Ovum
TMT intelligence | informa

On the Radar: Attivo Networks offers deception, vulnerability assessment, and response automation

The ThreatDefend portfolio includes all these capabilities

Publication Date: 24 Jul 2017 | Product code: IT0022-001040

Rik Turner

Summary

Catalyst

Attivo Networks develops technology for threat deception, with products for network and endpoint, as well as threat visibility/vulnerability assessment and incident response. Its deception capability works across a company's user network, data center, cloud infrastructure, remote office/branch office (ROBO), industrial control systems (ICS), Internet of Things (IoT), and point-of-sales (POS) networks. Decoys can be made to look like a wide variety of targets, including a human-machine interface (HMI) device in operational technology (OT), an IoT node, or a POS terminal.

Key messages

- ThreatDefend can be delivered as an appliance, as software, or as a service.
- It has modules for deception (network and endpoint), vulnerability assessment, and incident response.
- Attivo's deception is dynamic in that it changes, updates, and adapts to make it more difficult for an attacker to detect that it is being used.
- Its incident response product enables the creation of playbooks and can also be used for threat hunting.

Ovum view

Deception technology is still a relatively new area within cybersecurity, yet Attivo has already expanded beyond it into other segments, including response automation, which bodes well for its future in this emerging market.

Recommendations for enterprises

Why put Attivo Networks on your radar?

Unlike other deception vendors, Attivo's offering extends beyond network- and endpoint-based deception technology into vulnerability assessment and response automation, going as far as enabling threat hunting. This makes it a significant contender for any project to refresh an enterprise's security infrastructure. Attivo stands out for the dynamic nature of its deception technology, while its combination with response automation puts its product ahead of the pack in this market segment.

Highlights

Attivo first came to market with deception technology and calls what it offers now "next-generation" deception, meaning it is dynamic, with authenticity going beyond simple emulations and low-to-medium interaction decoys. Its deception assets now run the same operating systems and software as production assets, authenticating and refreshing or respinning after engagement to avoid attacker fingerprinting.

This year Attivo added machine learning to automate the creation, deployment, and updating of decoys and lures, maintaining their creditability and attractiveness to attackers and making them unavoidable.

Attivo's product portfolio includes: BOTsink Deception, ThreatStrike Endpoint Deception, ThreatDirect for Segmented and Remote Office Deployment, ThreatPath Assessment, ThreatOps for Incident Response Playbooks, and a central console capability called Attivo Central Manager (ACM).

BOTsink Deception creates a distributed decoy system to lure in attackers' BOTs and APTs. It includes an attack threat analysis engine, providing automated attack analysis, a threat intelligence dashboard, and forensic reporting. BOTsink integrates with prevention systems including firewalls, network access control (NAC), endpoint protection platforms, and security incident and event management (SIEM) platforms to block attacks in an automated fashion and expedite response actions. It also enables customers to hunt for forensic artifacts in other parts of the network and confirm the attack has been eradicated.

ThreatStrike Endpoint Deception is an agentless platform that places deception credentials on endpoints and servers, making them look like authentic employee credentials, applications, CIFS shares for ransomware bait, and other data. It supports Windows, Mac, and Linux and updates dynamically to avoid discovery. The bait sets "breadcrumbs" that lead attackers to an engagement server where attacks can be analyzed and an alert raised. Attivo says that unlike behavioral analytics, these alerts are based on actual engagement, providing the detail required to block and quarantine an attack.

ThreatDirect for Segmented and Remote Office Deployment provides a mechanism for getting deception into micro-segmented networks or where a standalone box is not viable. It also works for small or remote offices.

ThreatPath Assessment provides attack path vulnerability assessment based on likely attack paths that an attacker would have traversed through misconfigured systems or credential misuse. Topographical illustrations provide insight into how attackers can move laterally once they have engaged with their first endpoint system. Clickable drill-downs provide the details of weaknesses and IP addresses for systems that need to be isolated and/or fixed, while integrations with prevention systems can be leveraged for automated response actions and trouble tickets can be activated inside the dashboard.

ThreatOps for Incident Response Playbooks is designed to accelerate incident response by automatically taking disparate attack information, and correlating and displaying it on a dashboard where attacks can be scored and playbooks created. The playbooks apply drag-and-drop customization based on an organization's specific security infrastructure and policies. Data collected from multiple sources including memory forensics can then be used to create repeatable processes to streamline and simplify incident response

A central console capability called Attivo Central Manager (ACM) manages the products in global deployments of the technology.

