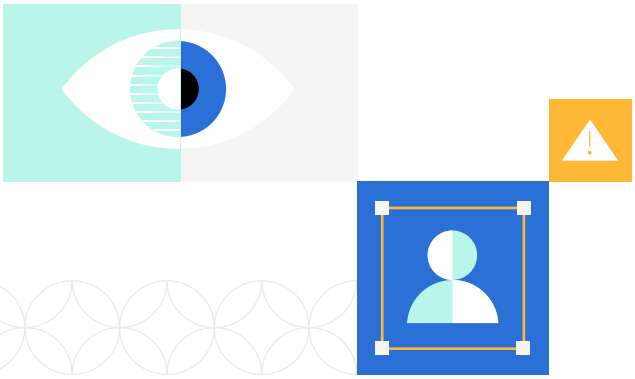
THE CYBER SAVVY BROKER'S GUIDE

Helping clients resolve security findings

Advise with confidence.

The best cyber insurance advisors proactively engage with clients by providing actionable guidance to help control losses, improve coverage, and stabilize premium.

Coalition helps you level up as a cyber insurance advisor by giving you the tools to confidently guide your clients through the complex cybersecurity and cyber insurance landscape. This creates powerful opportunities to turn difficult conversations about cyber risk into positive security and insurance outcomes for your clients.



Benefits of Proactive Engagement:

- Helping clients resolve critical exposures creates opportunities for positive engagement
- Help reduce the likelihood of frustration and stress of a claim
- Get the best protection and price for your client
- Improve client retention by making renewals faster and easier
- Build long lasting relationships with support throughout the policy period, not just at renewal

How to use this guide

At every stage of your client's cyber insurance journey — from the first quote to renewal — Coalition supports proactive engagement. This guide will empower you with the resources to confidently assist clients with **security findings** identified by Coalition's Active Scanning process, and use these findings to build stronger relationships with clients by helping to improve their security and insurability.

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **help@coalitioninc.com**

What are security findings?

Security findings are critical cyber exposures that are both discoverable in the client's environment and actively exploitable by threat actors. Coalition uses proprietary attack surface monitoring technology and real-time threat intelligence so we can provide each client with a customized view of the exposures that are the most severe and likely to be targeted. Every client can view security findings and additional technical details in their unique instance of Coalition Control™ (Control), our cyber risk management platform that helps clients actively detect, assess, and mitigate risks before attackers strike.

We think like a hacker to spot issues early.

So when your clients ask 'what does this mean?' you can explain how security findings are a leading indicator of the potential risks that could lead to a cyber incident or claim. These don't just make the organization a more likely target for bad actors but also impacts insurability and cost of coverage.

To learn more about how this benefits brokers and policyholders Explore Our Active Risk Platform.

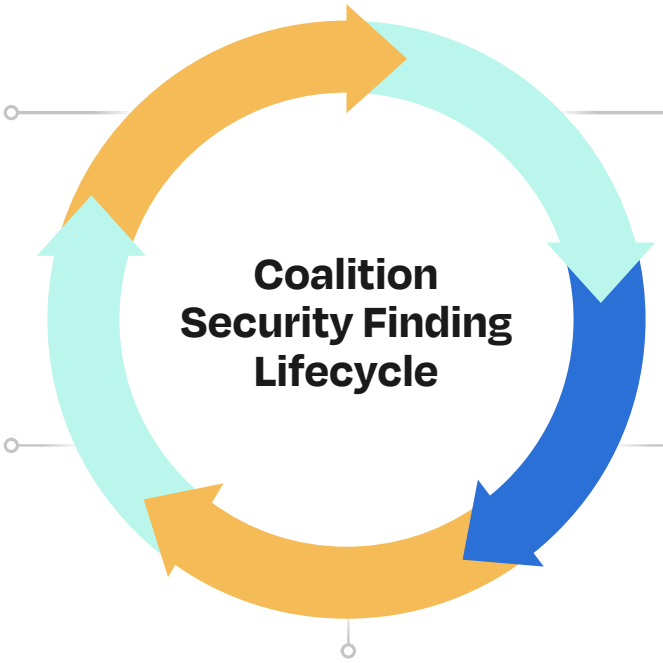
Common security findings

All security findings identified by Coalition's scanning align with one of these categories. Findings will vary based on the unique attack surface exposures of each client, but brokers can prepare by becoming familiar with some of the most likely and critical issues:

Microsoft Exchange: If your client is using on-premises Microsoft Exchange for email and calendar functions and making them remotely available, this creates a publicly discoverable and attractive point of attack for hackers.

Remote Desktop Protocol (RDP): This feature allows IT administrators and employees to remotely log into their corporate computers, but can also pose a significant risk. Threat actors often target this technology and exploit known vulnerabilities.

Open Risky Ports: Ports are essential to internet communication. Then the entire sentence would read: However, not knowing what ports are visible to bad actors or leaving misconfigured or vulnerable can create attractive attack vectors for hackers.



01. Active Scanning:
Attack surface scanning pre-bind, quarterly and based on threat activity

02. Detection:
Critical security findings identified, policyholder and broker notified

03. Review:
Your client reviews finding(s) in Coalition Control dashboard to determine validity, severity and next steps

04. Remediate:
Policyholder remediates findings, resolves false positives or implements compensating controls

05. Rescan & Close:
Your client submits attestation screenshot and/or initiates rescan in Coalition Control, finding closed and coverage bound

3 steps to help your clients resolve security findings

01. Review your client's security finding(s)

Supporting clients through this process starts by knowing where and when security findings are surfaced so you are prepared to answer questions, explain importance and help prioritize remediation.

Pre-bind security findings are identified in the Cyber Risk Assessment (CRA) and included as contingencies in all new business quotes; **Existing policyholders** receive alerts if security findings are detected throughout the policy period. Brokers also receive a weekly email digest of policyholders with critical findings that have been open for three (3) months or longer.

02. Educate your clients

Your role is not to fix security findings for your clients — it's to guide them to information and resources that make them less of a target for an exploit or claim. You don't need to guide alone. Use the Broker Resources page to find education and support resources that make it easy for you to help your clients through this important process. It is also critical to direct your clients to Control where they can find full technical details about security findings, expert remediation support and helpful resources to resolve each finding.

03. Resolve critical security findings

After remediation is completed, the final step is to make sure your client logs into Control to resolve all critical security findings by executing a rescan or submitting attestation screenshots. This step must be completed prior to binding a new policy and prior to renewal to ensure their most up to date profile is being reflected within Coalition's risk review.

Comprehensive protection from digital risk

Coalition offers a comprehensive cyber solution to protect your clients from digital risk. All Coalition policyholders access active monitoring and 24/7 security support, as well as additional resources. That's why our policyholders experience fewer claims compared to the overall cyber insurance market, as shown in our recent claims reports.

Make cybersecurity less daunting for your clients with **coalitioninc.com/control**

Still have questions?

Contingent new business quote:
Schedule a call with a Coalition Security Engineer

Existing policyholder or midterm security alert:
securitysupport@coalitioninc.com