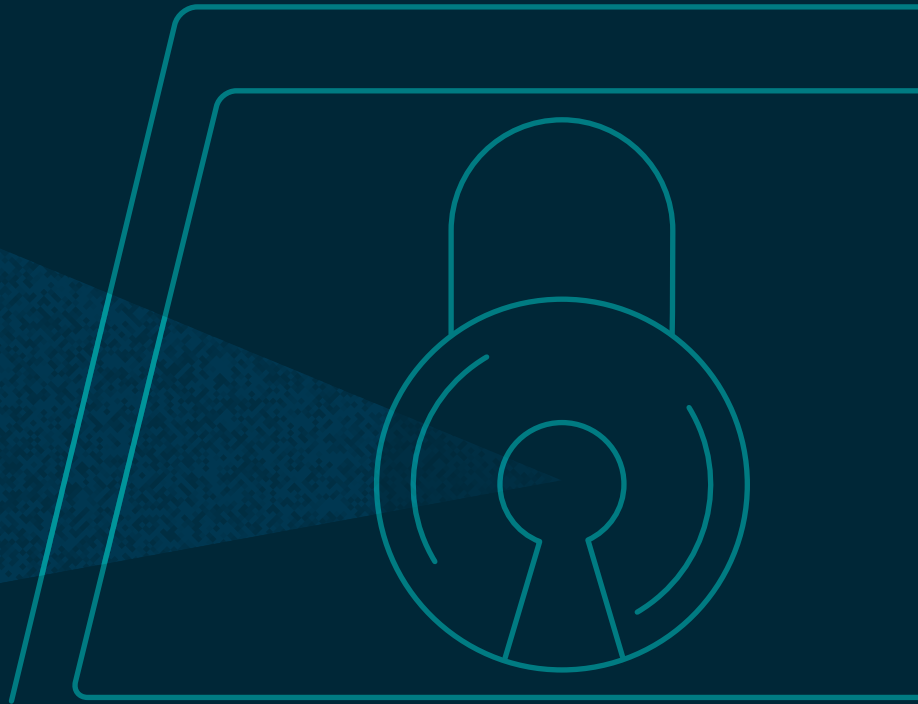




01.2023

# Coalition Cyber Insurance

## Product Overview and Guidelines





# table of contents

01	Coalition Overview
04	Cyber Insurance
07	Product Information
10	Coverages
13	Policy Management



## Coalition Overview

# Coalition

Cyber losses cost the global economy upwards of \$1.5 trillion each year, and yet the majority of businesses are under-insured and under-prepared to manage and mitigate the risks of an increasingly digital world. Coalition is addressing this gap by providing no-cost cybersecurity tools to prevent losses, security and incident response services to contain them, and comprehensive cyber insurance to help organizations recover.

Offering a free proactive cybersecurity platform, it's not just insurance but the most comprehensive cyber protection a small business can have. Coalition Cyber Insurance protects the value of your entire business

including financial, intangible, and tangible damage with up to \$15M. Its cybersecurity platform includes 24/7 security monitoring, automated security alerts, employee training, and access to security experts to prevent cyber incidents before they occur.

Coalition's insurance products are offered with the financial security of Swiss Re Corporate Solutions, Lloyd's of London, and Argo Group (A+, A, and A- ratings, respectively, by A.M. Best). After Attune's acquisition by Coalition, we are now the world's largest commercial insurtech provider.

<https://www.coalitioninc.com>



## **Complete Cyber protection**

Coalition takes a unified approach to digital risk. They support their insureds before, during, and after security incidents with active monitoring, incident response and comprehensive insurance.

### **Active monitoring – 24/7 security monitoring and alerts**

Their tools and team help secure an organization to prevent cyber incidents.

- **Instant Alerts (\$10,000 value)**  
Coalition's Attack Surface Monitor notifies a business of vulnerabilities in their public infrastructure throughout the policy period.
- **On-demand security support**  
Coalition's Security and Incident Response Team (SIRT) is always available to provide on-demand security support. Peace of mind included.
- **Free and discounted security tools**  
Access security services with Coalition-provided discounts for security awareness training, malware prevention, and more.

### **Incident response – Immediate response during security incidents**

Speed is critical when responding to security incidents, which is why Coalition is the only cyber insurance provider with a dedicated in-house cyber claims and incident response team.

- **Coalition Incident Response (CIR) problem and breach-related expenses** such as credit monitoring and regulatory penalties.
- Their in-house staff of incident responders, forensic specialists, and security engineers respond in minutes, not days, to help an insured recover from network intrusions, ransomware, and business interruptions.
- **Coalition Claims**  
Their expert claims team includes privacy attorneys & breach coaches who can help a business navigate the recovery process — including clawing back lost funds, managing vendors and law enforcement, and ensuring their claim is paid quickly



### **Comprehensive insurance to help one recover quickly**

Coalition's comprehensive insurance policy will help an organization recover financially and operationally so they can get back to business.

