OBJECT FIRST

Test Report

Independent Security Test Summary

Summary of 2025 Penetration Test Results from NCC Group

March 2026

nccgroup

Security Update

During Fall 2025, Object First commissioned an updated, code-assisted product security assessment of the Object First appliance by global cyber security experts at NCC Group. This new report follows prior assessments and reflects Object First's commitment to security and transparency. You can find the full NCC Product Security Assessment on their website.

Object First is committed to meeting IT security industry standards for its absolutely immutable backup storage appliance, which serves as a Secure-by-Design storage target for Veeam backup data. The Object First appliance is designed to protect Object First customers against data breaches or malware infestations. Even if all secrets, including administrator and bucket credentials, are known to the attacker, they still cannot modify any data stored within an Object First cluster.

In 2024, NCC Group conducted two rounds of penetration testing on the Object First appliance and its software, evaluating source code and production-ready devices over 54 days. The second round confirmed that all major issues identified in the first round had been remediated. For historical continuity and transparency, our original 2024 summary remains available on our website and the full report is available from NCC Group.

For the latest tests, we engaged NCC Group to conduct comprehensive penetration tests on the Object First appliance and its software to identify and address undiscovered risks. This paper provides a summary of NCC's findings and important security information about Object First's backup storage solution.

NCC's Takeaway

NCC Group's latest assessment confirms significant security enhancements since its Fall 2024 assessment. Issues have been addressed and risks reduced in previous focus areas, including authentication, authorization, input validation, and data exposure. In this 2025 engagement, only seven Low and Informational findings were identified, primarily related to code-level hardening and minor configuration adjustments. Core security controls, including immutability enforcement, privileged action reauthentication, system hardening, and the Honeypot feature operated as designed.

How was the assessment conducted?

NCC Group performed a Product Security Assessment (code-assisted) spanning the Object First appliance and supporting software, focusing on exploitable risk and malicious attack vectors. Testing ran from September 22, 2025, to November 5, 2025, with three consultants and 45 consultant days of effort. Physical access vectors (e.g., IPMI) were out-of-scope.

In-scope target and interfaces:

- **Management Console UI:** Web admin console for cluster setup and day-to-day operations
- **Management Web API:** Externally facing API supporting management functions
- **Object First Server (Ubuntu image):** The hardened appliance OS image
- **S3/STS API:** Front-facing API used by Veeam and other systems
- **Honeypot Feature:** Decoy services for threat detection and alerting

Who is NCC Group?

NCC Group is a globally recognized cyber security firm specializing in application and product security assessments, cryptography reviews, penetration testing, and secure development advisory services. Their methodology emphasizes exploitation realism, defense-in-depth validation, and Secure-by-Default design. For this engagement, NCC combined source code review with hands-on appliance and API testing to evaluate both design controls and implementation correctness.

Discoveries and Remediations

During the 2025 testing process, NCC identified 7 findings—0 Critical, 0 High, 0 Medium, 3 Low, and 4 Informational. The findings reflect hardening opportunities, not systemic weaknesses. Object First has triaged all items, and initiated remediation plans where applicable, aligned to Secure-by-Default and cryptographic best practices.

Risk Category Summary

Category	Risk Level	Example Issues Identified
Authentication	Low	MFA enforcement not available for all users (admin policy control)
Cryptography	Low / Informational	Weak hashing (MD5/SHA-1), SSL/TLS Certificate Verification not enforced for all inter-node communications, padding oracle risk, insecure RNG
Configuration	Informational	Presence of development utilities on the host image
Secure Coding	Informational	Unsafe C/C++ string and memory operations

Positive Security Observations

- **Overall Security:** All previously identified vulnerabilities were addressed prior to the conclusion of testing in 2025; no recurrences were detected.
- **Immutability Controls:** Admin re-authentication for sensitive actions; no deletion of stored data permitted.
- **Appliance Hardening:** Breakout attempts from restricted CLI to full shell were unsuccessful.
- **Honeypot Feature:** Correctly detected malicious activity (e.g., port scanning) and generated UI alerts; no misconfigurations or UI vulnerabilities found.
- **New Functionality (e.g., SNMP metrics, Honeypot):** Implemented best practices without introducing code injection or data exposure issues.

Zero Trust Data Resilience and Absolute Immutability

NCC's assessment reinforced the importance of implementing Zero Trust frameworks as part of the backup architecture. The Zero Trust Data Resilience framework is a model all organizations can use to assume breach and apply Zero Trust principles to backup software and backup storage to ensure rapid recovery from an attack.

Immutable backup storage is a key element of the Zero Trust Data Resilience framework. Absolute Immutability means that even the most privileged admin or attacker with access to backup storage cannot modify or delete data. This can only be achieved using a backup storage system that is "Secure-by-Design" with Zero Access to destructive actions, and this Zero Access must be verifiable with third party testing.

Evaluate whether your vendor is taking the time to have 3rd party agencies penetration test their products. Only then can you be confident that you can effectively recover from a ransomware attack.

Secure-by-Design: Our Foundational Commitment

Object First was founded on the principle that security must be built in from the start—not bolted on later. That's why we've signed CISA's Secure by Design pledge and are actively implementing its seven steps.

We also embrace the Zero Trust maturity model, the gold standard for modern cybersecurity, which assumes no entity is trusted by default and requires continuous verification of users, devices, and applications. For additional information, please refer to the Object First (Zero) Trust Center.

Our commitment goes beyond compliance. We align with leading IT security standards, ensure our appliance is Secure-by-Design and Secure-by-Default, and regularly engage independent third-party testing firms—sharing results openly with the community.

Object First's mission is unwavering: to safeguard your Veeam backup data and help you recover with confidence.