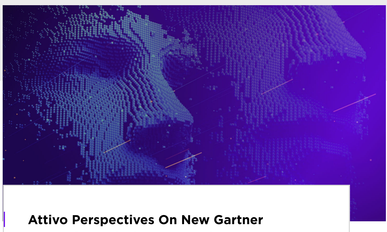

Attivo Perspectives On New Gartner Deception Solution Comparison

August 4, 2019
by SentinelOne

I am pleased to share that Gartner's newly released research report, Solution Comparison for Six Threat Deception Platforms is now available for subscribers. After months spent compiling research and product evaluations, the report goes into an extensive review on the breadth, depth, authenticity, and ease of use of deception platforms. I am very pleased with the outcome that points to Attivo Network's clear leadership in the space.

The report had 14 key criteria areas and ranked vendors from high, medium, low, to none. Attivo received 13 out of 14 high ratings, which is the highest score given to any solution. I am exceptionally pleased with the results. The report reinforces what we see in the market and in the growth of the Attivo customer base. Customers across the world and from all major industries have chosen the Attivo ThreatDefend platform for its comprehensive and scalable deception and because it can effectively detect and slow attackers regardless of the attack method used for lateral movement. The technology is uniquely designed to accurately and easily detect lateral movement including theft of local and domain credentials, network reconnaissance, Active Directory reconnaissance, and AD queries to find privileged domain credentials or target systems, exploitation attempts, misconfigurations, and Man in the-Middle attacks. The use of deception for insider threat detection of policy violations and misconfigurations is also quite common with over 40% of Attivo customers citing this as a top use case.

Fundamental to deception efficacy are attack surface coverage and believability. The ThreatDefend platform offers the **most authentic and credible deception through the use of "golden images" to project decoys and credible deceptive credentials that cannot be detected by tools like Honeypot Buster.** The solution also provides AD deception credential validations as well as time stamp updates so that an attacker cannot differentiate from the real credentials. Equally important, these credentials point to decoys that lead to a real OS that can respond and engage with the attacker to extract the full TTP inside of the management server's purpose-built 'sandbox'. Although using real applications and services is typically the preferred deployment method, in certain environments like IoT where emulation may be required, Attivo supports a wide variety of options as well as the ability to upload your own emulated images. Collectively, customers now have the ability to create decoys in any configuration that they wish.

The depth and the richness of the technology are essential to detecting advanced attackers who do not limit themselves to only one or two methods of attack.

Having the ability to scale with one platform across all attack surfaces ensures that customers won't outgrow their solution. Attivo provides the most expansive attack surface coverage, which easily scales across cloud environments, data center, remote and branch offices to suit the needs of both large and small enterprises. Machine-learning preparation and deployment make this extremely easy to manage from start to full operational capability. Additionally, Attivo offers the utmost flexibility in basic to advanced UI options as well as role-based viewing.

Going beyond the basics, Attivo not only provides the ability to achieve easy and accurate threat detection, but also delivers the flexibility to expand into additional use cases that uniquely include the ability to identify vulnerabilities and reduce attack surfaces, protect AD and redirected active attacks, and to automate the correlation of threat intelligence and incident response with over 30 native integrations further leveraging existing customer security investments..

Attivo's track record for being the deception platform of choice has been secured through both customer wins and bake-off's that yielded similar winning results to what was reflected in Gartner's research report. The report is a great validation to Attivo's technology leadership as well a useful resource in helping interested parties understand that deception solutions are far from similar and are definitely not equal in feature, functionality, or value.

Whether you are from a large or small organization or one with mature or basic security programs, deception provides a very easy and effective way to detect and shut down attacks from automated and advanced attackers. We look forward to the opportunity to share more about the overarching value of deception and why Attivo is the provider of choice for deception solutions.

I also invite you to check out other analyst perspectives on deception solutions. Please click here to view Cyber Source Data – Wellington Research deception vendor comparison and findings.

Read more about Cyber Security

- Protecting Domain Controllers from CVE-2020-1472 ZeroLogon and Other Zero-Day Vulnerabilities
- Detecting Unconstrained Delegation Exposures in AD Environment
- XDR Meets Identity Threat Detection and Response (ITDR)
- Top 10 Ways to Protect Your Active Directory
- Protecting Your Active Directory from AdminSDHolder Attacks
- Detecting a Rogue Domain Controller – DCShadow Attack