

ÓBUDAI EGYETEM
OBUDA UNIVERSITYJohn von Neumann Faculty of Informatics
deanReg. No.: NIK, 1960, 2026
Date: Budapest, 22 September 2026

EVALUATION REPORT

on the Laboratory Testing of the Yazata Network Security Device

Scope and Purpose of the Testing

The John von Neumann Faculty of Informatics at Obuda University tested the operation of the Yazata network security device in a laboratory environment. The purpose of the testing was to verify whether the device actually provides the basic network security and monitoring capabilities as advertised.

Test Results

Based on the laboratory testing, it can be concluded that Yazata provided the promised basic capabilities in the tested environment. During the testing, we verified the operation of DNS filtering and custom rules, active source-IP-based blocking, preservation of existing network addressing, unimpeded transmission of normal data traffic, local network scanning, and the functionality of the user interface and logging features. No separate client software needed to be installed on the protected endpoints.

Threat Intelligence Feature

A key finding of the evaluation was the verification of the Threat Intelligence feature's operation. The device uses a protection list based on threat intelligence that can be updated remotely. The loading and updating of the list were observable during the evaluation, and the actual operation of source-IP-based blocking was confirmed by laboratory tests.

The remotely updated Threat Intelligence engine enables the device's protection rules to adapt to newly identified threats. The updated threat intelligence is applied locally as part of network protection; therefore, modifying the protection does not require updating or configuring each individual endpoint separately.

Summary Evaluation

Based on the testing, Yazata delivered the verified core functions it promised in the tested laboratory environment. The device combines DNS protection, source IP-based blocking, network detection, and administrative oversight into a single network component. The remotely updatable Threat Intelligence engine provides the technical foundation for adapting to dynamically changing threats.

These findings apply to the laboratory environment described and the tests performed. The availability, operational, and licensing terms of the update service must be agreed upon separately with the manufacturer.

Sincerely,

Prof. Dr. György Eigner
dean
Obuda University
John von Neumann Faculty of Informatics

