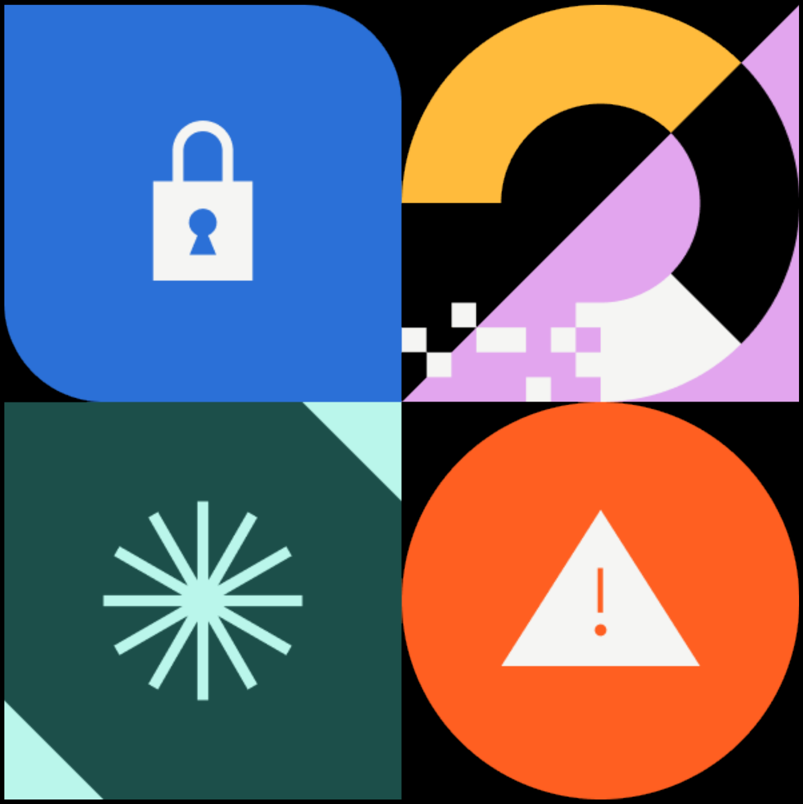
Coalition®

Generated on December 11, 2024

Cyber Risk Assessment

PREPARED FOR

Acme Corp



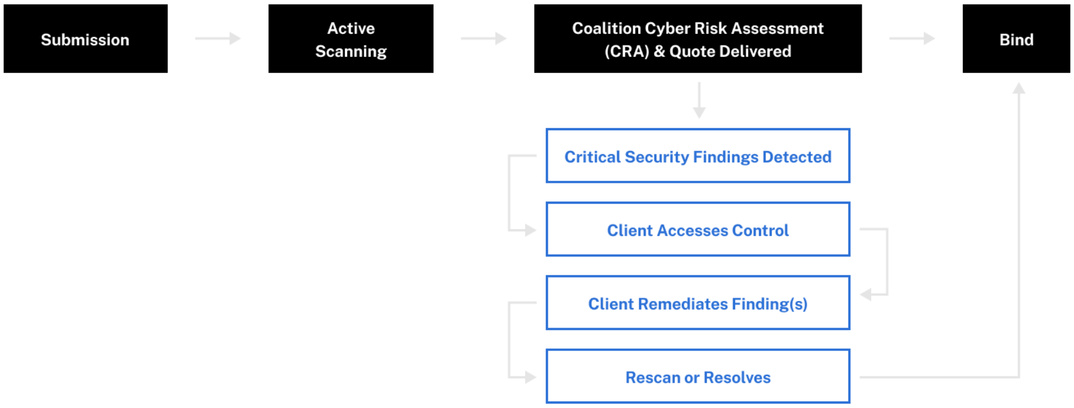
coalitioninc.com

Coalition Control®

Simplify contingency resolution with pre-bind access

Every organization that receives a quote and Cyber Risk Assessment (CRA) from Coalition also receives exclusive access to Coalition Control®. This allows Coalition to guide you through remediating critical exposures identified by our Active Risk Assessment and help you resolve them before binding coverage.

How does it work?


Submission
Active Scanning
Coalition Cyber Risk Assessment (CRA) & Quote Delivered
Bind
Critical Security Findings Detected
Client Accesses Control
Client Remediates Finding(s)
Rescan or Resolves

Follow these easy steps to make cybersecurity less daunting with Coalition Control:

1. **Coalition Conducts Active Risk Assessment**
Coalition uses proprietary attack surface monitoring technology and real-time threat intelligence to provide a customized view of the exposures that are the most severe, likely to impact insurability, and if not resolved could result in claims.

