How **ReliaQuest GreyMatter** Amplifies the Power of Microsoft Sentinel

Lately, many of our customer and prospects are asking us the same question:

"We purchased the Microsoft 365 bundle with its suite of security technologies. What should we implement first and how will this impact our security architecture?"

Below, we've listed a few things you should consider as you decide how to maximize your Microsoft 365 E5 license from a security perspective. They'll help you determine how a move to Microsoft security tools, including Microsoft Sentinel, can help improve your security posture and operational efficiencies while controlling costs.

One License, Many Tools and Many Decisions

You now have access to the full suite of Microsoft security tools. **What tool should you integrate first?**

There are several paths you can take to make your move to Microsoft 365 E5, but the good news is that you can integrate Microsoft security tools at a pace that makes sense for your organization. In this brief, we will explore what it looks like to start your journey with Microsoft Sentinel.

> Microsoft Sentinel centralizes event collection, detection, response, and investigation efforts.

Things to Consider Before You Make the Move

Where is your organization on its path to cloud transformation? If you have made the commitment to move to the cloud and want to optimize your cost structure, now may be the time to look at integrating Microsoft Sentinel into your security stack.

By sending event logs from other Microsoft products, including Defender for O365 and Defender for Endpoint, to Microsoft Sentinel, your transition is likely to be easy and seamless, and you'll minimize your storage costs.

Do you have an existing SIEM in place (Splunk, QRadar, Exabeam, etc.) and want to avoid affecting your organization's current security posture?

Consider maintaining your existing SIEM for non-Microsoft log sources, while directing Microsoft logs to Microsoft Sentinel. In this way, you can not only start to take advantage of your E5 license, but you can also ensure your team is trained on Microsoft Sentinel before you go all-in.

Before you begin to evolve your environment, you will want to identify key use cases, detection rules, data, and automation in your current SIEM.

Approach your migration to Microsoft Sentinel as a gradual process. Your team might have an overwhelming number of detections and use cases running in your current SIEM. Before beginning migration, decide which ones effectively address the risks that are most significant to your business.

Are there any potential blockers to your move?

For example, license expiration dates for your existing security tools, support for holidays and events, product launch dates, etc.

Do you have the skills you need to make the transition?

Is your security staff trained and ready for the migration? Do not underestimate the need to train and retrain.

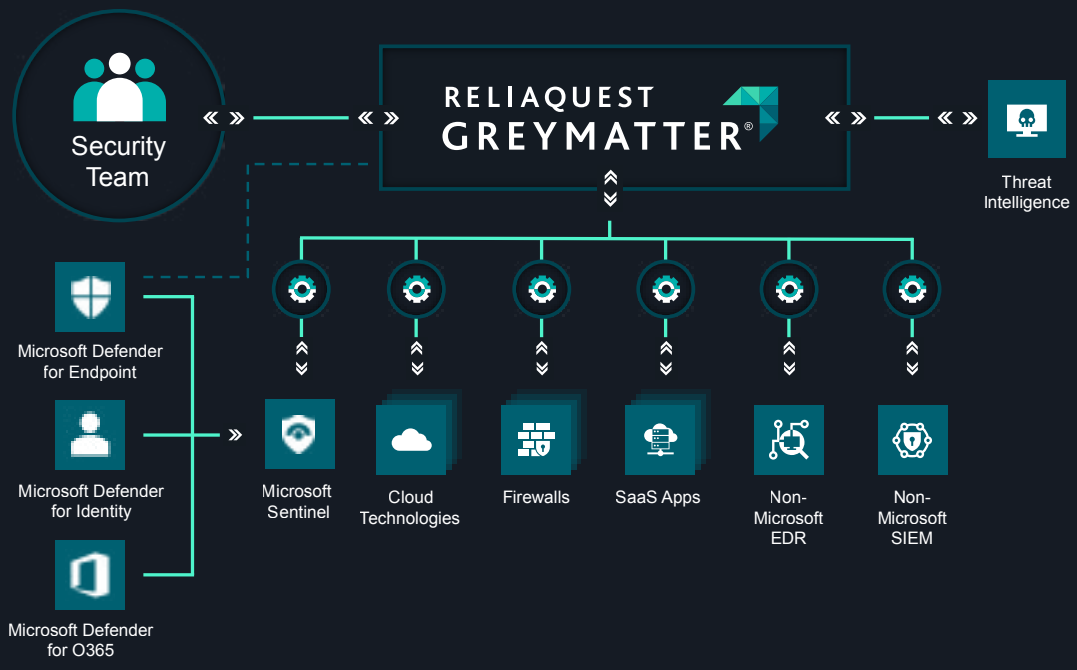
What is your data retention policy? If you are in a highly regulated industry, data retention mandates may influence your decision.

