Cymulate

Cymulate Research:

2022 STATE OF CYBERSECURITY EFFECTIVENESS

TABLE OF CONTENTS

01 METHODOLOGY & SOURCES

The reported results are based on the anonymized aggregated data of simulated attack scenarios and campaigns performed with the Cymulate Platform across a global user base. 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.

Cymulate Scoring Legend and Color Chart

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

The Cymulate Platform is comprised of a series of Modules, each focusing on an area of Cybersecurity Resilience and Security Posture Management. The total number of tests, campaigns, and scenarios analyzed for this report took place as over one million security posture validation assessments.

Continuous Automated Red-Teaming

- Phishing Awareness
- Full Kill Chain Campaigns
- Network Pen-Test

BAS Core

- Security Controls Validation: Email Gateway
- Immediate Threats Intelligence
- Security Controls Validation: Endpoint
- Security Controls Validation: Web Gateway

BAS Add-On Modules

- Attack-based Vulnerability Mgmt
- Security Controls Validation: WAF
- Full Kill Chain Scenarios
- Security Controls Validation: DLP
- Advanced Scenarios

Attack Surface Management

- Attack Surface Management
- Internal Attack Surface Management (VRT)

02 EXECUTIVE SUMMARY

Throughout 2022, Cymulate customers performed the equivalent of over 197 years of offensive cybersecurity testing within their production environments. This anonymized testing data was aggregated and summarized into a usage report that captures key insights into the state of overall cybersecurity resilience.

Key Findings include:

01 Known and cataloged industry-wide security issues remain unaddressed

A significant share of well-documented security weaknesses continue to be found during testing. Analysis found that 40% of the top 10 CVEs identified most by Vulnerability Management platforms were over two years old yet remain unpatched. These long-known vulnerabilities include issues such as unpatched CVEs and inadequately configured Identity and Access Management (IAM) and Privileged Access Management (PAM). Reliance on legacy infrastructure that no longer has upgrade/patch support requires organizations to leverage compensating security controls to offset this risk.

Common Examples: ProxyNotShell, Emotet
Why this is important to watch: Older threats may require upgrades and/or even migrations to mitigate, requiring budget and time allocation to address. Older threats still being actively used is an indicator that legacy and outdated platforms pose a direct risk to the overall resilience of the organization; and update/upgrade/replacement projects should be projected and begun as soon as possible.

02 Headlines Dictate Remediation Prioritization

There is a marked tendency among organizations to assess for immediate threats based on current levels of media attention, rather than actual risk level. This approach can lead to a misallocation of resources and a lack of focus on more pressing, but less widely covered threats.

Common Examples: businesses focus on AI-assisted polymorphic ransomware, as opposed to much more prevalent attacks such as the Clop Ransomware Threat Actor Group.
Why this is important to watch: While rapid-propagation and high-profile attacks should never be ignored, the loss of focus on less publicized attacks and methodologies can still lead to a breach and/or business disruptions. Organizations should mitigate based on threat and likelihood of attack, rather than media coverage. Continuous testing over time should also be factored in to offset increased attacker activity driven by attack kits being made available on the dark web.

03 The effectiveness of data protection measures is declining

The average data exfiltration risk score worsened considerably in 2022, jumping from 30 to 44, almost double its 2019 score of 23. The most egregious data exfiltration path was from cloud-service related assessments, which scored a dangerous 70 on average, followed by network protocols with not insignificant, medium-risk score of 43.

Common Examples: Blocking individual Cloud-based storage platforms (Box, Sync, etc.) – where new vendors come online constantly - as opposed to implementing Data Loss Prevention technologies.
Why this is important to watch: Network and Group Policies can definitely have a positive impact on prevention of data exfiltration; but threat actors know this and have begun relying on alternate exfiltration methods. Since platforms like AWS S3 and other Cloud storage systems cannot be blocked easily, they have become an exfiltration target of choice.

04 92% of the top 10 exposures are related to domain and email security

Analyzing the top 10 exposures detected through the External Attack Surface Management (EASM) module shows that the vast majority of detected exposures are spread across two main topics: web domain security (59.3%) and email security (32.8%). Such distinct correlation of detected issues across such a broad set of industries and organization sizes indicate that these issues will continue to be a problem for businesses throughout 2023.

Common Examples: Not implementing newer standards such as DNSSEC and SPF records, not strictly enforcing WAF requirements and/or TLS on all public-facing web resources.
Why this is important to watch: Unmanaged externally visible infrastructure (so-called ShadowIT) and a delay in implementation of newer standards are often difficult to detect with purely defensive analysis. Thinking like an attacker and simulating different techniques of attack (safely) is critical in finding these systems and gaps.

05 Breach and Attack Simulation has a significant positive impact on cyber resiliency

For example, when comparing the anonymized data between the first Endpoint Security assessment completed and the most recent assessments completed, there was a significant improvement in risk reduction over time when BAS testing was regularly performed. The improvements were seen consistently across customers of various industries and size.

- Windows Signature-Based (on-write/on-access) anti-virus scanning
  - Initial Average Risk Score: 95-100 – High Risk
  - Recent Average Risk Score: 38 – Moderate Risk
- Windows Behavioral-Based Detection (EDR/XDR) anti-malware defenses
  - Initial Average Score: 63 – Moderate Risk
  - Recent Average Score: 13 – Low Risk
- MacOS anti-malware defenses
  - Initial Average Score: 74 – High Risk
  - Recent Average Score: 55 – Moderate Risk
- Linux (multiple distributions) anti-malware defenses
  - Initial Average Score: 81 – High Risk
  - Recent Average Score: 51 – Moderate Risk

While the results for MacOS and Linux do still need improvement, the reduction in risk (26% and 24%, respectively) indicates a strong trend toward better anti-malware protection on these two sets of Operating Systems. In the case of Windows, the 79% decrease in risk scoring around behavioral based EDR/XDR solutions calls out both significant advances in the technology of these platforms and the impact of ongoing tuning and configuration efforts. It is notable that the scores for signature-based scanning on Windows, while still showing impressive improvement, did not keep pace with behavioral-based defenses. This is most likely due to signature-based detection being a secondary feature of EDR/XDR solutions, with less emphasis placed on that feature set. As market trends have indicated a mass-market shift to behavioral-based platforms for anti-malware, lower signature detection rates are not unexpected. It is a testament to the EDR/XDR vendors that over the course of the year, their signature-detection (often referred to as static analysis) has seen a 63% reduction in risk, even without directed tuning efforts within customer environments.