2. **Critical Security Findings Detected by Coalition**
If Critical Security Finding(s) are detected that impact insurability, they will be noted on the quote document as contingencies and in the Coalition Cyber Risk Assessment (CRA) provided with the quote.

3. **Activate your Coalition Control Account by following instructions provided by your broker**
Every current and prospective Coalition policyholder receives access to Coalition Control, not just those with security findings. New clients can request pre-bind access by contacting their broker. Existing policyholders can log into Coalition Control with a valid email address and policy number.

4. **Remediate Exposures**
Log into Coalition Control to review the technical details of any security findings, suggested remediation best practices as well as additional support resources.

5. **Rescan and Resolve**
After exposures have been remediated, follow the instructions to initiate a rescan and resolve contingencies directly in Control. As soon as contingencies are cleared an updated bindable quote will be reissued. Depending on the security finding, rescans could take up to 48 hours.

Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc.("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers.

Coalition's Active Insurance approach incorporates continuous Risk Assessments, Active Protection, and Active Response, providing policyholders with holistic benefits in protecting their organizations against dynamic risks.

This Coalition Risk Assessment provides a customized view of your organization's risk. Coalition collects and analyzes externally observable security data and integrates these findings with our proprietary claims and incident data to identify your organization's risk exposures. This objective assessment of your cyber risk enables your organization to take proactive measures to mitigate risk and improve your security.

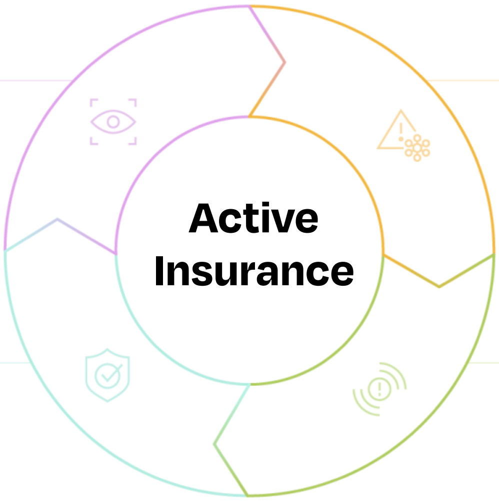
Coalition's Active Protection and Response provides a holistic risk management solution for your organization, including:

- Attack surface monitoring and third party risk management in Coalition Control
- Incident response support and in-house claims team
- Cybersecurity education resources

Sections

Risk Summary
Security Findings
Overall Risk Posture
- Data Leaks
- Malware
- Spam
- Malicious Events
- Honeypot Events
- Blocklisted Domains
- Torrents
- DMARC
- SPF

Glossary



ASSESS

Real-time, external view of cyber risk with customized recommendations

PROTECT

Identify and prevent new threats with tailored remediation guidance and support

COVER

Comprehensive coverage to help give peace of mind following an attack

RESPOND

Immediate expert support to minimize impact and speed up recovery

52% Reported incidents handled at no cost outside of the policy premium
Source

64% Fewer claims than the cyber industry average
Source

24/7 Support from our claims team

Risk Summary

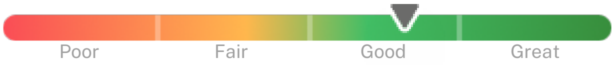
Acme Corp

Domains: acme.com Last Scanned: Dec 11, 2024

Cyber Health Rating

The Cyber Health Rating is a dynamic score that reflects the overall health of your organization's cybersecurity posture, with 100 representing optimal health. This rating considers factors such as attack surface exposure, and alignment with best practices to help you understand and improve your cyber resilience.

66 /100 Good



Critical Security Findings

Critical Security Findings are high-risk vulnerabilities that strongly correlate with cyber claims and security breaches. Addressing these findings is essential to reducing exposure and maintaining insurability.

◆ 2

How Much Would a Cyber Incident Cost?

Using demographic data on your organization, together with Coalition's global 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.

Your Inherent Risk Rating

Baseline level of cyber risk based on your industry and operational complexity, independent of your attack surface and security controls.