For example, if you need to maintain logs for 3, 5, or 10 years, Microsoft Sentinel may be the lower-cost data-storage option.

As you ramp up your use of Microsoft security tools, make sure your security operations team has adequate visibility and the ability to detect risks and investigate and mitigate alerts across your security tools, whether on-prem or in one or more clouds.

Ensure you can unify detection, investigation, and response across existing tools and new ones, while you integrate Microsoft security products at the pace that best suits your organization.

GreyMatter brings together telemetry from Microsoft and non-Microsoft security solutions to deliver singular visibility across the entire enterprise ecosystem.



- **Increased Visibility**
- **Reduced costs for cloud egress and data storage**
- **Leverages Microsoft Sentinel for Microsoft Telemetry**
- **Simplicity delivers resiliency**

Enhance Operational Efficiency and Reduce Costs with ReliaQuest GreyMatter and Microsoft Sentinel

Improve operational efficiency and reduce costs by:

- Integrating Microsoft Sentinel and Microsoft Defender tools into the GreyMatter security operations platform helps you optimize and leverage your Microsoft 365 investment, making it possible to run multiple vendor solutions in parallel with the Microsoft stack through a single pane of glass without adding more “swivel chair” security for your analysts.
- Providing Managed Microsoft Sentinel and Managed Defender (Endpoint, Active Directory, Identity, Office 365) tools with MDR outcomes.
- Deploying threat detection rules from GreyMatter directly to Microsoft Sentinel and Microsoft Defender for Endpoint for rapid detection and tuning.
- Reducing the need for expensive “data transformation” tools and avoiding cloud data egress costs by sending native Microsoft logs from Defender for Endpoint, Defender for O365, etc., directly to Microsoft Sentinel.

- Getting unparalleled visibility across your security infrastructure and the ability to investigate and take response action with bi-directional integration across any Microsoft and non-Microsoft solution, whether on-prem or in one or more clouds.
- Reducing the reliance on existing higher-priced SIEM vendors who impose data egress fees and charge high data storage costs.
- Improving security posture with actionable metrics and coverage maps to industry-standard MITRE ATT&CK framework.
- Automating security operations processes and using configurable playbooks to reduce MTTR from hours to minutes.

ReliaQuest GreyMatter is a security operations platform built on an open XDR architecture and designed to help security teams increase visibility, reduce complexity, and manage risk across their security tools, including on-premises, clouds, networks, and endpoints.

GreyMatter can ingest data on demand, no matter where it lives, so you can respond quickly to threats. It provides singular visibility across the entire enterprise ecosystem, unifying detection, investigation, and response.

APi Group used GreyMatter to increase visibility by 47% and Secures Expanding Attack Surface Across their Microsoft Office 365 E5 Security Suite.

3.5x Increase in MITRE ATT&CK coverage resulting in better, higher fidelity detections.

52% Decrease in response times while managing risk through automated playbooks.

APi GROUP

"The Microsoft stack is great, but one of the challenging things is that people cannot easily pick up the query language. So, when it comes to making accurate detections, you really need solid detection content- and that's where ReliaQuest comes into play for us."

RELIAQUEST®

reliaquest.com 800.925.2159 info@reliaquest.com

Copyright © 2023 ReliaQuest, LLC. All Rights Reserved. ReliaQuest, GreyMatter, Digital Shadows, and all related logos, product and services names, designs, and slogans are trademarks or registered trademarks of ReliaQuest, LLC or its affiliates or licensors. All other product names or slogans mentioned in this document may be trademarks or registered trademarks of their respective owners or companies. The ReliaQuest software, platform, portal and its entire contents, features, and functionality are owned by ReliaQuest, LLC and its affiliates. These materials are protected by United States and international copyright, trademark, patent, trade secret, and other intellectual property or proprietary rights laws. All other information presented is provided for informational purposes with no representations or warranties provided of any kind and should not be relied upon for any purpose. ReliaQuest has no obligation to amend, modify, or update the information contained in this document in the event that such information changes or subsequently becomes inaccurate. Printed in the USA.