Coalition®

GENERATED ON JUNE 1, 2021

Risk Assessment

PREPARED FOR

Acme

coalitioninc.com

Coalition is the leading provider of cyber insurance and security, harnessing the power of technology and safety of insurance to help organizations solve cyber risk. This Coalition Risk Assessment is the first step in this continuous monitoring process. Using externally observable data, this report provides an objective, evidence-based assessment of your cyber risk and overall security preparedness. As your dedicated risk management partner, our security team is available to provide additional context and help you to implement security and loss controls. Coalition policyholders receive 24/7 continuous security monitoring, all at no additional cost.

Sections

1 Executive Summary
2 Loss Costs & Benchmarking
3 Email Security
4 Vulnerabilities
5 IP and Domain Reputation
6 Malware
7 DNS
8 Sensitive Information Exposed
9 User Behavior

What is Cyber Insurance?
Coalition Features
FAQs
Glossary

This assessment is provided for informational purposes only. Risk-related analyses and statements in this assessment are statements of opinion of possible risks to entities as of the date they are expressed, and not statements of current or historical fact as to the security of any entity. YOUR USE OF THIS ASSESSMENT IS AT YOUR OWN DISCRETION AND RISK. THE ASSESSMENT IS PROVIDED ON AN “AS IS” AND “AS AVAILABLE” BASIS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, COALITION EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. COALITION DOES NOT WARRANT THAT (i) THE ASSESSMENT WILL MEET ALL OF YOUR REQUIREMENTS; (ii) THE ASSESSMENT WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE; OR (iii) THAT ALL ERRORS IN THE ASSESSMENT WILL BE CORRECTED.

1 Executive Summary

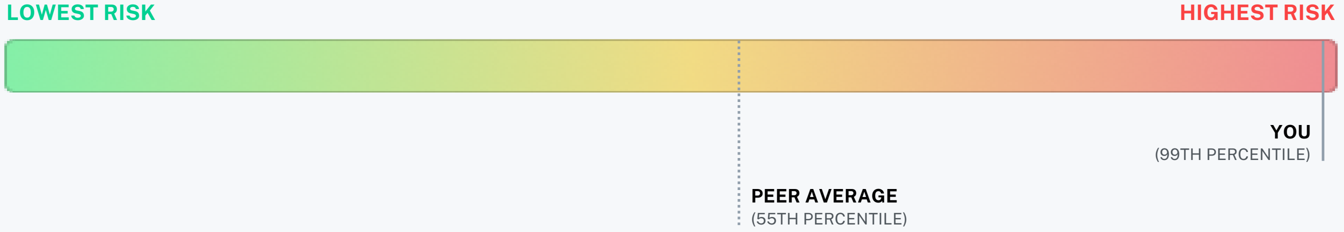
This assessment evaluates cybersecurity risk using data-driven, objective, and publicly available metrics together with Coalion's proprietary claims data. The findings and recommendations in this report are intended to help proactively identify, quantify, and manage cybersecurity risk. All findings can be investigated in greater detail using Coalition Control.

Acme

Domain: acme.com	Industry: Consumer Goods
Last scan: June 1, 2021	Employees: 3
Revenue: $0	Records: 0

You rank in the 99th percentile of all Coalition policyholders

Discovered vulnerabilities will not impact your coverage. However, resolving them may reduce your premium.



Vulnerabilities by Criticality

Prioritized list of vulnerabilities we found on your assets. Critical vulnerabilities represent an active threat and should be remediated as soon as possible.

CRITICAL RISK	HIGH RISK	MEDIUM RISK	LOW RISK
4	6	30	21

Detected Assets

Outside-in view of the Web properties we identified.

DOMAINS	IPS	APPLICATIONS	SERVICES	HOSTING
40	280	46	58	4

Vulnerabilities by Category

Security vulnerabilities found associated with your assets by level of security impact.

RDP	1
IoT	0
Encryption	21
Malware	0
SSL / TLS	19
Web	1
Storage	1

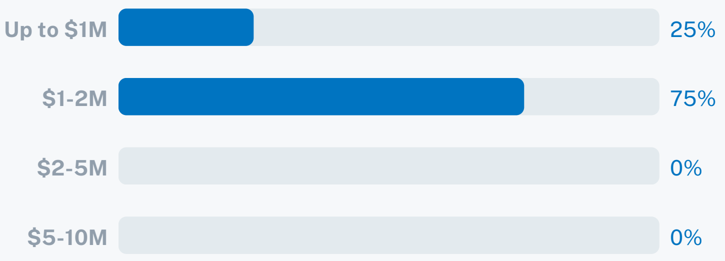
2 How Much Would a Cyber Incident Cost?

