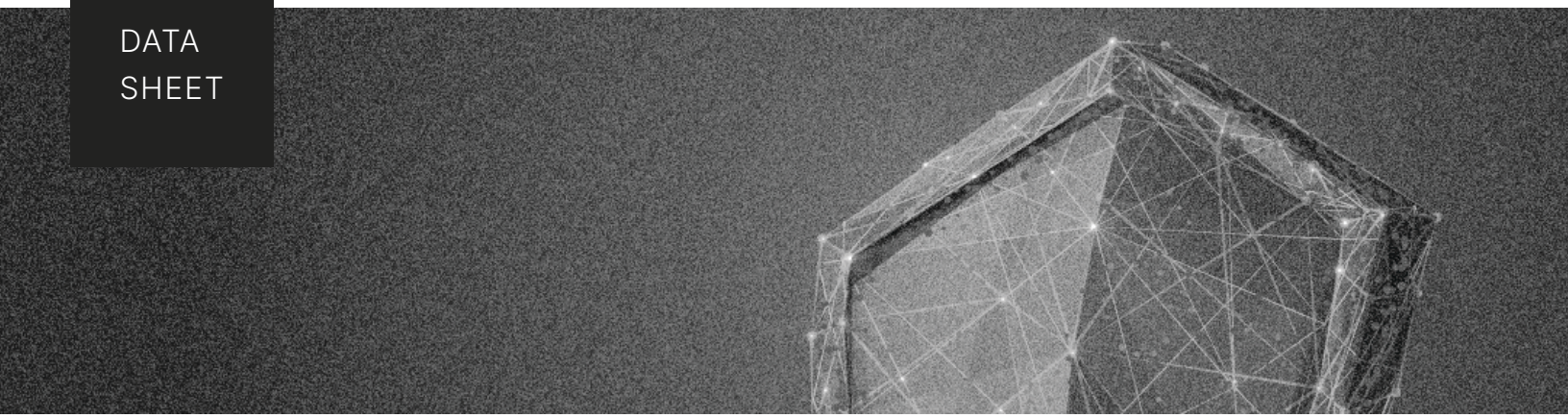
Recorded Future®

DATA SHEET



Recorded Future Integration with Microsoft Defender for Endpoint

BENEFITS

- Proactively blocking of threats before they impact the business
- Continuous threat protection, by automatically keeping your Microsoft Defender for Endpoint instance updated with the latest security intelligence
- Maximize your investment in Microsoft Defender for Endpoint by utilizing your Microsoft Sentinel Services

KEY FEATURES

- Real-time intelligence on known Command and Control servers and recently weaponized domains
- Out-of-the-box integration for delivering indicators to Microsoft Defender for Endpoint

This integration requires the organization to have a Microsoft Sentinel account with the Microsoft Sentinel application enabled

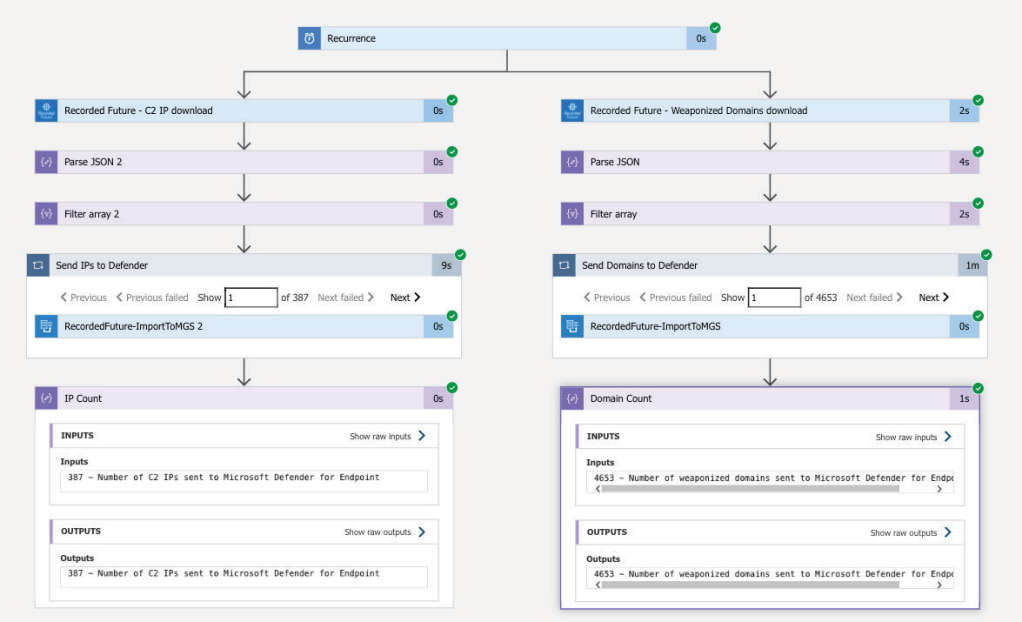
The ever-growing number and dynamic nature of threats make it extremely difficult to identify, triage, and prevent attacks. There's just too much information to analyze, too many security controls to update, and too little visibility to threat activity outside of your organization.

