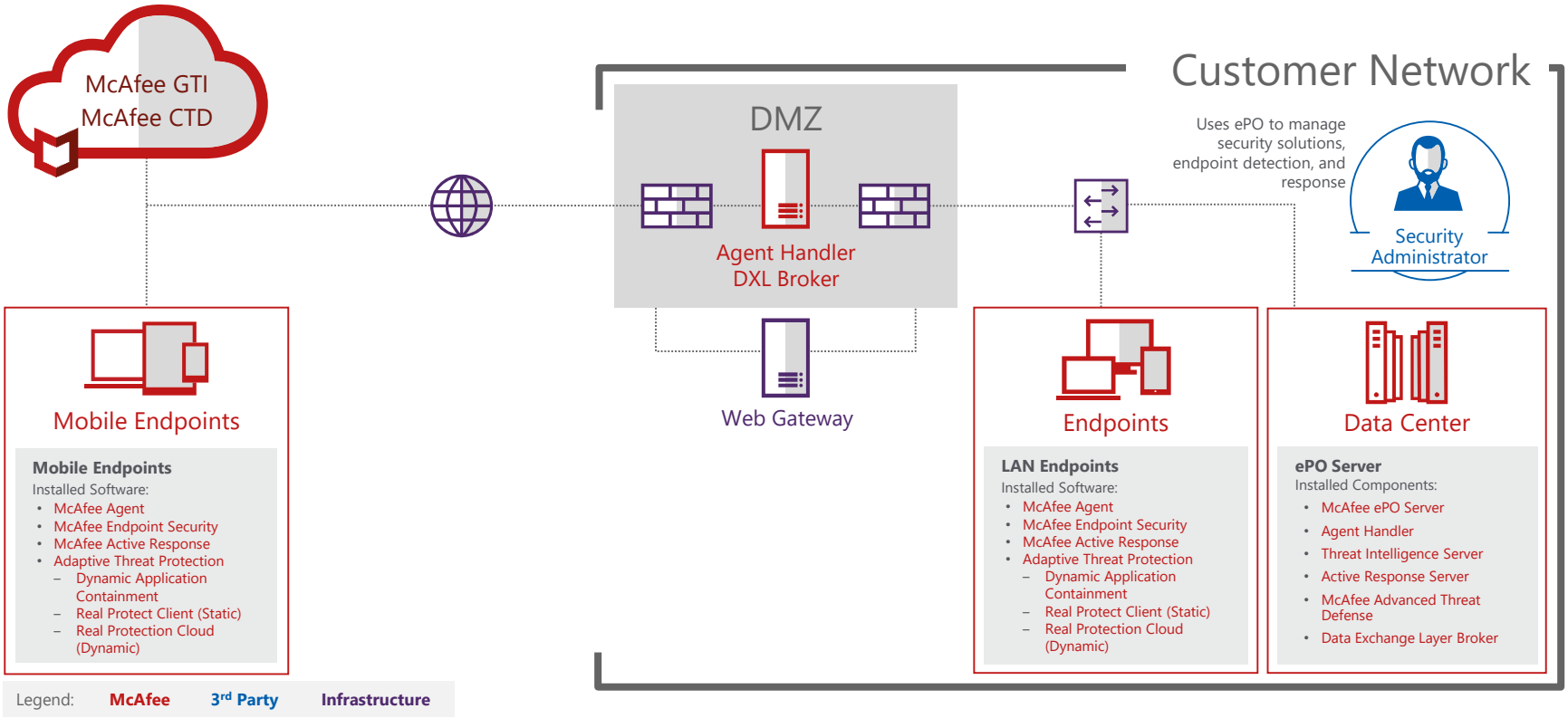
# Dynamic Endpoint



Today's Intelligent Endpoint has to do so much more than just "AV protection"

Today's endpoint has to PROTECT against advanced threats, DETECT new threats and CORRECT impacted systems.

To add another layer of complication the idea of a corporate or organizational "perimeter" to help stop attacks has all but dissolved.

McAfee has created a platform for the complete threat defense lifecycle and endpoint solution that Protects, Detects and Corrects.

# Protect

McAfee has redefined endpoint protection as NOT just anti-virus any more. It's also a platform that uses advanced machine learning and other technologies to calculate threats or using the cloud to query a behavior database.

To build a platform, McAfee has redesigned Endpoint Protection.  It is now a comprehensive solution that integrates Firewall, Web Protection, Threat Prevention, and Adaptive Threat Protection.

In addition to a comprehensive approach, it uses a smaller footprint and fewer system resources that allows it to run in the background not impact the user's experience.

Protecting the endpoint also means stopping threats before they ever get to their target. This requires a solution that is as mobile as the user, McAfee Web Gateway.  The MWG scans all incoming and outgoing web traffic to inspect for threats disguised in links, ads and other web delivered content.  It's proxy based configuration and SaaS deployment options makes this solution as nimble as your workforce.

# Detect

Detection of new threats used to be the job of labs and malware analysts but as threats multiply at an alarming rate, detecting new threats has become a requirement of all organizations

McAfee has given it's customers the Threat Intelligence Exchanged (TIE) as a means to analyze files that are new, unsigned, or otherwise unknown. This technology quickly puts the decision making power in the hands of the administrator to convict new threats and inoculate their entire organization, in addition to consuming threat intelligence from other sources.

Active Response provides a near real time flight recorder of process behaviors from the endpoint, allowing for deep investigations into threats that might be lurking. From clues within the new streamlined UI, an analyst is able to pivot off an individual IOC and determine if the risk has spread further into the environment.

Adding the sandbox Advanced Threat Defense (ATD) puts the power of a malware analyst at every endpoint. Advanced Threat Defense analyzes those files that can't be classified by other detection or protection technologies to determine their risk level. If their risk level reaches a specific threshold the entire ecosystem will be updated with the new intelligence and Protected from this threat even if it attempts penetration from another threat vector. In addition to an on premise ATD solution, Cloud Threat Defense (CTD) provides automatic cloud sandboxing in the cloud.

# Correct

Correcting or remediating an endpoint has previously been a laborious task that often required the infected machines to be immediately quarantined and re-imaged.  While each organization has their own method for correcting infected machines, McAfee has greatly reduced the effort required.

McAfee Active Response can quickly identify which machines, local or remote, have been infected using any number of IOCs or IOAs available.

Actions can even be automated to kill known bad processes or delete known bad files.

Instantly updating endpoints with new threat information and querying an entire organization in seconds couldn't be done without a high performance messaging bus.

These high speed, reliable connections are provided by the Data Exchange Layer (DXL).