RSAC 2017 in Retrospect

Hal Lonas | Chief Technology Officer | Webroot

The RSA Conference in San Francisco remains the premier event for the security industry. The sheer size of the event and the efforts vendors make to stand out amongst over 600 peers can make the RSAC experience a bit overwhelming. And with 40,000 attendees cramming every part of the venue, it's hard to even get your bearings, let alone figure out what's really worth paying attention to in our industry.

In speaking with some of the Webroot team members who attended the conference, it was clear that we all had different responses based on our respective fields of expertise. The one takeaway we all agreed upon, however, was that RSAC is ultimately more of a marketing conference—at least, that's true of the exhibit floor. Throughout, there were big flashy booths, crazy designs, demo screens, and, of course, industry jargon in delightful font treatments meant to dazzle and draw the eye.

During the conference, I hosted booth presentations on distinguishing between the hype and the real deal, and I could see from the questions I received that knowing the difference continues to be a challenge. The most frequently pushed buzzwords were "next generation" and "AI." Like many of our competitors, Webroot has also promoted its products as next-generation security. It's a great marketing term (think: new, improved, FREE), but it's hard to define, which makes it easier to dismiss more or less as meaningless fluff.

Artificial intelligence (AI) is easier to quantify, but it's still a nebulous concept. Like "next generation," AI is used as a marketing hook for technology that meets the definition in only the broadest sense. And it's important to note that many organizations use the term AI synonymously with machine learning; although the latter would be more accurate, it doesn't sound as sexy or futuristic as AI.

Another response worth mentioning came from the Webroot Security Operations Center Manager, who found himself awed by the variety of vendors and options. He continually saw a common theme of consolidation, but didn't walk away convinced. He believes combining different vendor solutions to meet today's complex security requirements can be beneficial, and also stimulates innovation.

The third response I'll highlight came from our Threat Research team, who spotted a clever bait-and-switch at another vendor's demo. Supposedly, a piece of never-before-seen malware was stopped in real time, but the keen observer could see that the "new" malware files had been swapped for older, easily detectable samples. This experience underscored the need for caution and skepticism when attending such events, but then, threat researchers are well known for being a tough crowd.

Regardless of terminology or even methodology, it was clear at RSAC that the security industry is finally embracing approaches that are critical for any hope of identifying zero-day threats and polymorphic malware. In closing, I'll add one thing: Webroot does use advanced machine learning—you might even call it "artificial intelligence"—to secure the connected world against next-generation threats. (No, really. We actually do.)