# The Whys and Wherefores of Innovation in the World of Cybersecurity

By Avani Desai

**Fifteen years ago the security market was much smaller with an eclectic mix of commercial and open source tools. Now we have a tidal wave of security vendors offering a staggering number of options. The article looks at the driving forces behind the vanguard in security and the new technologies that make up second-generation security solutions.**

Here we are in 2017, and it seems as if there is at least one new security firm filing papers in Delaware almost every day. Cybersecurity is a hot topic, with security threats and attacks increasing at a rate never seen before. This is creating a demand for fixes, and cybersecurity is big business with *CIO* magazine placing cybersecurity as one of their eight hottest startup trends of 2017.[1]

Fifteen years ago the security market was much smaller with an eclectic mix of commercial and open source tools. Now we have a tidal wave of security vendors offering a staggering number of options. This leaves security practitioners with a real problem: How do we balance the best of the new with the risks that our organizations face when we must consider legacy tools and infrastructure?

Fortunately, the security industry is helping us to solve this conundrum by bringing out new technologies. These technologies have been developed to replace first-generation security tools that relied on more closed infrastructures and a less distributed attack surface. These new generation tools offer a more intelligent approach toward dealing with a modern cybersecurity threat profile. Many of these new tools bridge the gap between modern working methods and legacy systems.

The article looks at the driving forces behind the vanguard in security and the new technologies that make up second-generation security solutions.

## Opportunities driving cybersecurity technologies

The explosion in security technologies is a reaction to the explosion in security threats. This is driving the market with vendors and investors alike wanting a piece of the cybersecurity pie, which has resulted in an increase in security spending—Gartner points out the market spend on security in 2016 being around the $82 billion mark.[2] And this spend is expected to increase markedly, with analysts Cyber Security Ventures forecasting the future cybersecurity market will be worth over $1 trillion by 2021.[3] These sorts of figures attract investment, and the first ever Cyber Investment Summit[4] was held last year in New York.

This is translating into vendors focusing in on certain trends and areas of technology to build a product to meet the changing security needs of commerce. The eyes of software design-

1 James A. Martin, "8 Tech Startup Trends to Watch in 2017," CIO, Nov. 30, 2016 – http://www.cio.com/article/3145457/startups/8-tech-startup-trends-to-watch-in-2017.html.

2 Gartner, "Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016," Gartner Newsroom, August 9, 2016 - http://www.gartner.com/newsroom/id/3404817.

3 Cybersecurity Ventures, "Cybersecurity Ventures Predicts Global Cybersecurity Spending Will Exceed $1 Trillion from 2017 to 2021," Cybersecurity Ventures – http://cybersecurityventures.com/cybersecurity-market-report/.

4 2017 Cyber Investing Summit – http://cyberinvestingsummit.com/.

ers and developers are not only on openings created by new technology paradigms, such as the Internet of Things, but also by new ways of working. This combination of technology and human ecology is bringing with it new cybersecurity attack vectors too—creating a circle of supply and demand. The security ducks are lining up to create a perfect landscape for cybersecurity good guys to take on cybersecurity bad guys with new and effective products.

The areas that are driving innovation in cybersecurity include the following.

**The complete deperimeterization of the enterprise:** The last 10 years have seen major changes in the way we work. Global Workplace Analytics[5] found that since 2005, non-self-employed, regular "at-home" working has increased by 103 percent. In other words, more of us work remotely. This change in the way we work brings with it technology challenges. How do you access your enterprise network remotely, being one such challenge. And when you do pop back into the office, do you use the same laptop you did at home? This has had the effect of breaking down the security walls previously used to keep the bad guys out. This area alone has opened enormous challenges: how to identify and authenticate a person across multiple domains, being just one example. This has opened market opportunities for security vendors who are developing solutions in the form of new security tools that can handle more complex policy challenges.

