CORVUS

Policyholder Experience

When purchasing a Corvus Smart Cyber or Smart Tech E&O policy, you're getting much more than insurance for a cyber incident.

You're getting the full backing of a team dedicated to making your organization safer across the policy term.

The Corvus Risk + Response team are cybersecurity, privacy and breach response experts whose singular goal is helping policyholders prevent and effectively respond to cyber incidents.

There are a few simple steps to take to get the most from the Risk + Response team. Review the steps below to get a sense of how we'll be working together.

Step 1

Get your quote

Get a view into your risk profile even before you're a Corvus policyholder. Thanks to the **Corvus Scan**, our proprietary technology for assessing cybersecurity risk, your quote for Smart Cyber or Smart Tech E&O includes a summary of your security posture: your overall cyber score, Ransomware Risk Score, industry benchmarks, and more. Plus, we'll notify you (and any other members of your team whom you'd like to sign up) if we find any **critical vulnerabilities** on your system so that your team can address them as soon as possible.

Step 2

Become a policyholder and complete your Policyholder Dashboard account setup

After working with your broker to select the right coverage, you'll be flying with Corvus! Soon after, you'll be invited to access your **Policyholder Dashboard**. There you'll find your most recent Corvus scan report available for download. Be sure to review the report and send any questions to services@corvusinsurance.com.

Step 3

Complete your vCISO Assessment

Navigate to the vCISO tab on your Policyholder Dashboard, our digital experience for exploring and improving cybersecurity. Complete a **five-minute questionnaire** called the **vCISO Assessment**. The assessment covers internal security controls and protocols at your organization that aren't visible to the Corvus Scan. Once completed, you'll see the **full set of findings** and recommendations on the vCISO page, indicating the highest-priority actions to make your organization safer.

Step 4

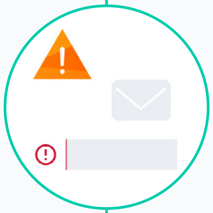
Engage services

With your vCISO complete, it's time to take action. The Risk + Response team offers complimentary and reduced-cost services to help you and your IT team improve your cybersecurity.

The Corvus Risk + Response team and select partners offer hands-on help with a variety of cyber risk management tactics and strategies. Visit our **Risk + Response services page** to see a complete list of options. You may request these services at any time through your broker or by emailing **services@corvusinsurance.com**.

Your vCISO assessment and responses may have identified specific controls that were lacking, such as multifactor authentication (MFA) or endpoint detection and response (EDR). Visit **corvusinsurance.com/vciso-services** to inquire about reduced-cost consultations..

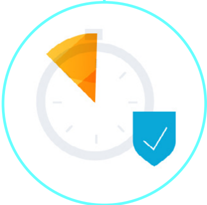
Note: We offer additional services for qualifying policyholders with over $100mm in annual revenue. If you qualify, your broker will provide information about these services.



Step 5

Receive ongoing alerts

Your Policyholder Dashboard will be **automatically updated** with new scan data quarterly, so we advise that you check throughout the policy term for any new recommendations. We'll also send you **Vulnerability Alerts** directly via email whenever we locate a critical vulnerability on your system or if we publish a general advisory about a cyber risk event such as a zero-day attack.



Step 6

Renewal

Before your renewal, we'll contact your broker and review your current cyber risk score to identify changes at your organization or broader risk factors that may have arisen. If your score appears likely to impact your renewal, we'll help you engage with services needed to make updates and have the strongest position possible before quoting.

Claims

While we take significant steps to reduce the risk of a cyber incident, no organization is completely safe. Should an incident occur, our claims team works with you to initiate contact with a privacy attorney to coach you through the process of responding to the incident. Read more about the steps of incident response **here**.