BOTsink operates out of band, attaching to the trunk port on a switch or as a virtual appliance in a datacenter, and does not therefore inject latency into the data path of legitimate traffic. It can be used against a variety of malware, including ransomware and polymorphic attacks, because malicious code is ensnared in a deception environment where it can be safely analyzed to prevent the attack from reaching, or becoming a pivot point to reach, production assets.

Background

Attivo Networks was founded in 2011 by EVP Mano Murthy, VP of product management Marc Feghali, and VP of operations BJ Shanker.

Murthy previously co-founded and held executive positions at Allegro Systems, Assured Access Technology, and Atlantec. Feghali held leadership roles at Cisco Systems, Echelon, 3Com, and Compaq, while Shanker was co-founder and director of operations at Allegro, and co-founder and VP of operations at Izspot. He has also held management roles at Cisco, Silicon Light Machines, NatSemi, and Amdahl.

Attivo's CEO is Tushar Kothari, who was previously CEO at Pacific Technology Partners, VP sales at NCR, EVP sales for Prysm, and SVP sales for Meru Networks and Juniper Networks. Tushar was also VP sales for Cisco and VP sales/GM for Linksys.

Attivo's engineering team is led by SVP Srikant Vissamsetti. Before Attivo, he was VP network security for McAfee/Intel Security. Venu Vissamsetty is VP security research and was previously director of software development for McAfee/Intel Security.

The company has so far raised $23m in two funding rounds, most recently announcing a $15m Series B round in May 2017, with participation from Omidyar Technology Ventures, Trident Capital Cybersecurity, Bain Venture Capital, and Macnica Networks.

Current position

Attivo brought its first product, the BOTsink Deception platform, to market in 2013. Since then, its portfolio has evolved, and it now refers to its product family as the ThreatDefend Deception and Response Platform, from which it can be modularly deployed and purchased as separate add-ons to the BOTsink.

- BOTsink Deception
- ThreatStrike Endpoint Deception
- ThreatDirect for Segmented and Remote Office Deployment
- ThreatPath Assessment
- ThreatOps for Incident Response Playbooks

Attivo declines to reveal its exact customer numbers, but says the entire deception market is currently somewhere around 250–350 enterprises; Attivo believes it is the largest player in this segment. Of its customers, 40% are in the Fortune 500.

In terms of the charging mechanism for Attivo's technology, the underlying ThreatDefend platform, which can be a hardware appliance or software, is acquired either via an upfront purchase price (capex), or can be delivered as a service opex). The individual products deployed on top of the platform come with an annual license fee based on the number of systems they are protecting (for example, endpoints, servers).

Attivo has already delivered solutions to address the anticipating attacker with real operating systems and golden image customization. In addition, what the company considers dynamic deception to overcome attacker avoidance and fingerprinting was released with its launch of version 4.0 earlier this year. On its roadmap, the company plans to enhance its capabilities in what it terms "advanced cyber warfare". This will include deceptions that cast doubt on the integrity of the data being stolen and will

provide mechanisms for data loss tracking (DLT). When asked about counter hacking, the company said that because of the legal minefield it represents for commercial entities, this functionality would only make sense for the military and intelligence communities. Its focus for the enterprise will be on creating ways to increase the cost and complexity of an attacker's endeavors, encouraging them to give up or move on to an easier target.

Data sheet

Key facts

Table 1: Data sheet: Attivo Networks

Product name	Platform: Attivo Networks ThreatDefend Deception and Response Platform Products: BOTsink (deception platform); ThreatStrike (endpoint deception suite); ThreatPath (threat visibility and vulnerability assessment); ThreatOps (Incident Response Automation); ThreatDirect (ROBO)	**Product classification**	In-network threat detection and response
Version number	4.1	**Release date**	Original: BOTsink (2013); ThreatDefend (2017)
Industries covered	Financial/insurance, power/energy, healthcare, government, entertainment, technology, retail, business services, telecom/utilities, insurance, transportation, hospitality, manufacturing, education	**Geographies covered**	Global
Relevant company sizes	Enterprise and government	**Licensing options**	Annual and multi-year licensing available
URL	https://attivonetworks.com/	**Routes to market**	Reseller and MSP channels
Company headquarters	Fremont, CA, US	**Number of employees**	103

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

On the Radar: Illusive Networks uses deception against cyber-attacks, IT0022-000923 (March 2017)

On the Radar: TopSpin adds IoT security capabilities to DECOYnet, IT0022-000886 (February 2017)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo