

TEST REPORT

QUELLSECURE

RANSOMWARE CYBERRISK

VALIDATION REPORT

Vendor: QuellSecure, Inc.

Test Period: January to April 2026

Build Version: QuellSecure 1.2.3.13

Last Revision: June 15, 2026

Table of Contents

01 Executive Summary	3
02 Introduction	6
03 Test Environment	8
3.1 Test Specifications	8
3.2 Baseline Configuration	9
3.3 Instrumentation and Monitoring Tools	10
04 Test Overview	11
4.1 Ransomware Samples	12
4.2 Ransomware Families	14
05 QuellSecure Build Details and Score Progression	16
06 False Positives	17
07 Telemetry and Event Data	18
08 Conclusion	19
09 Disclaimer and Legal Notes	20

Executive Summary

Ransomware continues to be one of the most significant and rapidly evolving cybersecurity threats, impacting organizations across all industries. Effective detection and rapid containment are critical to minimizing operational disruption, data loss, and financial impact. As a result, security solutions must demonstrate not only high detection accuracy but also consistent and reliable response capabilities across a wide range of threat scenarios.

QuellSecure Ransomware Detection and Prevention

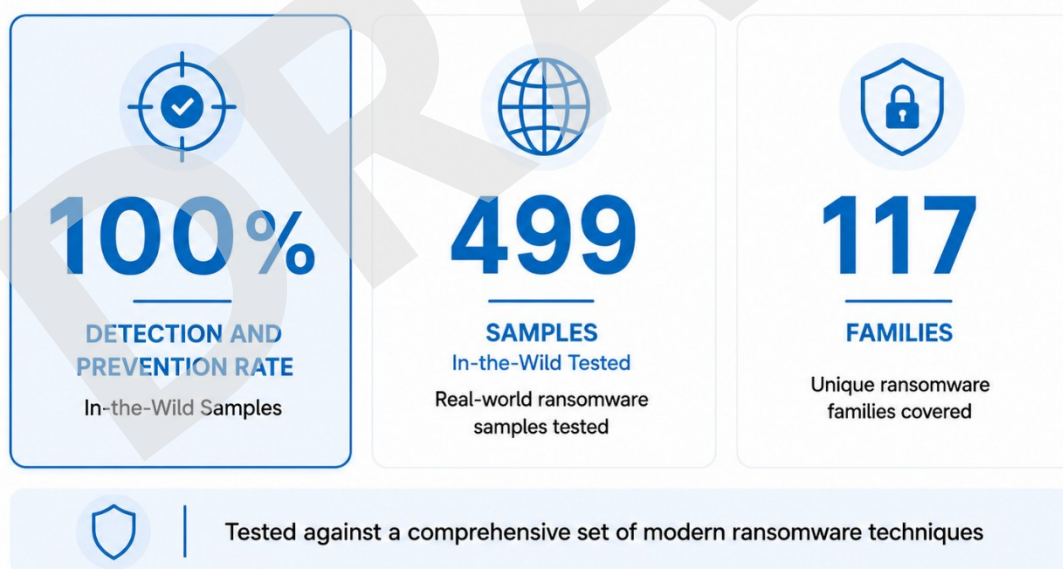


Figure 1: 100% Detection and Prevention for QuellSecure

SecureIQLab performed the validation assessment of the QuellSecure platform to evaluate its effectiveness in detecting and mitigating ransomware activity in real-world attack scenarios.

The evaluation was conducted between December 2025 to April 2026 using a comprehensive dataset consisting of 499 in-the-wild ransomware samples sourced from active threat intelligence feeds. In total, the dataset represents 117 unique ransomware families and reflects realistic adversary behaviors observed in production environments.

QuellSecure demonstrated exceptional performance against real-world threats, achieving a 100% detection and prevention rate across all 499 in-the-wild samples. Every sample was successfully identified and blocked, underscoring robust protection against active ransomware campaigns.

In addition to high detection and prevention efficacy, the solution demonstrated rapid intervention with an average of only 12 files encrypted prior to containment. Commonly encrypted files include documents and office files such as .docx, .pdf, .ppt, .xlsx, and .txt, along with media and design files like .jpg, .png, .avi, .mp4, and .ai. Additionally, more specialized formats such as .raw, .parquet, .E01, .heic, and .log were also affected.

