Incident Investigation & Response

- Manage customer endpoints and policies
- Network isolation
- File retrieval
- Kill processes remotely
- Remote scripting capabilities

Alert prioritization based on context
- Vulnerability reporting (ex. reporting on unpatched CVEs)
- Incident Response Platform (IRP) or orchestration integration?
- Process/attack visualization
- Linking telemetry (observable data) to recreate a sequence of activity, user behavior, process/application behavior, etc.
- Threat Intelligence integration (TIP, upload, webservice, etc) to enrich and contextualize alerts
- Process Creation
- DNS Monitoring
- URL Monitoring
- Network Connection
- Registry Access/Modification
- File Access/Modification
- Windows/WinEvent Hook
- Virtualize
- Remote Access
- Network discovery tool
- Network/Cloud sandboxing
- Vulnerability and patch management
- Mobile Threat Defense
- Mobile Device Management
- Consolidated EPP management console to report on, manage, and maintain, an application control database of known "trusted" applications?
- VDI support
- Ransomware protection
- Full Device Control (Device Control based on Device Class)
- USB device Control
- RDP/Remote Desktop security
- Application whitelisting
- Machine learning for process activity analysis
- Machine learning/Algorithmic

Telemetry data itself can be extended in real time
- Event chaining and enrichment on the endpoints
- Time-series analysis
- Static analysis of files using capabilities such as machine system, registry, COM on real endpoints
- Behavioral analysis (e.g. Analysis over active memory, OS
- Behavioral analysis (e.g. Analysis over active memory, OS
- Application/Process analysis (cloud sandbox)
- Blacklisting
- Put out fires after a breach
- Global, real-time support (24 / 7 /365)
- Clean web (phishing sites, keyloggers, spam)
- Information sharing with industry
- Includes ready-to-use cloud application connectors for:
  - Threat detection for cloud applications
  - Generating actionable incident response from cloud
  - Threat detection for cloud applications
  - Generating actionable incident response from cloud
  - Threat detection for cloud applications
  - Generating actionable incident response from cloud

Comparison:
- MCAFEE
- Threat Intelligence and Verdict
- Security Monitoring
- Incident Response (Handling)
- Incident Analysis
- Security Operations Center (SOC)
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners
- Only through partners