Most cyber incidents are manageable, however it is catastrophic loss that organizations need to be prepared for. Using demographic data on your organization, together with Coalition's claims data, we've modeled the probability that organizations in your peer group will experience a cyber loss over the next 12 months, as well as the expected severity of loss using a statistical model derived from 10,000 simulated years of cyber incidents. By comparison, we've also included benchmarking on the insurance limits purchased by your peer group.

Incident likelihood compared to average Coalition insured

0.4x as likely

Limits purchased by peer organizations



Estimated loss based on your organization's risk profile

	Overall	Ransomware	Funds Transfer Fraud	Data Breach
MEDIAN	$239,498	$105,645	$117,520	$16,334
1 IN 10 YEAR LOSS	$1,096,813	$260,484	$708,854	$127,475
1 IN 100 YEAR LOSS	$3,864,363	$457,909	$3,067,764	$338,690

* Data is from multiple sources, including Coalition's own data. Actual numbers may vary significantly from calculator estimates based on additional factors for a given business. The data provided is for informational and educational purposes only. Use of the Coalition Coverage Calculator should not be used as a replacement for a company's own due diligence in regards to their cyber risk. Access and use of the Coalition Coverage Calculator is predicated upon the acceptance of Coalition, Inc. Terms of Service.

3 Email Security

Improperly configured email servers make it easier for cybercriminals to commit fraud against your organization. Social engineering and email compromise are the leading root cause for losses reported by Coalition policyholders. This section identifies common email security measures to protect your organization.

3.1 DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that is designed to give email domain owners the ability to protect their domain from unauthorized use (known as email spoofing). The purpose of implementing DMARC is to protect a domain from being exploited in business email compromise attacks, phishing emails, email scams, and other cyber threat activities.

PASS
0

FAIL
1

Pass (0)

None

Fail (1)

acme.com

3.2 SPF

Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of an email. This measure specifies what email servers are allowed to send email from your domain. It helps ensure that someone cannot create an email server and send it as your domain unless you have authorized them to do so in your DNS records.

PASS
0

FAIL
1

Pass (0)

None

Fail (1)

acme.com

4 Vulnerabilities

This section describes the security vulnerabilities we detected on your assets, including vulnerabilities identified on your web applications and services.

4.1 Web Application Security

Securely configuring web applications can prevent cybercriminals from compromising your, and your user, systems and data.

HTTP Cookie without HTTPOnly flag

LOW RISK
1
Assets

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. One or more cookies were found not having the 'HTTPOnly' flag meaning that a malicious client-side script could read them. Using the 'HTTPOnly' flag protects these cookies from cross-site scripting attacks.

Recommendations

- Review each cookie to determine if it contains sensitive information and the 'HTTPOnly' flag to them.

References

- OWASP: HTTPOnly
- CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag

Asset	Source	Found
35.186.238.101:80 ‡	DNS A	Feb, 15 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

4.2 Services

Issues found with technologies and software running on your assets.

RDP configured with NLA

CRITICAL RISK
1
Assets

Remote Desktop protocol is generally used by organizations to facilitate remote access to their computer systems. However, when this remote access is publicly-accessible on the Internet it can leave the exposed system vulnerable to compromise. In fact, open RDP is the leading cause of ransomware and data breach claims filed by Coalition policyholders. Criminals routinely scan the Internet for such access points, as we have done, and use brute force password attempts or compromised passwords as a means to gain unauthorized access to an organization's network.

Recommendations

- Disable the service if not in use.
- Limit access only to the specific IP addresses that need to access it, either with filtered access or via VPN.

References

- Microsoft: Security guidance for remote desktop adoption

Asset	Source	Found
13.211.150.49:3389	SSL CERT	May, 01 2021

Possible Open Remote Desktop Protocol (RDP)

CRITICAL RISK
1
Assets

Remote Desktop protocol is generally used by organizations to facilitate remote access to their computer systems. However, when this remote access is publicly-accessible on the Internet it can leave the exposed system vulnerable to compromise. In fact, open RDP is the leading cause of ransomware and data breach claims filed by Coalition policyholders. Criminals routinely scan the Internet for such access points, as we have done, and use brute force password attempts or compromised passwords as a means to gain unauthorized access to an organization's network.

Recommendations

- Disable the service if not in use.
- Enable Network Level Authentication (NLA) on the remote server and limit access only to the specific IP addresses that need to access it, either with filtered access or via VPN.

References

- Microsoft: Security guidance for remote desktop adoption

Asset	Source	Found
13.211.150.49:3389	SSL CERT	Apr, 30 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

Microsoft DNS Server Exposed

CRITICAL RISK
1
Assets

Remote code execution vulnerabilities exist in Microsoft's Windows Domain Name System servers when they fail to properly handle requests. An attacker who successfully exploited these vulnerabilities could run arbitrary code in the context of the Local System Account. Windows servers that are configured as DNS servers are at risk from these vulnerabilities. To exploit these vulnerabilities, an unauthenticated attacker must be able to send malicious requests to a Windows DNS server.

