Hewlett Packard Enterprise

Brochure

Managing mobile information

Endpoint protection and enterprise file sync and share with HPE Connected MX

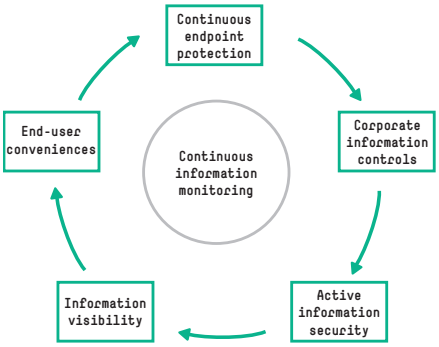

Figure 1. HPE Connected MX centrally manages mobile information throughout the enterprise

HPE Connected MX delivers mobile workforce productivity at the edge and business assurance at the core.

Introduction

Today, the producers and consumers of corporate information—digital citizens—are becoming increasingly mobile and carrying multiple devices. When you combine the uniqueness of each of these endpoint devices as well as the information access and usability needs of their users, with the businesses need to protect and secure corporate information regardless of where it resides, a rigid dichotomy between the enterprise and those mobile digital citizens develops quickly.

Consumer-grade utilities may offer broader accessibility, but they often lack the necessary security, controls, and visibility to understand and protect the enterprise information. Conversely, traditional approaches have largely been too heavy-handed and can adversely affect end-user experience and productivity. This ultimately means greater business risk and a reduction in the usefulness of the information to both the enterprise and the digital citizen.

To address this challenge, Hewlett Packard Enterprise introduces HPE Connected MX. By integrating policy-based endpoint protection with rule-based file synchronization and sharing of information, organizations—for the first time—have both an enterprise managed and collaborative mobile information solution, without compromising business expectations and mobile workforce productivity and conveniences.

Extending our Adaptive Backup and Recovery approach, HPE Connected MX enables enterprises to benefit from real-time analytics, auditing, reporting, and information compliance features that effectively delivers end-user conveniences. These capabilities are guided by organizational policies that reduce risk and exposure using an endpoint protection system that can be extended to meet new requirements and interoperate with many existing IT applications and services.

Take control of your mobile information with policy-based management
Leveraging centralized contextual policies, HPE Connected MX allows enterprises to easily apply granular endpoint protection, synchronization, and sharing policies at any level within the organization, resulting in automatic and continuous protection of the information. HPE Connected MX delivers end-user conveniences by allowing your mobile workforce to extend corporate policies, and create and manage customized protection configurations.

Securely preview, access, download, and share your information on any device and with any consumer
With native app support for smartphones, tablets, and Web browsers, HPE Connected MX enables users to securely synchronize and access their information from their device. Using its unique document preview feature HPE KeyView, HPE Connected MX prioritizes the value of the information to the consumer over the transfer and duplication of files over the connection. Based on defined policies, users can share information with others, both internally and externally. More importantly, organizational information is encrypted while in flight and at rest, using industry-standard 256-bit AES encryption algorithms.

Meet business assurance objectives with automatic, continuous, and extensible endpoint protection
To help protect information as it is created on the edge, HPE Connected MX enables enterprises to define and easily deploy policy-defined mobile backup configurations to endpoint devices. HPE Connected MX uses these configurations to automatically and continuously protect information on the edge. End-users can be authorized to create new endpoint protection rules or customize existing backup rules. HPE Connected MX resolves enterprise and end-user defined rules to prevent enterprise policies from drifting away from their intended purpose as new end-user defined rules are added.

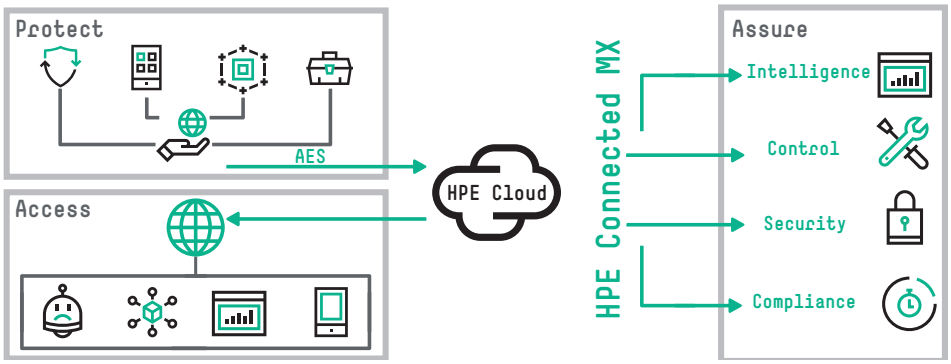

Figure 2. HPE Connected MX endpoint to enterprise architecture

Reduce exposure to legal and financial risk with defensible auditing and eDiscovery/early case assessment
Using an integrated analytics engine (HPE Haven OnDemand), HPE Connected MX facilitates a mobile information management workflow that can allow or prevent files containing specific characteristics or content (i.e., personally identifiable information) from being shared or synchronized. Additionally, enterprises can make use of HPE Connected MX search and analytics tools to identify information custodians allowing them to apply protection, synchronization, and sharing policies at a granular level.

