

# How GreyMatter Discover Can Mitigate The Most Common Exposures Organizations Face

Mark Noble  
GreyMatter Engineer

# What You Can't See **CAN** Hurt You

**50%**

Of incidents involve assets that are unknown or “uncovered”

# The Importance of Connecting Asset Visibility to DIR

Without a connection to your security operations workflow, discovery findings sit in a separate system. Exposures are identified, but not acted on.

Your team spends hours chasing basic asset details while attackers can exfiltrate data in less than 6 minutes.

# GreyMatter Discover Unifies The View of Your Attack Surface



# GreyMatter Discover Use Case: Endpoint Missing EDR



## Asset Discovery

- A new endpoint is discovered from Windows event logs in the SIEM and the vulnerability scanner



## Coverage Gap Analysis

- The unmanaged device isn't seen by other security tools and doesn't have an EDR agent installed



## Vulnerability Enrichment and Prioritization

- A critical unpatched vulnerability is detected on the device
- Asset is prioritized as a critical risk



## Exposure Remediation

- EDR agents are deployed to close gaps—blocking adversary from exploiting the exposure

GreyMatter Discover



**Thank you**

[www.reliaquest.com](http://www.reliaquest.com)

800.925.2159

[info@reliaquest.com](mailto:info@reliaquest.com)