- Protect the value of the entire business  
Coalition doesn't just protect an organization's network, their insurance policy protects an entire business with coverage for financial losses and liability arising from cyber incidents, technology failures, and privacy violations.
- Insurance one can depend on  
Coalition's insurance products are offered with the financial security of many of the world's leading (re)insurers including Swiss Re Corporate Solutions, Arch Insurance, and Lloyd's of London, among others.



## Cyber Insurance

### What is Cyber Insurance?

Cyber insurance (a.k.a. Cyber Liability, Privacy Liability, Internet Liability, Electronic Media Liability, and Network Security & Information Liability insurance) helps companies weather the storm from many technology-based risks that might impact them. This includes risks associated with a company's IT infrastructure and activities such as systems failure, cyber attack, or data breach.

### Common Cyber Risks

- **Ransomware**

A hacker has encrypted all of your files and won't unlock them until you pay a ransom. Not to worry we'll cover the costs to restore your data and get you up and running again.

- **Wire Fraud and Social Engineering**

A funds transfer request is sent to your controller by someone pretending to be your CEO. The funds may be out the door, but at least you're not out of pocket—we've got you covered.

- **Phishing and Data Breaches**

A hacker gains access to an employee's email or breaches your network. We'll cover costs to fix the problem and breach-related expenses such as credit monitoring and regulatory penalties.

- **Ransomware and malware attacks**

A bad actor encrypts and disables access to business-critical systems and data until a ransom payment is made. Data may also be exfiltrated and exposed if the ransom isn't paid.

- **Funds transfer fraud**

A bad actor uses social engineering, sometimes in concert with phishing attacks, to cause funds to be sent to the attacker instead of the proper recipient

- **Business email compromise**

Email intrusion resulting from spoofing, phishing, or spear phishing that can result in a data breach or funds transfer loss



- **Data breaches**

Exposure of Personally Identifiable Information (PII) or Protected/ Personal Health Information (PHI) of your customers

- **Legal and regulatory issues**

Violation of a legal or regulatory framework, such as GDPR or CCPA

- **Web application compromise**

Direct compromise of a web-based product, such as an eCommerce platform, as a result of a targeted attack

- **Technology errors & omissions**

A failure in the technology product or services results in business interruption or loss on behalf of your customers

### **Who needs Cyber Insurance?**

Any business with an online presence and/or dependency on the internet should consider getting protection against cyber risks. Using emails, having a website, storing data, having a point of sale, etc are a few examples of having a digital presence and this list is not exhaustive. A business should ask itself if they lost all access to digital presence would they be able to function?

### **Is a small business at risk?**

As small and midsize businesses become increasingly dependent on services and applications connected to the internet, they also become a larger target for cybercriminals looking to exploit vulnerabilities in their systems. Every password we set, tool we use, and network we access leaves us exposed and vulnerable to cyber threats.

Here are a few startling statistics

- 58% Percent of cyber attacks are targeting small businesses.
- 4-in-5 Number of SMBs reporting attacks that evaded their antivirus and intrusion detection software
- \$160,000 Average loss from a ransomware attack for a small business



Cybercriminals are finding it more profitable to target small and midsize organizations due to their ability to automate attacks and because businesses are more vulnerable due to the COVID-19 pandemic. In part, the rush to get up and running virtually quickly during the pandemic caused many smaller organizations with limited resources to overlook significant security risks. In fact, according to [Coalition's Cyber Insurance Claims Report](#), the frequency of incidents reported for organizations with fewer than 250 employees increased 57% from the first half of 2020 to 2021. Unfortunately for these smaller organizations, a ransomware demand can be catastrophic, averaging \$1.2 million in 2021 for Coalition policyholders.





## Product Information

Coalition's insurance products provide comprehensive cyber protection along with a free proactive cybersecurity platform that monitors risks.

### **Coalition Control, Coalition's Cybersecurity Services**

Coalition Control is the account home for all Coalition policyholders and technology customers, combining insurance, technology, and services from Coalition and its partners into a unified, dynamic online experience. Here are the platform features:

#### **Cyber risk assessment**

- Coalition now offers a Cyber Risk Assessment (CRA), free of charge, to all policyholders and brokers. The CRA is generated based on a subset of Coalition's underwriting platform data. They evaluate organizations the same way that cybercriminals do, using publicly available information about the organization's security posture. Understanding these signals allows organizations to better understand and prevent cyber risk.
- The CRA includes information on vulnerabilities, compromised credentials, and overall recommendations for the insured to help them understand their risk exposure and better their own security posture. They intend for this document to supplement the insured's existing cybersecurity program.
- For Policyholders, an up-to-date version of their CRA is available at any time on their Coalition Dashboard.

