Hewlett Packard Enterprise

HPE Connected MX

Delivering mobile workforce productivity at the edge and business assurance at the core

Organizations need an endpoint protection solution that delivers business assurance with corporate intelligence, control, security, and information analytics without compromising end-user productivity or conveniences. HPE Connected MX is a secure cloud based endpoint data protection solution that enables organizations to continuously protect information generated by an increasingly mobile workforce, and confidently deliver information accessibility while facilitating organizational visibility, control, and protection of information at the edge.

By integrating policy-based endpoint protection with rule-based file synchronization and sharing of information assets, Connected MX enables organizations, for the first time, to have a centrally managed solution for mobile information without compromising business expectations and mobile workforce productivity and conveniences. Centralizing the organizational information results in a consistent data protection strategy at the edge, facilitates granular information control, aligns data movement to corporate security procedures, and defines policies that affect both internal and external access to the organizational information.

With information hosted in a central repository, Connected MX builds on the Adaptive Backup and Recovery approach from Hewlett Packard Enterprise, enabling organizations to benefit from real-time analytics, auditing, reporting, and information compliance features. More importantly, with a centrally managed information repository bound by organizationally defined policies, the business can more effectively deliver end-user conveniences guided by a corporate strategy that centers on risk reduction and exposure.

Key features and benefits

Advanced endpoint backup and recovery—offers continuous, WAN optimized, and secure endpoint data protection:

- A single Connected MX agent delivers WAN-optimized backup to enhance efficiency over the most bandwidth-constrained networks. Patented SendOnce technology from Hewlett Packard Enterprise performs block-level deduplication within the agent, and data reduction occurs prior to network transmission.
- The Connected MX "express agent upload" feature speeds up the upload time by spawning multiple connections to upload data simultaneously. As a result of WAN-optimized backup and express agent upload, customers have observed 85 percent reduction in upload time in their environment.
- Connected MX implements a continuous data protection strategy enabling information to be protected almost immediately upon file creation or modification.
- Connected MX safeguards endpoint data from ransomware attacks with isolated storage, always-on file versioning, and extensible retention policies. Point-in-time data restore allows end-users to restore clean, unencrypted data from ransomware attacks.

Information visibility and accessibility—enables information accessibility on any device by authorized users with support for Windows®, Apple, Android, iOS, and Web browsers:

- Connected MX implements metadata-based search to enable users and administrators to find critical information fast.
- User search offers a single view of all of a user's information regardless of the originating device. Responsive information to search criteria can immediately be viewed in place, downloaded, restored, or shared.
- Using metadata search criteria, authorized administrators can search for all information of users within their administrative realm. Administrators can quickly identify information responsive to business, compliance, and eDiscovery requirements without having to restore user backups.
- File viewing, powered by HPE KeyView, enables information to be viewed from any user's device without requiring files to be downloaded to the device. The KeyView capability helps eliminate the need to deploy and use native file viewers on mobile phones and tablets.

Enterprise grade deployment and administration capabilities—empowers administrators with tools and real-time analytics to manage their Connected MX environment, end-user accounts, and endpoint information

- Silent device installation and registration capability helps organizations to deploy Connected MX agents on the endpoint devices without end-user's intervention
- Connected MX provides administrators tools to import end-users in bulk rather than add each account manually. The bulk account management tools allow deleting, updating, and placing multiple accounts on hold in one operation.
- Connected MX offers a wide range of reports spanning from device based reports to data trending, and end-user account based reports. The reports allow administrators to make data driven decisions based on the backup status, devices that are not backed up, data usage trends, and agent performance.
- With the administrator restore capability, the administrators can re-image an endpoint, or prepare a new endpoint device and restore all the end-user data before handing over the endpoint to the end-user.

File and folder sync and share—this optional feature provides sharing capabilities in a single platform to improve mobile workforce productivity.

- Connected MX file and folder sync and share capabilities enable users to sync files and folders with all of their mobile endpoint devices.
- Connected MX collaboration and folder share features provide real-time continuous view of files in a simple and secure way.

Information security—delivers secure mobile information protection and access through encryption, granular data privileges, and federated authentication:

- Connected MX leverages a FIPS-compliant AES 256-bit encryption algorithm within a multikey security implementation to offer maximum security to customer data. The Connected MX agent encrypts the data prior to network transmission.

- Connected MX supports the option of customers managing the encryption keys. Enterprises, depending on their security requirements, can store encryption keys in HPE's secure cloud, or manage the keys themselves within their premises. Connected MX is designed and tested to support OASIS KMIP compliant encryption key management server's high-availability architecture.
- Role-based access control within Connected MX enables administrators to be assigned the lowest level of privilege required to perform their assigned tasks.
- Granular audit trails enable customers to log and report administrative activity as well as information activity such as sharing and information flow within and external to the customer or organization.
- Connected MX enables customers to leverage their own secure source of identity for authentication. Security Assertion Markup Language (SAML)/ OAuth support enables integration with a customer-federated authentication strategy to improve security and manageability.

Policy-based control—delivers information control and management through policy "drift" compliance, policy-based protection, rule-based file sharing, and information access scoping policies:

- Connected MX employs an information-based policy engine. It controls more corporate data at a granular level than file types and folder paths. This enables organizations to deliver the appropriate information, which is protected and accessible by users and administrators.
- Personally identifiable information (PII) sharing policies, powered by HPE Haven OnDemand, can be deployed to identify and audit sharing activity that involves privacy-related information. Policy options support advising users of the presence of PII and when sharing a file that includes PII, an action is triggered according to the policy defined by IT.
- Backup policies enable administrators to govern the endpoint backup scope, helping remove the need for user involvement and data loss due to user error or omission.
- Connected MX supports network bandwidth throttling for both data upload and download. With this policy, the administrators can set the maximum network bandwidth each activity can consume.
- Additional policy options enable control over which information to sync, upload or download, or control view by access channel, and data transmission over metered (3G or 4G) connections.

The value of Connected MX

- Meet business assurance objectives with automatic, continuous, and extensible endpoint protection
- Protect endpoint data from ransomware attacks
- Take control of your endpoint information with policy-based management
- Reduce exposure to legal and financial risk with defensible auditing and eDiscovery or early case assessment
- Securely preview, access, download, and share your information on any device and with any consumer
- Analyze and visualize mobile information to support data-driven decision making
- Leverage existing IT investments and address future growth needs with service or application integration points
- Improve and enhance organizational productivity with end-user conveniences that do not compromise business assurance requirements

Technical specifications

The Connected MX endpoint protection agent can be installed on endpoint devices running Microsoft® Windows and Apple Mac OS. Connected MX apps are available for iOS and Android platforms.

Languages supported:
Connected MX v4.0: English only

Learn more at
hpe.com/software/connectedmx

Sign up for updates

4AA5-7728ENN, June 2016, Rev. 4