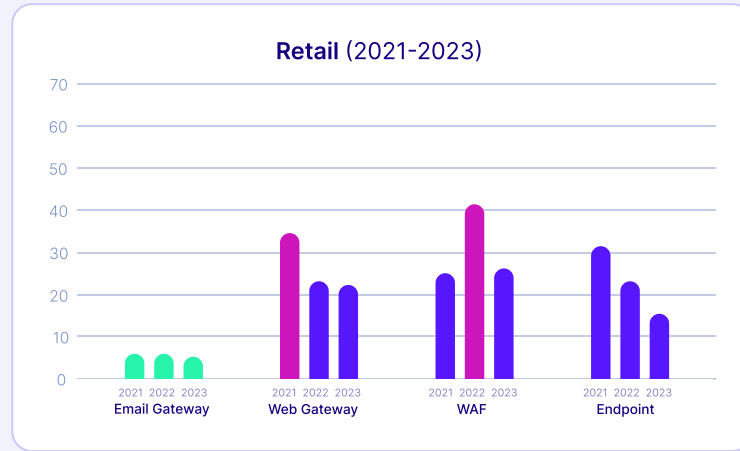
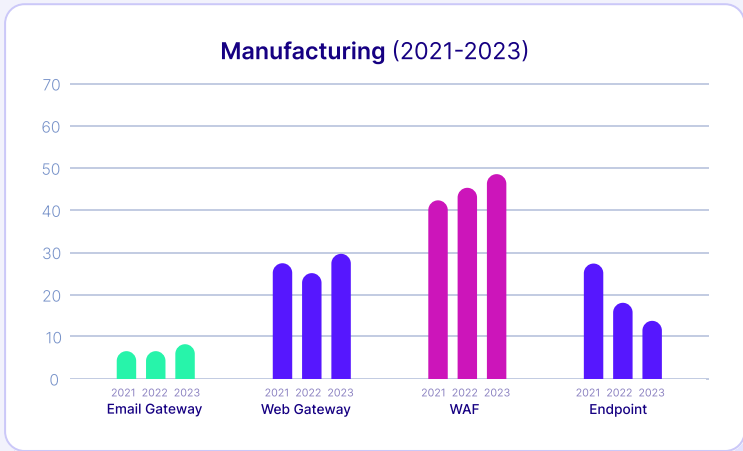
## Average Score per Control Over Time (Industry)



- Secure
- Low risk
- Medium risk
- High risk

To measure control effectiveness and baseline security posture, Cymulate uses a proprietary 0 to 100 scoring method based on known industry standards, including the MITRE® ATT&CK® Framework, NIST Special Publication 800-50, and other benchmarks.

## Average Score per Control Over Time (Industry)

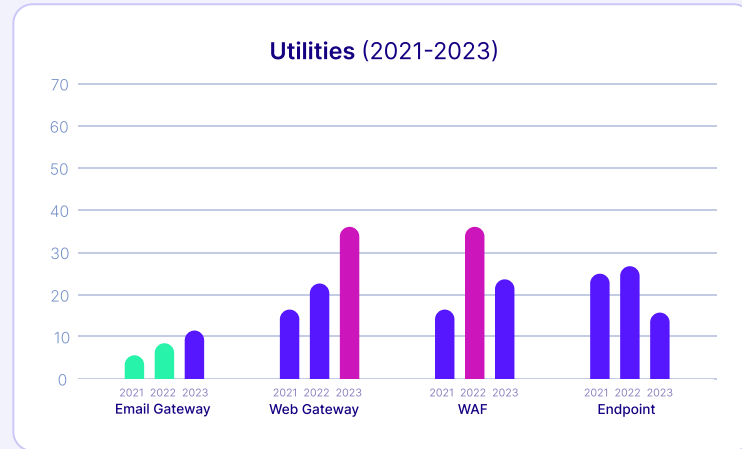
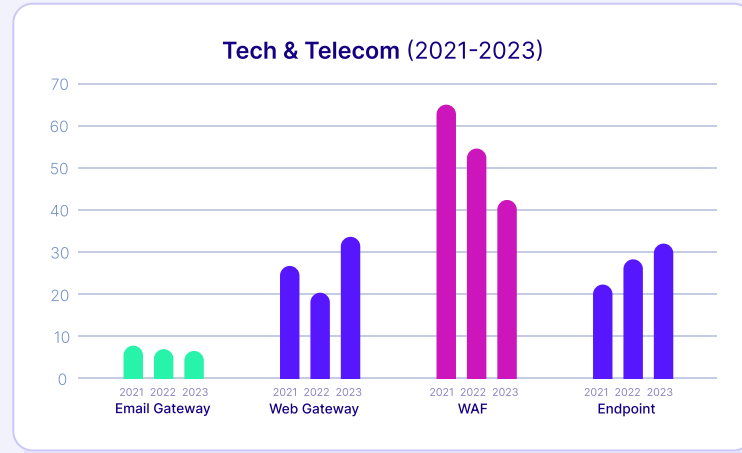


