SOLUTION BRIEF

Attivo NETWORKS®

ASSESSING DECEPTION TECHNOLOGY FOR A PROACTIVE DEFENSE

EXECUTIVE SUMMARY

Attackers have repeatedly demonstrated they can bypass an organization's conventional defenses. To remain effective, a modern Active Defense requires additional techniques that fill the gaps in conventional defenses. Deception Technology takes a new approach focused on in-network detection, closing visbility gaps and altering the balance of power in the defender's favor .

This paper takes a detailed look at what an ideal deception system should encompass, with an emphasis on how deception technologies can protect a production environment, including a checklist to help assess the options.

FACETS OF DECEPTION: CREATING A COMPLETE SOLUTION

Deception technology encompasses several interrelated components that work together to protect the environment. Modern deception technology is deployed inside the perimeter to provide accurate detection of reconnaissance, lateral movement, credential theft, malware infection, and data loss. Timely and accurate reporting gives the security team an advantage, letting them rapidly respond to an attack before the attacker can escalate. It is easy to deploy and maintain and can efficiently scale up to enterprise level, supporting global deployment across a variety of attack surfaces.

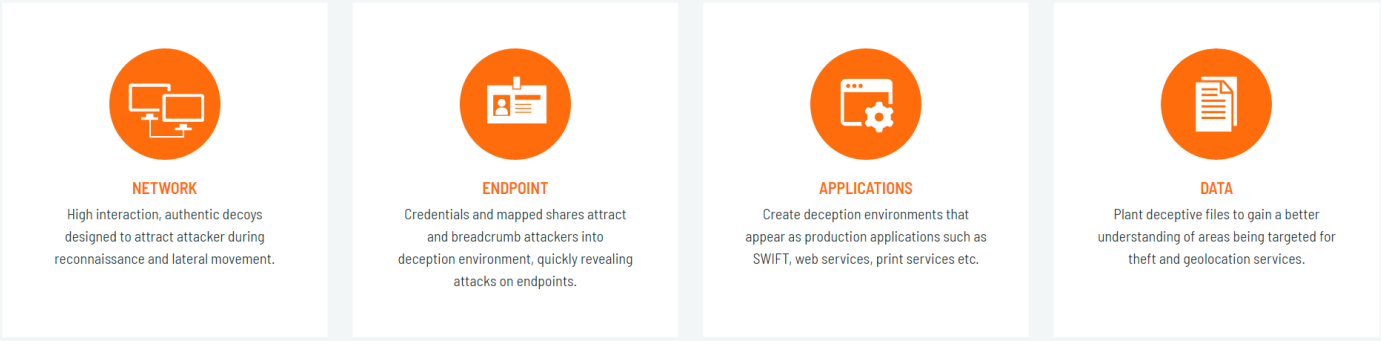
Modern deception technology is easy to deploy and maintain and can efficiently scale up to enterprise level, supporting global deployment across a variety of attack surfaces.

Deception techniques can be divided into two primary realms: Endpoint and Network. These realms complement each other, with each covering several, different, aspects of the environment to increase the probability of an attacker triggering one of them. Therefore, to detect threats from all attack vectors, it is critical to have both network and endpoint deception.

On the endpoints, attackers are frequently looking 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. That makes deceptive credentials, that lead an attacker away from production systems and towards decoy assets, highly effective. When properly integrated, these deceptive credentials are indistinguishable from production credentials and any attempt to use them on a production or decoy asset would be immediately identified. 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. Finally, planted, tagged, decoy documents provide an inviting target for attackers to exfiltrate that can then be tracked in the wild.

A complete deception system ideally provides decoys for servers, services, and other assets across the entire operational environment. These decoys serve as targets for an attacker. If an attacker attempts to leverage decoy credentials stolen from an endpoint, they are directed to one of the decoys where they are monitored and reported. If an attacker attempts to scan the network for potential targets, they should encounter a decoy that responds realistically, offering real services on a real operating system, inviting compromise and drawing them away from real assets, whether in a datacenter, user space, or across an IoT or SCADA network. If an attacker compromises any of these decoys, it will respond as if it were 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 an efficient response from the InfoSec team for mitigation, remediation, and root cause analysis.