🟩 Good

Revenue	Under 10M	🟩⬜⬜
PHI/PCI/PII Data	No records	🟩⬜⬜
Employees	51-250	🟥🟥🟥
Industry	industrials	🟥🟥🟥

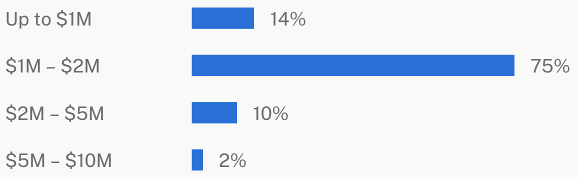
Incident likelihood compared to average Coalition insured

1.0x as likely

Estimated loss based on your organization's profile

Type of loss	Median	1 in 10 years	1 in 100 years
Composite	$108,072	$808,791	$4,165,621
Ransomware	$195,755	$1,193,304	$5,200,559
Funds Transfer Fraud	$95,108	$626,125	$2,905,121
Data Breach	$68,675	$534,102	$2,838,372

Aggregate limits purchased by peer organizations



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 Control's Terms of Service.

Security Findings

CRITICAL

2

Critical risks are contingencies that **impact premium and insurability** if not resolved.

△ HIGH

0

High risks can turn into critical risks if not resolved.

○ MEDIUM

0

Medium risks may turn to high risk if not resolved.

▽ LOW

4

Low risks may turn to medium risk if not resolved.

Attack Surface Analyzed

Sub Domains	7
IP Addresses	12
Applications	35
Services	28

For full list, go to control.coalitioninc.com

Critical Findings

Our Active Risk platform has identified the following critical security findings for your organization. To help reduce a **negative impact on insurability or a potential increase in your premium**, resolve these critical findings using the information provided.

SECURITY FINDING	ASSET
Open Remote Desktop Protocol (RDP) Frequent Claim Indicator	1
Possible Open Remote Desktop Protocol (RDP) Frequent Claim Indicator	1

Critical △ High ○ Medium ▽ Low

Open Remote Desktop Protocol (RDP)

CRITICAL

1

Assets Affected

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.

How can this be resolved?

- 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	LAST DETECTED
173.219.129.84:1000	SSL CERT	Nov 19, 2024

How can I test my fix and resolve a vulnerability?

1. Go to https://control.coalitioninc.com/security-findings/?findingsTab=active.
2. Select the security finding you want to test and click **Rescan**.
3. Your security findings will update and a new Cyber Health Rating will appear!

Not a Coalition Control user?

Sign up for free at control.coalitioninc.com

Shared host. This issue was detected in a 3rd party asset not directly controlled by your organization.

SECURITY FINDINGS

Possible Open Remote Desktop Protocol (RDP)

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.

CRITICAL

1

Assets Affected

How can this be resolved?

- 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	LAST DETECTED
173.219.129.84:1000	SSL CERT	Dec 4, 2024

How can I test my fix and resolve a vulnerability?

1. Go to https://control.coalitioninc.com/security-findings/?findingsTab=active.
2. Select the security finding you want to test and click **Rescan**.
3. Your security findings will update and a new Cyber Health Rating will appear!

Not a Coalition Control user?

Sign up for free at control.coalitioninc.com

Shared host. This issue was detected in a 3rd party asset not directly controlled by your organization.

SECURITY FINDINGS

Non-Critical Security Findings

Non-critical security findings have a risk severity of High, Medium, or Low. We still recommend remediating them as they could expose your organization to other types of cyber risk or become critical security findings later as threat actors change their tactics.

SECURITY FINDING	ASSET
▽ **SPF Policy Is Too Broad** The SPF policy includes an 'all' directive that renders the policy ineffective.	2
▽ **SMTP Sender Policy Framework (SPF)** The remote domain name doesn't have SPF (Sender Policy Framework) in place. This mechanism is a way to let a mail server know which mail servers are authorized to send emails on behalf of your domain. When a domain lacks an SPF policy, an attacker is able to send spoofed emails that look like they're... For full details, go to control.coalitioninc.com/security-findings/?findingsTab=active	1
▽ **DMARC Record Missing** 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... For full details, go to control.coalitioninc.com/security-findings/?findingsTab=active	1

How can I test my fix and resolve a vulnerability?

1. Go to https://control.coalitioninc.com/security-findings/?findingsTab=active.
2. Select the security finding you want to test and click **Rescan**.
3. Your security findings will update and a new Cyber Health Rating will appear!

Not a Coalition Control user?