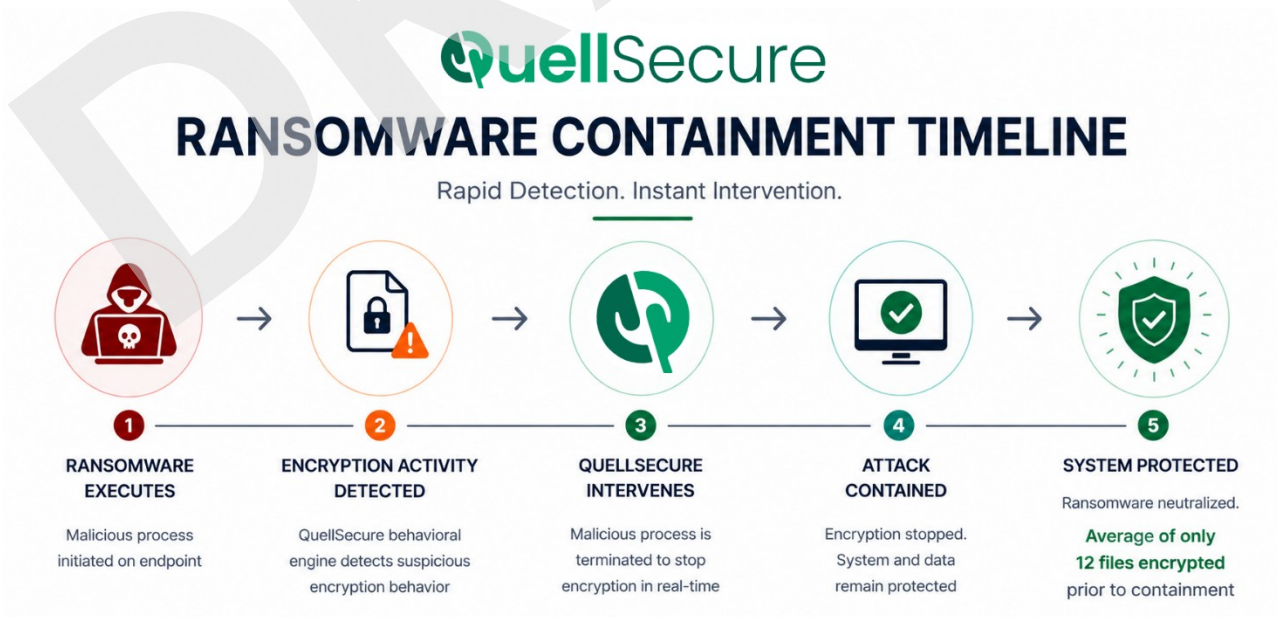


Figure 2: Ransomware Containment Timeline

QuellSecure demonstrated a modern behavior-based approach to ransomware detection and containment, focusing on rapid intervention after malicious encryption activity begins rather than relying

solely on pre-execution signature-based prevention. Unlike traditional solutions that attempt to block malware before execution, QuellSecure is designed to detect active ransomware behavior in real time and terminate the malicious process before widespread encryption or lateral impact can occur. This approach reflects a behavioral containment model rather than a purely pre-execution prevention strategy.

While some security products aim to prevent execution entirely and may report zero encrypted files when successful, such approaches can be more dependent on signatures, reputation systems, or known indicators of compromise. QuellSecure instead emphasizes resilience against unknown, modified, and behaviorally evasive ransomware variants by monitoring real-time encryption activity and rapidly interrupting malicious execution before large-scale damage occurs across the environment.

QuellSecure's lightweight installation requires minimal configuration, operates effectively in both online and offline environments, and is engineered for extremely low CPU, RAM, and network latency impact, making it ideal for organizations with limited IT resources or performance-sensitive systems.

02

Introduction

Ransomware continues to be one of the most visible and damaging threats in today's cybersecurity landscape. In recent years, ransomware has been behind some of the most high-impact cyber incidents. From the WannaCry outbreak that disrupted a significant portion of NHS services in England¹, to more recent attacks like the Change Healthcare Cyberattack² affecting data tied to over half the U.S. population, the scale and consequences have been severe.

Ransomware works by infiltrating a system, often through phishing emails, malicious downloads, or software vulnerabilities and executing a hidden payload. Once inside, it rapidly encrypts files on the system and sometimes across connected networks, making data inaccessible to users. The attacker then demands a ransom, typically in cryptocurrency, in exchange for a decryption key. Modern ransomware operations are highly organized and may also involve data exfiltration, where sensitive information is stolen and threatened to be leaked if the ransom is not paid.

¹ <https://www.england.nhs.uk/long-read/case-study-wannacry-attack/>

² <https://www.aha.org/system/files/media/file/2025/02/Change-Healthcare-Cyberattack-Underscores-Urgent-Need-to-Strengthen-Cyber-Preparedness.pdf>

