

**OBJECT  
FIRST**

**2026**

**Early Threat Detection for Veeam Backups:**

# **Object First HoneyPot Feature**

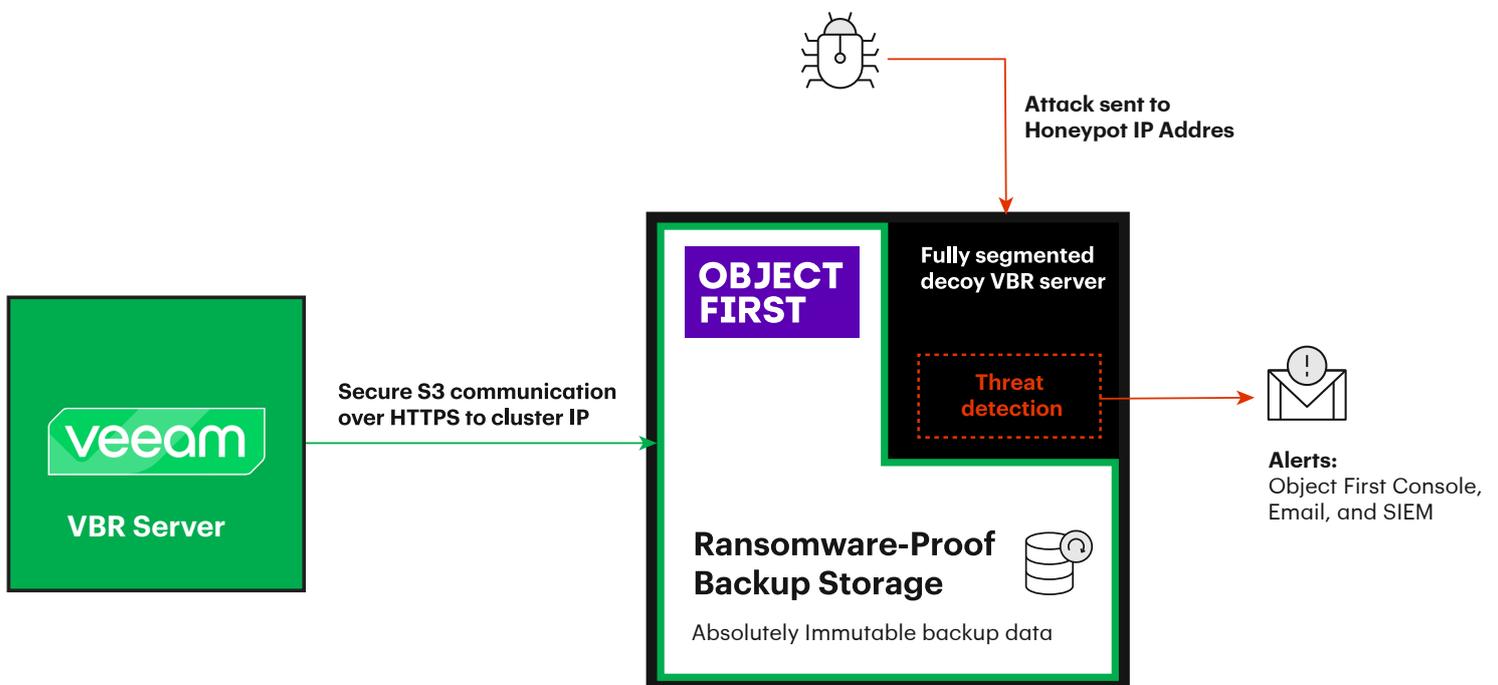
Ransomware attackers know your backups are your last line of defense. If your Veeam backups survive, you won't pay the ransom. That's why backup servers are often the first target.

**Object First's Honeypot feature**, included in the Object First 1.7 release, helps you detect suspicious activity targeting your backup environment, enabling you to be resilient and ransomware-proof when attacks, disasters, accidents, or insider threats occur.

## What Is a Honeypot—and Why Should You Care?

A honeypot acts like a **tripwire for cyber threats**. It's a decoy system that attracts attackers and alerts you when someone is probing your environment.

Object First's Honeypot simulates a Veeam Backup & Replication (VBR) server. If attackers scan or attempt access, you get an immediate alert.



# Business Benefits

- **Early Warning:** Detect threats before ransomware strikes.
- **Peace of Mind:** Adds security without complexity or extra tools.
- **Faster Response:** Alerts help you act before backups are compromised.
- **Compliance and Confidence:** Demonstrates proactive defense to auditors and stakeholders.
- **Zero Risk:** Enabling Honeypot introduces no risk to the security or integrity of the cluster or the immutable data stored within. Proven by the latest 3rd-party penetration testing.