Recommendations

- Disable the service if not in use.
- Apply the appropriate security update or mitigation as described in the Microsoft advisories.
- Review access to this service and limit access only to the specific IP addresses that need to access it, either with filtered access or via VPN.

References

- Microsoft Security: CVE-2020-1350
- Microsoft Security: CVE-2021-26897
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Asset	Source	Found
24.214.233.227:53	SSL CERT	Jan, 20 2021

CVE-2019-6977: PHP - imagecolormatch Out of Band Heap Write

MEDIUM RISK
1
Assets

gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data.

Recommendations

- Upgrade to PHP version 5.6.40, 7.1.26, 7.2.14, 7.3.1 or later.

References

- PHP: Changelog 5.6.40
- PHP: Changelog 7.1.26
- PHP: Changelog 7.2.14
- PHP: Changelog 7.3.1
- CWE-787: Out-of-bounds Write

Asset	Source	Found
54.243.193.135:8080	SSL CERT	May, 04 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

CVE-2020-1350: Windows DNS Server Remote Code Execution Vulnerability (SIGRed)

CRITICAL RISK
1
Assets

A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. Windows servers that are configured as DNS servers are at risk from this vulnerability. To exploit the vulnerability, an unauthenticated attacker must be able to send malicious requests to a Windows DNS server.

Recommendations

- Disable the service if not in use.
- Apply the appropriate security update or mitigation as described in the Microsoft advisory.
- Review access to this service and limit access only to the specific IP addresses that need to access it, either with filtered access or via VPN.

References

- Microsoft Security: CVE-2020-1350
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Asset	Source	Found
24.214.233.227:53	SSL CERT	Jan, 20 2021

Microsoft Remote Procedure Call (RPC) Service Exposed

HIGH RISK
2
Assets

Microsoft Remote Procedure Call (RPC) is a interprocess communication (IPC) mechanism that enables data exchange and invocation of functionality residing in a different process. That process can be on the same computer, on the local area network (LAN), or across the Internet. Current threat actor activity on the internet is focusing on targeting this service to deploy ransomware and other malware.

Recommendations

- Disable the service if not in use.
- Review access to this service and limit access only to the specific IP addresses that need to access it, either with filtered access or via VPN.

References

- RPC Technical Reference

Asset	Source	Found
24.214.233.227:49154	SSL CERT	Jan, 19 2021
24.214.233.227:135	SSL CERT	Jan, 23 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

CVE-2017-9798: Apache HTTPD - Use-after-free when using <Limit> with an unrecognized method in .htaccess ("OptionsBleed")

HIGH RISK
2
Assets

Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

Recommendations

- Upgrade to Apache version 2.4.28 or later.

References

- Apache: Changelog 2.4.28
- Apache: CVE-2017-9798
- CWE-416: Use After Free

Asset	Source	Found
66.111.7.8:443	DNS A	Apr, 24 2021
66.111.7.8:80	DNS A	Apr, 16 2021

CVE-2018-7584: PHP Stack Buffer Overflow

HIGH RISK
1
Assets

In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.

Recommendations

- Upgrade to PHP version 5.6.34, 7.0.28, 7.1.15, 7.2.3 or later.

References

- PHP: Changelog 7.0
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Asset	Source	Found
54.243.193.135:8080	SSL CERT	May, 04 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

Kubernetes Service Exposed

HIGH RISK
1
Assets

A Kubernetes server has been found exposed to the Internet. At the time of this finding authentication appears to be enabled, although this type of service should only be accessible by a restricted set of IP addresses since an attacker could execute commands across all pods and install ransomware or delete data.

Recommendations

- Follow the network best practices of Kubernetes by only allowing the necessary IP addresses.

References

- Kubernetes: Network Policies
- Kubernetes: Authentication/Authorization

Asset	Source	Found
140.238.13.176:8443	SSL CERT	Mar, 23 2021

Self-Signed Certificate

MEDIUM RISK
4
Assets

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Recommendations

- Purchase or generate a proper SSL certificate for this service.

References

- Cloudflare: What is an SSL Certificate?

Asset	Source	Found
13.211.150.49:443	SSL CERT	May, 01 2021
24.214.233.227:443	SSL CERT	May, 01 2021
13.211.150.49:3389	SSL CERT	Apr, 30 2021
66.111.7.8:443	DNS A	May, 01 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

Expired Certificate

MEDIUM RISK
3
Assets

The host is serving a certificate which has already expired.

Recommendations

- Purchase or generate a new SSL/TLS certificate to replace the existing one.