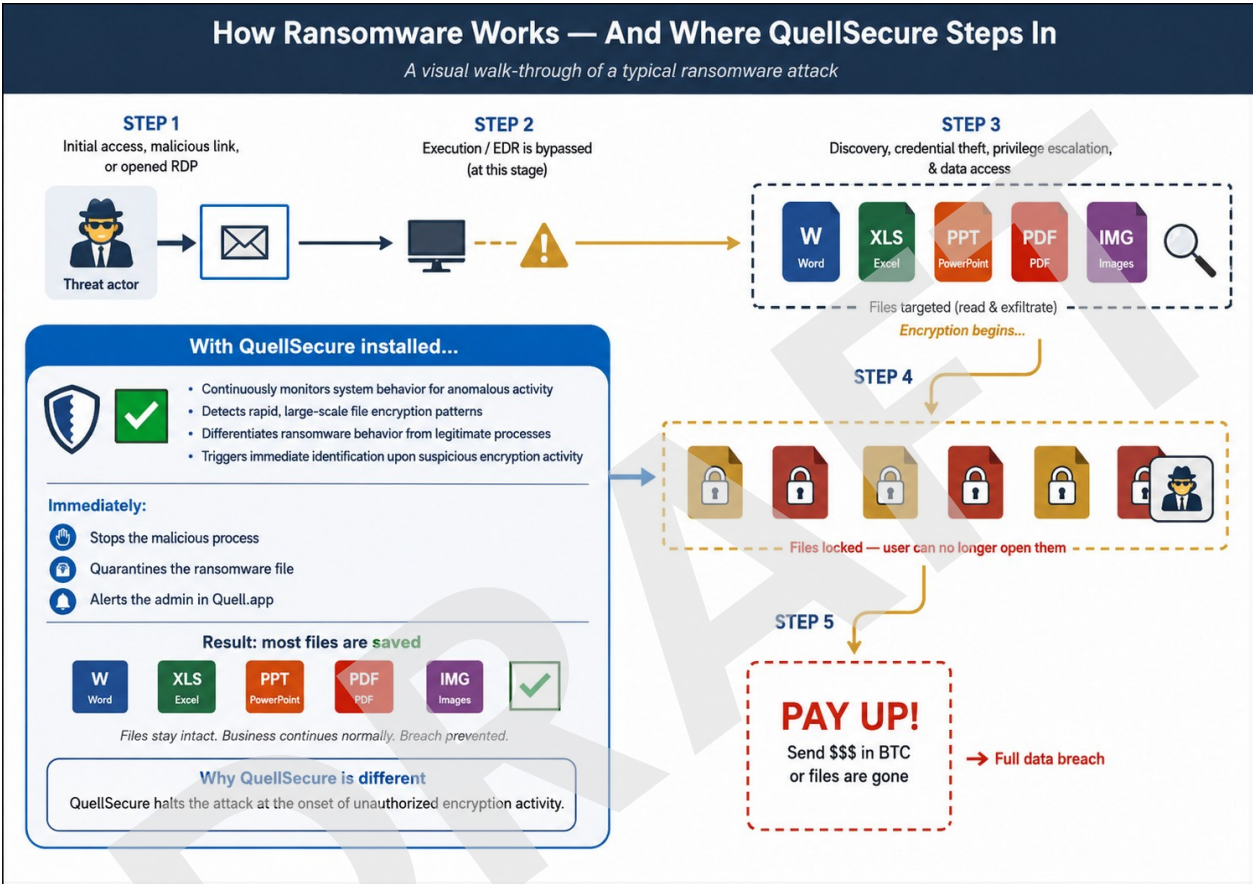


Figure 3: How ransomware works and where QuellSecure steps in

03

Test Environment

3.1 Test Specifications

Testing was conducted across two environments: a primary cloud-based virtual machine setup hosted on Microsoft Azure, which supported the majority of executions, and a physical desktop environment running Windows 11, used to validate behavior on bare-metal hardware for a smaller subset of approximately 20 samples.

Build	Outcome
Cloud Platform	Microsoft Azure
Azure VM SKU	Standard D8s v3 (8 vCPUs, 32 GiB memory)
Operating System	Windows 11 Enterprise, 24H2 (win11-24h2-ent)
Physical Test Machine RAM	16 GB
Physical Test Machine Storage	512 GB SSD
Patch Level	Standard Microsoft update level for the OS build at the time of image creation; no out-of-band patches were applied during testing to avoid baseline drift.
TPM	TPM 2.0 (required by QuellSecure registration)
Baseline Image	Pre-configured Windows 11 image with QuellSecure Agent, ~2,000+ dummy files, and evidence-collection tooling installed.

Figure 4 below shows the SecureQLab test lab setup and how QuellSecure is deployed within it.