92%

TOP 10 EXPOSURES ARE RELATED TO DOMAIN AND EMAIL SECURITY

> ORGANIZATIONS ASSESS RESILIENCE TO IMMEDIATE THREATS BASED ON CURRENT LEVELS OF MEDIA ATTENTION, RATHER THAN ACTUAL RISK LEVEL.

Top Security Threats of 2022 and Year over Year Global Trending

For the purposes of this report, security threats are broken down into four major categories:

- Top Common Vulnerabilities and Exposures (CVEs), based on data gathered both by Cymulate and Vulnerability Management partner platforms
- Top Tactics, Techniques, and Processes (TTPs) according to the MITRE® ATT&CK® classification system
- Top exposures based on the weighted average of validated information from Cymulate Assessments
- Top immediate threats based on the weighted average of validated information from Cymulate Assessments

Top 10 Immediate Threats Simulated in 2022

Manjusaka: a cyber-attack framework of Chinese origin, likely created for criminal use, it includes Windows and Linux implants and a ready-made command and control server.

Powerless Backdoor: a cyber threat popular among Iranian hackers, designed to avoid detection by PowerShell, and can download a browser info stealer, keylogger, encrypt and decrypt data, execute arbitrary commands, and kill processes.

APT 41 targeting U.S. State Governments: a Chinese state-sponsored hacking group that has been targeting US state governments using various tools and techniques such as Acunetix, Nmap, and SQLmap, and attack methods like phishing, watering hole attacks, and supply-chain attacks.

Lazarus Phishing Attack on DoD Industry: a phishing campaign carried out by the North Korean hacking group Lazarus, targeting job applicants in the US defense sector with malicious documents containing macros.

Industroyer 2: An APT-style malware that specifically targets industrial control systems (ICS) and critical infrastructure. A spinoff of the 2016 attack on Ukraine power grid.

Spring4Shell: Exploiting the Spring Framework vulnerability (CVE-2022-22965), it allows for remote code execution without authentication.

Follina Office Attack: Weaponizing Microsoft vulnerability (CVE-2022-30190), it allows for remote code execution without authentication.

Ransomexx: A ransomware-as-a-service (RaaS) model, financially motivated and believed to be related to the sprite Spider ransomware group based in Russia.

Quantum Ransomware: One of the fastest cases of time-to-ransom ever observed with initial access to domain-wide ransomware in just 3 hours and 44 minutes. The initial access vector for this attack was an IcedID payload delivered via email.

Mikubot: A new variant of bot malware that is being offered for sale in threat actor forums, written in C++ and works on Windows operating systems from Vista to Windows 11. The malware is standalone and is being sold for $1300 for 1.5 months of access or $2200 for a three-month subscription.

Analysis: These 10 most tested immediate threats listed below show that the most concerning emerging threats — as evidenced by the test frequency — share a number of characteristics:

- Most of the attacks are state-sponsored or carried out by known hacking groups
- Most of the attacks use phishing, watering hole attacks, and supply-chain attacks as the primary method of compromise
- Some of the attacks use known tools like Cobalt Strike, Sliver framework, APT41, Nmap, SQLmap, and Acunetix
- All of the attacks have a clear motive, such as financial gain or espionage
- The attacks are sophisticated and evasive in nature, specifically designed to evade detection and remain persistent within the target network

Another characteristic of those top 10 threats is that they were abundantly reported about in specialized, and often mainstream, press. As the list is based on the number of times these assessments were run, rankings are unrelated to the actual risk level posed by the threat in question. When organizations rely on an emergent threat's relative fame to select which threats to assess; they take the risk of not testing for potentially far more damaging, but less famous, emerging threats.

An interesting finding is that more emergent threat can be tied to state-sponsored threat actor groups. This includes both intelligence agencies and other overt nation-state actors, in addition to otherwise unaffiliated threat actor groups known to receive financial and architectural backing from nation-state groups.

Top Ten Vulnerabilities Confirmed Present by Vulnerability Management Tools

The CVEs in the table below are the 10 most detected CVEs in 2022, aggregated from multiple Vulnerability Management tools in partnership with Cymulate. Many of the vulnerabilities are related to Microsoft products and have high severity CVSS (Common Vulnerability Scoring System) scores. While several are capable of performing code execution themselves, it is worth noting that they are most often used in conjunction with other CVE's and techniques to create more complex attacks.

Vulnerability	Approximate Number of Detections	Description
CVE-2022-30190	39,955	Microsoft Windows Support Diagnostic Tool (MSDT) remote code execution vulnerability. Used in Follina attacks.
CVE-2021-34527	31,743	A remote code execution (RCE) vulnerability that allows threat actors to remotely inject DLLs. Used in conjunction with CVE-2021-34527 in PrintNightmare attacks.
CVE-2013-3900	15,806	Uncovered in 2013, CVE-2013-3900 is a WinVerifyTrust signature validation vulnerability that allows remote attackers to execute arbitrary code via specially crafted portable executables by appending the malicious code snippet while still maintaining the validity of the file signature. Used in a ZLoader malware campaign in early 2022.

Vulnerability	Approximate Number of Detections	Description
CVE-2022-2190	12,721	Microsoft HTTP protocol stack remote code execution vulnerability
CVE-2021-1675	11,220	Allows an attacker with low access privileges to use a malicious DLL file to escalate privilege. Used in conjunction with CVE-2021-34527 in PrintNightmare Attacks.
CVE-2021-31956	10,960	Windows NTFS Elevation of Privilege Vulnerability
CVE-2018-0798	6,853	Allows a remote code execution vulnerability due to the way objects are handled in memory, aka "Microsoft Office Memory Corruption Vulnerability."
CVE-2018-0802	6,786	Allows a remote code execution vulnerability due to the way objects are handled in memory, aka "Microsoft Office Memory Corruption Vulnerability." May be used alone, or in conjunction with CVE-2018-0802
CVE-2017-11882	6,505	Allows an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability."
CVE-2022-3786	5,380	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects

Analysis: An interesting discovery is that many of these vulnerabilities revolve around memory handling. Typically taking the form of buffer overflow or memory alteration techniques. Exploits using these types of vulnerabilities have been a component in multiple high-profile attacks – such as PrintNightmare, Follina, and others. This indicates that organizations may be relying heavily on more traditional attack detection, leading threat actors to focus on these tactics to evade defenses.

