CHECKLIST

Attivo NETWORKS®

ASSESSING DECEPTION TECHNOLOGY SOLUTIONS FOR A PROACTIVE DEFENSE

INTRODUCTION

Attackers have repeatedly demonstrated they can evade an organization's conventional defenses. To remain effective, a modern Active Defense requires additional capabilities that fill the gaps not covered by traditional security controls. Deception technology focuses on in-network detection, closing visibility gaps, concealing sensitive or critical information, and misdirecting attacks away from production assets, thus giving defenders the advantage.

The following discussion takes a detailed look at what an ideal deception system should encompass, emphasizing how deception technologies can protect a production environment, with a checklist to help assess the options.

FACETS OF DECEPTION: CREATING A COMPLETE SOLUTION

Deception technology encompasses several interrelated components that protect the network, from typical decoys to concealment and attack redirection. Modern deception platforms deploy deceptive assets inside the perimeter to provide accurate detection of discovery, credential theft, lateral movement, privilege escalation, and data exploitation or theft. It provides timely and precise alerting to give the security team an advantage, letting them rapidly respond to an attack before it can escalate. It conceals sensitive or critical data production assets from exploitation, preventing attacks from progressing. It also redirects malicious attack traffic to decoys from engagement, deflecting attacks away from production systems. Modern solutions are easy to deploy and maintain and leverage machine learning for decoy authenticity.

Deception techniques cover several facets: endpoint, network, Active Directory, and the cloud. These realms complement each other to create a scalable enterprise-wide fabric. Each covers different aspects of the environment to increase the probability of detecting, preventing, and misdirecting an attacker early in the attack cycle. Having all facets of the deception fabric deployed will provide the most comprehensive and effective detection coverage.

On the endpoints, attackers frequently look for valuable information or user credentials they can leverage to move laterally – often targeting Active Directory or other authentication servers to further escalate their privileges. Deception platforms create highly effective fake credentials that lead an attacker away from production systems and into decoy assets. When properly integrated, these decoy credentials are indistinguishable from the real thing. A deception platform can immediately identify any attempt to use these fake credentials on a production or decoy asset as suspicious. In addition, decoy file shares, hidden from live users, provide an inviting target for an attacker and can serve as a sinkhole for automated attacks, such as ransomware that try to encrypt assets across the network. The platform can also configure, plant, and track decoy documents, providing an inviting target for attackers and alerts for exfiltration attempts.

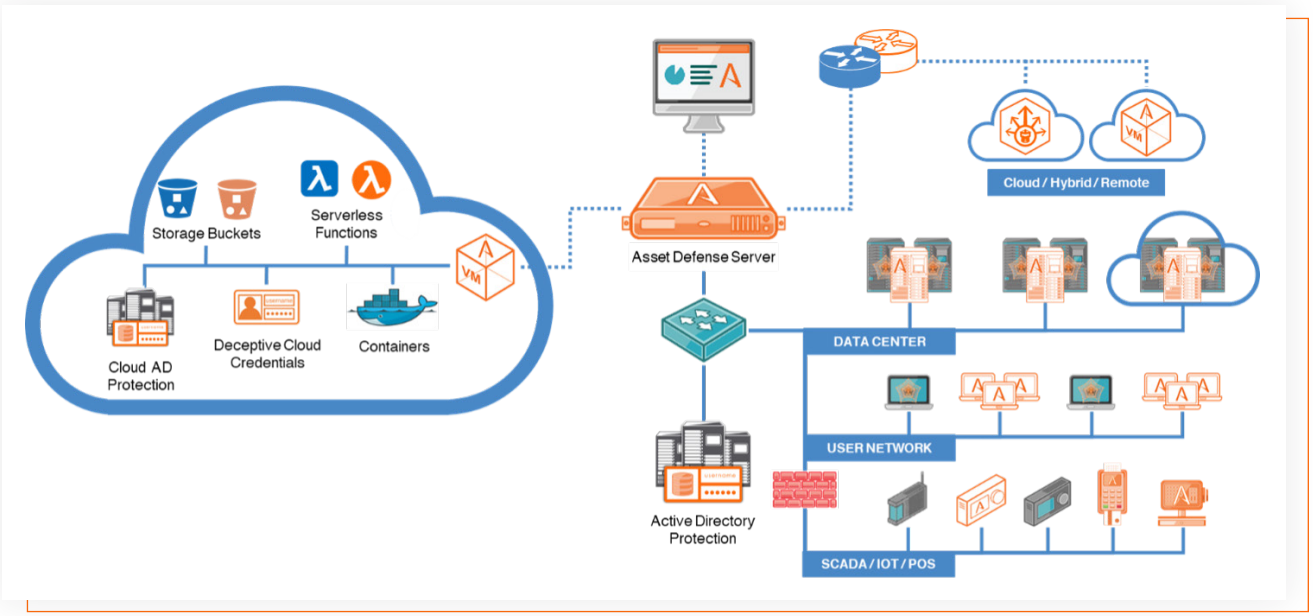
> "If an organization says they are not interested in deception, they are fundamentally ill-equipped to address modern adversaries and leave their organization willingly exposed."
>
> – CISO and Executive Advisor, Computer Networking Company

A powerful function within a deception platform is concealment, which provides the ability to hide and deny attackers access to sensitive or critical files, folders, credentials, network or cloud mapped shares, and removable storage devices on an endpoint, as well as privileged or important objects within AD. By preventing attackers from seeing or accessing these assets, defenders can derail their attacks, denying them the ability to exploit, steal, or compromise essential data and objects to progress their attacks.