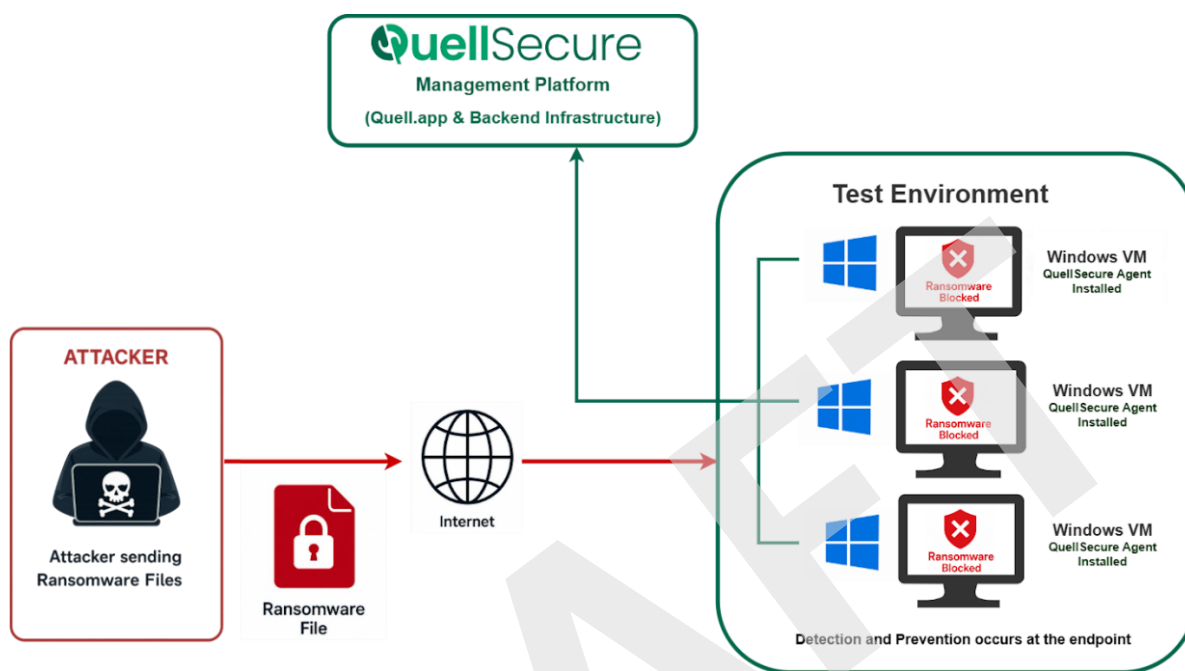


Figure 4: Test Environment Architecture

3.2 Baseline Configuration

The following modifications were made to the standard Windows 11 baseline to allow ransomware to execute uninterrupted and to ensure that the verdict reflected the QuellSecure behavior alone:

- ▶ Windows Defender real-time protection: Disabled. (Defender's own anti-ransomware controls would otherwise pre-empt QuellSecure and confound the test.)
- ▶ QuellSecure agent policy: Default policy was applied across all builds. No custom tuning, exclusions, or sensitivity changes were made on the agent — the product was tested as it ships.
- ▶ All other Windows security settings (Firewall, SmartScreen, UAC) were left at default unless a specific sample required adjustment, in which case it was noted in the per-sample evidence.

3.3 Instrumentation and Monitoring Tools

The following tools were employed for execution monitoring and forensic data collection:

- ▷ Wireshark – full network capture during execution.
- ▷ Process Monitor (Sysinternals Procmon) – file system, registry, and process activity trace.
- ▷ API Monitor – used during the initial phase of testing.
- ▷ Screen recorder – operated from the host (outside the guest VM) to ensure recording survived guest-side ransomware activity.

04

Test Overview

SecureQLab conducted a comprehensive and controlled evaluation to assess the effectiveness of the QuellSecure agent against ransomware threats. To ensure safe containment and eliminate risk to production infrastructure, all testing was conducted within a virtualized Azure environment isolated from external systems. Running the ransomware in this isolated virtualized environment had no impact on ransomware behavior, including activities such as potential command-and-control (C2) communications or cryptographic key exchange attempts, allowing SecureQLab to accurately assess product effectiveness under realistic operating conditions. Each sample was executed against the product, with detailed outcomes recorded and supported by forensic evidence such as network captures, process traces, and system activity logs. Throughout the process, SecureQLab identified and documented any product issues or inconsistencies, worked to reproduce them, and validated fixes by re-testing updated versions provided by the vendor. The test concluded with a detailed, per-sample scorecard and a complete evidence set, giving the client full transparency into product performance.

All testing was conducted using a strict clean-state methodology to ensure consistent and unbiased results. Each ransomware sample was executed on a freshly provisioned, fully isolated system, primarily cloud-based virtual machines, with a small subset validated on physical desktops, to eliminate any residual impact from prior tests. Before execution, the environment was verified and monitoring tools were activated to capture system, network, and process activity. Samples were then executed and observed over a defined time window, extended when necessary for delayed behaviors. After each run, results and evidence were recorded, and the test environment was completely reset before proceeding to the next sample.

Each sample was executed using the following sequence:

- ▶ Provision a clean test VM from the pre-configured baseline image (QuellSecure installed, dummy file set populated, monitoring tools in place).
- ▶ Verify the integrity and structure of the dummy file set on disk before execution.
- ▶ Start evidence-collection tools: Process Monitor (filtered for the sample's process tree), Wireshark capture, host-side screen recording, and the QuellSecure agent log stream.
- ▶ Execute the ransomware sample manually on the target VM.