References

- Cloudflare: What is an SSL Certificate?

Asset	Source	Found
140.238.13.176:10250	SSL CERT	Mar, 25 2021
85.10.225.138:443 ‡	DNS A	May, 01 2021
66.111.7.8:443	DNS A	May, 01 2021

FTP Service without SSL/TLS found

MEDIUM RISK
1
Assets

FTP service was found without SSL/TLS. This enables applications to communicate across a network in a private and secure fashion, discouraging eavesdropping, tampering, and message forgery. Using SSL/TLS provides three layers of protection: Encryption, Data integrity, Authentication

Recommendations

- Review the service usage and implement FTPS.
- Disable FTP and use SFTP.

References

- Wikipedia: FTPS

Asset	Source	Found
54.243.193.135:21	SSL CERT	Apr, 25 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

Email Service without SSL/TLS found

MEDIUM RISK
8
Assets

Email service was found without SSL/TLS. This enables applications to communicate across a network in a private and secure fashion, discouraging eavesdropping, tampering, and message forgery. Using SSL/TLS provides three layers of protection: Encryption, Data integrity, Authentication.

Recommendations

- Review the service usage and implement SMTPS.

References

- Wikipedia: SMTPS

Asset	Source	Found
135.180.1.14:25	SSL CERT	May, 05 2021
54.243.193.135:587	SSL CERT	Mar, 31 2021
157.131.143.13:25	SSL CERT	Apr, 20 2021
85.10.225.138:25 ‡	DNS A	May, 05 2021
54.243.193.135:25	SSL CERT	May, 05 2021
173.239.66.194:25	DNS A	May, 05 2021
54.243.193.135:143	SSL CERT	Mar, 09 2021
54.243.193.135:110	SSL CERT	Apr, 08 2021

MySQL Service found

MEDIUM RISK
1
Assets

A MySQL service was found running on the host. When found exposed this service becomes targeted by malicious actors trying to gain access. This is a huge risk from a data leak perspective as anyone could try to access your entire database.

Recommendations

- Disable the service if not in use.
- Limit access only to the specific IP addresses that need to access it, either with filtered access or via VPN.

References

- MySQL Website

Asset	Source	Found
54.243.193.135:3306	SSL CERT	Apr, 28 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

HTTP Service without SSL/TLS found

MEDIUM RISK
12
Assets

HTTP service found without SSL/TLS. HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the site. Users expect a secure and private online experience when using a website. Using SSL/TLS provides three layers of protection: Encryption, Data integrity, Authentication.

Recommendations

- Review the service usage and implement HTTPS.

References

- SSL Research: SSL and TLS Deployment Best Practices
- Mozilla Wiki: Security/Server Side TLS

Displaying 12 out of 12 entries

Asset	Source	Found
173.239.66.194:80	DNS A	Mar, 11 2021
24.214.233.227:80	SSL CERT	Feb, 17 2021
52.147.169.173:80	SSL CERT	Feb, 18 2021
157.131.143.13:80	SSL CERT	Feb, 08 2021
35.186.238.101:80 ‡	DNS A	Feb, 15 2021
66.111.7.8:80	DNS A	Apr, 16 2021
217.160.0.150:80	DNS A	Dec, 09 2020
54.243.193.135:10000	SSL CERT	Nov, 17 2020
54.243.193.135:80	SSL CERT	Feb, 05 2021
140.238.13.176:80	SSL CERT	Apr, 10 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

SPF Policy Is Too Broad

LOW RISK
4
Assets

The SPF policy includes an 'all' directive that renders the policy useless.

Recommendations

- Review the policy and ensure the final directive is '-all', enforcing the policy.

References

- Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1

Asset	Source	Found
rr.acme.com	SUBDOMAIN	May, 07 2021
gate.acme.com	SUBDOMAIN	May, 07 2021
acme.com	ROOT DOMAIN	May, 07 2021
mail.acme.com	SUBDOMAIN	May, 07 2021

Certificate Mismatch

LOW RISK
12
Assets

The server presents a SSL/TLS certificate that doesn’t match the server’s hostname.

Recommendations

- Purchase or generate a proper SSL certificate for this service.

References

- Let's Encrypt Website

Displaying 12 out of 12 entries

Asset	Source	Found
140.238.13.176:8443	SSL CERT	Mar, 23 2021
140.238.13.176:2379	SSL CERT	Nov, 11 2020
54.243.193.135:993	SSL CERT	Apr, 25 2021
54.243.193.135:443	SSL CERT	May, 01 2021
13.211.150.49:443	SSL CERT	May, 01 2021
135.180.1.14:443	SSL CERT	May, 01 2021
140.238.13.176:443	SSL CERT	May, 01 2021
24.214.233.227:443	SSL CERT	May, 01 2021
85.10.225.138:443 ‡	DNS A	May, 01 2021
157.131.143.13:443	SSL CERT	Apr, 24 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

DMARC Record Missing

LOW RISK
1
Assets

DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”, is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email. If it is insufficiently configured or missing, it may be possible for an attacker to send spoofed emails, which can be used to trick people into giving up sensitive information and spreading false information that may damage the company's reputation. For DMARC to be correctly setup, SPF and DKIM with correct configuration is a requirement.

