RELIAQUEST®

Solution Brief

Mitigating Impact from Ransomware with ReliaQuest GreyMatter and EDR Integration

End-To-End Detection, Investigation, and Response to Prevent and Reduce Impact.

Ransomware costs more than the ransom

Ransomware has become one of the most destructive attacks in cyber security in recent years. According to an industry report, ransomware attacks increased by 127% last year and is showing no signs of slowing down, making it the center of attention for many enterprises.

With the proliferation of ransomware, it's essential to understand the potential impact to the business. The cost of ransomware goes well beyond just the amount demanded. The effects of halting critical systems and disrupting business continuity can be devastating.

How well do you understand your coverage against this threat and what strategies should you have in place to mitigate its potential impact?

$1.85 Million — The average bill for recovering from a ransomware attack.

23 Days — Average downtime once attacked.

87% — The number of consumers willing to take their business elsewhere if a data breach occurs.

Why can't organizations protect and respond to ransomware attacks?

Oftentimes, it is difficult to know when you need to take the next step towards procuring additional security coverage. We have captured several scenarios we hope will help your organization decide when the time is right to invest in a ransomware protection.

Lack of EDR or Maximizing value from existing EDR

While ensuring you have a solid data backup system is a critical mitigating control, running effective Endpoint Detection and Response (EDR), email security, and Phishing protection programs are equally essential. Even if you have an EDR, many times there are not enough resources to properly run the system and keep it optimized against evolving threats. Important pieces to assess include:

- Do you have visibility across all your endpoints?
- What portion of your environment is EDR deployed, working, and visible? Is it tuned and up to date?
- Can you proactively hunt for threats?
- Do you know what your MITRE ATT&CK coverage looks like?
- Do you have someone building detection content?
- Do you have ransomware specific threat intel?

If your answer is NO to these questions, investing in an EDR is a crucial next step to protect your organization. And if you have EDR systems already, you need to ensure that it is optimized and detecting evolving threats and should be integrated with the rest of the ecosystem to ensure enterprise-wide incident response.

Common Challenges:

- Limited visibility at the endpoint
- Lack of staff/skills
- Too many tools
- Fragmented investigations
- Pace of bausiness change
- Expanding attack surface
- Manual and inefficient processes

Rapid business change

Most security operations teams face a dynamic business environment, hustling to ensure their security programs are keeping pace. As companies encounter M&As, digital transformation, and further globalization of the supply chain, it's difficult to ensure coverage across all environments.

Inability to proactively verify detection controls

Analysts are frequently swamped with outdated, inaccurate alerts that end up taking valuable time that could be spent on the most viable, damaging threats.

Take the right steps with your existing investments to mitigate the risk.

Leveraging the GreyMatter platform, analysts are provided rich context around a ransomware security event, with better visibility to detect an incident, identify the root cause, and assess the impact of a given threat.

How do we do it? Read our step-by-step process that explains how we provide end-to-end Ransomware protection for your organization.

Stop the initial entry

As the most common vector, blocking phishing attempts via a robust email security gateway, configured to the vendors "best practices" is your most effective entry control. But then there are those phishing attempts that inevitably evade even the best email security gateways. ReliaQuest can support the analysis of those attempts that are either detected after the "click" or "flagged" by a trained user and forwarded to the "phishing email" box.

Stop the spread

If initial email entry controls fail, your endpoint and EDR controls are your next "defense in depth" measure and are critical to stopping the initial exploitation and subsequent spread within an environment. ReliaQuest ensures that your EDR tooling and threat intelligence capabilities are in sync and up to date as rapid detection reduces the potential impacts, and therefore overall risk. In addition, ReliaQuest will assess the health of your EDR and determine what steps are needed to tune your content most effectively.

While EDR tools may be able to block and/or alert that ransomware has hit a system, you still need to investigate and identify the root cause of the infection to make sure it doesn't happen again. ReliaQuest provides this crucial support though our investigation and incident support capabilities.

Benefits of our end-to-end protection:

- 400% improvement in threat detection
- 5X threat hunting acceleration
- Ability to negotiate lower insurance premiums
- 350% ROI in less than 6 months
- Reduce noise by 90%
- Reduce likelihood of breach by 20%

Automate response

Based on root cause analysis cited above, subsequent attempts can be automatically mitigated via GreyMatter's automation plays. Examples include blocking malicious email domains, banning hashes, deleting files, or quarantining hosts.

Continuous surveillance

How does ReliaQuest provide continuous ransomware protection?

- Singular visibility across your ecosystem – on-premises and cloud
- Field-tested detection content packages optimized to your tools
- Automated breach and attack simulations to ensure that your security controls are effective and working
- Contextual enrichment of threats correlated with your detections
- Maps to MITRE ATT&CK framework that shows you, in real-time, your coverage
- Automation across the security lifecycle so you are efficient in detection, investigation, and response

ReliaQuest makes actively preventing, detecting, and analyzing ransomware simple by integrating and normalizing data from disparate technologies including SIEM, EDR, multi-cloud and point tools, on demand. It provides a unified view to immediately and comprehensively detect and respond to threats from across your environment.