Improve and enhance organizational productivity with end-user conveniences that do not compromise business assurance requirements
To empower the members of your mobile workforce and increase end-user productivity, HPE Connected MX delivers automated mobile backup and easy-to-use, intuitive self-service recovery from either existing backup sets, or file versioning capabilities that is integrated with enterprise-class file synchronization and sharing.

HPE Connected MX also extends the capabilities of the enterprise to the edge allowing end-users to search and analyze their information and customize the endpoint protection without compromising the broader business assurance strategies centrally defined by IT.

Analyze and visualize mobile information to support data-driven decision-making
HPE Connected MX provides a highly secure and centralized repository that consolidates scattered mobile information. Regardless of its point of origin, and how it is accessed, enterprises can unlock business value through analytics and visualization features to make more effective and data-driven decisions.

Using HPE Haven OnDemand platform services, this centrally stored information can be searched for specific content to:

- Facilitate adherence to corporate procedures and regulatory compliance
- Apply policies for backup, synchronization and sharing of corporate information based on metadata
- Identify subject matter experts or information custodians based on information ownership and use
- Generate defensible auditing reports based on information backup, recovery, sharing and share disposition along with how the information is being synchronized to other end-point devices

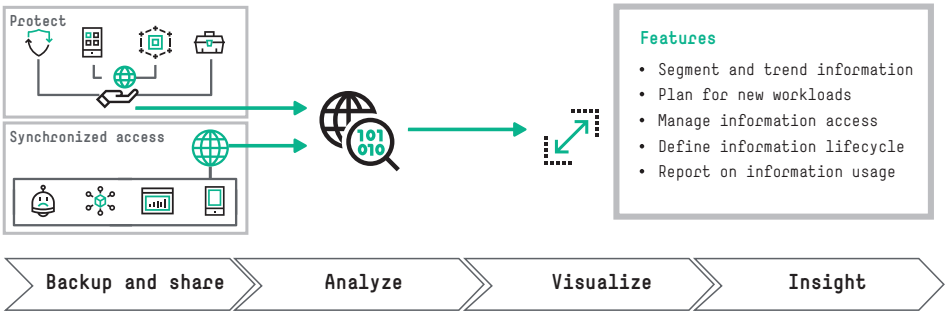

Figure 3. HPE Connected MX utilizes centrally stored, protected, and shared mobile information to extract business value using analytics and visualization

Developing solutions for major social and environmental challenges.
hp.com/hpinfo/globalcitizenship

Leverage existing IT investments and address future growth needs with service or application integration points

To effectively manage access to information, HPE Connected MX offers an enterprise-class Security Assertion Markup Language (SAML)-based authentication approach that integrates with existing IT security infrastructures (i.e., LDAP/Active Directory). HPE Connected MX enables enterprises to define information sharing realms for highly secure information tenancy defined by user-access policies. As a hosted solution, HPE Connected MX can be extended and enhanced to address the unique needs of the organization, alleviating the need to deploy multiple unsecure point-based solutions.

Key features

- Unified backup, file sync, and file sharing—unifies backup, sync, and sharing capabilities in a single platform delivering complete endpoint protection of mobile information while improving mobile workforce productivity
- Policy-based mobile information management—delivers information control and management through policy "drift" compliance, policy-based protection, rule-based file sharing, and information access scoping policies
- Information visibility and accessibility—facilitates information accessibility on any device by authorized users with support for Windows®, Apple, Android, iOS, and Web browsers
- Information usage analytics—defensible audit of how information is being accessed and shared against defined synchronization and sharing policies
- File previewing—unique to HPE Connected MX, the file previewing capability focuses on the relevance of the information first, and its transfer second, by allowing users to view information from their device
- Information security—delivers highly secure mobile information protection and access through encryption, granular data privileges, and federated authentication.
- Information compliance and auditability—HPE Connected MX integrates with HPE Haven OnDemand, enabling enterprises to meet compliance needs through data analysis for policy adherence, and metadata-based search for early case assessments and eDiscovery.

Conclusion

Addressing the challenges of managing mobile information within a dispersed corporate environment, organizations need an endpoint protection solution that delivers business assurance, which provides corporate intelligence, control, security, and information analytics without compromising end-user conveniences. HPE Connected MX enables enterprises to confidently deliver information accessibility to their mobile workforce while facilitating visibility, control, and protection of information at the edge.

Learn more at
hpe.com/software/connectedmx

Table 1: HPE Connected MX key features for the business and mobile workforce

	INTELLIGENCE	CONTROL	SECURITY	COMPLIANCE
Addressing corporate assurance needs	• Central information search • Defensible information disposition reports • Information usage analytics • Information custodian identification • HPE Haven OnDemand integration	• Contextual policies • Role-based access • Sharing realms • Policy "drift" oversight	• Authenticated service integrations • Granular data privileges • Policy-based file sync and share	• Automated protection • Retention management • Sharing analytics • Content search, audit
Addressing mobile workforce productivity	• Sharing visibility reports • Share disposition reporting • Information search • Information control	• Customizable policies • Explorer/finder integrated • Inclusion/exclusion rules • Synchronized backup	• Granular restore options • File version control • Synchronized restore • Device data migration	• Granular share options • Sharing lifecycle policies • Web-based access • File previewing

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA5-7604ENW, November 2015, Rev. 2