ARTIFACT SECURITY

QUELLSECURE

RANSOMWARE IMPACT EVALUATION

January 2026

Prepared by

Stefan Dumitrascu
Ana Maria Pricop
Erica Marotta

amtso
The cybersecurity industry's testing standard community
CONFIRMED COMPLIANT

Introduction

Stefan Dumitrascu

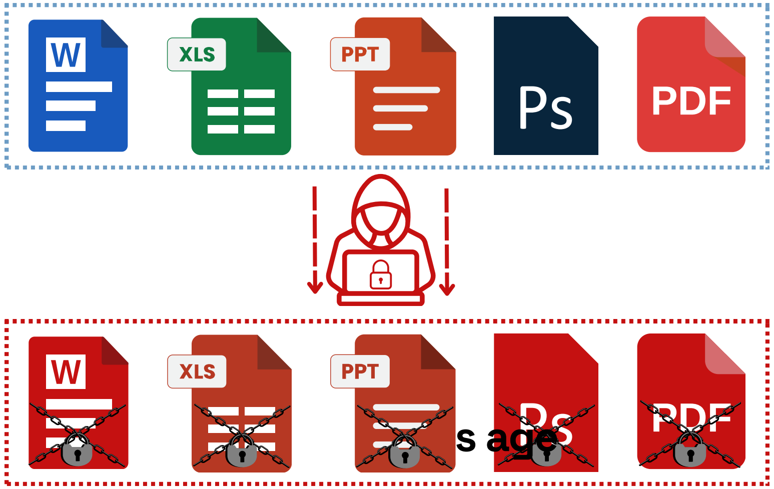
Chief Executive Officer

In the current threat landscape, ransomware dominates the news. Probably the oldest adage in cybersecurity is “It’s not a matter of IF but WHEN you will get hacked”.

Ransomware has been at the heart of some of the most disruptive attacks in recent history. Attacks such as Wannacry affected one third of NHS trusts in England. More recently the Change Health attack exposed the data of more than 50% of population of the US.

Ransomware is not just a nuisance, it‘s now a professionalized economic menace. While the largest organizations have the notoriety in the news, attacks in the SMB space come with great risks to business continuity and reputational damage.

Attackers find important files, encrypt them and demand payment



With so many ransomware operators around how do you deal with attacks when your traditional defenses break? What happens when your EDR gets bypassed?

State of Ransomware

88%
SMB INCIDENTS ARE RANSOMWARE*

$1.47M
REMEDIATION COST**

1⁄5
BUSINESSES CEASE OPERATIONS DUE TO RANSOMWARE.***

According to the Verizon’s 2025 DBIR*, ransomware is now present in 88% of all breach incidents involving SMBs. These are targeted by criminals because they are most likely to inflict critical damage. IBM’s Cost of Data Breach Report 2025** identifies the average cost to remediate an incident at $1.47 million, excluding the cost of any ransom payment. According to Mastercard’s 2025 Global SMB Study***, one in five businesses that suffer a major attack are forced to cease operations.

100%
DETECTION RATE

99%
RANSOMWARE IMPACT REDUCTION

7
AVERAGE # OF ENCRYPTED FILES

Quell detects ransomware encryption at the final moment, when files are being written. Less than **10 files are affected** before Quell intervenes to stop the ransomware attacks resulting in a **99% impact reduction.** Across all families tested, it maintained a 100% detection rate.