- ▷ Observe the system for 20–30 minutes by default. For slow-encrypting families known to delay activity (sleep/jitter, time-based triggers, or staged encryption), the observation window was extended to 1–2 hours.
- ▷ Record the verdict and capture all evidence artifacts.
- ▷ Tear down the test instance and provision a new clean VM from the baseline image. For physical-machine tests, the desktop was wiped and Windows 11 was reinstalled before the next test.

4.1 Ransomware Samples

SecureIQLab delivered a total of 499 ransomware samples to the client across the engagement.

The ransomware samples employed a range of encryption approaches, including symmetric, asymmetric, and hybrid methods, representing both legacy and modern cryptographic implementations.

In addition to cryptographic diversity, the samples employed multiple operational and process-variation techniques designed to improve stealth and execution efficiency. These included bitwise and blockwise encryption methods, segmented (partial) encryption, delayed encryption routines intended to evade behavior-based detection systems, batch-based encryption operations, and custom encryption implementation. Figure 5 highlights the percentage distribution of encryption techniques used within the in-the-wild ransomware dataset.

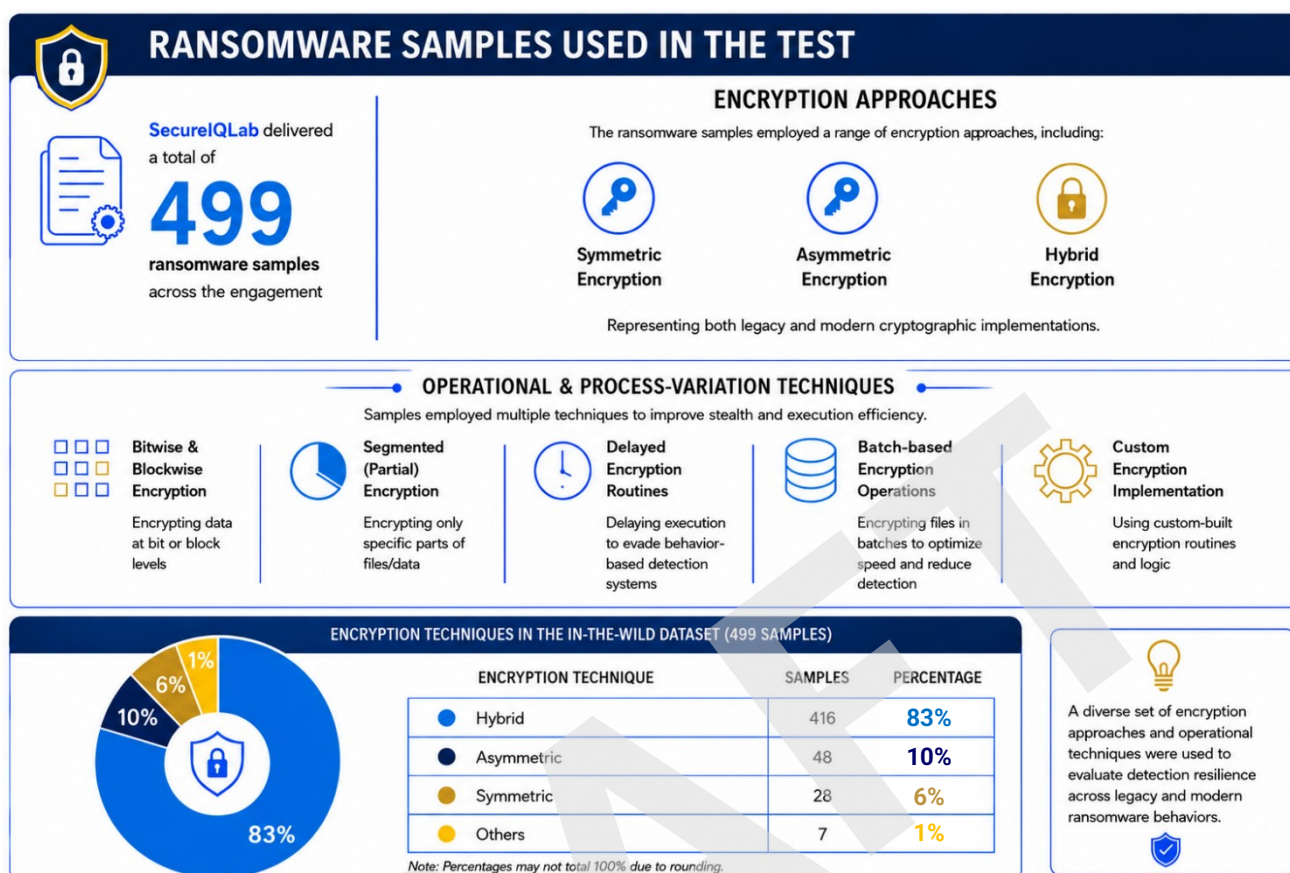


Figure 5: Ransomware samples used in the test

These samples were sourced from a combination of established malware-intelligence repositories and live ransomware tracking sources, including:

