DEV™
IT Simplified...

CASE STUDY

Managed Office 365 migration with Microsoft End-point Device Management (Intune)

Cloud Management

Migration of the legacy email solution to Office 365 with monitoring and support services for remote desktop and end-point management while integrating new functionalities such as Multi Factor Authentication (MFA) and spoof blocking.

PROTECTED

Client: **Protected by NDA**
Country: **UK**
Industry: **Managed IT Services Provider**

About the Client

The client is a UK based MSP offering services in managing IT landscapes on Azure Cloud and Microsoft Office 365 to its customers in film, media, and communication sectors. The client also specializes in setting up network infrastructures for large- and small-scale businesses.

Challenges

- With an increasing demand for migration of on-premise Microsoft Exchange to Office365 cloud, the client's business was experiencing an accelerated growth in such projects. The clients' current resources lacked the skill sets and expertise to handle and deliver such projects successfully.
- The clients' current infrastructure comprised of deprecated remote desktop management, unstructured network orientations, and lacked continuous support for their end-users.
- Without proper industry standards adherence and security compliance documentation, the clients' current resources and skill sets lacked support for efficient end-point device management for their end-user/customer.
- The clients' legacy e-mail solution was lacking compliances in terms of security and reliability. The on-premise Microsoft Exchange solution wasn't able to provide secure e-mail transmissions for spoof e-mail and e-mail auto-forwards to external domains.

Quicks Insights

Challenges

- The client's team lacked expertise on Office 365 migrations
- Deprecated remote desktop management solution
- Unstable and highly insecure legacy email solution

Solution

- Continuous control and standards documentation for e-mail solution migration
- Configured the solution with Microsoft Intune end-point management
- Restricted copy/paste and e-mail forwards to external domains

Result

- Reduced cost of delivery
- Highly secure and manageable email solution ecosystem
- Higher resolution rates with increased NPS

Technologies Used

- Microsoft Office 365
- Microsoft Azure
- Microsoft – End Point Device Management (Intune)

Approach

The challenges the client faced were critical in terms of sustaining their end-users and customers. To address the clients' needs in the most appropriate manner and following industry and platform best practices, our team of experts implemented a hybrid model using dedicated resources on Microsoft Office 365 and Microsoft Exchange.

Solution

- The clients' foremost priority was to manage the migration from on-premise Exchange to Office 365. To streamline the migration process, our team of domain experts implemented continuous monitoring and support checks for newest compatibilities of e-mail servers to Office 365.
- To enhance the security for the e-mail solution and provide a reliable and 'always-up' infrastructure environment, our team defined new e-mail flows, developed SoPs based on current compliance policies for securing instances.

The following was implemented to secure the e-mail solution:

  - To restrict data breach, spoof e-mail blocking was implemented with restrictions on auto-forwarding of e-mails to external domains.
  - Implemented SKF, DKIM, and DMARC functionalities with the new e-mail solution to only validate messages from trusted resources.
  - Configured the new email solution with Multi-Factor Authentication (MFA) and self-service password reset.

- Our team of experts also provided support services for more than 200 remote desktops to streamline the infrastructure.
- Microsoft End-Point Management (Intune) was used to configure the solution based on the client's specification and following industry best practice. The use of Intune provided a simple and quicker way to structure the entire solution ecosystem.
- To enhance security on data assets of the organization, we restricted copy/paste functionality for shared documents when accessed through mobile devices.

Benefits

- The client realized up to 40% reduced cost of delivery of services to its end-users.
- The client achieved higher issue resolution rates, in turn, leading to better NPS.
- Regular audits and monitoring of the solution offered increased security and governance compliance.

About DEV IT

DEV IT is public listed (NSE-DEVIT) organization based at Ahmedabad, India. For more than 2 decades, the organization has evolved into a multi-faceted unit with 1200+ strong, skilled workforce providing cutting-edge software and infrastructure solutions in Cloud, Data and Automation domain. DEV IT provides services to government departments, public sector organizations across several states in India as well as 100s of clients worldwide from diverse industry sectors: healthcare, travel and hospitality, manufacturing, professional services, retail, transportation and logistics and more.

Microsoft Gold Partner | Microsoft Cloud Solution Provider | aws partner network Consulting Partner | CMMI DEV/3 | CMMI SVC/3 | ISO 27001:2013 | ISO 9001:2015

Dev Information Technology Ltd.
14, Aaryans Corporate Park, Nr. Shilaj Railway Crossing,
Thaltej – Shilaj Road Thaltej, Ahmedabad – 380059, Gujarat, INDIA

Dev Info-Tech North America Ltd.
2425 Matheson Blvd E, 8th Floor,
Mississauga, ON, L4W 5K4, CANADA