What Is a Honeypot? Cybersecurity Deception Explained

With the continuously changing landscape of cybersecurity, organizations are trying to fight back and add more layers of security to outsmart the attackers. Over the years, one technique that has become very popular is the honeypot; to lure attackers away from valuable assets and gather intelligence on their tactics. Even though most security professionals are increasingly resorting to more sophisticated solutions such as deception decoys.

However, before we get into the new innovations, let's dive deeper into understanding – what is a honeypot?

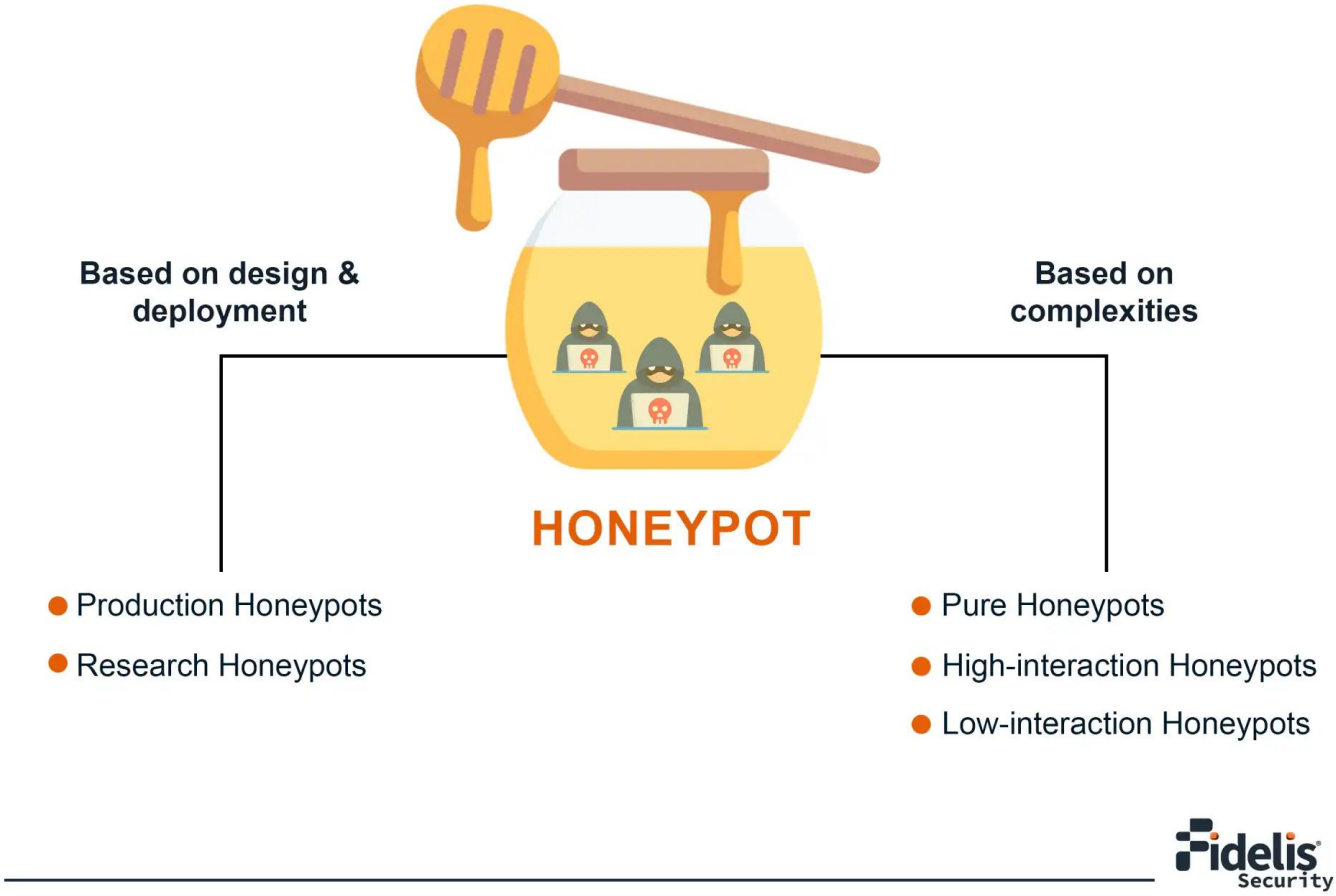
Defining Honeypots

A honeypot in cyber security refers to a decoy system designed to attract cyber attackers and gather information about their methods and intentions. Essentially, it serves as bait, drawing in potential threats by mimicking a vulnerable target.

This should be a controlled ambush, which allows security professionals to explore the operational behavior of cybercriminals. More than just a trap, it is designed to collect various kinds of data related to attack strategies, find any vulnerability in the network, and ultimately improve the overall security posture of an organization.