- ▷ ANY.RUN
- ▷ MalwareBazaar
- ▷ VX-Underground
- ▷ GitHub (publicly published research samples and proof-of-concept code)
- ▷ Ransomware.live

The in-the-wild set was curated to represent the most active and impactful ransomware families observed in the threat landscape, ensuring the product was evaluated against payloads it would realistically encounter in production deployments.

4.2 Ransomware Families

The SecureIQLab evaluation incorporated ransomware samples representing 117 unique ransomware families and groups, providing broad coverage across both historically significant and currently active threat actors observed in the wild. The testing included some of the most prevalent and operationally sophisticated ransomware groups observed in the wild, such as LockBit (3.0 and 4.0), Akira, ClOp, Black Basta, Conti, BlackMatter, Hive, ALPHV/BlackCat-related variants, REvil, Ryuk, DarkSide, Babuk, Ragnar-style operations, AvosLocker, Medusa, BianLian, Rhysida, Cactus, Qilin, and WannaCry. These ransomware families are known for advanced tradecraft, including hybrid encryption, intermittent encryption, and sophisticated key-management mechanisms.

In addition to major ransomware-as-a-service (RaaS) operations, the dataset also incorporated a large number of smaller, emerging, experimental, and niche ransomware variants such as Xorist, Chaos, JigSaw, HiddenTear, TeslaCrypt, CerBer, Dharma, GandCrab, Mallox, Makop, Lockergoga, Snatch, and many independently modified ransomware strains observed through threat intelligence feeds and underground distribution channels. Several samples also utilized custom encryption logic, delayed execution routines, reflective in-memory execution, and partial-encryption techniques designed to evade traditional detection mechanisms. By incorporating such a broad spectrum of ransomware groups and behavioral techniques, SecureIQLab ensured that the evaluation measured the effectiveness of QuellSecure not only against widely known ransomware families, but also against evolving and operationally diverse attacks of the modern ransomware threat landscape.

No. of samples used by Malware Family

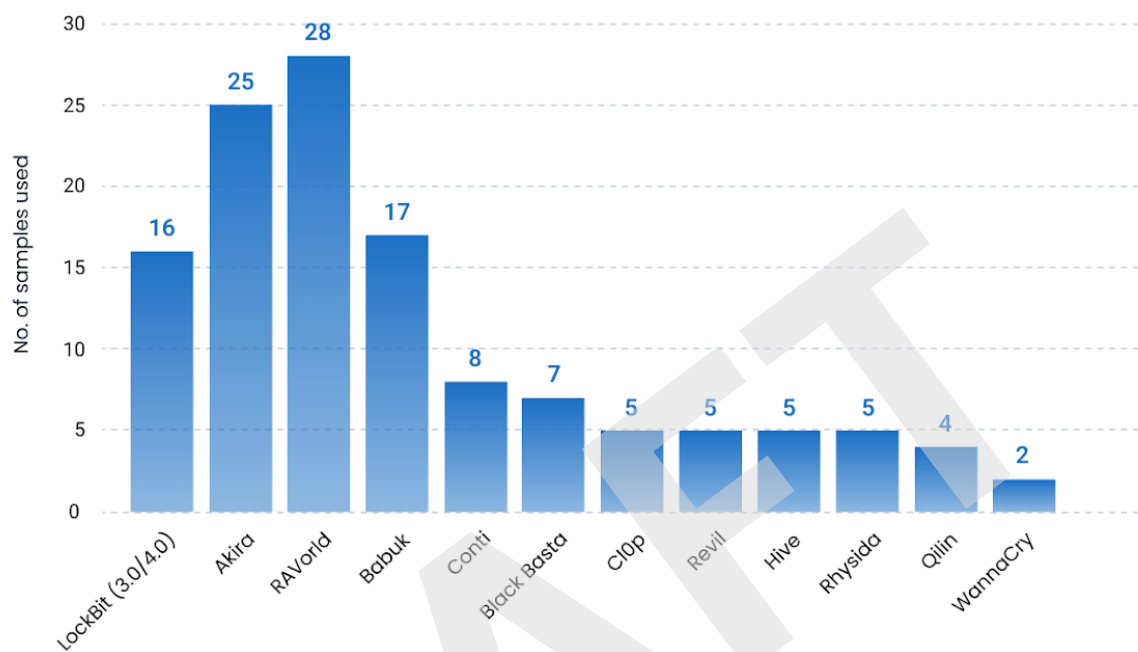


Figure 6: Most prevalent and operationally significant ransomware groups commonly observed in the wild

QuellSecure successfully detected and blocked all tested samples associated with these ransomware groups, including highly evasive and operationally mature ransomware-as-a-service (RaaS) families such as LockBit, Akira, Black Basta, Cl0p, REvil, and Conti. The results demonstrate strong effectiveness against both historically significant ransomware operations and currently active ransomware campaigns observed in the wild.