40% of these top 10 CVEs were over two years old yet remain unpatched. There are several possible reasons for this; including an overwhelming patch backlog, patches that would require an upgrade to critical platforms, or unmanaged systems that are still online in production environments (ShadowIT).

Vulnerabilities remaining unpatched after significant time may also indicate the use of compensating security controls to render the vulnerability unexploitable. Cymulate customers routinely confirm the efficacy of those compensating controls to aid in guiding patch management toward the most critical vulnerabilities which cannot be compensated for. While such controls can provide a temporary defense, customers will often use these findings to justify additional budgets for upgrades or new security control purchases.

40%

OF THESE TOP 10 CVEs WERE OVER TWO YEARS OLD YET REMAIN UNPATCHED

Top Ten Tactics, Techniques, and Procedures (TTP's) Discovered in Assessments

TTP's – defined by MITRE – are methods used as a component of a threat action. Though some may be disruptive or destructive on their own, most will be combined with other TTP's to create an attack strategy.

Notably, It is typical for Cymulate customers to run out-of-the-box attack simulations across the entire MITRE ATT&CK framework. Successful attack simulation using the techniques below made it through the security controls of more than 90% of the organizations. Using automated testing for these and other techniques has shown the ability to manage risk and, in many cases, substantial risk reduction for customers. See Risk Scoring Trends section.

Mitre ID	Name	Number of Cymulate Assessments
T1189	Drive-by Compromise	1,274,179
T1560	Archive Collected Data	454,414
T1537	Transfer Data to Cloud Account	256,820
T1055	Process Injection	232,815
T1041	Exfiltration Over C2 Channel	195,321
T1053	Scheduled Task/Job	179,738
T1059	Command and Scripting Interpreter	177,217
T1082	System Information Discovery	173,931
T1056.004	Credential API Hooking	172,383
T1048	Exfiltration Over Alternative Protocol	166,658

> DRIVE-BY COMPROMISE ACCOUNTS FOR **39%** OF THE SECURITY ASSESSMENTS AND IS BY FAR THE ATTACK TECHNIQUE MOST ORGANIZATIONS ARE CONCERNED WITH

Analysis: Looking at the most frequently assessed TTPs highlights leading cybersecurity concerns:

01 Drive-by Compromise Attacks

With over 1.2 million tests, drive-by compromise attacks top the chart as a major concern. A drive-by compromise is when an attacker compromises legitimate websites to gain access to a user's system, using evasive techniques such as Legacy URL Reputation Evasion (LURE), obfuscated embedded JS files, and dynamic downloads via BLob or data uri.
Highly Evasive Adaptive Threats (HEATs) are increasingly using initial access techniques such as drive-by compromise to bypass secure web gateways and other filtering technologies.

As drive-by initiation systems are hosted outside the organization's infrastructure, traditional scanning methods may not detect them until they have already launched within a browser session. Many also leverage obfuscation techniques such as transmission encryption, which would not appear to be overtly malicious since they are used for legitimate web traffic in addition to attacks. This results in the need for robust web gateway (firewall, proxy, etc.) controls combined with behavioral-based detection endpoint defenses. Web gateway systems are capable of being updated regularly (in some cases hourly) with known attack URL's and IP addresses. While not every attack will be recognized due to techniques like encryption, endpoint defenses that can analyze behavior can separate normal user activity from inappropriate activities.

02 Data Exfiltration Attacks

Data exfiltration has become another dominating concern, especially for Cloud environments. Over 900,000 assessments showed three distinct TTPs that can be used for data exfiltration or misappropriation purposes—T1560 (Archive Collected Data), T1537 (Transfer Data to Cloud Account), and T1041 (Exfiltration Over C2 Channel). Multiple examples of these forms of attacks use a Command and Control (C2) "channel" of communication to also exfiltrate data obtained during the attack. C2 systems are often web services that – in addition to sending data and commands to malware on a user system – can also be used as a target for uploaded information, data, and other objects.

Data Loss Prevention (DLP) and Cloud Security Access Broker (CASB) solutions can mitigate the discovered issues; however, these types of systems are typically complex to implement without disrupting business operations. They also require ongoing tuning to remain effective against new forms of threat activity. Current commonly used solutions, such as blocking access to known Cloud storage providers and restriction of USB storage, are of limited – but important - value. Threat actors have shifted operations to use Cloud storage which cannot be blocked without disrupting legitimate operations (such as AWS S3) or unknown website storage to avoid these blocks. Adding DLP and CASB technology to existing techniques of domain and USB blocking can aid organizations attempting to stem the tide of data exfiltration.