**Everything connected:** The Internet of Things (IoT) has taken off like a proverbial rocket. Industry sectors as different as agriculture and health are embracing the IoT and finding novel ways to increase productivity and lower costs. The downside to the IoT, however, is that some IoT vendors ignore the security knowledge and crank out shovelware that's vintage 1994. A second factor is the effect of creating a massively distributed attack surface for cybercriminals to take advantage of. The amounts of data and the complex life cycle of data being shared across multiple, disparate endpoints is a massive opportunity for cybersecurity vendors. In addition, the IoT is proving to be a perfect medium for DDoS attacks against commercial sites, as the Mirai botnet attack against the Dyn servers late last year testifies.[6]

**Compromise for an easy living:** Once upon a time, being a cybercriminal was hard work. You had to have a reasonable level of technical competence, and you usually had to know how to program. Now, cybercrime has entered the world of automation and is accessible to all. One of the greatest challenges of the security industry is the proliferation of "cybercrime-as-a-service" tools. The cybercrime "tools of the trade" have never been easier to use, with rental models springing

5 "Latest Telecommuting Statistics," Global Workplace Analytics – http://globalworkplaceanalytics.com/telecommuting-statistics.

6 Scott Hilton, "Dyn Analysis Summary of Friday October 21 Attack," DYN, Oct 26, 2016 – http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

up across the dark Web. And with 2016 and 2017 seeing greater numbers of malware appear than ever before,[7] cybercrime really does seem to pay. This onslaught of attack models with fluid and obfuscated malware signatures is yet another driving force for security firms to innovate in cybersecurity solutions.

**Extended supply chain:** A mix of globalization and Internet connectedness, including the IoT and cloud computing, has led to the supply chain becoming increasingly complex. Risk factors across the chain are forcing innovation to manage the wide scope of cybersecurity threats that can travel across the chain, impacting all members.

**Security policy updates:** As our working environment changes, the policies and legislation that cover the wider security arena are updating to accommodate those changes. Over the last two years several policy updates affecting privacy and security have been made. These include the NIST *Cybersecurity Framework*[8] updated in January 2017 and the executive order from the Trump administration on "Strengthening US Cybersecurity and Capabilities."[9] This executive order sets out the intention to look at ways of incentivizing private industry to adopt cybersecurity measures stating that:

> "All agencies shall comply with any request of the co-chairs to identify those economic policies and incentives capable of accelerating investments in cybersecurity tools, services, and software. "

## Which cybersecurity technologies are advancing these opportunities?

The opportunities set out above are driving innovation in several key areas in cybersecurity. Product designers and developers, as well as security consultancies, are focusing in on several of those areas, hoping to resolve the issues generated by the changes we are seeing in our work practices and technology. Below are some of the key technological innovations working towards cybersecurity threat resolution.

### Machine learning technologies/behavioral analytics

Machine learning algorithms are being deployed in several ways in the fight against cybercrime. One of the main applications of machine learning in cybersecurity is in event monitoring. Detecting events that are anomalies is often a way of spotting something untoward happening on a system. This may be malware becoming active on the system, or perhaps an insider threat coming to fruition. Without machine learning a human being must be skilled enough—and have enough time—to wade through the plethora of data to spot those anomalies. Machine learning algorithms, trained to identify unusual behaviors, are now being increasingly used to do this job.

One of the complaints about machine learning applied to cybersecurity is that it tends to throw up false positives. MIT has come up with a solution[10] to this using a mix of artificial intelligence (AI) and human interaction. The system, called AI2, uses machine learning to look through masses of data to find patterns, which it then presents to human operators who analyze those patterns. It has shown to be effective in spotting 85 percent of security breaches.

In the case of an insider threat, anomaly detection and trend spotting are even more subtle as it is often entitled users who are perpetrating the attack—being able to tease out legitimate events from illegitimate ones requires a layer of behavioral analytics.

There are a lot of companies working in machine learning and behavioral analytics as applied to cybersecurity. The companies are integrating AI and machine learning products directly into their commercial computers to offer advanced malware detection.

