


TAG

SecurityAnnual

2ND QUARTER 2024

IN FOCUS:



What Is the State of Cybersecurity Today?

ARTICLES / OPINIONS / INTERVIEWS



AN INTERVIEW WITH SEEMANT SEHGAL,
FOUNDER & CEO, BREACHLOCK

AN OFFENSIVE APPROACH TO CONTINUOUS ATTACK SURFACE DISCOVERY

Enterprise security teams have come to understand the importance of continuously monitoring their attack surface before the next potential incident occurs. With an offensive security strategy for continuous attack surface discovery and penetration testing, BreachLock, a pioneering cybersecurity firm, offers a novel approach to protecting your threat landscape.


In this interview, we highlight BreachLock's unique methodologies, strategies, and experiences, offering insights into their offensive approach to identifying and mitigating potential vulnerabilities in an attack surface. Our goal is for readers to gain useful ideas on dealing with this increasing need to view exposed cyber assets.

TAG: *Let's start with you sharing a little about what led you to found BreachLock?*

BREACHLOCK: After gaining experience at renowned global enterprises known for setting cybersecurity standards, I noticed a significant disparity in resource allocation between defensive and offensive security technologies. Upon analyzing the return on investment (ROI) from defensive versus offensive strategies, it became clear that offensive security consistently produced better results. For example, each penetration test identifies vulnerabilities and proactively addresses and closes potential entry points for hackers. So, I decided to delve into the reasons behind companies' relatively lower investment in penetration testing. Subsequent conversations ensued with multiple Chief Information Security Officers (CISOs) revealed an unmet need and gap in the market, with penetration testing methods proving inadequate for modern business requirements.

I identified four key shortcomings of traditional penetration testing: accuracy, agility, scalability, and cost-effectiveness, which stemmed from the fact that security tools operated on a point-in-time basis. Testing for system vulnerabilities was a singular event, typically conducted periodically or in response to impending audits or compliance requirements. At that time, the security industry had yet to develop the concept of continuous security. Human intelligence drove the existing offensive security landscape, while cybercriminals were already ahead of the game, using automated technology, and in some cases, AI, to scrape the internet for easy victims. Now, this battle is unwinnable without the use of technology.

Our automated algorithms and supervised NLP-based AI models help to refine BreachLock's proprietary Pen Testing framework.



That pivotal moment led me to address these challenges, culminating in establishing BreachLock in 2019 to pioneer the world's first full-stack Penetration Testing-as-a-Service (PTaaS) solution long before its widespread recognition or understanding. I conceived PTaaS to address the pressing demand for Offensive Security and a more continuous approach to safeguarding against an ever-evolving and expanding attack surface.

TAG: What is it about BreachLock that has catapulted you from a PTaaS start-up to a global cybersecurity leader in a short span of five years?

BREACHLOCK: Start-ups take two key areas for granted that ultimately make a difference to customers: the talent they hire and customer service. In recent years, a recurring pattern has emerged within the cybersecurity sector—a succession of startups buoyed by investor enthusiasm embarked on aggressive hiring sprees, often overcompensating employees to showcase rapid growth. This strategy, aimed at appeasing investors and projecting stability, ultimately proved unsustainable. When investors clamored for substantial returns and consistent revenue growth, these companies' unrealistic targets culminated in inevitable staff reductions.

I had no desire to entangle my company in the complexities of managing millions in investor funds or relinquish the autonomy to steer it according to my vision. Consequently, I chose to bootstrap BreachLock during its inaugural year. Then came the unforeseen challenge of COVID-19, where I couldn't meet my team face-to-face for the initial year and a half. Despite these obstacles, we surpassed \$1 million in revenue and witnessed expansion and growth, which became part of our initial success story. Our commitment extends to investment in innovative technology, sales, and customer service personnel.

At BreachLock, we recognize the importance of laying a robust foundation with our clients, dedicating ample time to establishing clear, tangible metrics that reflect an organization's security performance. In today's landscape, clients seek more than just security solutions—they require the ability to articulate a genuine return on investment to their executives and boards.

TAG: How does continuous attack surface discovery benefit from an offensive approach? Is being proactive a major component?

BREACHLOCK: Yes, a proactive or offensive approach is at the center of attack surface discovery. Continuous attack surface discovery is the ongoing assessment and monitoring of security controls, configurations, and potential vulnerabilities across the surface. This approach relies heavily on security automation, continuous monitoring, and integration as key enablers.

The idea of continuously monitoring the attack surface is born, once again, out of necessity. With the rise of automation and integrated security tools, it is no longer a wish but a viable part of an ongoing and proactive cybersecurity process focused on identifying and monitoring potential attacker entry points in an enterprise's digital environment. This approach involves constantly assessing and analyzing assets, networks, and systems to detect new or changing attack surfaces for weaknesses and exposures.

TAG: How is your platform designed and integrated with your offensive security solutions? What makes your platform different from your competition?

BREACHLOCK: BreachLock has conducted continuous security testing for over five years, performed thousands of penetration tests, and accumulated comprehensive knowledge of potential attack paths and Tactics, Techniques, and Procedures (TTPs) tailored to diverse technology stacks and contexts. Aligned with industry standards such as MITRE & ATTACK, OWASP, NIST, and OSSTMM, our automated algorithms and supervised NLP-based AI models help to refine BreachLock's proprietary Pen Testing framework. Integrated seamlessly into the BreachLock Platform, our framework safeguards precision and quality, automating routine tasks like report formatting, proof of concept integration, and basic vulnerability identification.

TAG: What future advances do you see in cybersecurity innovation? BreachLock already offers a unique AI/ML technology, so what's next?

BREACHLOCK: The future of cybersecurity has the potential for exciting developments, but one thing is certain: we will continue to face a never-ending battle against attackers and their increasingly sophisticated and covert methods. However, one significant trend likely to continue is the advancement of AI and ML in cybersecurity.

AI and ML technologies are already enhancing threat detection, automating responses, and identifying patterns indicative of cyberattacks. Over the next few years, we can expect these technologies to become even more sophisticated and pervasive. Conversely, attackers are increasing their use of AI to exploit weaknesses and launch attacks on systems and applications.