



GUARDPOT

Deception Platform

AVOSEC

Software Distribution

Contents

- What is a Honeypot?
- Why Guardpot?
- Guardpot Diagram
- The First Line of Defense
- Behavioral Analysis
- New Features
- Success Story Snippet
- User Experiences

What is a Honeypot?

Honeypot systems are specialized security solutions configured to mimic a real computing environment for the sole purpose of detecting cyber attackers, analyzing their behavior, and generating threat intelligence. These systems divert attackers' attention away from real systems, luring them into isolated, controlled, counterfeit environments. While the attacker believes they have successfully breached a critical system, all their actions are, in fact, being meticulously recorded by the system. These records include:

- Real IP address and geographic location
- Tools and attack methods used
- Usernames and passwords attempted
- Command and control (C2) connections
- Attempts at persistence or data exfiltration

This collected data is transformed into analyses of critical importance for understanding threats against the organization and taking precautions against future attacks. Thus, honeypot systems not only defend but also make corporate security strategies proactive by generating valuable cyber intelligence about attackers.



Guardpot

Guardpot lures attackers into an isolated environment that appears to be a real system, analyzes all their interactions in detail, and converts this data into real-time threat intelligence.

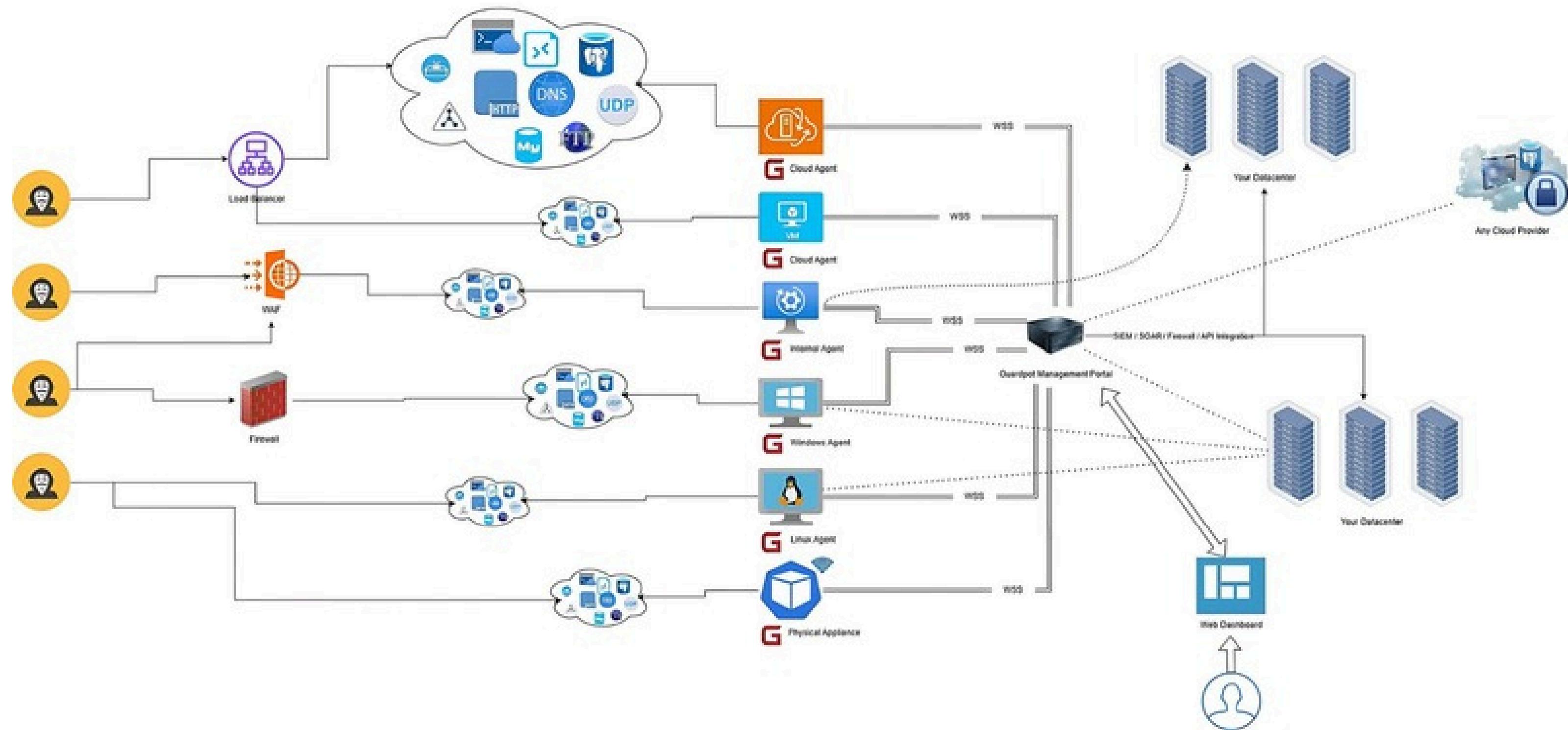
It deceives the attacker by simulating operating systems like Linux and Windows, and services like SSH, FTP, and Web one-to-one. While the attacker thinks they have breached the system, all their behaviors, from the passwords they attempt to the tools they use, are recorded. This information is analyzed instantly, and suspicious IPs are automatically blacklisted.

