LOGCOLLECT
COLLECT ONCE, ANALYZE EVERYWHERE

Product Capability

Logcollect is a software-only telemetry pipeline which supports the collection, enrichment, transformation and routing of security data from sources to multiple destinations. It is targeted to security operations that are struggling with distributing large volumes of disparate data, high operational costs, alert fatigue and missed threats. It is available as a software license or hosted in AWS. It is backed by a team that has extensive experience with security logging, SIEM and regulatory compliance. ***Collect once, analyze everywhere.***

Benefits

- **Cost reduction:** Apply data prioritization to route high value security data to expensive threat detection platforms for review by expert staff; route low value compliance data to highly compressed low-cost storage with automatic compliance report generation.
- **Optimized data ingest:** automated collection of security event data from a wide range of sources, such as servers, networks, cloud environments, applications, and agents
- **Data hygiene and curation:** filtering, normalization, and transformation of security data to reduce noise
- **Scale:** Reshape and redistribute security data to best fit platforms (SIEM, Data Lake, compressed low-cost storage, time series dB etc.)
- **Vendor agnostic:** Avoid lock-in, balance cost with performance and scale

Features

- Log collection from endpoints and all popular SaaS sources, no log left behind.
- Filter/forward logs to any SIEM, Data Lake or other security platforms
- Index logs in Elastic search, up to 30 days retention in fast SSD
- Highly compress (90%) and store for 400 days in low-cost disk, meet compliance needs
- Automatic report generation for any of 26 regulatory compliance standards
- Audit ready report review framework, demonstrate compliance
- Robust agent software for Windows endpoints
    - Collect all local Windows logs; receive and relay syslog from local firewalls
    - Extract device id from syslog and transform system name/fields
    - Fine grain filtering including with RegEx
    - Apply data prioritization to transmit security data immediately, all others in batch mode with compression
    - Route logs to multiple destinations (Splunk, Chronicle, MS Sentinel, Securonix etc.)
    - Transfer data securely using syslog over TLS
    - MSI package, no reboot required
    - Centrally manage agent health and configuration
    - In production for 10+ years, millions installed
- Simple licensing model based on number of endpoints, unlimited log volume