- Secure
- Low risk
- Medium risk
- High risk

To measure control effectiveness and baseline security posture, Cymulate uses a proprietary 0 to 100 scoring method based on known industry standards, including the MITRE® ATT&CK® Framework, NIST Special Publication 800-50 and other benchmarks.



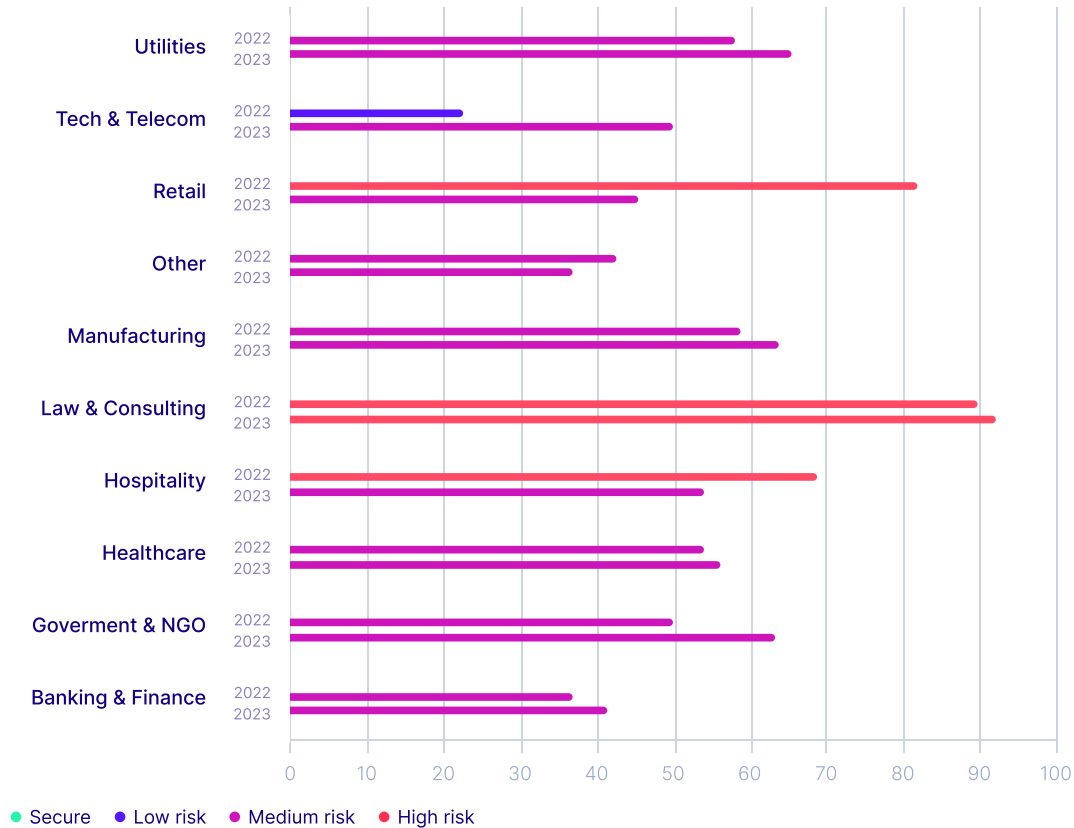
## Average Score per Control Over Time (Industry)



- Secure
- Low risk
- Medium risk
- High risk

To measure control effectiveness and baseline security posture, Cymulate uses a proprietary 0 to 100 scoring method based on known industry standards, including the MITRE® ATT&CK® Framework, NIST Special Publication 800-50 and other benchmarks.