Executive Summary

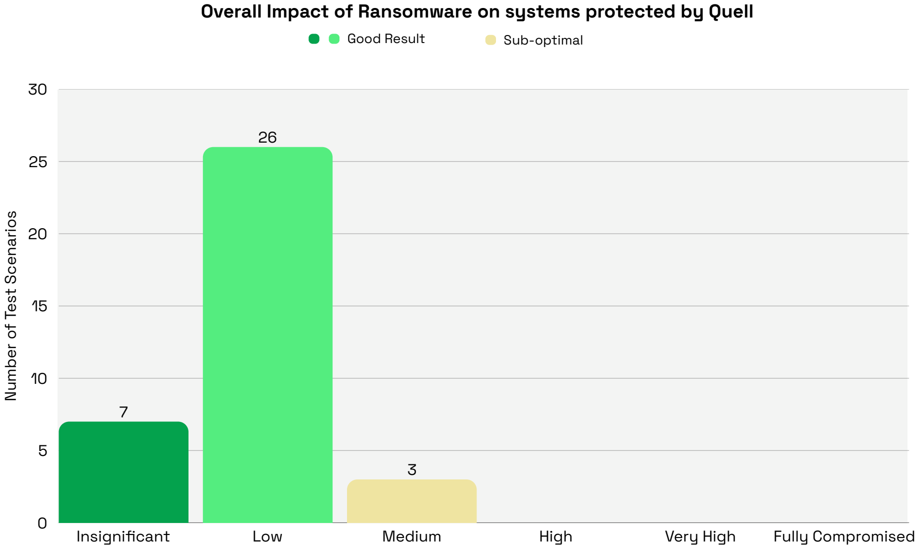
Evaluation notes

Quell's role is to add another layer of protection against Ransomware. Just as with any problem in cybersecurity, a layered approach is best to deal with this problem. The solution by Quell provides protection at the last moment, when files are being encrypted by the ransomware attack.

This acts as a final fail-safe when your traditional security products have been evaded. As it looks at the threat when the files are being written, it's not reliant on cloud lookups or tertiary technologies. In air-gapped environments it can prove especially useful as the product's efficacy is not influenced by network connection.

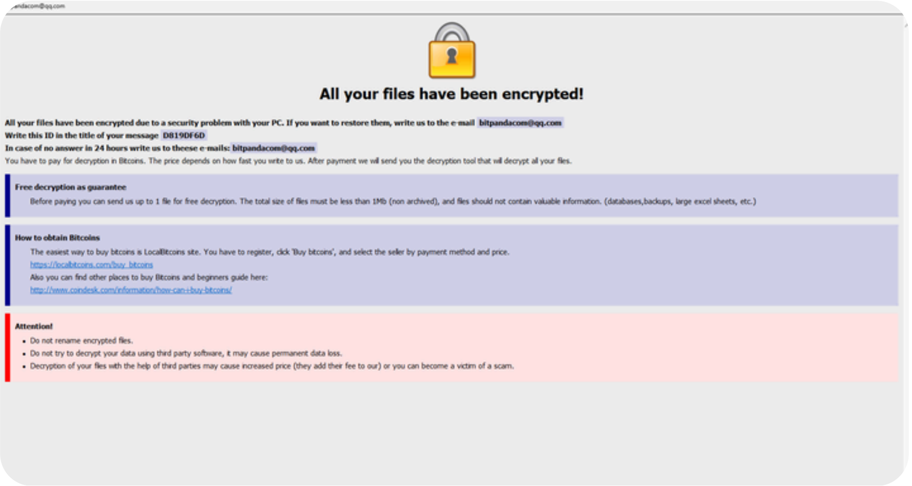
Overall Ransomware Impact Highlights

- Less than 1% of files encrypted across the whole evaluation (0.78%)
- 100% detection across all tested scenarios
- In most scenarios less than 10 files were lost to ransomware



Operational Ease and Features

Every IT team's worst nightmare is waking up to a screen like this. To limit the impact of ransomware events in the modern landscape a multi-layered approach should be implemented.



All your files have been encrypted!

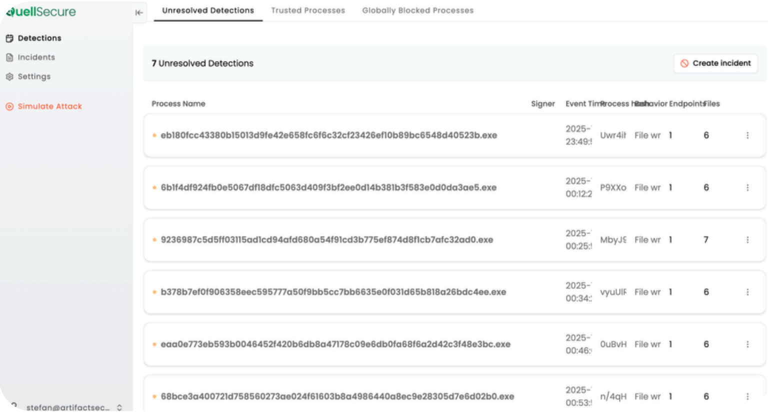
All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail bitpandacom@qq.com
Write this ID in the title of your message D819DF6D
In case of no answer in 24 hours write us to theese e-mails: bitpandacom@qq.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Quell's approach to ransomware protection centered on resilience, accepting that breaches will inevitably occur. Its agent analyzes encryption attempts and intervenes to stop them, ensuring the most valuable files are protected, minimizing the impact to an organization.