## Why Object First Honeypot Is Different

- **Built-In:** No extra software or hardware.
- **Simple Setup:** Enable in five clicks from the Object First Cluster Management dashboard.
- **No Expertise Required:** Perfect for IT teams of any size.

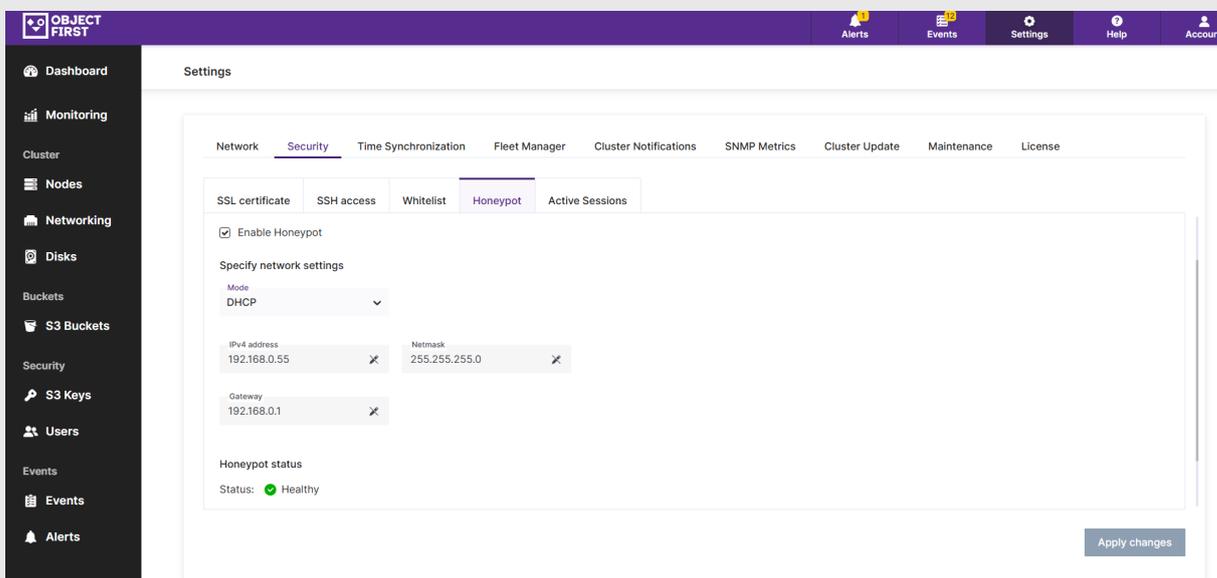
## How It Works

Once enabled, Honeypot monitors for:

- Multiple login attempts
- Port scans
- Probing sensitive protocols
- Unauthorized Veeam console access

Alerts appear in the Object First dashboard and are sent via email or through syslog forwarding to SIEM.

## How to Activate Honeypot in your Object First cluster



1. **Log in** to the Cluster Manager UI.
2. Go to **Settings > Security > Honeypot**.
3. **Check the box** to enable Honeypot.
4. Choose IP mode:
  - a. **DHCP**: Auto-assigns IP.
  - b. **Static**: Manually set IP and netmask.
5. Click **Apply Changes**.

Honeypot is now live and monitoring for suspicious activity.

The screenshot shows the 'Events' page in the Object First interface. The table below represents the data shown in the screenshot.

Severity	Time	Source	Object	User	Event ID	Description
Info	12/12/25, 02:43:06 PM	Management Serv...	Node: ootbisiem02	objectfirst	2332	User 'objectfirst' has successfully logged in.
Info	12/12/25, 01:09:09 PM	Management Serv...	Node: ootbisiem02	objectfirst	2333	User 'objectfirst' has logged out.
Warning	12/12/25, 12:16:39 PM	HoneypotService	Node: ootbisiem02	honeypot	7041	Honeypot: Several authorization attempts on proto...
Warning	12/12/25, 12:14:24 PM	HoneypotService	Node: ootbisiem02	honeypot	7033	Honeypot: Cumulative suspicious activity from fro...
Warning	12/12/25, 12:14:24 PM	HoneypotService	Node: ootbisiem02	honeypot	7031	Honeypot: Several requests with data received on ...
Warning	12/12/25, 12:14:24 PM	HoneypotService	Node: ootbisiem02	honeypot	7030	Honeypot: 9 port scans from 192.168.0.31 IP
Warning	12/12/25, 12:14:05 PM	HoneypotService	Node: ootbisiem02	honeypot	7033	Honeypot: Cumulative suspicious activity from fro...
Warning	12/12/25, 12:14:05 PM	HoneypotService	Node: ootbisiem02	honeypot	7031	Honeypot: Several requests with data received on ...
Warning	12/12/25, 12:14:01 PM	HoneypotService	Node: ootbisiem02	honeypot	7041	Honeypot: Several authorization attempts on proto...
Warning	12/12/25, 12:13:57 PM	HoneypotService	Node: ootbisiem02	honeypot	7033	Honeypot: Cumulative suspicious activity from fro...