## Average Data Exfiltration Score per Industry



Organizations face an increasing risk of data exfiltration with decreasing control effectiveness of their data loss prevention (DLP) controls. This increase in the data exfiltration risk for most organizations can be attributed to:

### Evolving threat landscape

Attackers constantly seek new means to circumvent traditional DLP, which often relies on predefined rules and pattern-matching.

### Increasing use of encryption

As encryption becomes the norm for legitimate traffic and data, attackers also use encryption to evade detection and blend into the environment.

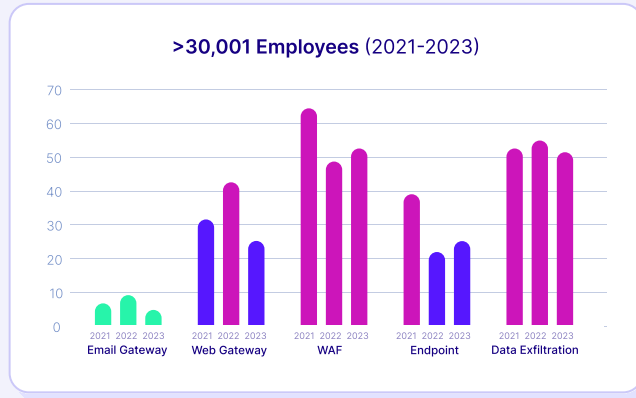
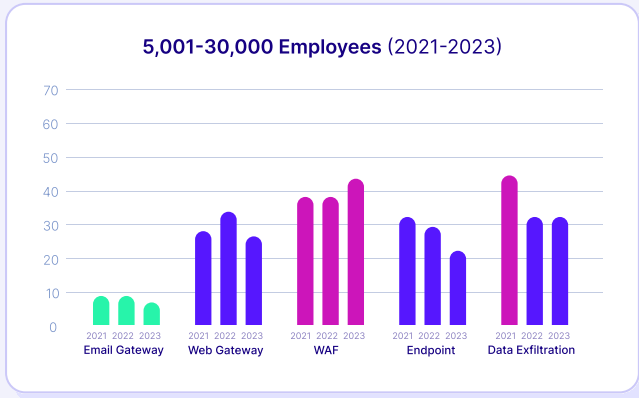
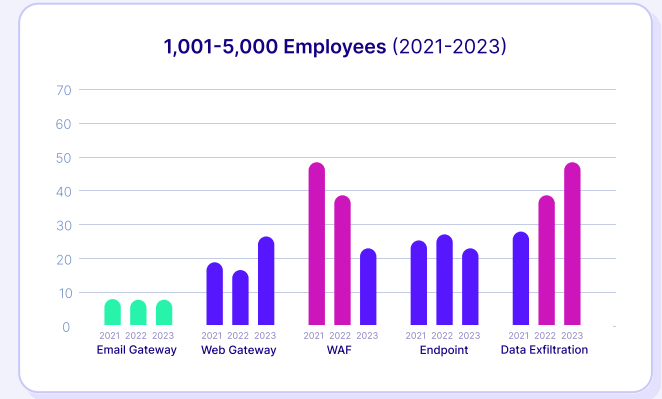
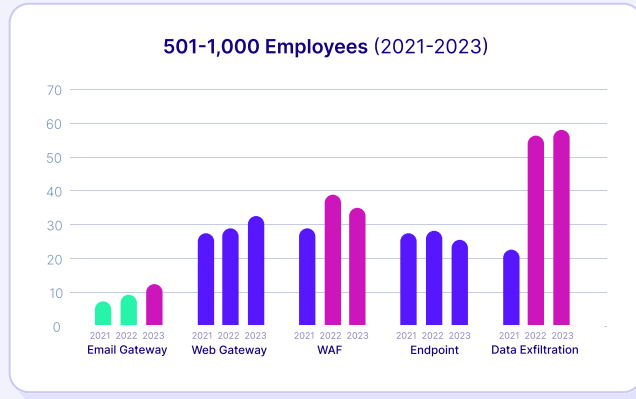
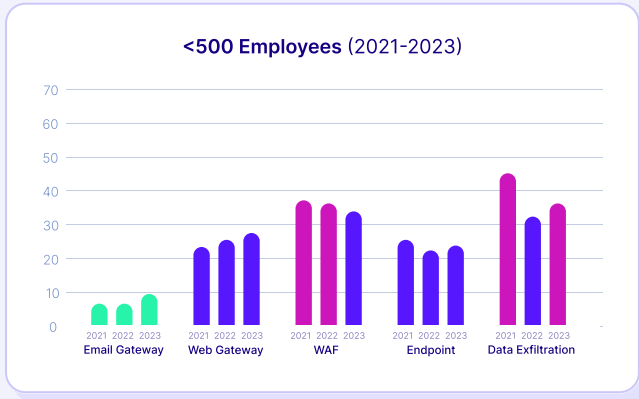
### Increasing volume and complexity of data