Recommendations

- Create a DNS record called _dmarc.[yourdomain] and add a TXT record to it with the value of the selected DMARC policy.

References

- DMARC Website
- Google Workspace: DMARC Record

Asset	Source	Found
acme.com	ROOT DOMAIN	May, 07 2021

SPF Policy Approves Too Many IPv4 Hosts

LOW RISK
3
Assets

Approving a large number of hosts to send mail on behalf of a domain creates a large attack surface.

Recommendations

- Review the addresses and ranges approved for sending mail and reduce them if possible.

References

- Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1

Asset	Source	Found
gate.acme.com	SUBDOMAIN	May, 07 2021
acme.com	ROOT DOMAIN	May, 07 2021
mail.acme.com	SUBDOMAIN	May, 07 2021

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

5 IP and Domain Reputation

Your organization's IP reputation depicts the quality of your email sending environment. This section lists reputational issues found with your IPs and domains, such as sending spam or performing malicious actions. These assets' reputations impact your organization's ability to send email from your IP.

5.1 Blocklisted Domains

NO RISK
0
Domains

Domains found in public blocklists - if one of your assets is found on these lists typically means that some type of malicious activity was performed.

Scan performed and no results were found.

5.2 Honeypot Events

NO RISK
0
Domains

Our distributed network of honeypots constantly listens for unsolicited connections and attacks. There is no reason for any of your assets to communicate with these honeypots. If an event appears in this section, there is a high probability of malware or malicious activity on your network. Some shared hosts randomly scan the internet to test delivery speeds, so if the asset shown is tagged as shared hosting, it might not be a malicious event

This feature has not been enabled for this organization.

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

6 Malware

This section lists your assets that have been connected in 3rd party blocklists (that are typically used by enterprise companies to block IP addresses or domains from contacting their assets) with recent malware infections or indicators of compromise.

Assets Associated with Malware

Assets we discovered where malware activity was detected.

NO RISK
0
Assets

Scan performed and no results were found.

Assets Associated with SPAM

Assets we discovered that send unsolicited communication.

NO RISK
0
Assets

Scan performed and no results were found.

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

Malicious Events

Any assets that performed malicious actions detected by us or third-party partners.

NO RISK
0
Events

This feature has not been enabled for this organization.

‡ Shared host (this issue was detected in a 3rd party asset not directly controlled by your organization)

7 DNS (Domain Name System)

We found the following DNS records associated with your organization. DNS records let the Internet know how to reach your email server, website, and other key functions, and are used by cybercriminals to assess your organization's attack surface.

A Records

Address Records are used to translate a human-readable string into a machine-readable IPv4 address.

Displaying 20 out of 40 entries

music.acme.com	173.239.66.194
root.acme.com	85.10.225.138
santan.acme.com	66.111.7.8
www.heartmaker.acme.com	135.180.1.14
www.labelmaker.acme.com	135.180.1.14
rr.acme.com	54.243.193.135
www.patton.acme.com	54.243.193.135
mail.patton.acme.com	54.243.193.135
patton.acme.com	54.243.193.135
www.mail.acme.com	135.180.1.14

AAAA Records

Address Records are used to translate a human-readable string into a machine-readable IPv6 address.

watches.acme.com	2001:8d8:100f:f000::2fd

CNAME Records

Canonical Name Records are used as an alias. This enables the utilization of external resources, and for those resources to appear as part of the organization's domain.

watches.acme.com

beepbeep.acme.com

MX Records

Mail Exchange Records denote where mail for a particular domain should be routed.

music.acme.com

rr.acme.com

mail.acme.com

santan.acme.com

patton.acme.com

gate.acme.com

NS Records

Name Server Records indicate the hosts that should be used as an authoritative source for records for a particular domain.

music.acme.com

santan.acme.com

patton.acme.com

beepbeep.acme.com

root.acme.com

rr.acme.com

acme.com

SOA Records

Start of Authority Records contain metadata around the parameters of retrieving records for a particular domain. These records contain a serial number, refresh duration, retry duration, expiry duration, and time to live duration.

music.acme.com

santan.acme.com

patton.acme.com

beepbeep.acme.com

root.acme.com

rr.acme.com

acme.com

TXT Records

Text Records are used for a variety of purposes. One of the most common functions is to hold Sender Policy Framework(SPF) strings. It is also frequently used to verify domain ownership.