05

QuellSecure Build Details and Score Progression

SecureIQLab tested four QuellSecure builds across the engagement. QuellSecure delivered each successive build after addressing previously reported issues. Builds 1.1.4, 1.1.5, and 1.2.3 were tested as regression cycles re-running the samples that had previously failed against the newer build to verify whether the vendor's fixes had resolved the gap. The in-the-wild sample set comprised 499 samples drawn from major active ransomware families. Cumulatively across the first three builds (1.1.3, 1.1.4, and 1.1.5), 42 of the 499 samples, equivalent to 8.4% of the wild set failed at some point and required regression re-testing. The remaining 457 samples (91.6%) were blocked across the earlier build cycles. The progression across builds was as follows:

Build	Phase	Outcome
1.1.3	Baseline build	Initial test of in-the-wild samples. The majority were blocked; a subset of failures was identified, isolated, and reported to the vendor for remediation.
1.1.4	Regression of failed set	Re-test of the failures from 1.1.3 against the vendor's fixed build. Most were now blocked; a small residual set continued to evade detection and was reported back to the vendor.
1.1.5	Regression of remaining failures	Re-test of the remaining failures from 1.1.4. All re-tested samples were blocked at this stage.
1.2.3	Final validation re-test	All 42 samples that had previously failed at any point during the earlier builds were re-tested on the final consolidated build, and every one of them was successfully blocked. Final outcome on the in-the-wild set: 499 out of 499 (100%) blocked.

Following the final 1.2.3 build and subsequent re-testing, QuellSecure successfully blocked all in-the-wild ransomware samples, achieving a 100% detection and prevention rate (499 out of 499 samples).

False Positives

False positive testing was included as a critical component of this evaluation because a security solution that successfully blocks malicious threats but disrupts legitimate business activity can negatively impact enterprise operations and productivity. As part of the assessment, SecureIQLab executed 90 legitimate samples, interleaved with 10 previously blocked ransomware samples to validate detection and prevention consistency and operational accuracy. Of the 90 legitimate samples tested, QuellSecure correctly allowed 67 samples while incorrectly blocking 23 legitimate samples. Figure 7 below summarizes the results of the false positive assessment, reflecting a false positive rate of 25.6%.

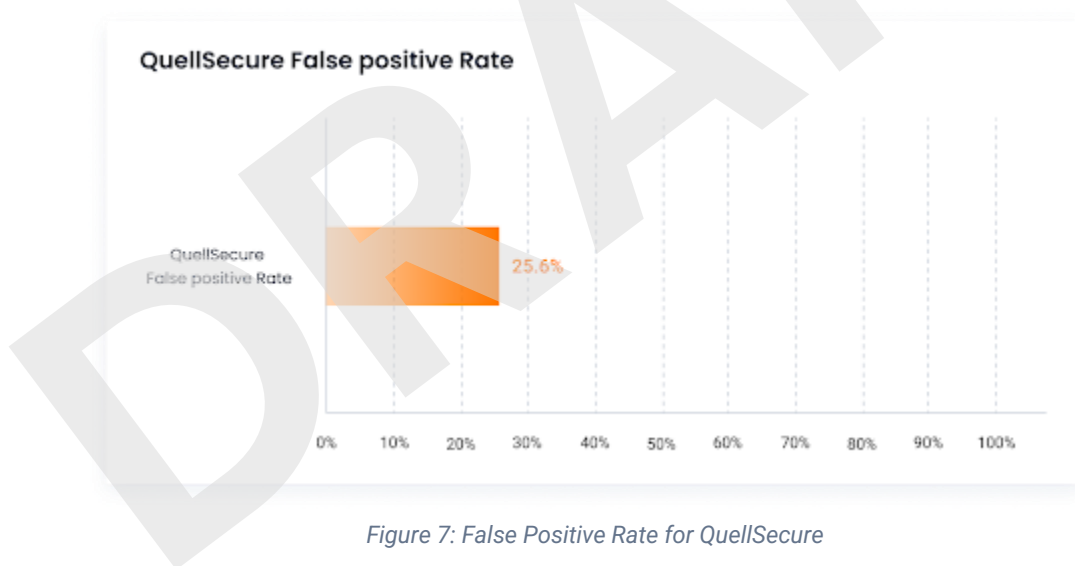


Figure 7: False Positive Rate for QuellSecure

Telemetry and Event Data

QuellSecure provides centralized telemetry and event visibility designed to give security teams insight into ransomware activity, detection outcomes, and endpoint response actions in real time. During the SecureIQLab validation engagement, QuellSecure continuously collected and surfaced security events related to ransomware execution, encryption behavior, process termination, quarantine actions, and system-level behavioral indicators through both the local desktop client and the Quell app web console. Throughout the engagement, QuellSecure telemetry captured ransomware-related behaviors such as active file encryption attempts, suspicious process execution, ransomware-triggered alerts, and containment actions including process termination and sample quarantine. 100% of the ransomware samples were quarantined and terminated during testing.