Honeypots have evolved to automated deception technology, which is more dynamic and acts as a smart alarm system.

Types of Honeypots



Honeypot cyber security is one of the most valuable tools when it comes to boosting your cybersecurity posture because they allow you to detect and analyze malicious activity. There are various types of honeypots – all with different purposes. Let's understand those various honeypots meaning.

Based on design and deployment, honeypots are categorized into two types:

1. Production Honeypots

Production honeypots are deployed in live environments in order to mitigate the risk by channeling attackers away from actual systems. In simpler terms, it is a decoy that has the same features as a real system in your organization. Thus, it can divert attackers or slow their progress while the security team addresses the problem.

2. Research Honeypots

Research honeypots are used to learn more about cyber threats and attackers' behavior, and new techniques of attack. Thus, they are used and maintained by security researchers or big companies to enhance their threat intelligence and develop advanced security tools.

Based on complexities honeypots are further classified into three types:

1. Pure honeypots

These are the most advanced honeypots. They are very sophisticated and not distinguishable from real systems. They provide the attacker with the whole operating environment with no

simulated aspects. They are extremely difficult to detect, but they require immense costs to be implemented, are very difficult to maintain, and also carry higher risks if attackers gain control of the system.

2. High-interaction honeypots

High interaction honeypots allow the attacker to interact with the system just like he would a normal system. The decoys are sophisticated and fully operational to enable security teams to track an attacker's progress, tools used and methodology. However, they are expensive to maintain to imitate the full services of production servers and are also open to compromise.

3. Low-interaction honeypots

Low-interaction honeypots can only simulate specific services or systems and have very limited interaction responses, they are designed to detect simple, automated attacks. These honeypots are imitations of network services, such as web servers or file-sharing systems with little interaction. They collect automated attack data and require less resources to maintain them, but are not as helpful for human-driven, advanced attacks.

Honeypots primarily are manually maintained, difficult to scale, and are statistically found by attackers as they lacked frequent activity, users and updates as lures. However, honeypot trap does provide valuable research use cases as well as in production environments leading to a variety of honeypot technologies including malware honeypots, email/spam honeypots, database honeypots for web services, canary traps with beacons, and multiple honeypots made into honeynets. Now that we know what a honeypot is, let's move on to why it's losing effectiveness in today's environment.

The Risks and Limitations of Using Honeypots

If you are strategizing honeypot trap into your existing cybersecurity, then you must be aware of certain risks and limitations associated with them. Although honeypots serve to distract attackers and provide insight into malicious activity, they also come with vulnerabilities that could potentially be exploited. Some of those vulnerabilities are:

1. Detectable by Sophisticated Attackers

One of the major disadvantages of honeypots is that skilled attackers can pivot to identify them over time. Although intended to simulate real systems, advanced cybercriminals may use honeypots with more suspicious configurations or traffic patterns that the bad actor can detect. A honeypot will only serve it purpose, until the fact that it is a honeypot detection occurs, revealing its true nature to the attacker.

2. Requires Maintenance and Monitoring

To stay effective, those honeypots must be updated, watched and kept working to match real systems as closely as possible. This ongoing care and upkeep present an operational burden and cost, requiring the allocation of someone to run the honeypot itself, sift through the data it collects, and identify false positives. Once you stop paying this kind of attention, a honeypot becomes ineffective and only does more harm than good.

3. Only Effective for Specific Threats

Honeypots are made to lure only a certain kind of attacker (or particular set); hence it is not a

comprehensive security tool. They are only useful for catching threats that interact with the decoy system, but we know realistically threat actors are clever and therefore they evade defenses by simply using other techniques or targeting other parts of the network.

4. Risk of Being Compromised

If misconfigured a honeypot can introduce vulnerabilities into the network. If an attacker learns to breach the honeypot, it will serve as a new entry point for hackers to access the extended network. Instead of securing the system, a hacked honeypot would turn into a trojan horse and could help attackers infiltrate the true infrastructure.

We know honeypots can be helpful (at least when it comes to threat detection and intelligence), but we also know they have their boundaries. They are not a silver bullet and should be used carefully as part of a bigger security toolbox so as to never cause more risk than they mitigate.

Outsmart cyber threats with Fidelis Deception®

- Our Fidelis Deception Technology solution includes:

- Decoys
- Breadcrumbs
- Active Deception

Get the Guide

How have Honeypots Evolved to Deception Technology?

Back in time, honeypots used to be very effective but as cyber threats got smarter and more prevalent, businesses realized they needed to evolve their security posture, leading to the emergence of advanced deception technologies.

The use of honeypots has evolved into deception technology as a step of moving from passive defensive postures to active approaches. The concept of deception technology is to provide an active defense through the use of decoys to lure, detect, and defend, without the issues of scalability, skilled and available resources, and containment versus detection that arise with honeypots.