The exponential growth in the volume and complexity of data within organizations makes it challenging for DLP systems to monitor and protect all sensitive information effectively.

### Integration and compatibility issues

As organizations adopt new technologies and systems like cloud and SaaS, DLP controls are often an afterthought and traditional DLP may face issues integrating with the systems.

## Average Score per Control Over Time (Org Size)



- Secure
- Low risk
- Medium risk
- High risk

To measure control effectiveness and baseline security posture, Cymulate uses a proprietary 0 to 100 scoring method based on known industry standards, including the MITRE® ATT&CK® Framework, NIST Special Publication 800-50 and other benchmarks.

# Key Takeaways

## for Adopting Exposure Management

Exposure management includes critical steps to validate threats with offensive testing that measures cyber resilience to active threats.

This is the year to transform security operations with threat exposure management. For a practical implementation that delivers immediate value, Cymulate provides the following guidance and takeaways to drive measurable results.

### 01. Think like an attacker

Exposure management requires an external perspective to see the biggest weaknesses and apply effective remediation or mitigation. This isn't about passing your next audit. It's about preventing the next breach.

### 02. Add or expand automated validation

Validation is the key difference between exposure management and vulnerability management. Rather than rely on annual penetration tests, you need tools that automate offensive security testing for continuous assessments of controls, threats and attack paths.

### 03. Take incremental steps

Think evolution, not revolution. If you don't have any form of automated security validation today, add breach and attack simulation (BAS) for the immediate benefit of control and threat validation. If BAS is limited to blue teams, add attack path mapping to validated vulnerabilities and reported misconfigurations. If you have mature offensive testing, correlate results with vulnerability management to prioritize the validated exposures.

### 04. Focus on meaningful action

Exposure management should drive tangible improvements to cyber resilience – not lists and inventories for the sake of documentation. If you're spending more effort creating the optimal view of risk than working to prevent the next breach, reduce your scope and focus on specific applications, domains and functional areas that you know need attention.

### 05. Drive proactive security, not GRC

For measurable results, exposure management should remain a SecOps function separate from the tedious nature of governance, risk and compliance-driven functions. You can't ignore compliance, but don't let checklist-driven processes corrupt the passion of your security engineers, threat hunters and red teams to stay ahead of the next threat.

# Learn More About Cymulate



A Practical Guide to  
Exposure Management

[DOWNLOAD EBOOK](#)



Cymulate Named a Customer's  
Choice by Gartner® Peer  
Insights™ 2024 VOC

[READ BLOG](#)



Schedule a Demo  
Get a private demo to see the  
benefits for your organization

[REQUEST A DEMO](#)

## About Cymulate

Cymulate, the leader in exposure management and security 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 500 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](http://www.cymulate.com).