Evidence collection incorporated QuellSecure agent logs alongside Wireshark captures, Process Monitor traces, screen recordings, and supporting forensic artifacts to validate the accuracy of the telemetry stream. However, several inconsistencies were also identified during testing. These included delayed event visibility in the Quell app console, inconsistent logging across similar events, silent blocking without corresponding telemetry records, inaccurate encrypted-file counts, and intermittent notification failures were subsequently addressed and improved during later build cycles.

Conclusion

The QuellSecure validation results demonstrate a highly effective and reliable ransomware detection and response capability, achieving a 100% detection and prevention rate across all 499 in-the-wild test cases. The system consistently identified malicious activity and executed appropriate containment actions, including quarantine and termination, across a diverse set of 117 ransomware families.



Figure 8: The QuellSecure 100% detection and prevention in-the-wild ransomwares, validated by SecureIQLab

These results indicate that QuellSecure is well-positioned to provide robust protection against modern ransomware threats, with strong behavioral detection and prevention capabilities that extend beyond traditional signature-based approaches.

Disclaimers and Legal Notes

THE CONTENT OF THIS REPORT IS PROTECTED BY UNITED STATES AND INTERNATIONAL COPYRIGHT LAWS AND TREATIES. YOU MAY ONLY USE THIS REPORT FOR YOUR PERSONAL, NON-COMMERCIAL, INFORMATIONAL PURPOSES. WITHOUT SECUREIQLAB'S PRIOR WRITTEN CONSENT, YOU MAY NOT: (I) REPRODUCE, MODIFY, ADAPT, CREATE DERIVATIVE WORKS FROM, PUBLICLY PERFORM, PUBLICLY DISPLAY, OR DISTRIBUTE THIS REPORT; OR (II) USE THIS REPORT, THE SECUREIQLAB NAME, OR ANY SECUREIQLAB TRADEMARK OR LOGO AS PART OF ANY MARKETING, PROMOTION OR SALES ACTIVITIES. THIS REPORT IS PROVIDED "AS IS," "AS AVAILABLE" AND "WITH ALL FAULTS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, SECUREIQLAB EXPRESSLY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING: (A) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (B) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF THE REPORT, OR THAT USE OF THE REPORT WILL BE ERROR-FREE, UNINTERRUPTED, FREE FROM OTHER FAILURES OR WILL MEET YOUR REQUIREMENTS. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING SENTENCE, YOU ACKNOWLEDGE AND AGREE THAT THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT DEPEND UPON VARIOUS FACTORS, INCLUDING FACTORS OUTSIDE OF SECUREIQLAB'S CONTROL, SUCH AS: (1) THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF INFORMATION AND MATERIALS PROVIDED BY OTHER PARTIES THAT ARE RELIED UPON BY SECUREIQLAB IN PERFORMING PREPARING THE REPORT; AND (2) THE UNDERLYING ASSUMPTIONS MADE BY SECUREIQLAB IN PREPARING THE REPORT REMAINING TRUE AND ACCURATE. YOU ARE SOLELY RESPONSIBLE FOR INDEPENDENTLY ASSESSING THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT BEFORE TAKING OR OMITTING ANY ACTION BASED UPON THE REPORT. IN NO EVENT WILL SECUREIQLAB BE LIABLE FOR ANY LOST PROFITS OR COST OF COVER, OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES ARISING FROM OR RELATING TO ANY TYPE OR MANNER OF COMMERCIAL, BUSINESS OR FINANCIAL LOSS, EVEN IF SECUREIQLAB HAD ACTUAL OR CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE.

COPYRIGHT © 2026 SECUREIQLAB, LLC. ALL RIGHTS RESERVED.

For more information about SecureIQLab and the testing methodologies, please visit our [website](#).

About Us

SecureQLab is a US-based independent, third-party cybersecurity solution validation and advisory provider. The SecureQLab security methodology is tailored to what enterprises want, blending research, risk management, and data modeling performed by our deep bench of security experts. SecureQLab is a member of the Anti-Malware Testing Standards Organization (AMTSO).

SECUREIQLAB INC.

9600 Great Hills Trail Suite #150W
Austin, TX 78759 USA
+1.512.575.3457
www.secureiqlab.com
info@secureiqlab.com