Use Case 1 – SIEM

Actions with Endpoint Solutions:

- Process Search
- Watch Lists
- Hash Search
- Device Query
- Patches to be Applied
- Vulnerabilities Discovered
- AV Deployment Status
- Software installed
- Processes running
- Files with Crypto-hashes (Malware)
- Configuration Compliance Status

Actions with Email Solutions:

- Message Rate
- Imposter Detection Trend
- DLP Detection summary
- Blocked Message Rate
- Top Antispam results
- Top Antivirus results
- Mail flow reports
- Connections by country
- Top 10 senders/receivers
- Top 10 quarantine trends
- Threat reports (macro detections, outbreak filtering, URL filtering, Virus filtering)