REPORT REPRINT

Attivo Networks' high-fidelity deception platform aims to fool attackers

DAN CUMMINS, ADRIAN SANABRIA

29 NOV 2016

The company's deception technology and platform are seeing a significant rise in market profile in 2016. Attivo offers a high signal-to-noise approach to detection, verification and attacker intelligence.

451 Research®

Attivo Networks' ThreatMatrix deception-based defense platform is designed to engage and fool attackers, thus providing security analysts with opportunities for real-time intelligence, as well as an automated means of shutting down an attack. Over the course of this year, Attivo and deception technologies have seen a significant bump up in market profile, as organizations seek early and efficient means to detect advanced threats. Attivo's platform, in particular, touches on several use-case categories, including detection, vulnerability management and analysis, controls and automation, and anti-malware.

THE 451 TAKE

Deception technologies generally, and Attivo specifically, have seen a significant rise in market profile this year. One reason for the bump is the typically low signal-to-noise ratio of traditional enterprise security systems, which spew tons of data and not nearly enough meaningful, actionable priorities. Attivo's platform is designed to do just that, while touching on important use cases for detection, verification, vulnerability management and analysis, controls and automation, and anti-malware. Potential customers appear to be catching on, recognizing the value of such breadth in the more cautious buying climate that has emerged this year, but we also note two other important benefits, which are attack verification and event prioritization. Attivo's method is eyes-on, as it were, to see and recognize critical behavioral signals among gobs of noise. We expect that network-based deception technologies will continue to rise in terms of relevance as a key adjunct to broad-based layered security, certainly in key verticals, and perhaps extending over the longer term to mainstream use.

CONTEXT

We sometimes hear that defensive security technologies need to adapt and play some offense, too. Offensive security includes capabilities and orientation to see and process intelligence and target opportunity data in the manner of an attacker. Target analysis is the focus of penetration testing, vulnerability management and attack simulators – each an area of intensified product and service innovation in recent years. Attack surface area has been broadly elevated to blatant conceptual risk, and technologies such as micro-perimeters can reduce and obfuscate application target profiles to very low levels. Network and endpoint targets are getting an upgrade as well, with deception technologies converting attacker data for active defense use cases.

Lack of dedication to improving contextual intelligence and work prioritization has come to the surface in the 2016 dialogue between customers and vendors. Vendors can look over customers' shoulders and see a range of underutilized commercial so-called 'solutions' – perhaps even their own. Deception technologies have evolved from honeypots and honeynets and are now mainstream in spots, such as a sandbox capability to overcome a malware's resistance to emulation.

As a product group, deception may have been, in recent times, mistakenly perceived as exotic or niche, likely to do well way above 451 Research's 'security poverty line.' Over the past five years, Attivo has accumulated an impressive reputation among Global 2000 and other companies with brand logos easily identified from the back of the room. In fact, though, the company is seeing accelerating interest and building profile among a very diverse group of customers, including non-Global 2000 firms, which constitute a substantial majority of Attivo's customers.

Initial deployments may be fairly modest, at roughly $50,000 depending on the number and capacity (i.e., VLAN coverage) of BOTsink devices and endpoints covered. The company's largest customers, however, deploy Attivo's platform for tens of thousands of endpoints, with impressive annual subscription commitments well into six figures. Attivo surpassed the 50-customer level in 2016, and has indicated live engagement conversations with more than 300 customers.

We believe the company could stay on pace in 2017 to more than double its customer base and approach $15m in sales bookings. Attivo's top verticals currently include healthcare, financial services, technology and energy. However, we believe any company with a vested interest in the competitive value of its intellectual property (or the business risk associated with its theft) will eventually mark some of the special capabilities of advanced deception technologies as worth real consideration.

LEADERSHIP

Attivo was founded in 2011. Disclosed external funding for the company totals $15m, including $8m in a series A round in 2015 provided by Bain Capital; the Board of Directors includes Enrique Salem, former Symantec CEO and now a managing director with Bain.

CEO Tushar Kothari came in to lead the company in mid-2013, about a year before BOTsink, a foundational part of the ThreatMatrix platform, was released to general availability. Prior to joining Attivo, Kothari was a consultant at Prism and Pacific Technology Partners. He is also a former VP of sales and general manager at Juniper and Cisco.

Srikant Vissamsetti is SVP of engineering for Attivo; he was a cofounder of IntruVert Networks, which was acquired by McAfee in 2003. At McAfee/Intel Security, Vissamsetti guided product development for the network platform, including behavior analysis. Another top Intruvert and McAfee software engineer and product development executive, Venu Vissamsetty, guides attack detection and analysis as Attivo's VP of security research.

Chief marketing officer Carolyn Crandall joined Attivo in 2015 from hyperconverged systems vendor Maxta; she previously held senior marketing executive roles with Nimble, Juniper and Cisco. Sarah Ashburn is SVP of sales, and previously held sales leadership roles at Symantec and VMware. Attivo's cofounders are executive VP and board member Mano Murthy, VP of product management Marc Feghali and VP of operations B.J. Shanker.

PRODUCTS

Attivo characterizes the market opportunity for its ThreatMatrix platform as one of continuous threat management, geared to early and high-efficacy detection, verification, and response to advanced external and internal threats. Attivo deploys out of band using a switch trunk port; components emphasize a lightweight yet comprehensive presence, authentic and dynamic behavioral deception, early and accurate detection capabilities, and scalability. Attivo competes roughly equally, we would say, on the basis of deception realism, detection accuracy and comprehensive capabilities.

