Cork Cyber Brings AI Remediation to the Software Stack, Automating the Work Others Can’t See

Cork closes 77% of eligible security tickets before a human gets there, returns dozens of technician hours a month to its partners, backs outcome with capital



BOULDER, CO, UNITED STATES, September 25, 2026 / EINPresswire.com/ -- Cork Cyber, the cyber risk intelligence, remediation and financial resilience platform built for MSPs, today announced the completion of its AI remediation loop, adding automated patching and vulnerability management to a platform that now spans 115 integrations across 11 categories. Cork also announced that it has expanded its Model Context Protocol (MCP) server so partners can query their own live cyber data from whatever AI tool they already use. The announcement marks the final leg of a two-year transformation. Cork began as a cyber warranty provider. It rebuilt itself around a harder question: whether an SMB is protected in the first place.

> “The dashboard era is over. We bring the data to the work, and we give MSPs peace of mind and the hours back.”
>
> *Dan Candee, CEO of Cork Cyber*

"Insurance prices risk, but it cannot change it. Security changes risk, but it cannot price it," said Dan Candee, CEO of Cork Cyber. "Cork does both, on the same telemetry, with capital behind the outcome. And we do it every day instead of once a year. We spot the gap, close it through the tools the business already runs, and pay if something gets through. That is the whole company in three sentences."

The time and the money

Manual patching and software vulnerability remediation is one of the largest hidden labor costs in managed services. Industry casework puts it at more than 60 technician hours a month for every 1,000 endpoints under management. Nearly 50% of the time, a full-time technician is doing nothing but chasing security gaps. Most RMMs patch operating systems and the most popular applications, browsers, PDF readers, natively covering a few dozen to a few hundred

titles. The software clients install runs far past that list, and most of the gaps it creates are already visible to tools in the stack. What they require is manual labor to remediate. That labor is what Cork automates: identification and remediation across more than 13,000 software titles, through Chocolatey and Winget, inside the RMM the partner already runs, with no new agent and no new console.

Within those RMM-based workflows, 77% of eligible security tickets now close before a human touches them. Each automated fix returns roughly $2.50 of technician labor, and the fixes run continuously.

"Cork secures not just the doors and windows, but also the dryer vent and doggy door. We see them across every building a partner manages, and closes and locks them automatically," said Candee. "Instead of handing a technician a list of 30 things to investigate on an endpoint, we handle 28 and hand back two. That is a far better use of highly skilled people. Time, security, and money, in that order. That is what we return, along with the peace of mind that the loop is running while everyone sleeps."

In April, Cork described its Auto Mapping release as the automation layer required to turn cyber risk visibility into scalable action. Today's release is that action. Automated Asset Analysis, Auto Mapping, Software Deployment Automation, and now automated patching and vulnerability management run the loop from detection to remediation inside the RMM a partner already owns.

Cork's open MCP server, expanded in this release, extends that philosophy to the data itself. Rather than requiring partners to adopt another dashboard, Cork makes its risk intelligence queryable from any MCP-capable AI tool a partner already works in, from detection through remediation to the financial outcome. For technicians, that means less switching between consoles and more direct access to their own data, in the tool where they already work.

"The dashboard era is over. A MSP's day lives in its PSA and its AI tool of choice, and no dashboard we could design would be perfect for a thousand different businesses," said Candee. "We bring the data to the work. Ask a question in the tool you already run, get your own live risk intelligence, act on it. More agency, in their hands, for less money. The best version of Cork is invisible until the moment you need it."

"Mapping was the foundation, and we said so in April," said Marcus Recck, Head of Product and Engineering at Cork Cyber. "Everything since, software deployment automation, automated patching, vulnerability management, are what that foundation was for. By combining the lenses of the individual tools in a partner's stack, Cork extrapolates risk signals no single product can see and now acts on them. Partners have already spent the money building their stack, and our job is to make that stack smarter, not tell them to rip it out. The loop from detecting a gap to closing it runs without a human in it for most tickets, and the MCP server means partners can interrogate every step of it from whatever tool they already work in."

The approach is drawing recognition beyond the partner base. Candee was named to Channel Insider's 2026 AI 50, alongside executives from Microsoft AI, AWS, OpenAI, Palo Alto Networks and Cisco, and Cork Cyber was named Pax8 Startup Vendor of the Year for 2026, recognition Cork attributes to the philosophy rather than the other way around.

Key capabilities announced today include:
• Automated patching and vulnerability management, completing the AI remediation loop from detection to resolution
• Patch coverage across more than 13,000 software titles through Chocolatey and Winget, versus the few dozen to few hundred titles most RMMs patch natively
• 77% of eligible security tickets closed before a human touches them
• More than 60 technician hours a month returned per 1,000 endpoints under management at full automation, with hours returned visible on the partner dashboard
• Roughly $2.50 of technician labor returned per automated fix
• 115 integrations across 11 categories, with the RMM as the source of truth
• Expanded MCP server access, letting partners query live cyber data from any MCP-capable AI tool
• Capital-backed outcomes on the same telemetry that drives detection and remediation

About Cork Cyber
Cork Cyber is the cyber risk intelligence, remediation and financial resilience platform built for MSPs. Cork connects across 115 integrations in 11 categories with the RMM as its source of truth. Cork attests that protection is genuinely in place across every client environment, closes the majority of eligible security tickets through automated remediation before a human touches them, returns the recovered hours to its partners, and backs the outcome with financial protection. For more information, visit https://corkinc.com/.

Daniel Delson
Magnitude, Inc.
daniel@magnitude-growth.com
Visit us on social media:
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/944934997

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.