#### **Claims Calculator**

- Coalition's Claims Calculator lets any broker plug in a simple set of inputs to simulate different risk scenarios and assess the cost of different cyber incidents. The calculator is fully customizable for each client and provides limit benchmarking data, case studies, and more.
- The calculator makes it easy to show potential clients how their organizations are exposed to risk when compared to their peers in a language they can understand.



## And more

- **Free Attack Surface Scanning & Cybersecurity Recommendations** – When vulnerabilities are identified, Coalition shows where they are and how to fix them.
- **Cybersecurity Partner Solutions** – Coalition partners with other leading cybersecurity companies to help one build out the security stack. Email security, endpoint detection and response (EDR), security training, remote access control, and solutions for advanced protection from malware are all available inside Coalition Control.
- **Policy Management & Private Community** – Policyholders can view all of their Coalition insurance policies inside Coalition Control. Review your coverage, speak with an expert, or connect directly with Coalition’s private, online security community for cybersecurity education and information.

## Admitted and Surplus lines products

Whether you are looking for an admitted or surplus lines policy, Coalition is committed to helping you solve cyber risk. However, there are key differences between the two products which we layout below.

### The admitted product includes:

- Breach Response Services – these are Coalition’s risk mitigation services provided to you when you’re facing an incident or potential incident. This is offered on all quotes, outside the limits, and with \$0 retention.
- Coverage for privacy action brought against you by the Securities and Exchange Commission (SEC). Note that this is available by endorsement on our surplus lines product but built into the base form on our admitted product.
- Available in 41 states and D.C.

### The surplus lines product includes:

- Multi-Factor Authentication (MFA) retention reduction
- Invoice manipulation
- Duty to cooperate endorsement
- Your obligations as an insured endorsement
- Regulatory Coverage Enhancement Endorsement – CCPA and GDPR
- Technology errors & omissions coverage (selectable)



## Who is covered?

Coalition's Cyber policy coverage extends to:

- The company listed on the insurance policy
- Any majority-owned subsidiaries of the insured company
- Senior executives\*
- Employees\*

\*Senior executives and employees are covered so long as their actions are in the normal scope of a company's business operations.

## Eligibility

Any US-based company (with a principal business address in the US) within a covered industry, and with revenue below US\$1 billion is eligible to purchase insurance coverage from Coalition. At this time, we are unable to provide coverage to companies in certain industries such as:

- Payment processors
- Data aggregators
- Casinos & gaming
- Cannabis/marijuana (anything with 'direct touch' such as growers, harvesters, dispensaries, and retail), among others

The following classes are also excluded:

- Gambling
- Adult Entertainment
- Social Media
- Cannabis
- Managed Service Providers (IT Vendors)



Coverages

## Coalition Insurance Coverages

### 1st party coverage vs 3rd party coverage

- A 1st party coverage pays the insured for covered losses they incur to recover from an incident. In other words, direct losses to their company (the 1st party).
- A 3rd party coverage pays for any damages to a 3rd party that the insured is liable for resulting from lawsuits—often filed by customers, vendors, or the government following an incident—as well as the costs to defend them.

### 3rd Party Liability Coverages

Network & Information Security Liability

Regulatory Defense & Penalties

Multimedia Content Liability

PCI Fines & Assessments

Coalition covers the expenses to defend any business and any damages resulting from its 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 its security, data breach, or privacy violation.

Bodily Injury & Property Damage

Technology Errors & Omissions

Coalition pays for the costs of defense and damages from a business' liability to a 3rd party when a failure in its security results in physical damage or injury.



## 1st Party Liability Coverages

Bodily Injury & Property Damage

Pollution

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

Computer Replacement

Coalition covers the costs to replace a business's computer systems that are permanently impacted by malware.

Fund Transfer Fraud

Coalition pays for funds transfer losses a business incur from a failure in its security or social engineering.

Service Fraud

Coalition pays for the additional amounts a business is billed by a cloud or telephone provider when it incurs fraudulent charges.

Digital Asset Restoration

Coalition pays for the costs to replace, restore, or recreate a business' digital assets that are damaged or lost following a failure of its security.

Business Interruption & Extra Expenses

Coalition covers financial losses resulting from a failure in a business' security, data breach, and even systems failure (including contingent/dependent BI), as well as the extra expenses it incurs to bring its company back online.

Cyber Extortion

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

Breach Response

Crisis Management & Public Relations

Coalition pays 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.