Modern deception technologies have the ability to adapt in real-time by employing advanced methods like machine learning and Behavioral Analysis, thus staying one-step ahead of cybercriminals. This helps organizations not only improve threat detection accuracy but obtain comprehensive details about the attack approaches used.

Automation is key to creating effective modern deception defenses, which should also accommodate the following features:

- **Automated discovery –** continuously maps networks, assets, resources and services creating profiles to learn the 'real' environment.
  Automated decoy creation – builds optimal decoys with interactive services and applications to engage attackers or malware with what they desire.

- **Automated deployment –** positions a wide variety of decoys in optimal locations with a mixture of breadcrumbs on real assets as lures to make deception deterministic.

- **Active response –** enables security teams to script and automate workflows for active response and investigation.
- **Automatically adapts –** to changes in networks, assets, resources or services to update discovery profiles and enable the automation of new and updated decoys and breadcrumbs.

Why is Evolving Honeypots to Automated Deception Important?

The automation integrated into modern deception defenses reduces the manual effort needed for creation, implementation and maintenance of the tool. Consequently, even a tier-1 security analyst in an organization can quickly and easily configure, deploy and manage multiple layers of deception on both on-premises environments as well as cloud-based environments today.

Traditional honeypots, albeit may have some value in specific contexts, but they are plagued with issues like maintenance of systems and scalability and security concerns that attackers might be able to attack the system itself. Conversely, futuristic deception technologies use interactive services, which offers more scalability and better security. Modern deception defenses also leverage Active Directory credentials and understand the placement of access credentials as lures next to decoys with interactive services and applications.

Decoys and breadcrumbs, structured for most human attackers, are also capable of dispelling malware threats in an unstructured data environment. Modern deception is based on honeypots, but automation and the integration with network traffic analysis have changed the playing field to enable successful and easy-to-maintain deployments. This enables a defense with no risk to data or resources, nor any impact to users or operations to provide high-fidelity alerts with few false positives.

To learn more about deception technology, read this page on Fidelis Deception®.

Honeypots vs. Deception Decoys

To help you better understand the differences and make an informed decision on upgrading your honeypot cybersecurity strategy, the table below highlights the key differences between honeypots and deception decoys across various features, including scope, maintenance, and cost-effectiveness.

Feature Honeypots Deception Decoys Purpose Gather basic information about the attackers by drawing them into a decoy system. Defend against attackers across multiple network layers, detect and response to the threats earlier. Scope of Coverage Limited to individual systems or specific environments. Extensive network coverage with decoys deployed at all layers (devices, servers, apps). Detection by Attackers Honeypot detection is easy for a skilled attacker due to

predictable behavior. More dynamic and harder to detect, mimicking real systems convincingly. Maintenance Frequent updates and manual monitoring required. Often automated, requiring less manual intervention. Risk of Compromise Attackers may potentially exploit inadequately configured honeypots. Low risk; designed to be resilient and adaptive to attacker behavior. Threat Detection Limited to specific types of threats targeting the decoy. Detects a wider range of threats, including

APTs

and lateral movement. Scalability Limited scalability, usually implemented in smaller networks. Highly scalable across large, complex networks with customizable decoys. Integration with Security Tools Basic integration with existing security tools. Seamless integration with advanced security tools (SIEMs, firewalls, etc). Operational Cost Lower upfront cost but higher maintenance costs over time. More expensive to implement but cost-effective in the long term due to automation and reduced breach potential. Use Case Basic threat detection in smaller networks Ideal for modern day enterprises who are serious about advanced cybersecurity strategies.

Turn Adversaries into Targets with Fidelis Deception

- Study Attacker’s Every Move
- Maintain Cyber Resiliency
- Active Deception

Download the Whitepaper Now!

Choosing the Right Deception – Fidelis Deception®

Not all deception technologies are created equal, and you must choose a solution that makes sense for your organization.

An example of an advanced deception solution is Fidelis Deception®, providing a mature and flexible solution to defend your network. Fidelis Deception® surrounds real assets with a minefield of decoys that imitate them but exist only to deceive and distract the attacker.

Fidelis Deception® is unique in its flexibility with integrating with existing tools and its ability to scale to meet the need of both large and small businesses. It allows threats to operate in a live environment for longer periods without disrupting operations, meaning that attackers are constantly busy and distracted while providing your security team with invaluable insights on how they work within your network. And the real-time alerts and dashboards means you respond faster to incidents and have less potential fallout.

In summary: our strategies to defend against cyber threats should evolve as the threats themselves do. Transitioning from traditional honeypots to advanced deception technology marks a significant advancement in empowering organizations with the actionable threat intelligence necessary to fortify cyber defenses.

Our Customers Detect Post-Breach Attacks over 9x Faster

See how Fidelis:

- Cut threat detection time by 9x
- Simplify security operations
- Provide unmatched visibility and control

Book a Demo Now!