Ante el constante aumento de las amenazas de seguridad en el Cyberespacio, el disponer de un entorno centralizado de visibilidad y gestión de tu infraestructura de RED se ha convertido en una pieza fundamente para hacer frente a los nuevos requerimientos de visibilidad sobre infraestructuras híbridas, convergentes y distribuidas. De Igual forma, el DNS se ha convertido en pieza clave como servicio, pero también una vía preferente para infecciones por malware o tácticas de Cyberespionaje para fuga de datos, veremos como a través del sistema DNS de Infoblox podemos detectar y combatir estas nuevas tácticas de infección, así como encajar nuestra solución de una forma cooperativa con otras soluciones de seguridad. Estableciendo así, un ecosistema de seguridad con mayor visibilidad y resistencia ante las nuevas y futuras amenazas del Cyberespacio.

Su sistema de red de dominios (DNS) es una herramienta esencial para mantener su negocio en funcionamiento. Por desgracia, también es una herramienta para romper su negocio y robar datos. Por ejemplo, el 91% del malware utiliza DNS para realizar campañas.

¿Por qué DNS es tan popular entre los atacantes? Tiene un diseño abierto, y la mayoría de las soluciones de seguridad no proporcionan una vista de DNS. Es el punto ciego en su seguridad.

Necesita una solución que proporcione una vista completa de su red, incluyendo DNS, y las amenazas que residen en ella. La solución debe ofrecer protección interna, externa, de nube, remota y de infraestructura de roaming completa contra vulnerabilidades de DNS. Y debe generar una inteligencia de amenazas precisa y unificada para que pueda aprovechar esos conocimientos sobre toda su infraestructura de seguridad.