### Deception technologies

As antivirus software struggles to keep up with the increasing numbers of malware types, the new vanguard in malware prevention—deception techniques—is being used to fight "fire with fire" in the world of cybercrime. These are traps to catch a cybercriminal in the act. They are usually small pieces of code, or fake assets, left on a system that are strategically placed to entice and catch a hacker, sending alerts once tripped. Several companies are offering this type of new approach to preventing malware infection.

### Cloud access security brokers

In our new world cybersecurity order, we have two challenges that are compounding problems: one is the movement of services into the cloud, and the other is the lack of security talent. This is opening new solutions via security-as-a-service. Gartner predicts that by 2020 85 percent of enterprises will be using a cloud access security broker (CASB), but just

7 AV Test, "Malware" – https://www.av-test.org/en/statistics/malware/.

8 NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, January 10, 2017 – https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf.

9 "Read the Trump Administration's Draft of the Executive Order on Cybersecurity," Washington Post – https://apps.washingtonpost.com/g/documents/world/read-the-trump-administrations-draft-of-the-executive-order-on-cybersecurity/2306/.

10 Adam Conner-Simons, "System predicts 85 percent of cyber-attacks using input from human experts," MIT News, April 18, 2016 – http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418.

what does this technology offer? A CASB is a software application or "middle-man" that ensures your security policies are applied across the divide between on-premise devices and your cloud provider. A CASB will enforce policies around authentication, encryption, single sign-on, and tokenization to protect the security and privacy of data, following the NIST *Cybersecurity Framework*[11] protocols.

### Evolving alternatives to signature-based malware detection

Malware detection is becoming difficult because cybercriminals are becoming ever more aware of methods of avoiding detection. The recent Stegoloader[12] malware, which uses an obfuscation method known as steganography, is a case in point. To counter this, new technologies to detect malware are being developed. Solutions such as anti-exploit software can protect against the harm of online exploit kits, which are typically behind the drive-by-download phenomena of automated malware infection through browser-based vulnerabilities. Firms offer protection against malware infection through a community approach: endpoint detection being based on the output from security intelligence gathered across millions of endpoints. This is a very responsive approach compared to the older signature-based antivirus solutions. As it is, the protection of endpoints from malware is likely to be an ongoing and multi-layered approach, using machine learning, deception techniques, and alternatives like anti-exploit products.

### Browser isolation/remote browsing

With many of our security attacks entering through the window of the browser, this then seems a natural point to apply protection. Browser isolation, or remote browsing, places a browser session within a virtual machine, isolating it from the rest of the network. Even if a worker goes to a malicious site, any malware on the site will not affect him nor the rest of the network.

## Let battle commence

The past three years in the world of cybersecurity have been disturbing. According to an IBM/Ponemon Institute study[13] the average cost of a data breach for a US company in 2016 was just over $7 million, a seven percent increase over 2015—also a bad year for data breaches. Ransomware costs have also spiraled in 2016 with an estimated $1 billion paid out.[14] With cost levels of this magnitude hanging over our heads, we have little choice in turning to security vendors to help us. Thankfully, the industry is taking this seriously and building fit-for-purpose second-generation toolkits that will give us the means to take on the cybercriminals and win them at their own game. The mix of intelligent solutions, with an awareness and understanding of the tricks of the cybercriminals trade, will give us the ability to not be so many steps behind.

## About the Author

*Avani Desai is a principal and the Executive Vice President at Schellman. She has more than 15 years of experience in IT attestation, risk management, compliance, and privacy. Avani's primary focus is on emerging healthcare issues and privacy concerns for organizations. She may be reached at avani.desai@schellmanco.com.*

11 "Cybersecurity Framework," NIST – https://www.nist.gov/cyberframework.

12 Lordian Mosuela, "How It Works: Steganography Hides Malware in Image Files," Virus Bulletin – https://www.virusbulletin.com/virusbulletin/2016/04/how-it-works-steganography-hides-malware-image-files/.

13 "Cost of Data Breach Study," IBM Security – http://www-03.ibm.com/security/data-breach/.

14 Danny Palmer, "The Cost of Ransomware Attacks: $1 Billion This Year," *ZDNet*, September 8, 2016 – http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/.