7 Unresolved Detections

Process Name	Signer	Event Tim	Process Hash	Behavior	Endpoints	Files
eb180fcc43380b15013d9fe42e658fc6f6c32cf23426ef10b89bc6548d40523b.exe		2025- 23:49:	Uwr4il	File wr	1	6
6b1f4df924fb0e5067df18dfc5063d409f3bf2ee0d14b381b3f583e0d0da3ae5.exe		2025- 00:12:2	P9XXo	File wr	1	6
9236987c5d5ff03115ad1cd94afd680a54f91cd3b775ef874d8f1cb7afc32ad0.exe		2025- 00:25:	MbyJ$	File wr	1	7
b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee.exe		2025- 00:34:	vyuUlF	File wr	1	6
eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc.exe		2025- 00:46:	OuBvH	File wr	1	6
68bce3a400721d758560273ae024f61603b8a4986440a8ec9e28305d7e6d02b0.exe		2025- 00:53:	n/4qH	File wr	1	6

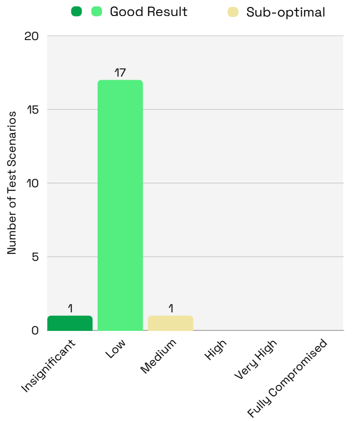
Quell's interface removes complexity so responders can focus on identifying and resolving incidents. This approach empowers a small security team to have an immediate impact on limiting the impact that ransomware has on an organization.

Targeted Industries

Results by Industry

organizations must move beyond general defense strategies and implement specific measures tailored to their industry. It's important to look at how the product behaves against ransomware targeting different verticals. This analysis is crucial for specific granularity when understanding and mitigating risk for your organization.

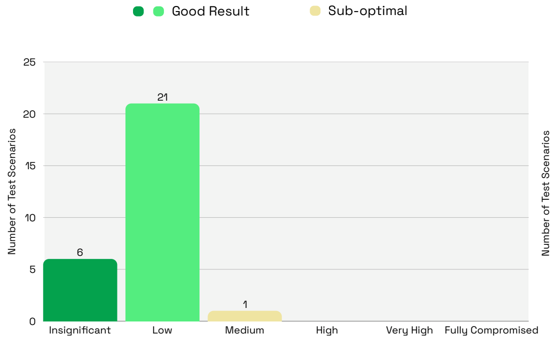
Impact of Healthcare Ransomware on systems protected by Quell



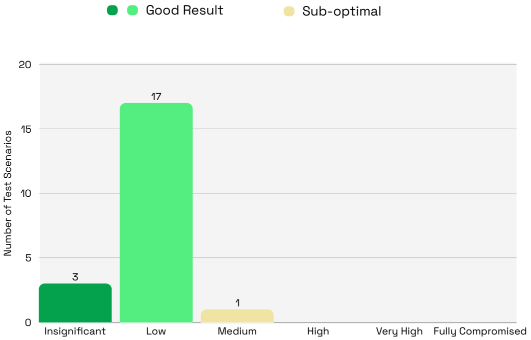
Across three critical infrastructure sectors, Quell performed consistently. The vast majority of the attacks were effectively neutralized before the impact reached Medium state. While each industry and organization faces their own regulatory hurdles and attack vectors, the results show that Quell can be part of mature security programmes to achieve predictable returns on investment.

This stability across sectors demonstrates that an industry-specific targeting does not result in a degradation of security performance.

Impact of Manufacturing industry focused Ransomware on systems protected by Quell



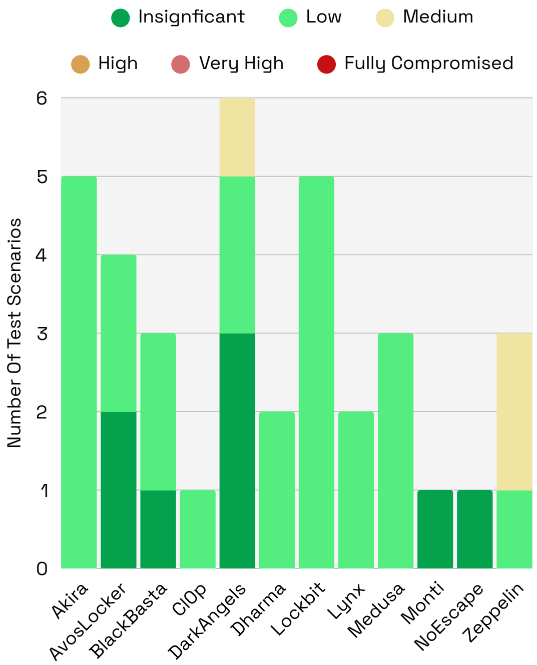
Impact of Education industry focused Ransomware on systems protected by Quell



Group Breakdown

Results by Group

When it came to designing this test one of our core goals was group diversity. There is no single silver bullet solution that will 100% protect against all types of ransomware no matter what other tests or marketing claims may say.