47%

INSUFFICIENT WEBSITE PROTECTIONS

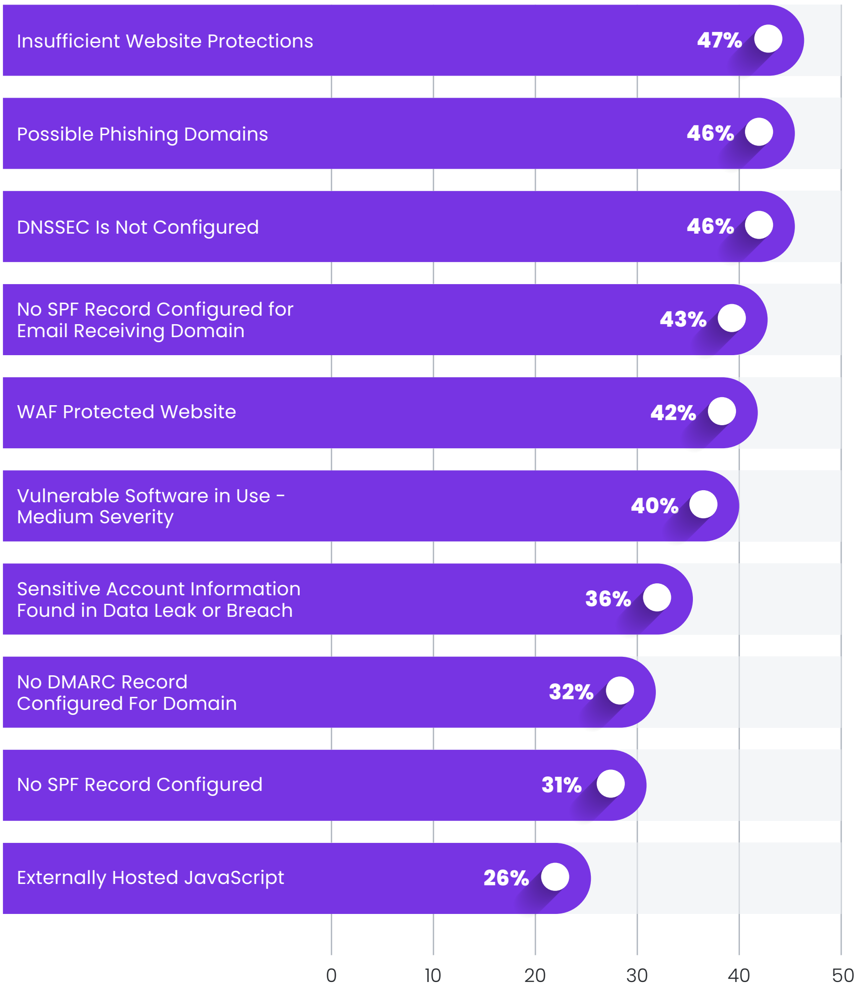
46%

POSSIBLE PHISHING DOMAINS

46%

DNSSEC IS NOT CONFIGURED

Top Ten External Exposure Types



Analysis: The Cymulate External Attack Surface Management (EASM) module discovered a variety of exposed digital assets that a potential adversary can take advantage of. The highest number of instances were DNSSEC (Domain Name System Security Extensions) not being configured, a lack of DMARC (Domain-based Message Authentication, Reporting & Conformance) record configuration, vulnerable software in use, possible phishing domains, insufficient website protections (e.g. not utilizing a WAF), sensitive account information found in data leaks or breaches, and a lack of SPF record configuration for email receiving domains.

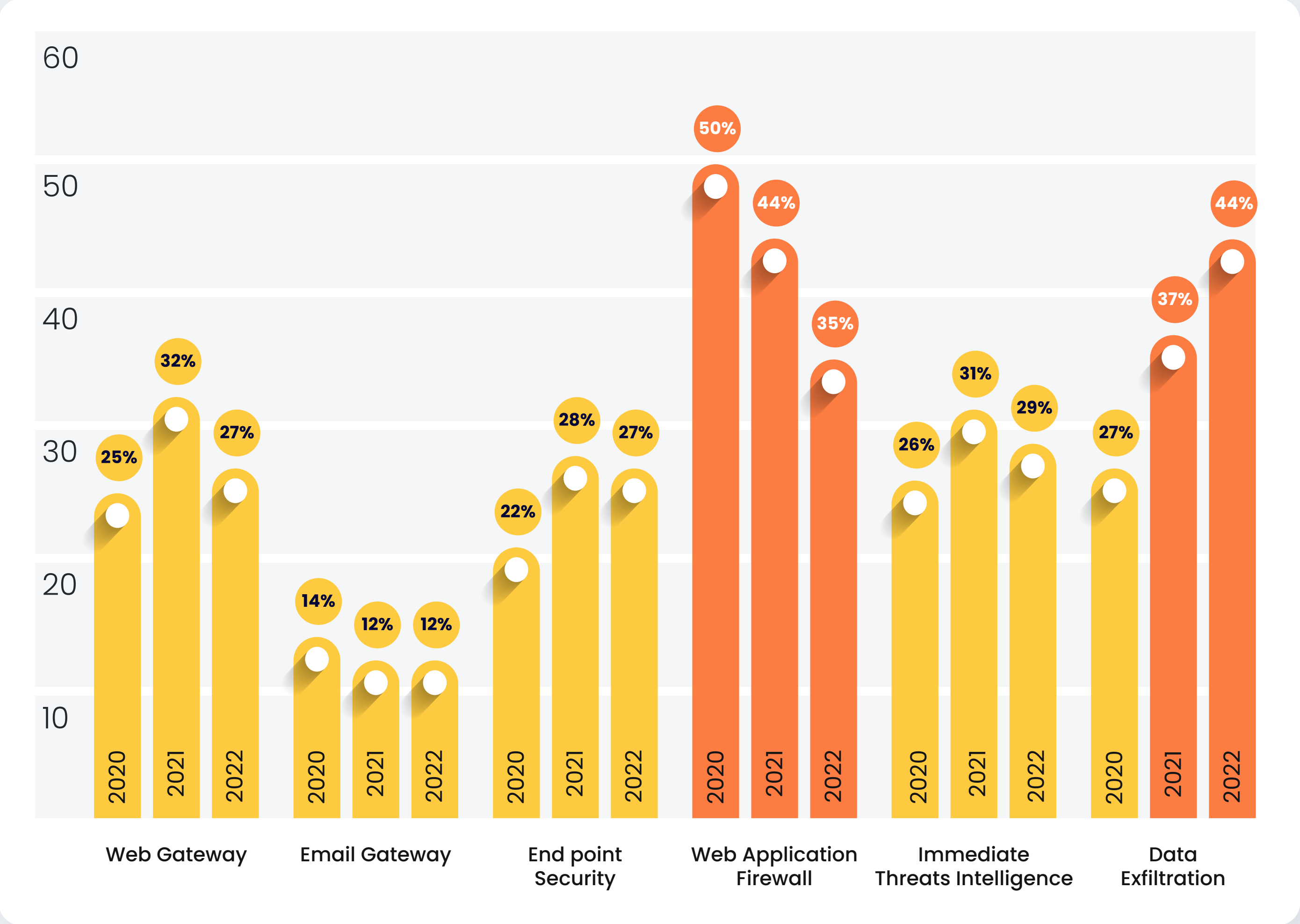
- DNSSEC is a security protocol that is used to protect the integrity of DNS data, by digitally signing DNS data to ensure that it has not been tampered with in transit or substituted with inaccurate responses. When DNSSEC is not configured, DNS information is left vulnerable. The two most common methods of using DNS as part of threat activity are cache poisoning and takeover. DNS cache poisoning is the action of attempting to respond to a legitimate DNS request with threat activity responses, thereby "poisoning" the local DNS cache and allowing a threat actor to consistently re-direct a user or application to a different target for a period of time. DNS takeover is an operation where a threat actor gains control of a legitimate DNS server/system and alters records to re-direct users requesting one resource to a different resource instead. These types of attacks can lead to data breaches, phishing attempts, and other malicious activities if not controlled, with DNSSEC being one method of imposing that control.