By default, Guardpot collects threat data from over 50 countries. This global data pool, combined with custom-generated IoCs (Indicators of Compromise) for you, provides a stronger defense.

It works integrated with SIEM and firewalls, making internal threats and vulnerabilities visible before they even materialize. Guardpot is not just a trap; it is a strategic component of active defense, behavioral analysis, and cyber intelligence.



Guardpot Diagram



The First Line of Defense

-The Misconception

Honeypot systems are often seen as a luxury security tool to be acquired in the final stage.

-The Reality

When Guardpot is positioned at the very front of the system:

- It catches the attacker at the network's outer gate
- It analyzes their behavior and reveals their identity
- It isolates threats without burdening other security layers
- It reduces detection time to minutes, or even seconds

"If a Firewall is a fire extinguisher, Guardpot is a smoke detector: It warns before the fire starts, and the attacker is neutralized before they can even touch the system."

- The New Approach

Guardpot should be the first point of contact in the security architecture. Because the best defense now is to monitor the attacker without letting them in.



Behavioral Analysis

1. Objective

To uncover not just the attacker's IP, but their intent and methods.

2. What is Analyzed?

- Attack Method: Brute-force, dictionary, exploit attempt, port scan
- Timing: Active hours, repetition interval, persistence
- Commands and Movements: Which directories are accessed, which commands are attempted
- Service Target: Which services are being forced (e.g., SSH, FTP, HTTP)
- Tools: Nmap, sqlmap, custom payloads
- Source Country / Location: Geographical analysis
- Proxy/Tor Usage: Level of anonymity
- Behavioral Pattern: Human or bot? Targeted or random?

3. Outcome

- Similar attackers are matched through automatic profiling
- Suspicious behaviors are detected early with AI-supported analysis
- The attacker's character, not just their identity, is defined
- Contextual, meaningful alerts are generated for security teams



New Features

1. VGN- Virtual GuardedNetwork

Provides a chained VPN architecture with a multi-step tunneling structure. It ensures complete anonymity by hiding the user's IP and creates a secure communication infrastructure.

2. Secure Link

Generates encrypted links for the secure sharing of sensitive data. It minimizes the risk of data leaks with time-limited and single-use access links.

3. Web Surface

Maps the organization's internet-facing surface by scanning for open ports and services. It identifies risky configurations through visibility analysis and enables quick action.

General Benefits

- In-depth analysis, expanded security coverage
- Effective control against both external and internal threats
- Proactive defense, system visibility, and sensitive data security all in one



New Features

4.G-Token

Guardpot provides multiple types of realistic deception baits that mimic real files and configurations. When any bait is accessed, Guardpot logs the source details and sends instant alerts through your chosen channels.

Available bait types include:

- Web application vulnerability baits (Web Bugs)
- QR code baits
- Word and Excel document baits
- Executable (.exe) baits
- OpenVPN & WireGuard config baits
- Kubernetes (K8s) config baits
- JavaScript & CSS website clone baits

Baits can be deployed manually or automatically to targeted endpoints via Active Directory integration.



Success Story Snippet

Guardpot was integrated into an environment as a one-to-one

replica of the externally-facing mailsystem. Within the first 24 hours of installation:

- It was observed that system administrators' correct passwords were being attempted.
- System administrators changed their passwords due to the possibility of a password leak.
- Shortly after, the new passwords also began to be tested on Guardpot.
- Thanks to LDAP integration, very rapid action was possible; real password attempts were automatically reported to system administrators via notification channels.
- It was discovered that the attacker had established persistence in a way that could replicate the Active Directory database.

The attacker was already inside, monitoring passwords and cloning Active Directory. Guardpot made them visible for the first time. Due entirely to real user behaviors, no alarms had been generated in the organization, which had end-to-end EDR, XDR, NGFW, Standalone IPS, and WAF deployments. Illuminate your blind spots with Guardpot!