- root.acme.com
- acme.com
- gate.acme.com
- rr.acme.com
- mail.acme.com

8 Sensitive Information Exposed

This section details information found in 3rd party vendor leaks that are associated with your organization or assets.

Leaked data in 2021

There were no 3rd party data breach events in your organization.

Leaked data in 2020

Names, Geographical Locations, Genders, Geographic Location, IP Addresses, Physical Addresses, Passwords, Hashed Passwords, PII, Email addresses, Phone numbers, Personal information, Social connections, Email Addresses, Document Titles

Cit0day	20 leaks	**Nitro**	9 leaks
Promo	1 leaks		

Sample of 20 out of 29 email addresses found in leaks:

geewee@acme.com, coyote@acme.com, js@acme.com, alex.leader@acme.com, rebus@acme.com, fredderf@acme.com, password@www.acme.com, webmaster@acme.com, wcoyote@acme.com, xxx@acme.com, poster08@acme.com, agne.ambrasaite@acme.com, mivlad@acme.com, acme@acme.com, jim@acme.com, blah@acme.com, exis@acme.com, jef@mail.acme.com, periquito@acme.com, joe.bloggs@acme.com

Leaked data in 2019

Names, Usernames, Geographic locations, Credit status information, Homepage URLs, Employers, Bios, Email addresses, Dates of birth, Genders, Passwords, PII, Physical addresses, Job titles, Phone numbers, Social media profiles, IP addresses

Displaying 6 out of 10 data breach events

Verifications.io	1,146 leaks	**the-collections**	172 leaks
data-contacts	19 leaks	**Pastebin**	3 leaks
ApexSMS	1 leaks	**mgmresorts.com**	1 leaks

Sample of 20 out of 1,293 email addresses found in leaks:

gotham@acme.com, x0a0at@acme.com, lweiss@acme.com, tripod@acme.com, savannah.le@acme.com, fredderf@acme.com, mtrimas@acme.com, b.chang@acme.com, lucas@acme.com, mccarthy@acme.com, anon@acme.com, fausto@acme.com, s.gao@acme.com, smith@acme.com, edmondsj@acme.com, kathleen@acme.com, cduffy@acme.com, angel@acme.com, alan.hayes@acme.com, lorrainel@acme.com

Leaked data in 2018

Names, Usernames, Geographic locations, Employers, Email addresses, Dates of birth, Genders, Passwords, PII, Physical addresses, Job titles, Phone numbers, Spoken languages, Social media profiles, IP addresses

Displaying 6 out of 9 data breach events

datanleads.com	100 leaks	**Adapt.io**	30 leaks
pdlCollection	18 leaks	**Customers Live**	17 leaks
HauteLook	8 leaks	**StrongholdKingdoms**	1 leaks

Sample of 20 out of 175 email addresses found in leaks:

adi@acme.com, antonio.alvarez@acme.com, mahendran@acme.com, sclark@acme.com, ryan.booker@acme.com, hjones@acme.com, www.shahbazqadri@acme.com, jean@acme.com, john@acme.com, jayden.garrison@acme.com, savannah.le@acme.com, mjones@acme.com, ad@acme.com, aeles@acme.com, rtalwwar@acme.com, acme1@acme.com, jsmythe@acme.com, psandoval@acme.com, hunter@acme.com, fminchella@acme.com

Leaked data in 2017

Usernames, Passwords, PII, Email addresses

BreachCompilation	109 leaks	LiveJournal	6 leaks
MyHeritage	1 leaks		

Sample of 20 out of 113 email addresses found in leaks:

coyote@acme.com, jshmoe@acme.com, mcstsr@acme.com, tripod@acme.com, john@acme.com, marcialou@acme.com, jake@acme.com, exlwndr@acme.com, roadrunner1530@acme.com, q@acme.com, jef@mail.acme.com, toon@acme.com, steveacme@acme.com, nospam@acme.com, gtg@acme.com, lillbern@acme.com, mcstar@acme.com, bugs@acme.com, dre@acme.com, jarabacoa79@acme.com

Leaked data in 2016 and older

Astrological signs, Religions, Website activity, Purchasing habits, Credit status information, Education levels, Work habits, Payment histories, Family structure, Email addresses, Physical attributes, Dates of birth, Political views, Drinking habits, Parenting plans, Sexual fetishes, Security questions and answers, Physical addresses, Personal descriptions, IP addresses, Drug habits, Names, Usernames, Geographic locations, Relationship statuses, Password hints, Fitness levels, Home ownership statuses, Income levels, Travel habits, Genders, Ethnicities, Passwords, PII, Sexual orientations, Job titles, Phone numbers

