

## BQ

# Esta empresa europea de productos tecnológicos implementa tecnología inalámbrica, seguridad y switching de Meraki para la gestión unificada



- Empresa europea líder en tecnología con 1200 empleados y oficinas en Europa y Asia.
- El panel basado en la nube proporciona una gestión centralizada de ubicaciones distribuidas.
- Oficinas conectadas que comparten recursos mediante VPN de sitio a sitio con capacidad de autoreparación.



BQ es una de las empresas líderes del sector en Europa. Entre sus productos más destacados se encuentran smartphones, tablets, impresoras 3D y PrintBots. Se trata de una empresa que tiene oficinas en Europa y Asia, más de 1200 empleados y que comercializa productos en más de 50 países. El objetivo de BQ es crear y distribuir tecnología que eduque, inspire, abra puertas, elimine barreras y que sea accesible para todos. BQ se concibe a sí misma como una empresa educativa cuyo objetivo es ayudar a las personas a comprender la tecnología a través de su uso, además de inspirar a otros para que la desarrollen.

Para continuar con la filosofía educativa de BQ basada en la tecnología, el método “hazlo tú mismo” y la iniciativa de código abierto, el Director de TI, Mario Fernández, necesitaba una infraestructura de red de calidad que reflejara estos ideales y cimentara las iniciativas globales que la empresa desarrolla. “Nos dimos cuenta de que era necesario que los equipos se conectaran en una única red gestionada desde una sola ubicación. En una empresa internacional en crecimiento como esta, necesitábamos un alto grado de flexibilidad y la capacidad de personalizar”.

BQ eligió a Cisco Meraki como la solución ideal para optimizar la gestión de toda la red, lo que les permite configurarla y adaptarla de manera sencilla a medida de sus necesidades. En palabras de Mario Fernández, “abrir nuevas oficinas de BQ y ponerlas en marcha ahora es mucho más fácil gracias a Meraki. La gestión centralizada en la nube nos permite controlar toda la red desde un único panel, sin

tener que desarrollar un sistema nosotros mismos. Está todo hecho, así que lo único que tenemos que hacer es usarlo”.

A través del panel centralizado para la gestión unificada, BQ implementó appliances de seguridad, switches y puntos de acceso en sus diversas ubicaciones. Sin la necesidad de estar in situ, el equipo de TI puede gestionar cada una de las ubicaciones remotas a través del panel, tener visibilidad del uso de la red e implementar los cambios que sean necesarios.

Mediante la VPN automática de sitio a sitio integrada en los appliances de seguridad MX, Mario puede conectar cada una de las ubicaciones. Puede incluso conectar equipos ya existentes que no estén equipados con la VPN de Meraki en la misma red. De este modo se logra una distribución perfecta de los recursos. El carácter autorreparable de las conexiones VPN de los dispositivos MX permite que permanezcan actualizados en entornos de IP dinámicos. A su vez, BQ utiliza control de tráfico y límites de ancho de banda por cliente para regular la utilización de la red, lo que posibilita un uso adecuado de esta entre todos sus empleados.

Para garantizar la seguridad de la red, Mario ha implementado una serie de medidas de seguridad como la detección de malware, prevención y detección de intrusiones e incluso filtrado de contenido gracias a la tecnología SNORT de Sourcefire. Cada una de estas funciones se habilita fácilmente pulsando un botón o seleccionando las categorías que hay que bloquear como contenido para adultos, phishing y hacking. Además de evitar el acceso a cierto contenido, MX puede dar prioridad a ciertos tipos de tráfico

vital e incluso sincronizar el routing VLAN con políticas de grupo más granulares. Estas políticas de grupo se han diseñado para permitir configuraciones más personalizadas para usuarios individuales, dispositivos e incluso tipos de tráfico.

Los switches de acceso de capa 2 y capa 3 de Meraki proporcionan a BQ una personalización por puerto en función de las necesidades individuales de cada ubicación. Las políticas de acceso se pueden habilitar en cada puerto que requiera que los usuarios introduzcan sus credenciales 802.1x para el acceso por cable. Gracias al panel unificado, Mario y el personal de TI pueden navegar por toda la red sin ningún tipo de problema. Pueden hacer clic en cada puerto e identificar el dispositivo o punto de acceso Meraki conectado. Esto permite controlar cómo se utiliza cada red dentro de toda la organización.

**“Vigilar el uso de la banda ancha en cada red nos permite reaccionar rápidamente y prevenir así la pérdida de servicio. Con un par de clics podemos bloquear a un usuario, aplicar una política de filtrado de contenido y limitar el ancho de banda para las diferentes aplicaciones.”**

– Mario Fernández, Director of IT

El personal de TI tiene un control total que va desde el núcleo de red a los dispositivos del usuario final. Tanto los empleados como los invitados, proveedores o usuarios son dirigidos a uno de los 15 SSID por red que se ha personalizado completamente para su grupo. Mario ha definido unas restricciones de ancho de banda por dispositivo, ha implementado limitaciones con firewalls de 7 capas y ha establecido unas políticas de control de tráfico personalizadas para la empresa. Una de las principales ventajas de la solución Meraki es que todas estas configuraciones se pueden aplicar



seleccionando la opción de un menú desplegable o rellenando los campos correspondientes. El equipo de TI no necesita formación específica ni usar líneas de comandos complejas para obtener los resultados que desean.

BQ se encuentra en plena expansión y, por lo tanto, sigue abriendo nuevas oficinas. Gracias a Meraki, BQ puede ampliar su red sin ningún impedimento y gestionar cada una de sus ubicaciones desde un único emplazamiento. Esta centralización propicia una mayor eficiencia y eficacia al tiempo que permite a cada una de las distintas oficinas compartir información de forma rápida y segura.

El Director del personal de TI Mario Fernández explica: “las políticas de seguridad pueden usarse como plantillas para luego adaptarlas a cada red. Al añadir un nuevo dispositivo a la red, esta se configura inmediatamente”. La interfaz de Meraki es muy completa e intuitiva e incluye herramientas de supervisión, diagnósticos remotos y detección de incidentes potenciales que permiten a BQ detectar problemas con facilidad. Todo esto, en combinación con el sistema antimalware, garantiza la seguridad de las actividades de BQ y las protege frente a amenazas externas. “Vigilar el uso de la banda ancha en cada red nos permite reaccionar rápidamente y prevenir así la pérdida de servicio. Con un par de clics podemos bloquear a un usuario, aplicar una política de filtrado de contenido y limitar el ancho de banda para las diferentes aplicaciones”, concluye Mario.