Coverage	Coalition	Others
Business Interruption & Extra Expenses	✓ see enhancements below	✗ sometimes
Contingent Business Interruption	✓	✗
Funds Transfer Fraud	✓	✗ sometimes (submitted)
Cyber Extortion	✓	✗ sometimes
Computer Replacement	✓	✗
Bodily Injury & Property Damage	✓	✗
Pollution	✓	✗
Service Fraud	✓ see enhancements below	✗
Network & Information Security Liability	✓	✓
Regulatory Defense & Penalties	✓	✓
Multimedia Content Liability	✓ see enhancements below	✓
PCI Fines & Assessments	✓ no submit	✓ submitted
Digital Asset Restoration	✓ see enhancements below	✓
Breach Response	✓	✓
Crisis Management & Public Relations	✓ see enhancements below	✓

Enhancements	Coalition	Others
Pre-claims assistance	✓	✗
Covers all prior acts	✓	✗ sometimes
Systems failure	✓	✗
Waiting period	✓ as low as 1 hour	✗ 8+ hours
Business services costs	✓	✗
Cost of system upgrades	✓	✗
Reputation Repair	✓	✗
BYOD coverage	✓	✗
Social media / IoT coverage	✓	✗ sometimes
Cybersecurity apps	✓	✗



## Policy Management

### Referrals/Secondary reviews timeline

Accounts/submissions with exposures that require additional investigation before providing a response need a secondary review. These exposures and triggers may include:

- Security concerns discovered by Coalition's technology and deep web scans
- Requests for limits of \$5M and above
- Companies with over \$100M of revenue/ratables
- Sensitive industries such as Cryptocurrency and Healthcare
- Prior claims history or knowledge of circumstances that could lead to a claim

When a submission triggers secondary review, Coalition seeks to make a decision on quote terms within 24 hours of submission. Potential decisions can include:

- Release of a Coalition quotation
- Declination (don't worry – this is rare!)
- Release of a Contingent quotation

### Why is the domain field important?

For generating a Cyber quote we ask for the insured's company website. If the insured does not have a website, please fill out the email address. Although optional, it is highly recommended. Here is why.

- **What is a domain and why do we need it?**
  - Consider a domain to be the digital address of a business's online presence. This includes all domains, subdomains, and IP addresses.
  - When a property insurer looks at physical locations, they look at buildings construction (bricks and sticks), sprinklers, if the building is located in a flood or earthquake zone, etc. This additional information allows the insurer to both underwrite and make recommendations to reduce the insured's risk (firewalls were a construction technique long before they were a thing in IT). Similarly, we use the domain information to holistically assess an insured's cyber risk.
- **How does adding a domain help you?**
  - Less chances of referral – Having complete information reduces the need for us to follow up
  - Accurate pricing – Accurate risk assessment on our part leads to a more accurate pricing



- Better protection against cyber attacks – Coalition offers tailored recommendations to improve the insured’s cybersecurity
- We ask for a complete list of the business’s domains because we need to assess the cyber risk of more than just the public-facing website. We need to look at the organization’s risk as a whole, and we need to do it entirely from the outside, just like a would-be attacker.

### **Policy Servicing (Endorsements, Cancellations, Reinstatements)**

- Attune Customer Care will handle all policy servicing, including endorsements and policy changes by submitting a request on the portal [support page](#).
- Brokers may also contact Attune Customer Care via live chat from 9am to 6pm EST Monday through Friday or via phone at 1-888-530-4650.

### **Billing**

- Attune provides direct bill for this product.

### **Reporting a Claim**

- Policyholders may report an incident or file a claim 24/7/365 online, within the policyholder dashboard, or by calling Coalition’s toll-free claims line at 1.833.866.1337.
- Once an incident or claim has been reported, the policyholder will be able to upload documentation relevant to the incident or claim directly from the policyholder dashboard. You may also track the status of the claim from within the dashboard as well.

### **Claims process and timeline**

- Coalition aims to pay out the claim thirty days after it is filed. To minimize delays, insured should report the claim as accurately as possible, provide all pertinent information, and respond promptly to the adjuster assigned to their claim.
- If a claim is submitted involving a 1st party claim or loss, the adjuster will make every effort to expediently estimate the loss. Following a final determination of coverage and confirmation of value of covered damages, the adjuster has the ability to approve up to 50% of first-party loss above any applicable retention and subject to the policy limits. Coalition will work with the insured to understand your situation and make additional funding available if at all possible.
- A final determination of payment will be made after coverage for the loss or claim is finalized between the insured and the carrier(s). Any time a determination of payment is made, insured will either be reimbursed, or amounts owed may be directly settled on their behalf (based upon their business needs) within five (5) business days.





[attuneinsurance.com](http://attuneinsurance.com)



YouTube

44 WALL STREET, FLOOR 22  
NEW YORK CITY, NY 10005