



Case Study

ECMD

ECMD needed to address their rapid growth

As a building materials supplier for big box stores, independent lumber yards, and pro chains, ECMD has doubled in size over the past 5 years. However, this growth placed significant strain on ECMD's security posture and resources. Despite using both software-based safeguards and an MSSP, critical gaps still existed.

Steve Brown, VP-MIS, knew that monitoring the firm's cybersecurity health and managing ransomware risks were crucial to continued growth. In the wake of major events like Log4j, Colonial Pipeline, and SolarWinds, Steve was concerned his business was at increased risk from ransomware.

As Steve monitored his changing risk environment, he realized that the more sophisticated their IT operations became—and the larger they grew—the more vulnerable they were. He was unwilling to compromise on security, so he started looking for a vendor he could trust.

"[Security] is not a problem you can spend your way out of. No one can say they are 100% secure." For Steve Brown, Critical Insight's accessible offerings allowed him to budget for the right protection.

"We're IT professionals, but security is not our primary job. Critical Insight catches things we might not and investigates them with more specific skills."

Precise, value-oriented communication is a cornerstone of Critical Insight's services. For Steve in his role as head of IT, this approach to communication brings him peace of mind. "The notes Critical Insight send that explain their process, findings, and recommendations are so well written and rich. My strong impression is that your competitors aren't doing that kind of thing. It's the perfect fit for what we need."

At Critical Insight, we refuse to overload our clients with excess information, noise, or distractions. We provide information that's concise, effective, necessary, and timely.

Proactive service provided by top-notch talent is another cornerstone of Critical Insight. With our ties to education, we prioritize talent

education, retention, and prioritization. Staying on top of potential risks and investigating issues with real-time information makes all the difference, according to Steve Brown. "Speed of response is key. When Critical Insight catches an event quickly, that's their job and what they do."





“A comprehensive package offering is a primary differentiator of Critical Insight.”

The odds of them catching an event quickly around the clock is much more likely than what we could do. That turns the odds in our favor and lessens the risk and impact to ECMD.”

With a broader non-SOC offering that provides both prevention and

response to intrusion—something many competitors don’t offer—we demonstrate an ability to proactively reduce risk, conduct testing, and respond to incidents rapidly.

Confidence in cybersecurity empowers ECMD to scale its offerings, embrace opportunities, and grow in meaningful ways.