We tested Quell against a diverse range of ransomware families. Each family has their unique techniques employed for encryption, whether it was the speed-focused Akira family or sophisticated evasion techniques of AvosLocker, the results showed consistent performance. The negligible instance of Medium severity scenarios further reinforces the resilience of the detection and protection technology from Quell.

Ransomware Family	Operational Profile	Enterprise Risk
Akira	Highly active, known for rapid encryption.	Represents the new wave of RaaS focused on speed.
AvosLocker	Established, often uses complex internal obfuscation.	Benchmark for defense against established tactics, techniques, and procedures (TTPs).
BlackBasta	High-profile, frequent targeting of large enterprises.	Key indicator of resilience against financially motivated, mature RaaS operations.
ClOP, DarkAngels, Dharma	Mid-tier/evolving threat actors.	Ensures broad coverage across diverse behavioral profiles.
Lockbit	Historically the most prolific RaaS operation.	Essential benchmark for preventing large-scale organizational compromise.
Lynx, Medusa, Monti, NoEscape, Zeppelin	Diverse and geographically dispersed groups.	Validates efficacy against varied TTPs and encryption methodologies.

How we tested

It's essential for any test to reflect the real world. While everything happens in our controlled environment, we take great pride in our test framework's real-world approach. This ensures our findings offer an authentic representation of how the product reacts to threats encountered in the real world.

This test was focused on fully updated Windows 11 workstations.

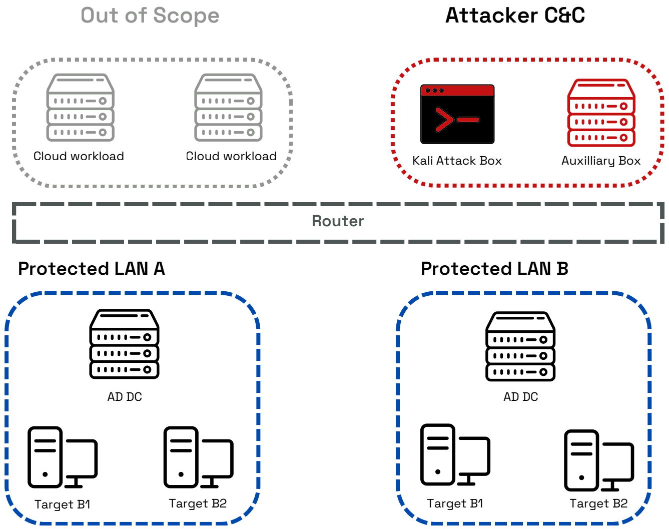
Rating Impact

We evaluated the effectiveness of Quell's agent post initial intrusion. As attackers made their way through the network and identified key targets, we measured the number of files that were encrypted when Quell's agent was deployed.

Severity	Insignificant	Low	Medium	High	Very High	Fully Compromised
Encrypted # of files	1 ≤ 4	5 ≤ 15	16 ≤ 50	51 ≤ 100	100 <	Complete

The thresholds we established range from Insignificant to Fully Compromised. It is impossible for our measurements to determine which ransomed files are more important than others. Depending on how sensitive your organization is to ransomware, you may want to define your own thresholds.

Infrastructure



Conclusion

Ana M. Pricop

Chief Business Officer

We believe in empowering security vendors with transparent, actionable insights while giving an accurate representation of the product's performance against the threats facing customers.

Through collaboration and continuous refinement we aim to constantly push security forward. If you have any questions regarding the testing, the results or are interested in more detailed view please don't hesitate to reach out to us. This test was executed under the AMTSO Standard.
Link to the testing page can be found here.

Quell's agent is a lightweight solution to the most prevalent threat targeting organizations worldwide.

Its ease-of-use, quick deployment and low TCO make it a valuable reinforcement in a multi-layered approach to security.

amtso
The cybersecurity industry's testing standard community
CONFIRMED COMPLIANT

Contact Us	→	info@artifactsecurity.co.uk
Website	→	www.artifactsecurity.co.uk