Additionally, a full-featured deception platform can redirect attack traffic conducting port scans or attempting connections to production systems and forward them to decoys for engagement. This function misdirects attacks away from the production assets to the decoy environment, forcing the attackers to engage with the deception fabric. It generates alerts very early in the attack cycle during discovery and lateral movement activities. Here, the attackers unknowingly engage with the decoy, thinking it is a production system. At the same time, the decoy alerts on the engagement and records all attack activity for forensic collection and threat intelligence development.

A complete deception system ideally provides decoys for servers, services, and other assets across the entire operational environment, including the cloud. These decoys serve as targets for an attacker. If an attacker attempts to leverage stolen decoy credentials from an endpoint, they end up in the decoy environment, which monitors and records their activities. An attacker scanning the network for potential targets should encounter a decoy that responds realistically, offering services on a whole operating system environment, inviting compromise while drawing them away from production assets, whether in a datacenter, userspace or across an IoT or SCADA network. If an attacker compromises any of these decoys, it will respond as a live asset. A high degree of interaction assures an attacker won't easily identify the system or service as a decoy, enabling detailed forensics and efficient response from the InfoSec team for mitigation, remediation, and root cause analysis.

Deception platforms deliver clear and concise alert data to the information security team to efficiently respond to events. Along with its user interface, the ideal deception platform would integrate with other components of the defense architecture, including network, endpoint, and other monitoring systems. Native integrations that automate responses can dramatically improve the team's efficiency and response times. These combined capabilities lead to faster and more efficient incident response, improved adversary intelligence to identify potential targets and threat paths, and better overall security.



ASSESSING DECEPTION TECHNOLOGY

Not all deception technologies are created equal, and not all vendors deliver a complete solution to fill the gaps in a conventional defense-in-depth posture. When an organization is reviewing any cyber deception solution, there are some basic questions they need to address.

WHAT ENVIRONMENTS DO YOU NEED TO SUPPORT, AND DOES THE SOLUTION COVER THEM?

- Userspace networks?
- Datacenter networks?
- Device networks (IoT, OT, SCADA, ICS)?
- Cloud environments?
- Hybrid environments?
- Remote worksites?

HOW EFFECTIVE IS THE SOLUTION'S DETECTION?

- Against reconnaissance?
- Against stolen credentials?
- Against local or AD credential enumeration?
- Against activities targeting Active Directory?
- Against lateral movement?
- Against attackers "on the system"?
- Against malware propagation, including ransomware?
- Against local data discovery?

HOW COMPREHENSIVE IS THE DECEPTION OFFERING?

Deception lures are based on a variety of deception techniques placed on endpoints and servers and are used to entice attackers into engaging with the deceptive environment. To be most effective, lures should cover layers 2-7 with a regular refresh cycle.

- What type of deception lures are available?
  - Network
  - Server
  - Endpoint
  - Application
  - Data
  - Database
  - Cloud
  - Active Directory

> Deception technology provides a valuable addition to an organization's defense-in-depth posture by adding the means for an Active Defense.

- Are the deceptions static or dynamically updated?
- Can real credentials also be concealed, leaving only lures to be seen?
- Is machine learning available for automated preparation, deployment, and operations?
- What operating systems, applications, and services does the platform support out of the box?
- Can one create decoys from golden images?
- How easy are the lures to deploy and update?
- How much control does one have over the decoys?

HOW AUTHENTIC IS THE DECEPTION?

Decoy servers run real or emulated operating systems and services designed to lure attackers away from production assets. The most authentic decoys run real operating systems that the organization can customize to match the production environment.

- Are the servers running real or emulated operating systems?
- Are the decoy services real or emulated?
- Do the services match the production environment?
- Can one load a "golden image" or customize services to make the decoys indistinguishable from production servers?
- Can the decoys match device networks, such as medical devices, telecom, SCADA, or IoT environments?
- How easy is it to refresh the environment or rebuild after an attacker engagement?

HOW DIFFICULT IS IT TO DEPLOY AND OPERATE?

Different deception solutions have additional network considerations and offer a range of "environmental awareness" provided by machine learning to simplify deployment. How easy will this solution be to deploy and scale?

- Is the solution installed in-line or on a trunk port?
- If in-line, what network and compute changes must one address?
- If on a trunk port, how many VLANS can it accommodate?
- Do endpoint deceptions require an agent to maintain?
- Does the solution provide machine learning to analyze the environment and aid deployment?
- How much deployment automation comes with the solution?

> "Doubling the amount of gain that I have from my traditional security tools"
>
> – Director of Cybersecurity at Large American University

HOW WELL DOES THE ENGAGEMENT SERVER ANALYZE, IDENTIFY, AND REPORT ON ATTACKS?

