## Endpoint Firewall

### Combined network, endpoint, cloud

- **Protocol analyzers for 40+ different protocols such as TCP, UDP, HTTP, SSL, SMB, etc.**
- **Full packet capture**
- **Integrated threat intelligence integration**
- **Log data collection/correlation**
- **Tuning of monitoring rules for reduction of false positives**
- **Live remote inspection**
- **Central monitoring of all endpoints**
- **Customizable policy creation**
- **Preemptive containment**
- **Manage customer endpoints and policies**
- **Memory snapshotting**
- **Filesystem snapshotting**
- **Network isolation**
- **Quarantine and removal of known "trusted" applications?**
- **Reporting interface identifying events to aid investigation**
- **Linking telemetry (observable data) to recreate a sequence of events for threat hunting**
- **Threat Intelligence integration (TIP, upload, webservice interface or API for searching with YARA/REGEX/ElasticSearch/IOC)**
- **Time-series analysis**
- **Adaptive Event Modelling**
- **Thread Creation**
- **DNS Monitoring**
- **Registry Access/Modification**
- **File Access/Modification**
- **Device Driver Installations**
- **Windows/WinEvent Hook**
- **Interprocess Memory Access**
- **Virtualize**
- **Create Virtual environment for any unknowns**
- **Run unknown scripts, PE, or viruses**
- **Remote scripting capabilities**
- **Mobile Threat Defense**
- **Data loss prevention**
- **Consolidated EPP management console to report on, manage, and maintain, an application control database of known "trusted" applications?**
- **Manage, and maintain, an application control database of known "trusted" applications?**
- **VDI support**
- **Protect/block ransomware when "Out of Service" or "Disconnected" or "Not Connected" application**
- **Agent self-protection/remediation or alerting when there is an attempt to disable, bypass, or uninstall it**
- **Host Based IPS**
- **URL Filtering**
- **Automatically creates network traffic baselines and identifies deviations from baseline for immediate response.**
- **Protection Against Undetected Malware**
  - **Memory protection and exploit prevention**
  - **Process isolation**
  - **Machine learning/Algorithmic learning (not including signature based malware detection)**
  - **Signature-based anti-malware protection**

### Extensive threat hunting (scenario - based)

- **Dedicated cybersecurity expert**
- **Global, real-time support (24 / 7 /365)**
- **Information sharing with industry open source threat intelligence feeds**
- **Internal security sensor logs (IOCs)**
- **Log collection from cloud environments**
- **Threat detection for cloud applications**

### Default Deny Security with Default Allow Usability

- **DRAGON ENTERPRISE**

### Security Orchestration, Analysis and Response (SOAR)

- **Integration**

## Expert Human Analysis

- **Holistic security approach Combined network, endpoint, cloud**

## Neutral Human Analysis

- **No Limit from the internet?**