- Domain-based Message Authentication, Reporting, and Conformance (DMARC) - in combination with Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) records – allows the organization to dynamically deal with inbound email messages that do not comply with the organization's security processes and rules. DKIM permits validation that the email message was not compromised in-flight, while SPF allows an organization to specify which servers and IP addresses are permitted to send mail on that organization's behalf. If the sender of a message is using both controls, DMARC allows a receiver to validate the message or quarantine/block the message if it cannot be validated. While DKIM and SPF must be configured by the message sender, DMARC can be set up at the receiving mail server to prohibit delivery of non-DKIM/SPF enabled email sources. Though these methodologies for email security are not new (DKIM was introduced in 2011 and SPF in 2014), a large majority of organizations do not yet use these technologies, limiting the value of DMARC for receiving mail servers. Wider adoption of all three technologies can greatly enhance email validation checks and overall resilience.

40%

OF WEB DOMAIN SECURITY EXPOSURE COME FROM ABSENT OR FAULTY DNSSEC

Risk Scoring Trends from 2020 to 2022



Analysis: Cymulate allows for testing specific layers of security controls through its modular platform, trends can be determined within the layers of a defense-in-depth strategy. This has surfaced specific findings:

- Web Application Firewall (WAF) operations continue to trend toward lower overall risk over time. While the risk scoring is still higher than many organizations would prefer, operations to close gaps and further security around public-facing web architectures are improving.

- Defenses against data exfiltration have grown weaker over time. The most common reasons for this trend are that threat actors have switched to using services which are difficult – if not impossible – for organizations to block, such as AWS S3. This has reduced the effectiveness of network-level blocking and resulted in a net-increase in risk.

- The year-over-year trend for the Web Gateway, Email Gateway, Endpoint Security, and Immediate Threat Intelligence modules remains stable, with the Cymulate score trending toward the Low Risk classification, and Email Gateways trending toward minimal risk scores.

- As was first visualized in the 2021 Annual Report from Cymulate, the massive shift from office-based workforces to remote work saw a corresponding uptick in overall risk across most security controls when compared to 2020. Technology teams adjusted to managing the remote workforce and further defined and implemented new cybersecurity strategies to account for it. Overall risk scores began trending down near the end of 2021 and throughout 2022 with the exception of Data Exfiltration, as noted in the Expanded Analysis section below.

03 BREAKDOWN

The tables below reflect the average performance scores of cybersecurity posture in different industry sectors, regions, organization sizes, and security controls. These scores are established by Cymulate customers running active assessments against areas of their infrastructure and organization. The scoring system is based on multiple parameters, including CVSS (Common Vulnerability Scoring System), NIST (National Institute of Standards and Technology), and Microsoft DREAD (Damage, Reproducibility, Exploitability, Affected Users) frameworks in addition to the MITRE® ATT&CK® Frameworks. Scoring is ranked from 0-100, with lower scores indicating lower levels of risk.

Industry

Industey Sector/ Vector - Module	Web Gateway	Email Gateway	WAF	Endpoint Security	Immediate Threats	Data Exfiltrarion
Banking & Finance	23	12	28	23	24	35
Education	48	12	50	33	36	100
Government & NGO	29	11	58	27	37	51
Healthcare	18	6	37	27	29	53
Hospitality	34	13	51	27	36	82
Law & Consulting	37	16	38	31	38	67
Manufacturing	34	11	22	26	33	53
Retail	21	7	42	22	30	93
Tech & Telecom	27	11	54	31	58	51
Utilities	29	16	36	17	30	32
Global Weighted Average	27	12	35	27	29	44

Table 1: Average industry sectors risk scores for specific attack modules

Analysis: Data Exfiltration is by far the most successful technique able to bypass defenses. Financial and Utilities are the only sectors succeeding in keeping their Data Exfiltration risk score below 50. The second most underperforming security solution is WAF, where the top three verticals that perform best are Finance, Utility, and Manufacturing. With the notable exception of the Education sector, most verticals are showing overall cybersecurity resilience and improvement in multiple areas; though each has one or more areas of controls that would benefit from additional oversight.

Region

Region/ Vector - Module	Web Gateway	Email Gateway	WAF	Endpoint Security	Immediate Threats	Data Exfiltrarion
APAC	35	18	35	25	24	47
EMEA	25	12	35	25	28	42
LATAM	14	12	17	26	28	38
North America	35	10	42	37	40	49
Global Weighted Average	27	12	35	27	29	44

Table 2: Average regional risk scores for specific attack vectors

Analysis: North America tends toward higher levels of risk overall, with Latin America showing the lowest levels of risk. Each region exhibits both strengths and gaps, indicating that – while cybersecurity resilience is improving – there is significant room for improvement across the globe.

Organization Size

Oranization Size/ Vector - Module	Web Gateway	Email Gateway	WAF	Endpoint Security	Immediate Threats	Data Exfiltrarion
>500	29	11	37	22	28	61
501 - 1000	31	15	15	29	37	40
1000 - 5000	23	11	44	24	27	35
5000 - 30 000	37	13	40	38	23	47
>30 000	22	11	41	26	31	52
Global Weighted Average	27	12	35	27	29	44

Table 3: Average risk scores for specific attack vectors by organizations sizes

Analysis: Results are fairly comparable across all levels of organization size. This is most likely due to more smaller businesses leveraging the services of Managed Security Services Providers. An interesting finding is that the risk around Data Exfiltration is problematic regardless of the size of a given organization, primarily due to both the expense and complex implementation of DLP and CASB solution sets creating slower than expected adoption.

