From Manual to Modern: Epicor’s Success with Kenna.VM

With Kenna Security, a global software company deploys Modern Vulnerability Management and builds a culture around risk reduction

Outgrowing Manual Processes

More than 20,000 organizations in 150 countries rely on enterprise resource management solutions from Epicor. The company is no stranger to complexity: With more than 45 years of experience, Epicor industry-specific software simplifies the complex workflows for manufacturing, distribution, retail and services industries.

But Epicor inevitably faced some complexity of its own. When Epicor acquired a new company, it acquired its IT environment as well, which led to multiple ticketing systems, or multiple instances of the same systems. All this complicated the task of scanning, tracking and remediating vulnerabilities.

This also resulted in the company’s existing vulnerability management (VM) environment couldn’t keep up. “We had a very manual operation requiring full-time effort by one or two of our security operations analysts,” recalls Tim Zeimann, senior manager of IT Security Operations at Epicor, describing a vulnerability management process based on CVSS scores and a homegrown prioritization tool. “Analysts would review the vulnerability scan output and try to rank items that need to be fixed, while identifying the top three to five things we wanted our group to fix that month. That was all done manually, by diving through spreadsheets.”

What was missing, says Zeimann, was accountability and visibility into the team’s progress. Business units were given a month to fix assigned vulnerabilities and it would be another month before anyone knew if the fix was made. Meanwhile, numbers-laden spreadsheets left senior executives in the dark about the team’s progress in reducing cyber risk.

To match the company’s pace of growth and to make meaningful strides in risk reduction, it was clearly time for an upgrade. The solution that ticked all the necessary boxes was Kenna.VM.

With Kenna, we're delivering so much more with so much less recurring effort.”

Tim Zeimann
Senior Manager of IT Security Operations
Early Wins Fuel Engagement—And Excitement

After deploying Kenna.VM to monitor and assess its growing ecosystem of applications and digital assets, Epicor chalked up an early win that not only helped team members see the value of risk-based VM, but it made risk reduction a team sport.

First up: make sure that Epicor wasn't compromised by high-profile risks, which Zeimann dubbed "critical headline vulnerabilities." Focusing on these vulnerabilities gave remediation to teams with an achievable first goal.

As the security operations team began onboarding members from various remediation teams, they assigned each team a Kenna risk meter, which measures the security risk posed by a group of assets. "It gave them a milestone of completion where they could actually get these risk meters down to zero," recalls Zeimann. "They had their first sense of accomplishment and said, 'Okay, we attained that goal. Now what do you need us to do?'"

That effort uncovered something else: how their automated patching process wasn't fixing all critical vulnerabilities targeted across more than 10,000 assets. Here again, Kenna.VM's risk meters allowed the team to identify and fix missed updates. "We started seeing a noticeable move in their risk scores because they were getting the automated patching to work," Zeimann explained. "So the net result was actually much greater than we first expected."

Driving Accountability Up And Risk Scores Down

The success of that initial effort had a ripple effect, notes Sean Carr, Epicor's senior director of IT Security Operations. "Clear, actionable risk meters allowed our business units to understand their priority action items and see the immediate result of their efforts," Carr recalls. "People have become accountable to their risk level."

With its self-service environment and risk meters customized by asset groups, Kenna.VM allows system owners to monitor their scans more frequently. "We've seen a huge difference in the past year where folks are clamoring to reduce their risk scores and make sure that they don't have the highest score within their sector," says Carr.

Delivering More With Less Recurring Effort

One of the biggest advantages from adopting Kenna's Modern Vulnerability Management solution has been holistic reporting. In the past, communicating risk reduction efforts to senior executives was a challenge. The security operations team did the best it could with its existing tools, but ultimately leadership was left sifting through piles of data that resulted in a murky understanding of VM efforts and even the company's risk posture.

That changed dramatically with Kenna Security. Now all of Epicor's infrastructure vulnerability data—whether in its data centers or in the public cloud—is visible through a single pane of glass. Pulling together a clear, comprehensive report that can be handed off to anyone, whether fluent in IT or not, is simple and fast. Reports that once took an average of 30 days to compile are now available in as little as two hours.

And the leadership is loving it. "After Tim initially showed me some quarterly metrics tracking how many vulnerabilities our team closed and how many remain, I really wanted to see more," recalls Epicor Chief Information Security Officer (CISO) John Van Hoogstraten. "With segmented risk meters showing progress across all aspects of our infrastructure, I can now go to other C-level executives and board members and demonstrate the progress we're making in reducing risk. And for the first time, everybody understands what I'm talking about."

And those analysts who used to spend the majority of their time compiling reports? They're still hard at work, but now they're focused on fine-tuning scanning capabilities to ensure asset owners and managers get the most timely results possible.

Epicor rallied around risk—and around Modern Vulnerability Management. The result? A more efficient, holistic and accountable approach to VM. And that's progress anyone can understand.