Microsoft

MICROSOFT
CASE **STUDY**

OVERVIEW

Microsoft is a household name because of its omnipresent operating system "Microsoft Windows". It is one of the world's biggest Multinational Technology companies that offer a variety of well-known products like Microsoft Office, Internet Explorer, Xbox and Microsoft Surface etc; Microsoft has recently acquired LinkedIn and Skype in 2016.

REQUIREMENT

Being one of the market leaders in technology, Microsoft wanted an automated system to authenticate and approve visitor access through their network. Once a visitor shares his details with the security staff, the same was sent to be authenticated by the person he has come to meet. Upon successful verification the guest would be allowed within the premises and would receive an SMS with an OTP to connect to the WiFi if he so desires.

HOW WE HELPED

- Reduced OpEx and CapEx
- Visitors were given access after approval
- Easy tracking of number of users, bandwidth control, policy management and reporting
- Large volume of data to perform analytics
- Integrated BYOD support
- Simplified and centralized network management
- A reduction in network fault calls
- Ability to remotely control, monitor and troubleshoot
- Ubiquitous Wi-Fi coverage and stronger signal
- The ability to support high density environments with more concurrent users per access point
- Access point Monitoring
- Proximity marketing

MICROSOFT CASE STUDY

Microsoft installed an automatic system where visitors were given WiFi access after authentication by the person they came to meet at their office.

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and services. Its best known software products are the Microsoft Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers. Its flagship hardware products are the Xbox video game consoles and the Microsoft Surface tablet lineup. As of 2016, it is the world's largest software maker by revenue, and one of the world's most valuable companies.

Microsoft was founded by Paul Allen and Bill Gates on April 4, 1975, to develop and sell BASIC interpreters for the Altair 8800. It rose to dominate the personal computer operating system market with MS-DOS in the mid-1980s, followed by Microsoft Windows.

Microsoft has numerous offices across the globe and these offices are technologically very advanced. For their Indian offices Microsoft needed an automated system to authenticate and approve guests that want to enter their premises or connect to the office's WiFi network. To accomplish this, the solution had to be very secure so that there were no unwanted or unauthenticated logins, owing to Microsoft's nature of work. Also the overall security of the network had to be ensured.

Usually when there is a meeting at any office premises, the visitor needs to fill out a form at the reception or security office, and he is then allowed inside. In certain cases the security guards ask the visitors to verify their number by sending an OTP as well.

Let us consider a use case scenario, suppose Mr X has an appointment with Mr Y (a Microsoft employee) and he comes to his office for a meeting. As Mr X and Mr Y are acquaintances, there is a risk in allowing Mr X to access the building and the WiFi without any policing or authentication. To eliminate this dilemma, there needed to be an automated system that allowed Mr X to enter the building and connect to WiFi only when

Mr Y authorises it. Moreover, the extent of Mr X's access had to be curtailed and policies for his usage had to be implemented.

In Microsoft's case, the entry verification was automated by leveraging the WiFi network. So now when Mr X reaches the reception, he is asked for his details and the name of the person he wants to meet. After receiving these details, Mr Y automatically receives an email and SMS that has a link to verify that he has a meeting with Mr X and he should be granted access. After positive identification by Mr Y, Mr X is allowed in the building and receives an SMS with an OTP to access the WiFi if he so desires. Now, while Mr X is in the building, he will be allowed to have limited access to the internet and his activity will be monitored.

Indio's Unibox solution is simple and easy to implement, as it is a smart box which requires no additional programming from the clients end. This plug and play device was installed at all Microsoft offices in India after months of PoC as they wanted to test it in several situations.

As a result of the installation, the time taken by a guest to enter the premises was shortened and the procedure was more secure as each guest was authenticated by the employees. This SOP also helped save the time and effort required at the front desk by the receptionist/ security staff.

Excerpt
https://en.wikipedia.org/wiki/Microsoft