snare
A PROPHECY SOLUTION

Effective Compliant Logging While Reducing Size and Volume of Logs Generated

Effective Compliant Logging While Reducing Size and Volume of Logs Generated

How often do we hear, “I’m swamped with the amount of data we collect?” It's a common problem when all log data is collected without considering resource costs, network bandwidth, or destination management.

Using an agentless log collection approach can worsen the issue, as it limits control over what data is collected, creating a “catch-all” scenario. This leads to excessive log data, much of it redundant, and results in massive data stores that become difficult to sift through during an incident. Different compliance and regulatory rules, depending on the organization’s sector, determine what data needs to be collected and how long it must be retained.

The challenge is to streamline log collection to ensure compliance and audit governance while maintaining a manageable stream of relevant data. Event log data may also need to be directed to different destinations or separated to meet compliance and audit requirements.

- Limited log collection capabilities
- Will only collect logs attaining to an incident
- No user interface (UI)
- No filtering options
- No destination management

What a Solution Could Look Like

The first question is which log data needs to be collected. The answer depends on the market sector your organization operates in and its compliance and audit requirements. Adopting a prescriptive and granular approach is key to streamlining log collection.

Step 1 involves identifying the event logs that must be collected and filtering them at the source to ensure only these events are captured.

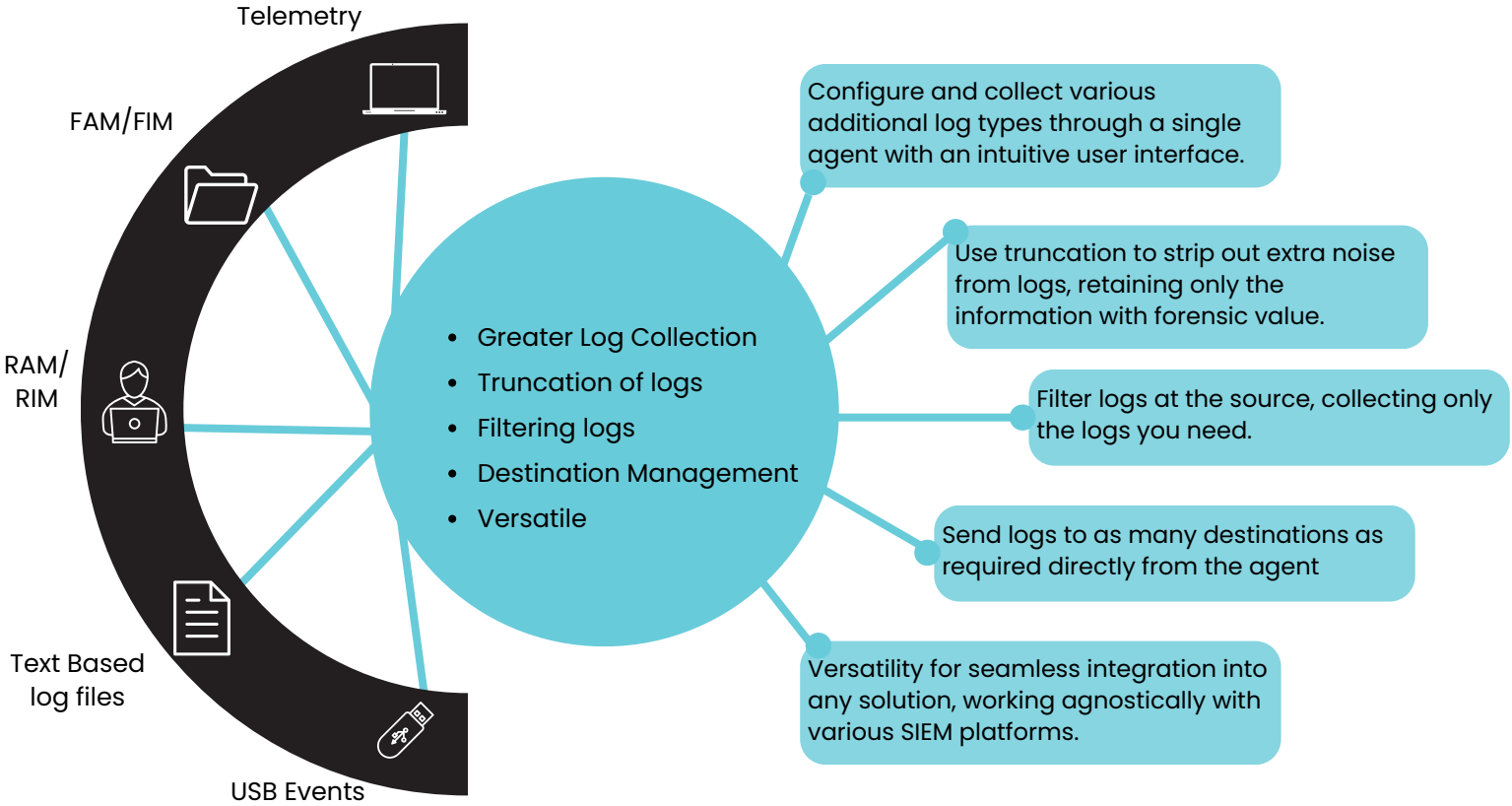
Step 2 focuses on identifying noisy events and removing unnecessary data at the source, so only the forensic values of each event log are collected, transmitted, and stored.