Displaying 6 out of 25 data breach events

Antipublic	85 leaks	MySpace	44 leaks
Mate1	17 leaks	Dropbox	12 leaks
Disqus	7 leaks	YouPorn	1 leaks

Sample of 20 out of 167 email addresses found in leaks:

testco@acme.com, coyote@acme.com, jshmoe@acme.com, mp@acme.com, mcstsr@acme.com, js@acme.com, tripod@acme.com, john@acme.com, joedonn@acme.com, jake@acme.com, buggsbuny@acme.com, rico@acme.com, exlwndr@acme.com, roadrunner1530@acme.com, q@acme.com, jef@mail.acme.com, toon@acme.com, steveacme@acme.com, nospam@acme.com, b348juyta@acme.com

9 User Behavior

This section details risky behavior we've observed from individuals within your organization. We use open source intelligence to measure the cyber hygiene of user accounts. If compromised, these accounts could compromise your organization as well.

9.1 Password Quality

Using strong, unique passwords for all services can help prevent common criminal techniques such as 'brute forcing' or 'credential stuffing.' This section shows an analysis of the complexity and length of passwords found in data leaks for your organization.

Analysis by Characters

We recommend using longer passwords or passphrases, which are more challenging to guess or brute force.

LOWERCASE	UPPERCASE	NUMBERS	SPECIAL CHARACTERS
85.7%	8.8%	67.2%	2.9%

Analysis by Composition

We recommend creating complex passwords that use a combination of alphanumeric characters and symbols.

ONLY LETTERS	ONLY NUMBERS	LETTERS & NUMBERS	WITH EVERYTHING
31.5%	11.3%	54.2%	0.8%

9.2 Torrents

Torrent downloads are often illegal and very often bring files infected with malware into your network. In this section we list the torrents seen being downloaded by your assets.

This feature has not been enabled for this organization.

What is Cyber Insurance?

Cyber insurance (a.k.a. Cyber Liability, Internet Liability, Electronic Media Liability, and Network Security & Information Security Liability insurance, among other countless monikers) helps companies weather the storm from many technology-based risks they face. This includes the risks associated with a company's information technology infrastructure and data that may be impacted by a systems failure, ransomware attack, funds transfer loss, or data breach.

Our coverage

We protect your entire business from today (and tomorrow's) cyber threats, with up to $15 million of cyber and technology errors and omissions insurance coverage.

3rd Party Liability Coverages

We cover the expenses to defend you and any damages resulting from your liability to a 3rd party.

Network & Information Security Liability

Regulatory Defense & Penalties

Multimedia Content Liability

PCI Fines & Assessments

We cover the expenses to defend you and any damages resulting from your liability to a 3rd party, or for regulatory fines & penalties, multimedia wrongful acts (such as infringement, defamation, piracy, etc.), and PCI fines & assessments resulting from a failure in your security, data breach, or privacy violation.

Bodily Injury & Property Damage - 3rd party

We pay for the costs of defense and damages from your liability to a 3rd party when a failure in your security results in physical damage or injury.

Technology Errors & Omissions

We pay for the costs of defense and damages from your liability to a 3rd party when the failure of your technology service or product is the cause of loss.

1st Party Liability Coverages

We cover the direct expenses and damages your organization incurs as a result of a cyber incident.

Bodily Injury & Property Damage - 1st party

Pollution

In the event of a security failure (i.e., physical cyber attack), we'll even cover losses resulting from bodily injury or damage/impairment to your tangible property, as well as damages resulting from any liability you may have to a 3rd party, including regulatory fines & penalties and pollution liability.

Computer Replacement

We cover the costs to replace your computer systems that are permanently impacted by malware.

Fund Transfer Fraud

We pay for funds transfer losses you incur from a failure in your security or social engineering.

Service Fraud

We pay for the additional amounts you're billed by a cloud or telephony provider when you incur fraudulent charges.

Digital Asset Restoration

We pay for the costs to replace, restore, or recreate your digital assets that are damaged or lost following a failure of your security.

Business Interuption & Extra Expenses

We cover financial losses resulting from a failure in your security, data breach, and even systems failure, as well as the extra expenses you incur to bring your company back online.

Cyber Extortion

We cover the costs to respond to an extortion incident, including money, securities, and even virtual currencies paid.

Breach Response

Crisis Management & Public Relations

Reputation Repair

We pay for the costs to respond to a breach including 3rd party incident response and public relations experts, customer notification costs and credit monitoring, media purchases, and legal fees; and advise in connection with the incident, among others.

Global Coverage

Our coverage is global, providing you with protection from cyber threats near and far.

- **Worldwide Coverage**
- **Cyber Terrorism**
- **Internet of Things**
- **Social Media**

In the event of a security failure (i.e., physical cyber attack), we'll even cover losses resulting from bodily injury or damage/impairment to your tangible property, as well as damages resulting from any liability you may have to a 3rd party, including regulatory fines & penalties and pollution liability.

