DATASHIELD™ | an ADT company

The **PACKET ADVANTAGE** | with DATASHIELD MDR

- These are the Top 7 Reasons Why Packet Level Detail is Far Superior to Simple Logs -

1 **ROOT CAUSE ANALYSIS -** Logs usually provide insight into how devices responded, but full packet capture tells the story of what actually happened. Packet data eliminates ambiguity and provides context that simply isn't available in any other alerting or monitoring medium.

2 **HIGHER RESOLUTION ALERTING -** Packet capture provides insight into the life cycle of a session, what it contained, and how it evolved. This is extremely valuable for alerting, and provides threat analysts with more tools to detect malicious activity faster and with greater accuracy.

3 **PROTOCOL DETAILS -** Packets provide hundreds of additional data points that can be queried, analyzed, and correlated that aren't available in logs alone. Deeper inspection of protocols gives both security analysts and system engineers better awareness of their environment.

4 **VENDOR AGNOSTIC -** With access to raw data, an analyst does not need to rely on what an IDS/IPS/firewall vendor thinks is important in a session. While useful and often relevant, vendor severity thresholding may not keep pace as quickly as needed with the evolving threat landscape.

5 **FORENSIC REPLAY AND RECONSTRUCTION -** The ability to replay a session and extract files or other artifacts enriches and advances threat intelligence and investigations. This eliminates doubt as to the contents of a flagged event and gives analysts more actionable data and intelligence on what's actually moving over the wire.

6 **DEVICE POLICY VETTING AND ENHANCEMENT -** Comparing packet data to IDS/IPS/firewall responses can aid in network hardening by identifying misconfigurations and device rules that are inadequate in stopping malicious activity. Packet data improves security posture and helps get the most out of existing security infrastructure.

7 **REDUCED FALSE POSITIVES -** Logs simply don't contain the wealth of data seen in packets. There are fewer avenues of whitelisting available in logs, whereas packets may have dozens of headers, payload specifics and enrichments that can be used to refine and streamline noisy alerts. Packet data reduces analyst – and customer – workload, enriching the entire solution.

ABOUT **DATASHIELD**™

DATASHIELD acts as an extension of your cybersecurity team providing continuous monitoring with "eyes on glass" 24X7.

A technology agnostic approach with active hunting, forensic analysis and remediation actions, are baked into the methodology.

GET PACKET LEVEL DETAIL –
Eliminate Cyber Threat Uncertainty

PARTNER WITH
DATASHIELD
& STAY DEFENDED