User Experience

- Ease of Integration

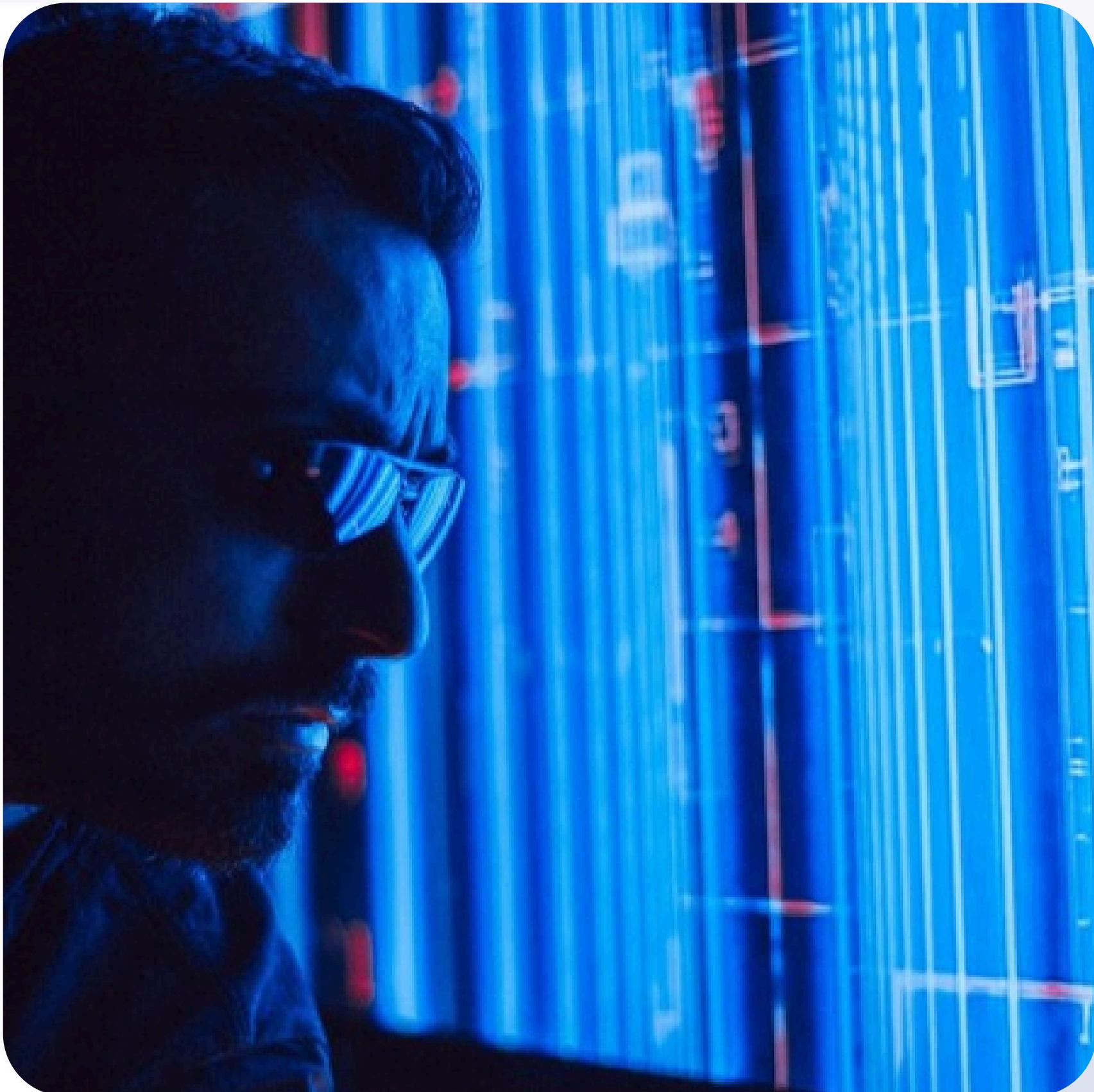
- Full installation time: 60 minutes on average
- Simple integrations for SIEM/SOAR/Firewall
- Cloud/On-Prem support

- Operational Gains

- Organization-specific IoC database.
- Early detection of password vulnerabilities.
- Ability to monitor targeted attacks.
- Mapping of the security infrastructure.

- Most-Liked Features

- Automatic blacklisting.
- Activity tracking screens.
- Live attack monitoring.
- Anonymization with VGN.





Thanks!

avosec.com

info@avosec.com