Security Controls

Vector - Module / Annual weighted avarage risk score	2019	2020	2021	2022
Web Gateway	19	34	31	27
Email Gateway	32	34	12	12
Web Application Firewall	36	40	41	35
Endpoint Security	17	21	21	27
Immediate Threats	31	31	32	29
Data Exfiltration	23	31	30	44

Table 4: Average yearly risk scores for specific attack vectors

Analysis: Looking at the trends over the last four years of data, Data Exfiltration is – as expected from the other data in this report – trending toward higher levels of risk. Endpoint security has also exhibited a slight but still significant uptick in overall risk from the previous year; most likely caused by a sharp and severe uptick in "double-extortion" ransomware with exfiltration. Other layers of security controls either show a decrease in overall risk, or remained the same as the previous year.

The overall indications are that organizations are focusing more on security control sets and policies within applications and domains. With additional focus on data control and upkeep/tuning of endpoint defense solutions, risk could be universally decreasing over the next year.

Additional Extended Analysis: Data Exfiltration and WAF

Two areas of security controls – those around reducing data exfiltration, and the operation of Web Application Firewalls – saw an increase in overall risk over the course of 2022. As each of the other layers of controls saw some measure of decrease in risk, Cymulate further analyzed the available information to gain additional insight into these two areas of security controls.

Extended Analysis: Data Exfiltration Concerns

Data Loss Prevention continuous assessment results were almost uniformly poor, and considerably worsening this year over last. Even in the best-performing organizations, risk scores rarely dipped below 40 – indicating moderate risk overall. This trend warrants additional review, with an eye to the following major sources of risk:

Cloud Services

The average Cymulate score for data exfiltration over cloud services was 70 indicating the high risk. This indicates that several areas of data control are not well-defended:

- **Exfiltration by Collaboration Applications:**
  Data (files and text) is sent over Slack, Teams, and other collaboration tools; which can evade detection by many security tools as the activity appears to be legitimate business operations.

- **Exfiltration by Upload to Cloud Storage:**
  Data is sent to cloud storage services (AWS S3, Google Drive, etc.), which can evade detection by many security tools which would see generic web traffic; especially if exfiltrated via API calls.

- **Exfiltration via Code Repository:**
  Data is sent to code repository services (such as GitHub). Security controls not tuned to recognize code sets may not classify it as proprietary or confidential data.

In all three situations, networking controls may not provide sufficient defense against exfiltration. As blocking of Cloud Storage providers like AWS S3 would result in significant business disruption, meaning it is difficult if not impossible to entirely block communication. Collaboration services have become critical infrastructure with organizations due to more and more remote employees, and therefore cannot be blocked. Code repository traffic is mandatory for all organizations who build applications - either for internal purposes or as a product – and therefore connectivity to GitHub and other repository services must be permitted.

DLP and CASB solutions, specifically configured to see and analyze these avenues of data movement, can provide more complete and accurate data protection than network and firewall blocks can hope to achieve. An SSL-Decryption Proxy is also recommended, in order to decode TLS-encrypted traffic to API's and Cloud storage vendors in order to curtail evasion.

Network protocols

The removal of sensitive data to websites, servers, and services is a significant contributor to data loss. The most commonly used network exfiltration methods are:

- **Telnet exfiltration:** a protocol for remote login, which can also transmit data.
- **SFTP exfiltration:** a secure file transfer protocol.
- **DNS exfiltration:** Domain Name Services, used to identify the location of resources on the Internet and internally.
- **DNS Tunneling:** : leveraging DNS protocols to create a tunnel for the transmission of information.
- **ICMP Tunneling:** ICMP is a protocol for identifying if another system is responding to requests, but can also allow for data transmission.
- **Browser HTTP and Browser HTTPS exfiltration:** transmission of data to a web server or service using an interface/object within a web browser.
- **HTTP and HTTPS exfiltration:** transmission of data to a website/server without the use of a browser.
- **Open Ports Exfiltration:** data can be transferred to another site, device, storage platform, etc. over non-standard ports that may be open on a firewall.

Some services, such as SFTP, telnet, and ICMP can be blocked by organizations if not required for business operations, which would limit the potential for using those services to exfiltrate data as well. Proxy solutions can be used to block the ability to upload data via HTTP and HTTPS – with or without the use of a browser. Open ports which are not required by the applications and tools used by the organization can also be blocked by closing said ports at the firewall and/or VPN. While these techniques are viable, this still leaves techniques like exfiltration by DNS and DNS tunneling (along with any necessary services that are required by business operations) available to threat actors. Data Loss Prevention technology, combined with SSL-decryption proxy systems and firewalls, are the best way to restrict exfiltration via network protocols that must remain available.

Email

Email is a popular method for the exfiltration of small but targeted amounts of data that is considered sensitive, proprietary, confidential, or otherwise high-risk for the organization. There are several methods used for the exfiltration of data via email:

- Purposeful attachment-based email exfiltration occurs when a user specifically attaches a sensitive file to an email message destined for a recipient outside of the organization.
- Accidental attachment-based email exfiltration occurs when a user mistakenly sends an email with a sensitive file attached to a recipient outside of the organization or otherwise to a recipient that was not intended to receive it.
- Exfiltration by email body can take the form of copying and pasting text and images that are considered sensitive into the main body of the email itself; and can also refer to embedding the sensitive data into the body of the email as code such as javascript "comments."
- Encryption can also be used to evade detection by encrypting the sensitive data or the entire email before transmission – reducing the chances that filtration systems will be able to recognize the controlled data in an encrypted form.

Encryption of email can be strictly controlled by the organization – for example, by only permitting the transmission of encrypted email if the organizationally-approved methods for encryption are utilized. By rejecting any other form of encryption in the email and/or its attachments, organizations can ensure that all mail is filtered and examined before transmission. Purposeful and accidental transmission of attachments can be controlled by leveraging Cloud Access Security Broker (CASB) techniques and native and 3rd-party filtration tools to limit what types of attachments may be sent by any given user. While these can be complex to configure, they are a proven method of limiting exfiltration by attachments in email. Tools are available, and are being continuously enhanced, to examine the body of an email to detect inappropriate information being transmitted as text, embedded images, and embedded code. This area of data loss prevention is evolving over time, as better Artificial Intelligence and Machine Learning tools are created to parse the language of an outbound email in order to properly identify valid versus inappropriate text and images. Specifically blocking the ability to transmit embedded code within the body of an email is a valid method to limit risk in this area as well, but care should be taken to avoid disrupting business processes that require certain scripting and other code within email.