Sign up for free at control.coalitioninc.com

◆ Critical △ High ○ Medium ▽ Low

Overall Risk Posture

Your overall risk posture is a holistic look at your organization's cyber exposure. This includes assets, data exposures and technologies that threat actors may exploit identified by our Active Data Graph.

RISK	Data Leaks	**4,221** leaks
SECURE	Malware	**0** detected
SECURE	Spam	**0** detected
SECURE	Malicious Events	**0** detected
SECURE	Honeypot Events	**0** detected
SECURE	Blocklisted Domains	**0** detected
SECURE	Torrents	**0** detected
RISK	DMARC	**1** failures
RISK	SPF	**1** failures

Data Leaks

This section details the potential impacts of data leaks and phishing. Phishing is often the initial entry point in breaches, and exposed data, like passwords, can be used in subsequent attacks.

2,991 Passwords Breached

Characters	
Lowercase	85%
Uppercase	19%
Numbers	62%
Special Characters	13%

Use long passwords or passphrases, which are more challenging to guess or brute force. Do not reuse passwords.

Composition	
Letters Only	35%
Numbers Only	11%
Letters & Numbers	41%
With Everything	9%

Create complex passphrases or passwords that use a combo of random alphanumeric characters and symbols.

RISK
4,221
Emails

RISK
1,594
Phone Numbers

SECURE
0
Auth Tokens

RISK
94
Credit Cards

SECURE
0
Credit Card PINs

SECURE
0
SSNs

What are your most common breaches?

4,221	Email addresses
2,991	Passwords
1,881	Names
1,603	City
1,594	Phone numbers
1,462	Postal Code
1,432	Usernames
1,397	State
1,228	Physical addresses
1,153	Country Code

Where are your breaches occuring?

532	Sensitive Source
258	B2B USA Businesses
214	Collection #2 Combo List
185	PUREINCUBATION
170	Sales Intelligence Company Leak
147	Collection #4 Combo List
142	2019 Antipublic Combo List
137	US-based Data Broker Leak
135	Combolist of 1.4 Billion Credentials
133	Adobe Systems

Need more info?

Go to control.coalitioninc.com/data-leaks/ for a full list.

Not a Coalition Control user?

Sign up for free at control.coalitioninc.com

OVERALL RISK POSTURE

Malware

Assets we discovered where malware activity was detected.

SECURE

0

Assets Detected

ASSET	SOURCE	LAST DETECTED

Scan performed and no results were found

Spam

Assets we discovered that send unsolicited communication.

SECURE

0

Assets Detected

ASSET	SOURCE	LAST DETECTED

Scan performed and no results were found

OVERALL RISK POSTURE

Malicious Events

Assets detected by Coalition or a third-party partner, noted for their performance leading to attempted or successful unauthorized network intrusion by a threat actor. These attempts can lead to malware, ransomware, or other cyber incidents.

SECURE

0

Assets Detected

ASSET	TAGS	LAST DETECTED

Scan performed and no results were found

Honeypot Events

A honeypot is a legitimate security mechanism that is purposely vulnerable to high-risk exploits in order to identify malicious assets that attempt to infiltrate it. Our distributed network of honeypots listens for unsolicited connections and attacks. Your assets should not communicate with our honeypots. Events in this section indicate malicious activity on your network is likely. Shared assets are not an indicator of malicious events.

SECURE

0

Assets Detected

ASSET	TAGS	LAST DETECTED

Scan performed and no results were found

OVERALL RISK POSTURE

Blocklisted 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.

SECURE

0

Assets Detected

ASSET	SOURCE	LAST DETECTED

Scan performed and no results were found

Torrents

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

SECURE

0

Assets Detected

ASSET	NAME	LAST DETECTED

Scan performed and no results were found

OVERALL RISK POSTURE

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.

RISK

1

Domains Failed

PASS (0)	FAIL (1)
	acme.com

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.

RISK

1

Domains Failed

PASS (0)	FAIL (1)
	acme.com

Glossary

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

Frequent Claim Indicator
A security finding that frequently leads to claims and severely impacts your Cyber Health Rating.

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.

Remote Desktop Protocol (RDP)
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.

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

Services
Technologies used to deliver services from your assets.

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

This assessment was prepared by

Coalition Incident Response, Inc.
44 Montgomery Street
Suite 4210
San Francisco, CA 94104

For more information, visit coalitioninc.com/security

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.