- Can the system identify attacks without known attack patterns or signatures?
- How comprehensive, safe, and manageable is the analysis environment?
- Can the solution collect information from attacker Command and Control engagement?
- How comprehensive and usable is the available attack information?

- Depth and actionability of dashboard
- Clarity of information
- Detail drill down
- Role-based views
- Threat Intelligence gathering and ability to append with 3rd party information
- MITRE ATT&CK mappings
- Report formats: IOC, PCAP, STIX, CSV, etc.
- Native 3rd Party Integrations
- Automated or manual SIEM integration? Can it query the SIE for deception failed login?
- Integration with Firewall or Network defenses?
- Integration with Endpoint defenses?
- Integration with Patch Management, etc.?
- Integration with existing SOC systems?
- How accurate and detailed are the alerts?
- Can one customize alerts based on the level of attack found?
- How clear is it to quickly identify areas of most significant concern?
- Is the detail required for incident response and quarantining infected systems available?
- Are automatic or scheduled reports included?

> Not all deception technologies are created equal, and not all vendors deliver a complete solution to fill the gaps in a conventional defense-in-depth posture.

HOW DOES THE DECEPTION SOLUTION FIT WITHIN MITRE SHIELD

- Which tactics categories does it fulfill?
- Channel
- Collect
- Contain
- Detect
- Disrupt
- Facilitate
- Legitimize
- Test
- Of the 33 Shield technique, how many does it cover?
- Of the 190 Shield use cases, how many does it cover?
- How much forensics does the solution collect to provide learning opportunities as defined by Shield?

ATTIVO NETWORKS CYBER DECEPTION FABRIC

The Attivo Networks ThreatDefend® platform provides a customer-proven solution to prevent identity compromise, privilege escalation, and attack lateral movement.

The platform's cyber deception elements include data cloaking, misdirections, lures, decoy systems, and documents. The data cloaking function is a concealment technology, which derails attackers as they can no longer find or access the data, files, AD objects, and credentials they seek.

Additionally, the solution's lures and decoys work hand-in-hand to obfuscate the attack surface, collect forensic data, automatically analyze attack data, and automate incident response through its 30 native integrations. The platform provides the most comprehensive in-network detection solution, deploying a detection fabric that scales to on-premises, cloud, remote worksites, and specialty environments such as IoT, SCADA, POS, SWIFT, and network infrastructure.

The platform's identity security solutions deliver insight into credential and attack path exposures and Active Directory Domain, user, and device-level exposures for organizations seeking increased security based on least privilege access.

Machine learning makes deployment, operations, and scalability easy. Centralized management consoles make adding new functionality seamless while providing organizations the flexibility to add features at a pace that meets their business needs. Attivo deception customers include 50% of Fortune 10. However, over 65% of the company's customers are under 5000 employees, demonstrating the scalability and value of the ThreatDefend platform.

The ThreatDefend Platform modular components include the following:

- ADAssessor solution, which identifies AD exposures and alerts on attacks targeting it.
- Endpoint Detection Net suite consists of the ThreatStrike® credential lures endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement.
- Attivo BOTsink® deception servers provide decoys, gather attacker threat intelligence, and automates incident response with its orchestration playbooks.
- ThreatDirect deception forwarders support remote and segmented networks. Attivo Central Managers are available as management consoles.

> "Attackers only have to be right once, while security people have to be right all the time... Deception flips that paradigm... now the criminals need to be right all of the time too."
>
> - Director of Security Operations & Threat Management at Large Insurance Company

ATTIVO BENEFITS

- Most comprehensive and scalable solution on the market
- Most authentic deception environment where every decoy is a fully customizable OS VM
- Collects the most forensic data of any solution
- Easy to deploy, manage, and maintain using machine learning to automatically customize network, endpoint, and Active Directory decoy assets
- Provides the most coverage for endpoint, Active Directory, the cloud, and remote worksites
- Unique concealment technology protects production data beyond what other offerings provide
- Protects identities, Active Directory, data, and production assets across the entire enterprise
- Proven global professional services

The ThreatDefend Platform has been recognized as the industry's leading cyber deception solution since its inception. The company has won over 150 awards for its technology, innovation & leadership.

SUMMARY

The threat landscape is rapidly evolving and conventional defenses are often unable to keep up with the latest attack vectors and intrusion techniques. It takes more than traditional prevention defenses to outmaneuver and win against today's adversary. Deception technology provides a valuable addition to an organization's defense-in-depth posture by adding the means for an Active Defense. This will increase an organization's efficiency, improving reaction time, and reducing dwell time in the event of an attack. While not all deception technologies are created equal, this paper should provide useful benchmarks to evaluate and assess any deception technology vendor in question against an organization's business and environmental needs.

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. ThreatDefend® Platform customers gain unprecedented visibility to risks, attack surface reduction, and speed up attack detection. Patented innovative defenses cover critical points of attack, including at endpoints, in Active Directory (AD), in the cloud, and across the entire network. Concealment technology hides critical AD objects, data, and credentials. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys derail lateral movement activities. Attivo has won over 150 awards for its technology innovation and leadership www.attivonetworks.com