Our features

These are some of the tools available to help you improve your cybersecurity.

On-demand Support and Training

Security & Incident Response Team (SIRT)
Coalition is the only cyber insurance provider with a dedicated team of cybersecurity experts available to you at all times.

Security Awareness Training
Send simulated phishing tests targeting your own employees. Curricula's phishing awareness training simulates real-world phishing attacks, then trains your employees how to defend against them.

Proactive Monitoring and Alerts

Attack Surface Monitoring
Continuous monitoring, attack surface discovery, scanning, reporting, and alerting for organizations of any size.

Security Solutions

DDoS Prevention
Distributed denial of service (DoS) attacks attempt to make your Internet-based services inaccessible when you need them. Protect your websites and applications, and prevent disruptions from malicious traffic through our partnership with Cloudflare.

Endpoint Detection and Response (EDR)
Coalition offers a comprehensive threat detection solution, with a Coalition-negotiated discount, that includes protection from dangerous attacks such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions.

FAQs

Frequently Asked Questions about Coalition Risk Assessment.

Who is Coalition?

Coalition is the leading provider of cyber insurance and security, combining comprehensive insurance and proactive cybersecurity tools to help businesses manage and mitigate cyber risk. Backed by leading global insurers Swiss Re Corporate Solutions, Arch Insurance Group, Lloyd's of London, and Argo Group, Coalition provides companies with up to USD $15 million of cyber and technology insurance coverage in all 50 states and the District of Columbia, as well as CAD $20M of coverage across 9 provinces in Canada. Coalition's cyber risk management platform provides automated security alerts, threat intelligence, expert guidance, and cybersecurity tools to help businesses remain resilient in the face of cyber attacks. Headquartered in San Francisco, Coalition has presences in New York, Los Angeles, Chicago, Dallas, Washington DC, Miami, Atlanta, Denver, Austin, Vancouver, and Toronto.

How does Coalition determine my security ranking?

Our security ranking provides a relative measure of an organization's risk and security posture compared to other organizations we have evaluated. In order to determine the ranking of an insured, we correlate identified risk conditions with Coalition's proprietary loss and claims data. Unlike traditional security ratings, that make arbitrary assumptions on the relative impact of an identified risk condition to generate a security score, Coalition uses actual loss and claims data to identify the most significant risks to an organization. The result is not only a more accurate assessment of risk, but actionable prescriptions to help an organization invest its resources against the most impactful remediation actions.

Where does the underlying data from Coalition's risk assessment come from?

Coalition passively collects external data on an organization's Internet facing IT infrastructure, compromised system events, file sharing events, and configurations from many different sources. Coalition does not perform active collection of information, including penetration testing against an organization's networks, without the explicit permission of that organization.

How can I learn more?

To learn more about Coalition visit coalitioninc.com, or our knowledge base at help.coalitioninc.com. As a dedicated risk management partner to our policyholders, Coalition's team of security and insurance experts are committed to helping you implement security and loss controls, all at no additional cost.

Glossary

This section defines some of the terminology used throughout this report.

Asset
Web properties that your organization owns, such as an IP Address, Domain, or Subdomain.

Data breach
A cyber incident where your customer or employee data is accessed, and possibly exfiltrated, by a third party.

Domain
Web address associated with the organization. Example: coalitioninc.com

Hosting
Some type of hosting provider or hosting technology being used in one or more of your assets.

IP Address
An IP address associated with your company. Example: 1.1.1.1.

RDP
Remote Desktop Protocol (also known as a Remote Desktop or RDP) is a feature that enables employees to remotely log into their corporate computer from home. While it may be convenient for employees, RDP can also function as an open door for hackers to break into your corporate network.

Services
Technologies used to deliver services from your assets.

Secure Sockets Layer (SSL)
SSL is a cryptographic protocol designed to provide secure communications over a computer network.

Technologies
Technologies found being used in one or more of your assets.

Torrents
Torrenting is a peer-to-peer file-sharing mechanism whereby assets that are hosted on your computers may be downloaded by other people who are outside of your organization.

Coalition®

Cyber Risk, Solved.®

This assessment was prepared by

Coalition, Inc.
1160 Battery St. Suite 350
San Francisco, CA 94111

For more information, visit coalitioninc.com

Swiss Re | Arch Insurance | LLOYD'S | ARGO PRO

Coalition's products are offered with the financial security of Swiss Re Corporate Solutions (A.M. Best A+ rating), Arch Insurance Group (A.M. Best A+ rating), Lloyd's of London (A.M. Best A rating), and Argo Pro US (A.M. Best A- rating).