Deception systems do not work in a vacuum and will deliver clear and concise alert information to the information security team so they can efficiently respond to events. Along with its own user interface, the ideal deception solution would integrate with other components of the defense architecture, including network, endpoint, and monitoring systems. Native integrations that automate responses can dramatically improve the team's efficiency and response times. Combined, these 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 deception solution, there are some basic questions they need to address.

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

- User space networks?
- Datacenter networks?
- IoT and SCADA device networks?
- Cloud environments?
- Hybrid environments?

HOW EFFECTIVE IS THE SOLUTION'S DETECTION?

- Against reconnaissance?
- Against stolen credentials?
- Against lateral movement?
- Against attackers "on the system"?
- Against malware propagation, including ransomware?

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

HOW COMPREHENSIVE IS THE DECEPTION?

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
- Are the deceptions static or dynamically updated?
- Is machine-learning available for automated preparation, deployment, and operations?
- What operating systems, applications, and services are supported out of the box?
- Can you create decoys from your own golden images?
- How easy are the lures to deploy and update?
- How much control do you 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 can be customized to match the protected environment.

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

HOW DIFFICULT IS IT TO DEPLOY AND OPERATE?

Different deception solutions have different network considerations and can offer a range of "environment 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 be factored in?
  - 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 is included with the solution?

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?
  - Dashboard
  - Clarity of information
  - Detail drill down
  - Role based views
  - Threat Intelligence (e.g. Virus Total)
  - Report formats: IOC, PCAP, STIX, CSV, etc.
  - Native 3rd Party Integrations
  - Automated or manual SIEM integration? Can it query the SIEM 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 they be customized based on level of attack finding?
  - How clear is it to quickly identify areas of greatest 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 ATTIVO REMOVES GAPS AND REDUCES ATTACKER DWELL TIME

The Attivo Networks® ThreatDefend™ Platform is designed to provide complete coverage across an organization's environment, including datacenters, user space, cloud environments, and specialized networks. At its core, the BOTsink® server provides realistic, high-interaction decoy systems and services across multiple VLANs, from a platform that is easy to maintain and easy to deploy. The Attivo Networks BOTsink solution is available as a physical or virtual appliance and can easily deploy into a Cloud environment such as AWS, Azure, Openstack, Oracle or Google Cloud. The ThreatDirect™ system projects decoys into remote networks using minimal resources, seamlessly extending coverage into remote locations. This empowers an organization to extend BOTsink coverage without requiring additional equipment.

The ThreatStrike™ component of the Attivo Networks solution places deceptive credentials, file shares, and other assets on the endpoints to lead an attacker into the decoy environment and away from production assets. These deceptions are easy to deploy across multiple host operating systems and can be placed using standard administrative automation tools. Using integrations with the local Active Directory servers, the deceptive credentials appear authentic without compromising live assets. Finally, the ThreatPath solution gives the security team visibility into credential use and trust relationships by displaying how an attacker could leverage orphaned and exposed credentials or misconfigurations to move laterally through the environment.

> Modern deception technology is easy to deploy and maintain and can efficiently scale up to enterprise level, supporting global deployment across a variety of attack surfaces.

With the ThreatDefend™ user interface, the security team can see events as they happen and has the ability to drill down into the details to understand how an attacker is behaving within the decoy environment. Additionally, native integrations with numerous 3rd party security applications makes the security team more efficient by enabling a fully automated response that reduces their workload.

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 deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide variety of specialized attack surfaces. The portfolio includes expansive network, endpoint, application, and data deceptions designed to efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 65 awards for its technology innovation and leadership.
For more information, visit www.attivonetworks.com.