

McAfee Cloud



ePO Cloud

Cloud Software Management

- Web Gateway Cloud Service
- Endpoint Security
- Cloud Reporting
- Cloud Threat Detection



Web Protection

- Web Gateway Cloud Service
- AWS Hosted Web Gateway
- Protection Anywhere



Global Threat Intelligence

- URL Reputation
- File Reputation



Security Administrator

Uses ePO to manage security solutions and remediate threats



Compliance Officer

Manage data controls and creates policies for Security Administrator to implement
Assigns data ownership

Web Protection

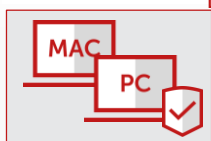
- Web Gateway (On-Premise)
- Web Hybrid (On-Premise and Cloud)
- Web Gateway Cloud Service (In Cloud)

Network Data Protection

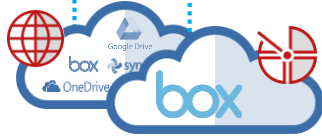
- **Prevent** – Enforces Email and Web Data Controls
- **Discover** – Crawls your Data Repositories
- **Monitor** – Scans for Violations in the network stack



Remote Users



- Web Protection
- McAfee Client Proxy



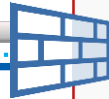
Cloud Storage Repositories

- Box

Cloud Application Control

- Shadow IT Visibility
- Cloud Application Controls
- Granular Policy Control

Secure ICAP



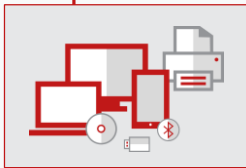
Main Office

Virtual Stack

- Promiscuous Virtual Interface

Network Stack

- Span or Tap Interface



Endpoint Data Protection

- Endpoint Data Loss Prevention
- Drive Encryption
- File and Removable Media Protection

Data Repositories

- CIFS, FTP, HTTP(S)
- SharePoint, Oracle
- MSSQL, MySQL, DB2

Domain & Directory Services

- Active Directory
- DNS
- OpenLDAP
- eDirectory



Software Management

- ePolicy Orchestrator
- Content Security Reporter



- Here is a reference architecture for McAfee's Pervasive Data Protection solution. It incorporates Endpoint and Network Protection along with Web Protection into a solution which effectively protects data as it moves within and out of your network.
- Endpoint and Network Data Protection offers consistent compliance policies from the endpoint to the cloud.
- Web Protection provides a consistent user experience and malware protection wherever the users may be. Leveraging the McAfee Cloud enables organizations to reduce their infrastructure costs.
- You can see McAfee DLP offers solution at every egress point whether its at the endpoint, in storage or on the network.
- Please note that McAfee DLP does NOT have to work with McAfee Email or Web Gateway, it can work with any email and web gateways that support ICAP or port mirroring.

- **ePO** – Centralized endpoint management console
- **Threat Intelligence Exchange (TIE)** – Provides threat intelligence from multiple sources to identify threats within the environment
- **Endpoint Security** – Optimized endpoint anti malware solution that provides threat prevention, web controls, and firewall.
- **Drive Encryption** – Full disk encryption that protects data on a mobile devices if it is lost or stolen
- **File and Removable Media Protection** – Provides file encryption that protects data on systems, file shares, removable media, and cloud services.

- **DLP Endpoint** – Safeguards sensitive data and ensuring compliance by protecting sensitive data such as PCI, PII, and PHI wherever it lives—on premises, in the cloud, or at the endpoints
- **DLP Manager** – Manages Network DLP Devices
- **DLP Monitor** – Allows you to gather, track, and report on data in motion across your entire network
- **DLP Discover** – Finds and categorizes sensitive data that resides on your servers, network, shares, and databases
- **DLP Prevent** – Protects against data loss by ensuring that only non-sensitive data leaves the network
- **Web Gateway** – On-premises Web Security solution providing best-in-class malware protection evolving threats.
- **Web Gateway Cloud Service** – Cloud based offering of the very same flexibility that you get on-prem.
- **Web Protection** – Combined protection of Web Gateway on-prem and in the cloud with the Web Gateway Cloud Service