Recorded Future helps security teams reduce their risk exposure by collecting, analyzing, and delivering actionable security intelligence. With this integration, high confidence indicators are automatically sent to Microsoft Defender for Endpoint, so that security teams can proactively protect their organizations from emerging threats.

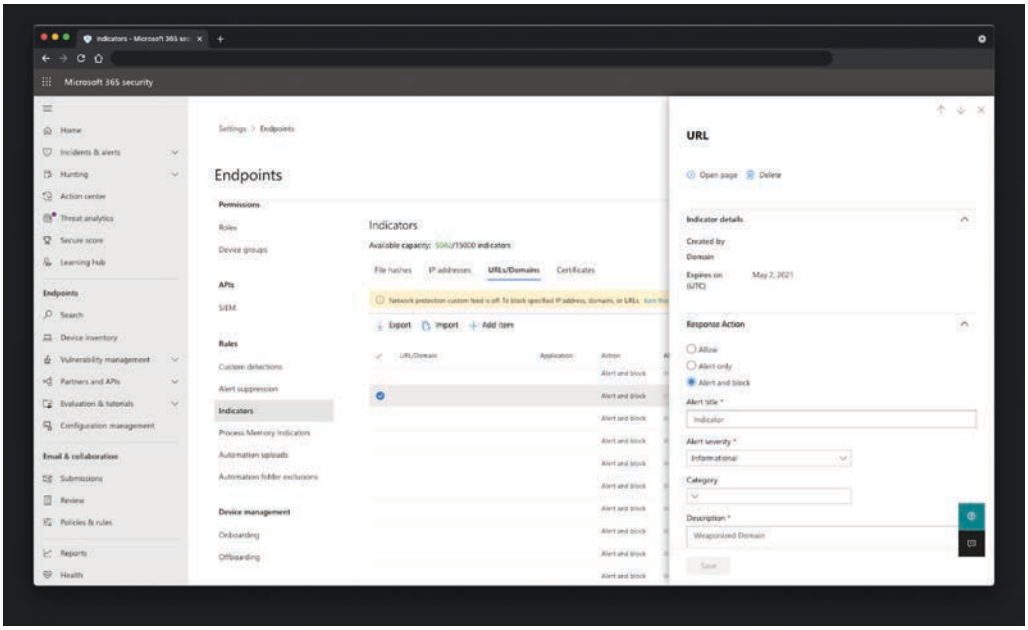
Proactive Threat Prevention

Recorded Future continuously monitors hundreds of thousands of open, closed, and technical sources to determine where emerging threats are coming from. This security intelligence, in the form of high risk IP addresses and domains, can be automatically and continuously delivered into Microsoft Defender for Endpoint, formerly known as Microsoft Defender ATP, for alerting and blocking suspect network traffic. As a result, endpoints and their corresponding users will be automatically protected from malicious sites and potential damage to their organization.

The Recorded Future integration with Microsoft Defender for Endpoint provides out-of-the-box protection against known high risk Command and Control IP addresses, as well as newly registered domains that appear to have been weaponized. This is accomplished through Microsoft Sentinel Logic Apps, and relies on the Threat Intelligence capabilities of Microsoft Sentinel to deliver the indicators of compromise into the Defender for Endpoint indicator repository in real time.



The integration uses a Microsoft Sentinel logic app to deliver high confidence indicators to Microsoft Defender for Endpoint, via the Microsoft Graph Security.



Recorded Future indicators appear in Microsoft Defender for Endpoint and are preconfigured for "Alert and Block"

ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

www.recordedfuture.com @RecordedFuture