Cybersecurity startups are proliferating, but sorting out what works and what doesn't is tricky

December 14 2015, by Russ Mitchell, Los Angeles Times

His reputation scorched by Edward Snowden, the former director of the National Security Agency is heading a cybersecurity startup that aims to shortcircuit data leakers, cyber warriors, terrorists and thieves.

Keith Alexander's new company, IronNet, is just one of dozens, possibly hundreds, of cybersecurity startups, a group that over the last couple of years has attracted nearly $5 billion in investments.

"It's the new hotness," said Alex Pinto, who runs the MLSec Project, an open-source cybersecurity outfit.

"There are so many startups out there you could not fall over and not hit one," said Eric Schou, director of product marketing for security at HP Enterprise.

Like many others, IronNet employs a technology called behavior analytics or behavior modeling, which purports to learn hacker patterns and monitor networks to detect foul play before serious damage is done.

Whether any of these startups can effectively employ what looks like cutting-edge technology is hard to say, because, like cybersecurity in general, their doings are wrapped in secrecy.

Good luck to any potential customers trying to sort out what works and

what doesn't. Cybersecurity websites are filled with fancy technical language with little detail.

IronNet, for example, says it offers "breakthrough, patent-pending technology" with "complex behavioral modeling, big data analytics and proactive responses." One company says it uses "hyper-dimensional security analytics," while many companies don't bother to explain how their systems work at all, at least not until you contact the sales rep.

(Asked for clarification, an IronNet spokesman issued this prepared statement: "IronNet's approach merges a team with unmatched cyber experience with the latest in analytics and advanced computing. This unique combination has provided a new level of threat detection for IronNet's initial set of customers and already has a demonstrated record of proven success.")

Behavior analytics is "a big deal" for cybersecurity, said Avivah Litan, vice president at research firm Gartner. "But it's already a buzzword. Everybody says they have it."

As an idea, behavior analytics is powerful: Machine-learning programs analyze the normal operations of an organization's data systems - computers, and the humans that use them - and sound an alert when something looks fishy.

Simpler versions have been used for many years, with some success, particularly useful for uncovering financial fraud. But monitoring individuals who shunt around a company's money is trivial compared with tracking billions of pieces of software code streaming in, out and through computer networks.

"You get a lot of false positives," Litan said. "Companies are getting thousands and thousands of alerts a day."

"There is a lot of confusion," Pinto said.

By choice or necessity, the security companies don't want to reveal how their systems work, making it hard to know whether their systems work, until you've bought in.

The confusion, Pinto said, serves the companies' marketing departments. The software is complicated. The approach is "trust us." The explanations, he said, boil down to, "Because the math!" with the knowledge that most buyers don't have doctorates from MIT.

Machine learning is real. It works for clearly defined problems on which the machines have been trained. But how long before it's dependable and affordable and practical to perform behavioral analytics for cybersecurity is yet to be determined.

With a "rising threat" and "increasingly confusing technologies" to deal with it, top corporate executives need advisors they can trust, said Andrea Bonime-Blanc, lead cyberrisk governance researcher for the Conference Board, a research group funded by hundreds of companies.

Boards of directors, she said, are heavily populated by finance people and chief executives from other companies, "not tech people." She strongly encourages CEOs to recruit board members with strong technical skills along with an ability to think strategically.

She knows that's a tall order. Never mind board members: cyberskills are in short supply in just about any organization. There are 300,000 cybersecurity jobs unfilled in the U.S., she said.

So, for the moment, with all the cybersecurity startups advertising fancy-sounding technologies, how is a corporate executive or business owner to figure out what works? Product demonstrations won't cut it - each

company has its own set of needs.

"The best way is proof of concept," Litan said. That is, install the new systems, test them, find out if they work. But that only makes sense "if they can afford it," she said.

What about small businesses that can't? Strong passwords and crossed fingers may have to do, for now.