Calls from the Wild: Stories of Risk + Response at Corvus

At Corvus, our approach to working with brokers and clients on Cyber and Tech E&O accounts involves hands-on, expert cybersecurity guidance paired with technology that enables efficient service. Our proprietary Corvus Scan does the heavy lifting, shortcutting both the lengthy data collection process and analysis of the results. Then, the vCISO security questionnaire further homes in on risk areas and improves automated recommendations.

All of this means our Risk + Response team efficiently guides clients through prioritizing improvements to cybersecurity, and gets to spend the most time working with accounts whose questions or issues require an expert touch. Here are a few of the ways our approach helps clients become safer and more resilient.

Technology to Stay Ahead

Unlike "off the shelf" scans contracted from third parties, Corvus is constantly iterating and improving our Corvus Scan to meet the needs of the current risk environment. That includes alerting policyholders to the presence of software (or certain versions of software) that has been discovered to be vulnerable.

These alerts have real long-term impact: of those policyholders who patched a critical vulnerability during their policy period, the vulnerabilities Corvus alerted on were patched within 40 days on average while the others took more than 100 days.

These notifications come in addition to many other scan factors in a report provided upon binding a policy with Corvus, as well as quarterly during the policy term. The Corvus R+R team will walk through the report's recommendations with policyholders upon request.

> The vulnerabilities Corvus alerted on were patched within 40 days on average while the others took more than 100 days.

Corvus Risk + Response Manager
Adriana Perovic

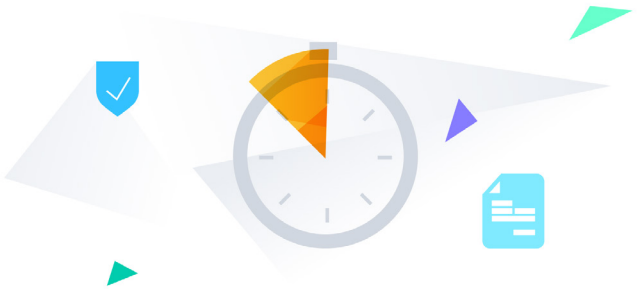
"I recently had a call with an insured discussing the results of their scan report, and how to best utilize our services. When the Policyholder later noticed a dip in their Corvus Score, they scheduled a follow up call. They hadn't realized this dip was due to the new Microsoft Proxyshell alert we are scanning for, which popped up on their latest report and resulted in a lower score. When I explained the change in score was due to that vulnerability, they acted. The team mentioned that it's unlikely they would have ever found the vulnerability without our alert! Upon re-scanning, their score went back to normal.

The company's CFO said that this is "a fantastic program that helps us to cover our bases with cybersecurity."

North American Healthcare Practice Leader & Chief Sales Officer at Hub International
Peter Reilly

"The insights that my healthcare clients get from the Corvus Scan are invaluable. During the quoting process, Corvus helped my client, a rural hospital, identify two open RDP ports and avoid a potentially devastating breach. This level of service is a significant value add in a hard cyber market and makes my clients treat me as their hero."

Timing is Everything in Security



To remain strategically defensive against threat actors, speed matters. When Palo Alto Networks (PAN) issued a security advisory regarding a critical vulnerability, our in-house security experts assessed the risk. As is the case in any zero-day, once the word is out, it's a race for organizations to patch faster than threat actors can feasibly launch an attack or gain access to their systems. Within 7 hours of the PAN news breaking, the R+R team had alerted all potentially impacted policyholders, while formal notifications from the U.S. CISA took another full day to appear.

Feedback from Alerted Corvus Policyholders

"Thank you very much for this information! What a great service. I've just submitted a ticket."
– SVP of Production, Construction/Contracting Firm

"Thank you very much for the notification, it is wonderful to know we have another layer of security awareness with Corvus."
– IT Manager, Logistics and Wholesale Supply Company

Hands-on Service

Because most cases are able to be quickly handled with information derived from the Corvus Scan, our team can dedicate extra time to clients with unique situations. One recent instance involved numerous meetings and messages back and forth — and some elbow grease from the Corvus Data Science team — to find a solution. The team discovered that an unpatched server was missed in prior analysis due to miscommunication between a client and their managed service provider. The broker on that deal, Ashley Ganne of Brown & Riding, says: "During this difficult time in the market, it is imperative to have a team like Corvus who is willing to take the time to help the insured dig into not only their system — but also the vulnerabilities brought by their vendors."

This can be unusual for some clients who aren't expecting this kind of service from a carrier, but policyholders and brokers alike benefit from a hands-on approach.

Corvus Risk + Response Manager
Fayon Atkinson

"I recently had a scan review call where the policyholder invited their IT consultant. The IT consultant was so appreciative of what we were doing — engaging in conversations about proactive measures — because none of his other clients' carriers talk to them until they have a claim, when it's too late."

Broker at Wholesale Brokerage

"Your services [in Risk + Response] have been requested specifically after I mentioned how fantastic our last call was! You all did a fantastic job explaining the purpose of the report and why it shows what it shows. [We] appreciate the expertise you add to these calls."