By its nature, post-breach deception technology has to be able to detect and inform on attacks that were able to overcome other defenses. Attivo designed ThreatMatrix for detection and tracking, and indicates that customers derive strong value from their ability to follow, in a safe environment, attack steps and lifecycles, including lateral movement, privilege escalation, polymorphic obfuscation, and time-triggered strategies. The ThreatMatrix platform includes BOTsink engagement servers and decoys, ThreatStrike endpoint deception suite, ThreatPath for attack path vulnerability assessment, and Attivo Central Manager for larger deployments and threat intelligence.

Attivo's approach to deception is designed to facilitate simulation of user networks, endpoints, datacenter and cloud environments, industrial control systems, IoT and point-of-sale environments. Despite the company's comprehensive approach, setup is said to require only a few hours and typically does not result in a need for additional or dedicated staff, according to customer feedback indicated on the Attivo marketing hub. Attivo also indicates strong interest across its customer base for integration between Attivo and incident response activities. Out-of-the-box integrations with major perimeter, endpoint and SIEM vendors facilitate automated blocking and quarantine of attacks based on ThreatMatrix detection and analysis.

An additional console (ThreatOps, in development) will add bidirectional controls to bring Attivo's detection and verification capabilities to a wider security operations footprint, including attack intelligence sharing, playbook enhancements, attack scoring and threat hunting. BOTsink appliances and cloud instances are available in two sizes, depending on the number of VLANs supported. ThreatStrike deception objects may include credentials, browser cookies, ransomware bait with attacker engagement and file detainment, and email phishing (ribbon bar) icons for users to submit suspicious messages for analysis. The suite is sold by endpoint device.

ThreatPath calculates potential vulnerabilities associated with misconfigurations and misused credentials and is priced by endpoint, and complements Attivo's adversary tracker, which indicates attacker movement and associated timelines. Management reports good trajectories for average deal size and renewals; service terms are typically 12 months, but occasionally run to multiyear.

TECHNOLOGY

Deception is but one example of simulation technique applied to cybersecurity challenges; we believe security vendors leveraging simulation for a range of use cases may be on the cusp of breaking into wider view. Deception technology platforms have evolved from honeypots and honeynets to encompass a cross-section of techniques, including detection through simulation (i.e., deception), sandboxing, attack verification, attacker surveillance through engagement, automation, forensic analysis, and increasingly wider assimilation with production environments.

Attivo's BOTsink engagement (deception) server hosts the company's core Multi-Correlation Detection Engine (MCDE), which includes a network sandbox. Management contends that the design approach for MCDE provides for not only high-fidelity attack verification and drill-down inspection, but also vital integration with incident response activities, including forensics, compliance (e.g., chain of custody) and automation. The company indicates that some customers are also using MCDE to ingest artifacts from other sensors and detection systems. MCDE analytic output (including IOC, PCAP, STIX, CSV formats) can be viewed through Attivo's Threat Intelligence Dashboard or SIEM consoles, and used by prevention, isolation, or remediation workflow systems.

Components of a comprehensive deception setup include an engagement server and a diverse set of decoy lures (typically virtual machines) running over real OS instances, including network services, endpoints, credentials, data and file shares, servers, cloud environments and applications. Realism in decoy targets is critical, and includes attributes such as golden images of customized environments, currency and logical proximity to actual targets, and protection with similar fortifications. Recently introduced Camouflage is Attivo's branded framework for authenticity through dynamic behavioral deception, and it underscores the company's targeted edge in terms of breadth and depth for the platform's lures. Camouflage updates in field trials include automated self-learning for disparate environments, and continuous post engagement bait freshening (i.e., decoy respins) to avoid attacker fingerprinting and evasion.

COMPETITION

Deception and other simulation technologies meet a growing need for advanced behavioral-driven detection and analysis to improve, if not change, traditional network security, and not merely perimeter-based weaknesses. The deception product and services market is young and greenfield; proof-of-concept trials and exploratory discussions between vendors and potential customers outnumber deployments, deals in progress and head-to-head bake-offs by a wide margin. However, our sense is that the sales opportunity pipeline is expanding rapidly and will continue to fatten over the next 12-36 months, as customers in particular add their voices in support of deception technology's detection, verification and intelligence quality capabilities.

Attivo's best-known competitors with a primary focus on deception technology are TrapX and illusive networks – these startups have raised $19m and $30m of capital funding to date, respectively. Other startups with a deception technology focus include Cymmetria and TopSpin Security. Vendors with a wide range of core capabilities are also including deception capabilities as features (e.g., ForeScout) or are launching discrete deception-based products (e.g., GuardiCore, vArmour).

SWOT ANALYSIS

STRENGTHS

Attivo Networks' deception platform offers efficient, behavioral-driven detection and analysis to improve network security, including perimeter-based weaknesses. The company's forward-looking design and comprehensive approach address several use cases, including detection, vulnerability management and analysis, controls and automation, and anti-malware.

WEAKNESSES

We believe that Attivo faces marketing and company-building challenges in elevating the profile of its value proposition for datacenter, endpoint, cloud and valuable data assets as significantly more strategic than that associated with tactical deception techniques, such as honeypots and honeynets.

OPPORTUNITIES

Attivo is raising its marketing and sales profile in the greenfield market for deception technology. We believe the company has ample opportunity to invest growth capital and see rapid returns from proof-of-concept trials and an enlarged sales opportunity funnel. In addition, large and experienced customers could add their voices in support of deception technology's detection, verification and intelligence-quality capabilities.

THREATS

Deception technology remains a young market, and still lightly funded, relatively speaking. We expect the segment to attract VC and consolidators who may enter the market through acquisition. A diverse group of existing security technology vendors, with a wide range of core capabilities, are now including deception capabilities as features or are launching discrete deception-based products.