## Hands-On Testing

These quick, controlled tests help to demonstrate the Object First Honeypot feature's detection capabilities in a lab setup.

1. Open PowerShell and attempt to SSH into Honeypot (using the IP address displayed in your Honeypot).

SSL certificate	SSH access	Whitelist	Honeypot	Active Sessions
Mode DHCP				
IPv4 address 192.168.0.55		Netmask 255.255.255.0		
Gateway 192.168.0.1				
<b>Honeypot status</b>				
Status: <span style="color: green;">✔</span> Healthy				
Active node:  ootbisiem02				
<button>Restart Honeypot</button>				

## 2. Enter any password; all attempts will be rejected.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Geoff.Burke> ssh 192.168.0.55
The authenticity of host '192.168.0.55 (192.168.0.55)' can't be established.
RSA key fingerprint is SHA256:Ujk9CxJk2YSM4M/ONgyfrZr6Cx8p3HmlUhtWS+tLjG4.
This host key is known by the following other names/addresses:
  C:\Users\Geoff.Burke/.ssh/known_hosts:9: 192.168.0.44
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.55' (RSA) to the list of known hosts.
geoff.burke@192.168.0.55's password:
Permission denied, please try again.
geoff.burke@192.168.0.55's password:
Permission denied, please try again.
geoff.burke@192.168.0.55's password:
geoff.burke@192.168.0.55: Permission denied (password).
PS C:\Users\Geoff.Burke> |
```

Event details✕

**Severity:** ⚠ Warning

**Time:** 12/04/25, 10:50:21 AM

**Source:** HoneypotService

**Object:** Node: ootbisiem02

**User:** honeypot

**Event ID:** 7041

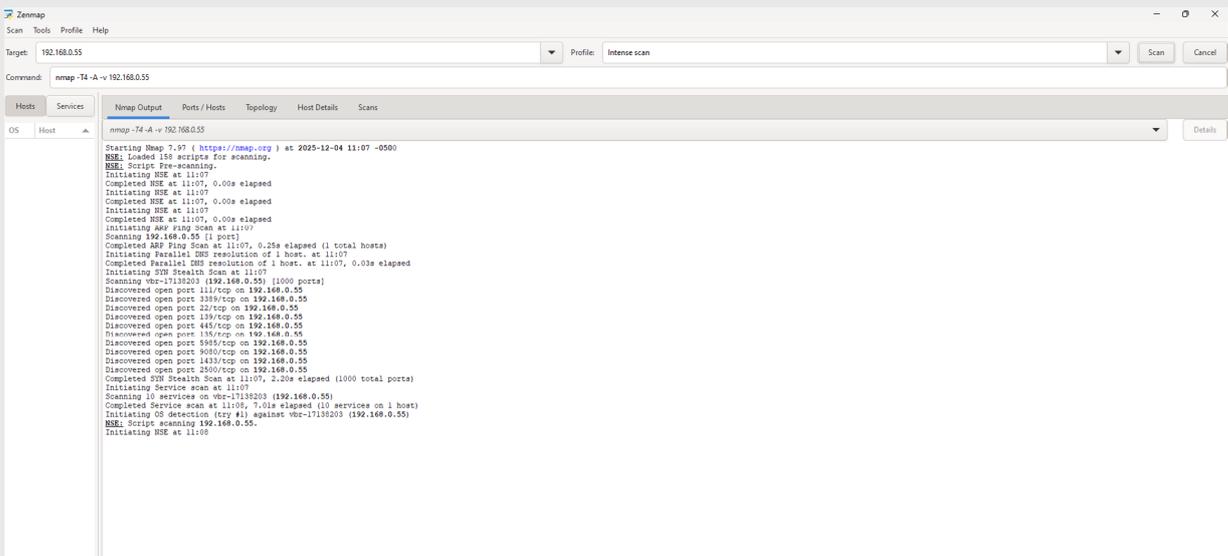
**Event description:**

Honeypot: Several authorization attempts on protocols: ssh from 192.168.0.31 IP

Copy to clipboard

Close

### 3. Use an authorized in-house security scanner—such as Zenmap—to test Honeypot.





**OBJECT  
FIRST**

# Simply Resilient for **Veeam**