Physical

The removal of sensitive data via physical devices is an issue that has been a concern of organizations for decades. From the earliest removable floppy disks to the current generation of flash drives and removable storage, different techniques have been used to leverage physical media to exfiltrate information:

- The theft of physical hard drives from laptops and other portable infrastructure remains a concern, though less common by far as other methods of data theft are significantly easier to carry out. Encryption of all hard drives (magnetic and solid-state), rendering the data useless without proper authorization, will provide additional defense in the event the physical media is stolen.
- Removable storage devices are a more pressing concern. USB ports regularly need to be available and as such the act of physically disabling (blocking) such ports is of limited use due to the disruptive impact on business operations. Restriction of the types of devices that may be connected offers more defensive coverage and can be performed by implementing Group Policy Objects and through other administrative means. It should be noted that many devices exist that identify themselves as Human Interface Devices (HID) and other non-storage devices; but have the ability to store data in some form. This means that other data exfiltration defensive controls, such as Data Loss Prevention systems, still have a vital role in this form of data security.
- There is good news in this area over the course of 2022. While overall risk is still higher than desired, There is good news in this area over the course of 2022. While overall risk is still higher than desired, organizations performing assessments over time with Cymulate have shown clear gains in reducing their overall risk of data exfiltration events via physical media/removable storage.

Extended Analysis: Web Application Firewall

Web Application Firewalls (WAF) are utilized to reduce the ability of a threat actor to coerce a website or service into performing operations that should not be accessible to site/service users. Organizations have, over the course of 2022, made strides in closing gaps that can be addressed by WAF operations; either through implementation and tuning of physical and virtual WAF appliances and/or hardening website and service components and policies. Even with these gains, however, the overall level of risk seen across the anonymized dataset was consistently in the Moderate- to High-Threat range. Threat activities that can be blocked by WAF or WAF-like defenses take many forms, each with different levels of impact to the site or service in question, and to the organization as a whole:

Command Injection and SQL Injection

A command injection is an attack which seeks to execute arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user-supplied data (forms, cookies, HTTP headers, etc.) to the underlying website or web server systems. Used as part of a larger attack, command injection allows a threat actor to run other commands and actions with the privileges of the compromised application.

SQL injection targets data-driven applications by inserting malicious SQL statements into an entry field for execution. Such attacks can be used to spoof identity, tamper with existing data, cause repudiation issues such as changing balances, allow the exposure and theft of data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database system to perform further attack actions.

Command and SQL injection attacks are by no means new, in fact they have been identified on the Open Worldwide Application Security Project® (OWASP) Top Ten list for nearly two decades, with the first OWASP Top 10 in 2003 noting “Injection Flaws” as a point of concern. Organizations regularly and diligently work to reduce the potential for injection attacks to be successful, but several factors limit the ability to mitigate completely:

- The proliferation of open-source libraries in 3rd-party products used by the organization poses a significant challenge. As the list of libraries used in any given product may not be publicly visible or easily obtained from the vendor, ensuring that none of the libraries are susceptible to injection attacks remains problematic even in cases where good or excellent relationships with the vendor exist.
- As public-facing resources, websites and web applications are also highly visible and scannable by threat actors. This leads to issues with these platforms being easily identified by threat actors to use for the targeting of attacks.
- In extreme cases – such as the ProxyShell-type attacks which leveraged a form of command injection against Microsoft Exchange servers – the system in question must be visible to the Internet, cannot be patched without upgrading or migrating the platform, and relies on a vulnerable component to function properly.

In all three of these cases, the best defenses include a Web Application Firewall which refuses to pass any known command or SQL injection requests to the web server and/or database. It should be noted that in cases such as ProxyShell, additional controls must also be brought to bear, but strong WAF solutions that are kept tuned and updated are a valuable and powerful first line of defense. The higher risk scoring in comparison to other security controls is an indication that WAF solutions may not be undergoing regular updates and tuning operations, allowing newer attack requests to pass through the WAF and reach the website and database systems.
In addition, the Cymulate External Attack Surface Management data indicated that a significant portion of organizations have at least some websites and services that are not defended by a WAF, while the “main line” sites do benefit from that form of protection. There are two common reasons for this:

- Sites and services that are considered non-essential, or are used as development platforms, are not placed behind WAF systems in an effort to reduce budget and/or to provide easier access.
- ShadowIT services and systems are in active use but are not managed by the IT group of the organization, therefore they are not placed behind a WAF system.

In both of these situations, the recommended course of action is to place these public-facing systems – once identified – behind a WAF or prohibit them from being visible to the greater Internet.

Server-Side Request Forgery

Simply stated, a Server-Side Request Forgery (SSRF) attack is the act of a threat-actor coercing a public-facing system into performing an unauthorized action on a non-public-facing system. In doing so, an attacker could obtain data, change settings, or disrupt systems that would normally not be visible or exposed directly to the Internet. Because SSRF attacks could perform Remote Code Execution (RCE) operations, these attacks are extremely dangerous and create significant risk in an organization. What differentiates between command injection and an SSRF attack is the request sent to the server. In command injection, the goal is to perform an operation on the web server/system itself. In SSRF, the goal is to trick the web server/system into performing an operation on some other system – masking the threat actor by having the action appear to be performed by the web server/system itself.

Common examples range from gaining access to internal data for the purpose of exfiltration, establishing a "foothold" within the internal network for further incursion efforts, or altering and/or destroying data to create reputation damage, business disruptions, or simply sow chaos.

As more applications are migrated to Cloud platforms (but retaining access to internal systems), the risks posed by SSRF become more and more relevant to organizations of all sizes.

Well-tuned WAF solutions can be configured to reject all known SSRF requests, to prevent them from passing through to the web server/service, and therefore preventing that server/service from being coerced into initiating a process on anything else in the organization. When combined with networking controls, endpoint defenses, and strict policies and procedures; the risk of a successful SSRF being performed is dramatically reduced.

