halcyon

Case Study

Separating Clean: Milacron Builds Ransomware Resilience into Its Independence from Day One

Corporate carve-outs can create heightened cybersecurity complexity, particularly during IT separation. After Bain Capital acquired Milacron, VP of IT Jeff Mowry understood the opportunity to implement a next-generation ransomware solution. He chose Halcyon.

Milacron holds a distinction no other American company can claim: it is the last U.S. owned and operated manufacturer of plastic injection and extrusion molding machines. Its competitors are all overseas, in China, Europe, and Canada. That kind of singular position comes with a lot to protect. When Jeff Mowry, VP of IT, and Kevin Wilhelm, Global Director of IT Infrastructure and Operations, joined the company, their first priority was standing up an independent security org from the ground up, and doing it without disrupting a manufacturing business in the process.

A High-Risk Window Every M&A Team Know, But Few Plan For

The period between a corporate acquisition and full IT separation is a high-risk moment for cybersecurity. Networks and access controls converge, the security posture of the prior owner becomes, at least temporarily, your own. Mowry knew this from prior M&A experience, and he was unwilling to absorb inherited risk.

For Mowry, the principle was straightforward: he could only have full confidence in a security posture he had built himself. Inheriting an environment mid-transition, however well-maintained, meant inheriting assumptions he hadn't validated and configurations he hadn't set.

"I have a hard time having confidence in solutions I don't implement or have control over," he says. "That drove us to make sure we had something in place that we owned from day one."

Guidance from Bain Capital pointed in the same direction. Separation periods offer ransomware operators opportunity: gaps in tooling, overextended IT teams, environments in flux. Both Mowry and Wilhelm had dealt with ransomware events at prior companies, and neither was interested in leaving the question of ransomware resilience to chance during the transition.

"Better safe than sorry," Wilhelm says. "It felt like a smart play to add an extra layer, and Halcyon seemed highly focused on what its goal was. If ransomware gets through everything, all your defense in depth, and it executes and starts uploading

MILACRON®

Customer Snapshot

- Customer: Milacron
- Sector: Manufacturing
- Milacron's the last U.S. owned and operated manufacturer of plastic injection and extrusion molding machines, serving customers across medical, industrial, and various other sectors.
- HQ: Cincinnati, Ohio

Key Results

- Deployed and live during corporate window's highest-risk window, before IT separation was complete.
- Key material capture ran in detection mode from day one, ahead of final prevention tuning.
- Halcyon delivered unique, independent, ransomware-specific visibility from day one of the transition.
- Deployed across the full manufacturing environment, including OT infrastructure, with zero business disruption.
- Weekly customer success check-ins for five months, staying hands-on through every phase of the rollout.

keys, you've got a final fail-safe of being able to at least decrypt whatever had been encrypted."

Customers often describe Halcyon as an 'additional layer'. In the broadest sense, which is accurate. But the framing understates the distinction. Every other tool in a mature security stack detects, blocks, or responds to threats broadly. Halcyon is built for one outcome: if ransomware executes, it will not succeed. Key material capture is not a redundancy feature. It is the only mechanism in most environments that can help to recover systems when ransomware gets through everything else.

With the prior owner's security infrastructure still partially in place and full independence months away, Mowry made a deliberate decision to add a layer of protection his own team controlled, purpose-built for the one threat he was least willing to delegate.

"We knew that this is a high-risk time when you're separating companies for cyber risk. So we intentionally purchased Halcyon to give us that additional layer of protection."

Jeff Mowry, Vice President of IT, Milacron

"Even in Detection, It's Still Alerting Us."

Halcyon's ability to deliver value in detection mode, without requiring full prevention configuration first, was a critical differentiator for Mowry's situation. Milacron was a new environment for a new IT team; moving to prevention mode before fully understanding the business would have introduced its own risks. The ability to learn the environment and contain exposure simultaneously, while still capturing key material if ransomware executed, was exactly what the moment required.

"Sometimes moving from detection to prevention causes business impact," Mowry explains. "Not knowing the business at that point, I felt the time to reach a full prevention stance would be a lot longer than I was comfortable with. So, with Halcyon layered on, even though we were in detection only, we could still get the key, limit the damage, and at least recover."

During the TSA period, while the transition was still underway, Halcyon surfaced activity across the environment and provided Mowry's team visibility they owned and controlled independently. The team has since moved to full prevention mode, integrated Halcyon into the security operations center, and completed the separation on schedule.

"There were times where we would get alerts with Halcyon before anything else surfaced them," Mowry says. "Even in detection, it was still alerting us."

Deploy Without Breaking the Business.

Deploying a new security tool into a manufacturing environment while simultaneously standing up an entirely new IT organization required patience and precision. Milacron's factory floor runs on operational technology that has to be treated differently than standard endpoints, and Mowry's principle throughout the rollout was firm: deploy it correctly, or don't deploy it at all.

What made that discipline possible was the engagement from Halcyon's customer success team. Milacron met weekly with their customer success manager for approximately five months, with Halcyon's team functioning as a working extension of the Milacron IT team rather than a vendor checking in from a distance.

"You don't get that a lot with bigger companies," Mowry says. "We're a mid-size company, and Halcyon gave us the attention like we were a big company." The result was a deployment the business never felt. No escalations, no complaints, no incidents tied to the rollout. "Anytime we can introduce a new security tool into a business without the business complaining, that's a success," he says.

Presented to the Board. Built on Evidence.

Mowry has already briefed Milacron's board on Halcyon, presenting it as the ransomware-specific layer the company established as part of building its independent security posture from the ground up. The message he took to leadership is the same one he'd take to any peer asking whether EDR alone is enough.

"It's a good preventive solution. If today's AI gets through, it's an extra layer I would not go without."

With full independence now established and Halcyon integrated into the SOC, Milacron's confidence in its ransomware posture continues to build. A network segmentation project and firewall refresh are underway, part of a longer-term security program Halcyon supports without replacing.

"Our confidence levels continue to increase as we become more mature, as we stand out by ourselves. "We have confidence in Halcyon to not only help. Prevent something from happening, but also to recover quickly in the event that something does happen."

Jeff Mowry, Vice President of IT, Milacron

What Milacron's Approach Means for Manufacturing

For manufacturing organizations navigating ownership changes, infrastructure transitions, or rapid growth, Milacron's approach offers a clear model: don't wait for an incident to force the ransomware conversation. Build the layer that closes the gap before the gap becomes a crisis, especially during the moments your environment is most in flux.

"It's about defense in depth," Mowry says. "And this is that extra layer I would not miss.