

## ACTIVE INSURANCE

# Frequently Asked Questions

## What is Active Insurance?

Active Insurance is cyber coverage offered with a cyber security platform designed to prevent digital risk before it strikes. It's a term we're using to describe the type of coverage Coalition provides today. Active Insurance combines the power of cybersecurity technology and cyber insurance to provide coverage that is built for the digital economy.

Active Insurance stands in stark contrast to traditional insurance, which we believe wasn't built for the speed and amorphous nature of digital risks, leaving many organisations unprepared for the modern realities of cyber risk to their business.

### Active Protection

Monitoring and alerting<sup>2</sup> to identify and prevent risk before it escalates

### Active Risk Assessment

Underwriting, quoting, renewals, and digital risk profiles<sup>2</sup> powered by real-time data



### Active Response

Incident teams<sup>1</sup>, In-house expert claims teams<sup>3</sup> and leading coverage if an incident occurs

Continued →

## Active Insurance: FAQ

---



### How is Active Insurance different from traditional insurance?

Coalition's Active Insurance goes beyond traditional insurance offerings, providing both brokers and policyholders with in-depth, personalised profiles of digital risk. Active Insurance provides cyber security technology and expert support before, during, and after a cyber incident occurs. Unlike traditional insurance, our Active Insurance product provides a business with continual risk assessment and monitoring<sup>2</sup>, along with rapid response by our internal experts to address risks that move at digital speed.



### Is there anything that's additionally required from the broker or policyholder to register or maintain "Active" status?

No. All policyholders get access to our digital capabilities<sup>2</sup>, coverage, incident response<sup>2</sup> and claims teams. Brokers have access to elevated resources and our team's expertise as well as a fast and efficient quoting and renewal experience. Through their Coalition Control dashboard, policyholders can monitor their customised risk assessment based on data provided to Coalition in order to keep on top of their business' changing risk profile. With Active Protection, policyholders also receive continuous alerts concerning any emerging risks and key changes to their risk as Coalition Inc becomes aware of them.



### How can my client maintain visibility of their changing risks?

Policyholders can access their personalised risk profile through Coalition Control™<sup>2</sup> at any time. The Control dashboard summarises the findings from Coalition's initial risk assessment and incorporates active threat monitoring updates. If there are any questions about the Coalition Control profile information, brokers can reach out to their local business development contact for answers and additional resources.



### Will my client's coverage or premium be affected by any mid-term security notifications?

Premium and coverage is not impacted by security notifications during the policy term. It may be affected by mid-term adjustments. All security alerts are intended to bring awareness and provide guidance on minimising risk exposures and loss prevention. While these alerts will not lead to any changes to coverage or premium during the policy term, an insured's failure to address critical vulnerabilities identified during the policy term may impact their ability to renew their cyber coverage with Coalition. Security notifications are aimed at keeping our policyholder's business safe from digital threats and the Coalition team<sup>2</sup> is always available to assist in quickly addressing identified risks.

Continued →

## Active Insurance: FAQ

---



### **Does Coalition access my client's network? Is all this information public?**

Coalition\* does not access a policyholder's network, instead we identify and assess policyholder risk through an outside-in approach using non-invasive techniques. Our powerful scanning technology leverages threat intelligence data to expose policyholder's externally facing risks and existing vulnerabilities. These scans rely on information provided during the application process, such as the company name and all their associated domain addresses. Automated scans then canvas publicly available sources and data from the dark web to identify exposures. Coalition views these risks from the adversary perspective, highlighting how potential vulnerabilities are viewed by a threat actor. The goal of the risk assessment is to identify where these risks exist in an understandable way and provide guidance on how to prevent future losses.



### **If there is a risk that is flagged within Coalition's Active Protection process, is there a time limit on when critical changes need to be made by the insured?**

Once a risk or vulnerability is detected on a policyholder's system(s), the policyholder is notified of any critical action or changes that may be required in order to address the identified risks. These notifications are intended to alert the policyholder and broker to risks or vulnerabilities that create exposure for the policyholder, which could lead to a claim. As your risk management partner, Coalition strongly recommends that policyholders closely review and address these risks in a timely manner to minimise exposure of a cyber event and claim. Our business development team and security support centre\* are available to provide help and guidance to our policyholders during the term of their policy.



### **Can my client get help from Coalition if there is a risk identified through Active Protection that needs to be fixed or addressed?**

Absolutely! Our Coalition policyholders always have access to a member of our business development team, underwriters, or security support team<sup>2</sup>. We are always here to help.

For any technical questions, we have an in-house team of security support and incident response experts<sup>2</sup> that can provide expertise when addressing cyber threats or vulnerabilities.

Continued →

## Active Insurance: FAQ

---



### How does my client get in touch with Coalition to report a claim? Has this process changed?

#### Cyber Policyholders

There are three ways to reach out to our Coalition team in the event of a cyber policy claim:

1. Contact our 24/7 hotline at 0808 134 9559
2. Sending an email to [claims@coalitioninc.com](mailto:claims@coalitioninc.com)
3. Connect with our live chat function from our website to talk to a Coalition team member



### What if my client needs help with implementing the security changes Coalition flags?

Through Coalition's [securitysupport@coalitioninc.com](mailto:securitysupport@coalitioninc.com) Coalition policyholders have access to a team of security analysts and consultants\* who can help review and guide policyholders on how to implement fixes to address risks or vulnerabilities that our risk assessment or monitoring process identifies. Our policyholders also receive proactive guidance from this team throughout the policy term aimed at identifying ways the policyholder can address risks and avoid filing a claim.



### Will my client get reports on activity or recommended changes throughout the policy term?

In addition to critical security alert emails, Coalition policyholders have access to view any recent activity through Coalition Control\*. Policyholders can view recent risk reports and receive guidance on their exposures and how they can be minimised. Coalition Control is also where policyholders will be notified of any further action that is required based on the nature of the alert.

\*Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel. <sup>2</sup>Services may be provided by Coalition Inc, an affiliate of Coalition Risk Solutions Ltd. <sup>3</sup>Claims services are provided by Coalition Risk Solutions Ltd and Coalition, Inc.