Throughout 2022, the average risk score around SSRF defenses did decrease, but remained in the Moderate- to High-Risk range. More frequent updates and tuning of WAF solutions, along with ensuring that all public-facing systems reside behind the protection of that WAF, are the most impactful defensive measures. This does not remove the need for other security controls, but greatly helps to ensure that such attacks are more likely to fail.

> “WEB APPLICATION PROTECTION EFFICACY IS LOWER IN NORTH AMERICA & AMONG MEDIUM SIZE BUSINESSES, VALIDATIONS SCORES SHOW”

04 SUMMARY AND RECOMENDATIONS

Usage data from Cymulate users indicates that risk reduction progress is steadily occurring year-over-year. As seen with EDR risk score reductions and with the year-on-year overall trend of risk reduction in other areas of cybersecurity resilience, organizations continue to make strides in reducing risk even while economic and global conditions remain challenging. While some areas still require more oversight, such as WAF management and DLP, the overall trend continues to be a lowering of overall risk. Data security remains a significant area of concern with data loss prevention techniques suffering a third annual increase in overall risk.

With the sole exception of the Education sector, organizations of all sizes and verticals saw the same trends of lowered overall risk. 2022 saw significant targeting of Educational organizations, and success in attacking them.

When looking at the aggregated data throughout the user base, Cymulate recommends the following five best practices to heighten security posture resilience in 2023:

01 Increase awareness among employees that phishing attacks have become more advanced and complex, and continually strengthen technological defenses

Attacks through email are not the only vector that cybercriminals are using for phishing attacks. 2022 saw many advancements in phishing attacks through text, voice messaging, phone scams, messaging apps, QR codes, and business application suites. In addition, the advent of freely available and extremely proficient Artificial Intelligence services has allowed threat actors to create frighteningly accurate phishing templates to use against individuals and corporations. Organizations should focus on reinforcing employee awareness across devices; and explain techniques gaining in popularity with threat actors. In addition to more focused training for users, organizations should continuously evaluate the effectiveness of technological controls against phishing and other communication attacks; remediating and tuning where necessary on a regular basis. Bolstering anti-phishing/anti-malspam capabilities such as sandboxing and restricting what devices can access corporate resources should also be an area of increased focus.

02 Impose MFA, include a token or biometric-based ID verification

Multi-Factor Authentication – though it has been available for more than two decades – continues to see slow adoption in the corporate sphere. Part of the resistance to MFA is so called “notification fatigue,” where users see so many requests for one-time passcodes and prompts for authentication that they either push back against more systems using MFA or mindlessly approve any request without considering the possibility of fraud. Both can be satisfied by taking advantage of tools which incorporate biometric factors and leverage Single Sign-On (SSO) technologies. Biometrics both reduce the number of actions that must be taken, and cause users to be more conscious of authentication actions that are still required. Biometrics are also harder to bypass by obfuscation, which is an added benefit. SSO technologies reduce the number of times a user will be challenged for a token, fingerprint, or other factor; with the result again being few actions per day, and more focus on each action that does have to be taken.

03 Adopt solutions to assist handling elevated accounts and reduce the risk of credential abuse

2022 saw a significant rise in the number of direct attacks on organizations' identity stores and IT administration platforms. Additionally, attackers became more skilled at compromising power user accounts when poor identity management or other factors such as a shift to a remote workforce left these critical accounts vulnerable to compromise. The Verizon DBIR 20022 also draws attention to use of stolen credentials to attack web exposed attack surfaces. Addressing these issues entails securing the handling of secrets and elevated account privileges. The use of Privileged Account Management (PAM) and other Identity and Access Management (IAM) solutions can greatly aid in both the management of these secrets and in their control. Of particular note are solutions that combine IAM with provisioning and deprovisioning systems, ensuring that accounts no longer needed are effectively and quickly removed from the system automatically.

04 Unmanaged infrastructure is ubiquitous, and incurs significant risk

Unmanaged infrastructure – also called "ShadowIT" – occurs in nearly every organization. From a business unit contracting with a service provider outside the purview of the IT team, to technologically inclined users setting up their own VPN systems; every organization has at least some. While it may not be practical to eliminate ShadowIT from being created, regular scanning and assessments to detect it are a must. Once identified, decisions can be made on either removing it or managing it to control overall risk.

05 Improving data protection should be a top priority

Over the last several years, there has been a considerable rise in the number of successful "double-extortion" ransomware attacks. These are attacks where the threat actor not only encrypts organizational data, but also steals a copy and removes it to an external data system. If the organization refuses to pay the ransom, not only does the data remain encrypted, but the threat actor threatens to make the stolen copies public. This can result in consequences from reputational damage, to embarrassment of clients, customers, and executives, to regulatory fines and other repercussions. While the primary focus of security efforts is – and should remain – controlling the ability of a threat actor to successfully execute the attack in the first place, exposure management must become a key component of cybersecurity resilience. If the attack is executed, then restricting the ability of the attacker to exfiltrate the data becomes the primary method of defense for the organization. Data Loss Prevention solutions, along with Cloud Access Security Broker platforms, become an extremely critical line of defense.

01 INCREASE EMPLOYEE AWARENESS

02 GET BACK TO BASIC HYGIENE

03 CONTROL IDENTITIES

04 DISCOVER EXPOSURES IN ADVANCE

05 MONITOR THE PATHS TO SENSITIVE DATA

05 ABOUT CYMULATE

The Cymulate exposure management and cybersecurity control validation platform delivers a comprehensive and scalable solution for reducing vulnerabilities and communicating risk levels between technical teams and business leadership. Executives receive consumable reports that benchmark control efficacy and exposure to immediate threats. Security professionals gain the ability to continuously challenge, validate, and optimize their on-premises and cloud cyber-security posture. Attack-based vulnerability management, full attack kill-chain testing, and end-to-end visualization across MITRE ATT&CK® and NIST frameworks are displayed in intuitive dashboards and within contextual reports. Over 120,000 automated and threat intelligence-led risk assessments are simple to deploy, while being relevant to organizations of all cybersecurity maturity levels. An open framework makes generating unique and automating tailored penetration scenarios and advanced attack campaigns easy for red and purple teaming exercises.

For more information, demo, or free trial visit www.cymulate.com.