Security teams gain immediate value by reducing log sizes and ingestion costs. Over time, the value grows through storage tiering and data routing, which allow logs to be redirected to the most appropriate storage locations.

Once filtered, logs must be sent to their destinations. Cyber policies may require logs to be stored in multiple locations, segmented by compliance rules or legal and audit requirements. For instance, payment card information (PCI) data may need to go to one destination, while domain controller data is stored elsewhere

Initial discussion and technical evaluation → Proof of concept (POC) and technical walkthrough → Deployment

Snare Architecture

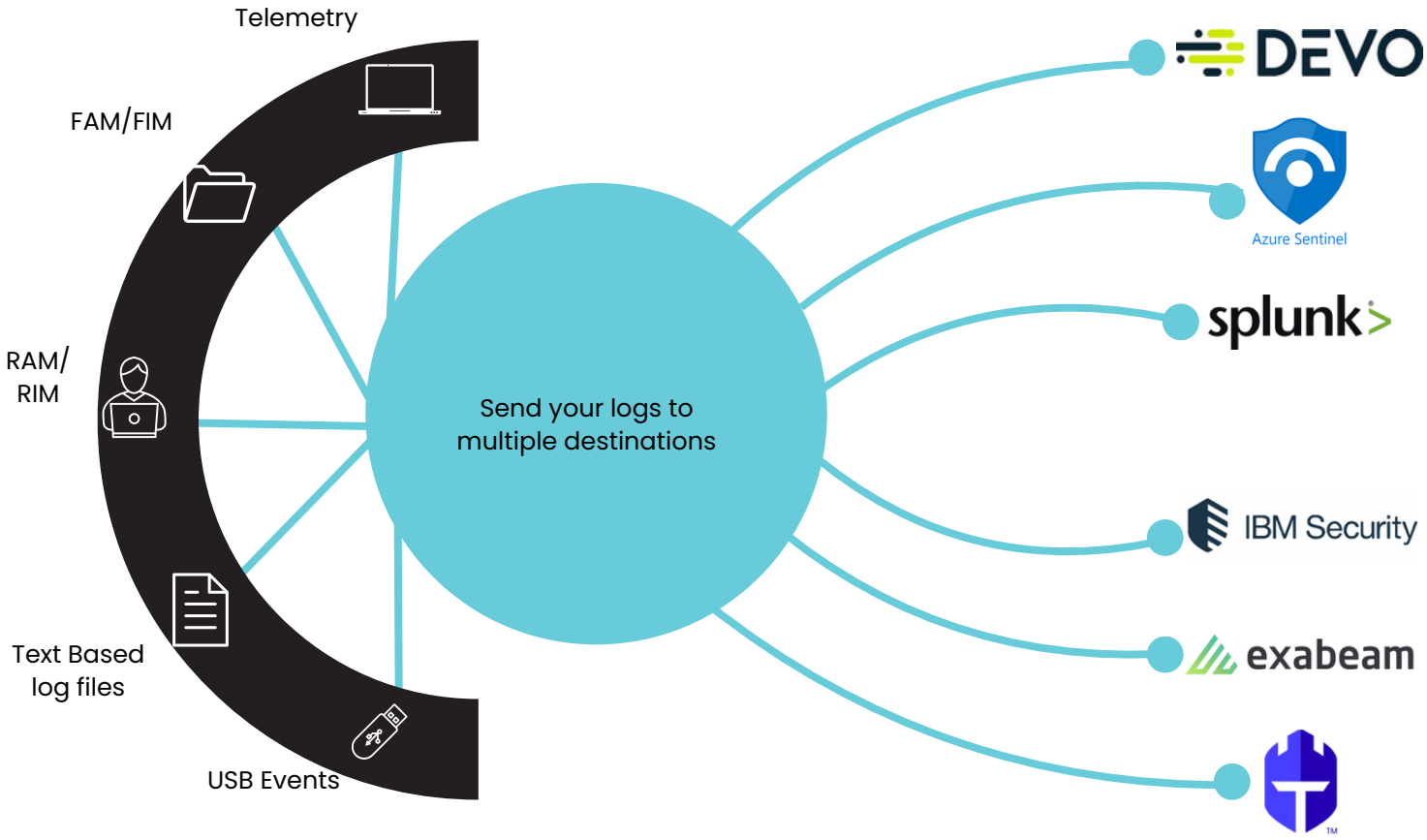


This is where data pipeline management (DPM) tools for security come into play. DPM tools can route, reduce, redact, enrich, or transform data to meet organizational needs.

Efficient Log Collections and Storage

A streamlined approach to efficient log collection and destination management lets organizations:

- Collect only the data needed, reducing resource utilization.
- Lower the volume of log data collected.
- Decrease the size of event logs generated.
- Ensure transmitted log data contains only forensic values.
- Minimize the impact on network bandwidth during transmission.
- Direct logs to specific destinations based on event type and content.
- Reduce storage requirements at each destination.
- Shorten detection and resolution times for incidents by storing only forensic values.



snare
A PROPHECY SOLUTION

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com