

SelectiveTRUST by KnectIQ
Test and Evaluation Report
FINAL

Version 2.0

Team Members
Salvatore Paladino
Brandon Haines
Tiffany Mahoney
Aaron Porter
Andres Rodriguez
Eric Sognefest

April 29, 2024

Prepared by
Assured Information Security, Inc.
153 Brooks Road
Rome, NY 13441
(315) 336-3306

Executive Summary

This report details Testing and Evaluation (T&E) of KnectIQ's SelectiveTRUST product. T&E was performed by Assured Information Security, Inc. (AIS) under contract FA8750-19-C-0013, titled Full Spectrum Cyber Capabilities (FSCyCap).

The purpose of this evaluation was to determine if SelectiveTRUST's capabilities meet currently defined functional, operational, and security objectives. Test objectives were formulated and agreed upon by the SelectiveTRUST developers and the T&E team prior to test execution.

T&E consisted of verifying the platform deployment process, validating the technology's overall functionality, assessing the system's efficacy against spoofed or compromised devices, identifying potential vulnerabilities in the client/server software and their communications, and testing cross-platform compatibility.

Based on the comprehensive evaluation of SelectiveTRUST, it has been determined that it provides all claimed functionality related to a zero-trust based capability. It has also been determined that it is sufficiently robust and secure for integration into an enterprise-level or DoD security infrastructure for advanced threat protection and data integrity assurance. Its operational readiness for pilot deployment further substantiates its viability as a strategic cybersecurity asset.

T&E findings are further summarized below:

Robustness Against Threats: SelectiveTRUST demonstrated exceptional resilience against adversarial actions, with no vulnerabilities found that could lead to the decryption of protected data.

Operational Maturity: The technology proved to be mature enough for operational piloting, having performed well in all test objectives, including cryptographic protections, multi-platform compatibility and comprehensive security evaluations.

Overall, T&E determined that SelectiveTRUST is a robust solution - no weaknesses were discovered that could directly lead to recovery of encrypted plaintext. SelectiveTRUST was found to be sufficiently mature for operational piloting, with only minor items noted on product consistency and usability, many of which have been addressed in the 'remediation response' sections of this report.

Testing also yielded the following recommendations:

Pilot Deployment: Organizations considering bolstering their cybersecurity posture can pilot KnectIQ's SelectiveTRUST technology with negligible operational risk.

Further Evaluation: Continuous evaluation and monitoring during the operational pilots will provide additional insights into further use cases and areas for enhancement.

Strategic Implementation: Given its robust security features and operational readiness, SelectiveTRUST is suitable for strategic implementation across sectors requiring digital agility and high levels of data, device, network, and cloud security.

Description of the SelectiveTRUST Technology

SelectiveTRUST by KnectIQ represents a significant advancement in cybersecurity, providing a reliable, secure, and efficient solution to modern cyber threats without the vulnerabilities associated with traditional security measures.

The below description of KnectIQ's SelectiveTRUST technology was informed by developer provided documentation and publicly available internet sources.

Background

In an era where cybersecurity threats are rapidly evolving, organizations across various sectors face the critical challenge of protecting sensitive data from a multitude of threat vectors, including the increasingly prevalent insider threats. Traditional cybersecurity solutions, which often rely on stored secrets such as credentials, keys, and certificates, present material vulnerabilities. In the event of these secrets being compromised, the repercussions range from data, device, and network breaches to significant national security risks.

To address the limitations of current solutions, KnectIQ's SelectiveTRUST technology offers single-use, dynamically generated keys, and is operated on the control plane, ensuring the system never "sees" the data¹.

Overview

KnectIQ's SelectiveTRUST technology emerges as a pioneering solution to these challenges. It embodies the principles of Zero Trust architecture, offering an enterprise-class system dedicated to secure access, data loss prevention, and secure communication and data sharing across all classification levels and partner domains. SelectiveTRUST distinguishes itself by ensuring secure device authentication and authorization of every interaction, transcending traditional limitations associated with existing cybersecurity tools, tactics, and processes².

¹ From KnectIQ Website – www.knectiq.com

² From KnectIQ Website – www.knectiq.com