VIGILANT

VIGILANT VS RELIAQUEST

Managed Detection & Response (MDR)

When you choose Vigilant, what other suppliers call "options" come standard under our complete solution.

Unlimited Incident Response* Services at No Additional Cost

RELIAQUEST	VIGILANT	OUTCOME
Does not do IR	Comprehensive forensic IR	Risk decrease and lower cost

With comprehensive forensic IR, Vigilant is fully invested in our clients because our outcomes are directly tied to yours. ReliaQuest's lack of investment means that if they fail at their job, they may lose you as a client, but no further impact on them. We also ensure you never have to worry about uncontrollable costs going up due to the number of IRs. ReliaQuest does not – which can be costly.

Vigilant has a very defined IR response process which includes UNLIMITED Incident Response that covers the service(s) you subscribe to with no hidden up-charges which lowers costs and risk dramatically.

Complete Cybersecurity Lifecycle Care

RELIAQUEST	VIGILANT	OUTCOME
Event-driven alerts	Proactive analysis and preventative remediation	Threats identified and contained

Vigilant's proactive analysis offers guided responses and preventative breach remediation as part of the Cybersecurity Lifecycle, along with an Adaptive Intelligence Process™ that identifies and contains threats faster. ReliaQuest only provides event-driven alerts.

Vigilant also assigns a Client Success Manager for all things related to your MDR service, so you can always count on regular strategic conversations.

Proudly 100% U.S. Based SOC

RELIAQUEST	VIGILANT	OUTCOME
Staff offshore for SOC	100% U.S. Based	Trusted and vetted analyst, no shared resources

Vigilant does not rely on shared resources. Our secure 24/7/365 SOC is here in the U.S. – always within reach – to provide the trusted and vetted analysts you deserve. ReliaQuest staffs an offshore SOC and offers a U.S. based option that only provides a limited service.

Better Correlation Between Multiple Source Points

RELIAQUEST	VIGILANT	OUTCOME
SIEM, EDR	EDR, NDR, Microsoft 365	Correlation between multiple source points

Vigilant's proprietary detection logic provides real-time insight on what's happening in your environment by fusing together network, endpoint, and Microsoft 365 Exchange data.

Vigilant's source content collection results in a more confident and coordinated confirmed response, which keeps attacks from being successful.

* Unlimited incident Response coverage is only for contracted Vigilant services

TIMELINE OF AN ATTACK

VIGILANT PREFERS THE CERTAINTY OF BLACK-AND-WHITE VS. GREY

With Vigilant Managed Detection and Response the operative word is "managed." Our advanced technologies are always backed by human intelligence that takes decisive action quickly. We are so confident in our approach to VigilantMDR services that we back them with our Unlimited Breach Response warranty.

VIGILANT	VS. RELIAQUEST
Threat in the environment is observed	Threat in the environment is observed
Ticket is issued	Ticket is issued
Client is called	Client is called
Device that was infected is confirmed	
Device is quarantined	
Custom detections are created via correlations with Network and End Point to identify other potential risks within the organization on other identified devices/networks	
Threat activity is blocked	
Environment is scanned for any additional persistence mechanisms	ReliaQuest recommends actions to take, but does not assist with the remediation without costly add-ons
Persistence mechanisms are removed to ensure the Threat Actor has no access back into the environment post threat remediation and removal	No correlation between sources (due to no Tier One network visibility and no packet capture depth)

CUSTOMER QUOTE

> I have been extremely happy with the services Vigilant provides because I can sleep at night knowing I am not going to get breached. They are my secret weapon against attackers.

VIGILANT

Let Us Prove It. Ask Us How

855-238-4445 | www.vigilantnow.com | sales@vigilantnow.com