



Peter Evans and Xtract One were featured on SecurityInfoWatch on March 9, 2026.

Feature Summary: Peter Evans, CEO of Xtract One, was featured in a SecurityInfoWatch article entitled, “Why Security Leaders Are Rethinking the Security Triangle.” The piece, presented in Q&A format, features an interview with Peter discussing the key points of Xtract One’s recent white paper, including how advances in AI and sensing technologies are prompting facilities to reconsider long-standing trade-offs between ingress speed, detection accuracy, and threat identification. Peter begins by explaining why the traditional “security triangle” was adopted, noting, “All activities are constrained when an organization is trying to optimize for multiple objectives. In software development, engineers will often say that there is a balance between quality, cost, and development time, and that you can optimize for two, but not three.” Peter elaborates, sharing that, “This is true of physical security, and true when further constrained by the limited capabilities of traditional solutions that were built to solve a different problem 50 years ago.” The Q&A continues, and Peter reflects on how legacy systems have forced facilities to choose between increasing sensitivity and being overwhelmed by false alerts that slow the ingress experience, or reducing sensitivity and risking missing smaller threats. Later in the piece, Peter addresses a few common misconceptions that system operators still have about AI’s role. He states, “The biggest misconception is that AI makes security autonomous. AI transforms what humans do, not whether humans are necessary. The technology provides better information, but it’s still up to humans to evaluate the threat assessments, determine responses, and execute the appropriate security protocols. The difference is operators spend time on actual security work instead of alert management.”

The article continues, and Peter highlights the operational impact and cost of false alerts, along with how AI can address these challenges. He notes, “Every false alert consumes operator attention, disrupts traffic flow, and often requires secondary screening... Multiply that across thousands of daily screenings... For mid-size facilities, false alert management costs reach six figures annually in wasted labor alone.” Peter further explains that AI allows operators to focus on assessing actual threats rather than managing false alerts. The article concludes with Peter’s reflection on the larger shift, where security leaders question long-standing trade-offs and focus on technologies that deliver actual results. He asserts, “The conversation about the security triangle misses a bigger point: we’ve been optimizing the wrong thing for 50 years... the triangle was always a symptom of inadequate technology, not a security principle.” Peter wraps up the Q&A by discussing the future of the security triangle, advising, “The security triangle is cracking. What comes next depends on whether the industry has the courage to move beyond compromises it’s accepted for too long.”

Outlet Summary: SecurityInfoWatch.com is the leading resource for professionals in the physical and electronic security industry. It delivers in-depth analysis, breaking news and original reporting that security executives, systems integrators, consultants, service providers and manufacturers rely on to stay informed and competitive.

Outlet Social Media:

Facebook: [@SecurityInfoWatch](#)

X (Formerly Twitter): [@SecInfoWatch](#)

LinkedIn: [@SecurityInfoWatch.com](#)

YouTube: [@SecurityInfoWatch](#)

Feature Links:

[SecurityInfoWatch](#)

[LinkedIn post](#)

***JMG is monitoring for the Q&A to be featured in SecurityInfoWatch's newsletter, Frontline, and will share once it's live.*