Estrategia de Seguridad y Gestión de Dispositivos en Marval O'Farrell Mairal

prisma soluciones tecnológicas

Introducción

Desde su fundación en 1923, Marval O'Farrell Mairal ha sido un referente en el ámbito legal argentino y latinoamericano. Con más de 300 abogados especializados en diversas áreas, la firma maneja asuntos complejos y transacciones internacionales. Proporciona asesoramiento integral a empresas multinacionales que buscan expandirse en América Latina, destacándose en transacciones corporativas y financieras, litigios, propiedad intelectual, derecho laboral, competencia, energía, compliance y telecomunicaciones. Marval O'Farrell Mairal es un socio estratégico que protege y promueve los intereses de sus clientes en cada paso del camino.

El estudio Marval O'Farrell Mairal se embarcó en un ambicioso proyecto para mejorar su estrategia de seguridad y la gestión de dispositivos mediante la implementación de tecnologías de Microsoft. Este proyecto se desarrolló en un contexto de ciberseguridad madura, lo que requirió capacidades avanzadas para su despliegue.

El estudio contaba con diversas tecnologías y una estrategia definida de seguridad de la información en el marco de la norma ISO 27.001. El proyecto ayudó a complementar la estrategia existente y aprovechar nuevas funcionalidades de tecnologías Microsoft ya adquiridas, pero no desplegadas. El proceso fue realizado a través del programa global de Microsoft: FastTrack para servicios de seguridad en Microsoft 365 que comienza con una evaluación inicial de las necesidades y el entorno de la organización. A partir de esta evaluación, se elabora un plan detallado de implementación que incluye guías y recomendaciones personalizadas.

Durante la fase de implementación, Prisma Soluciones tecnológicas, como Partner certificado en dicho programa configura y despliega los servicios de seguridad necesarios, asegurando una integración fluida con los sistemas existentes. Además, se proporciona capacitación y recursos para que el equipo adopte y utilice eficazmente las nuevas herramientas de seguridad.

Soluciones implementadas

Uno de los principales desafíos fue lograr la coexistencia entre la solución de seguridad TrendMicro y Microsoft Defender, que buscó una integración con el resto de la plataforma, incluyendo Intune. La gestión de vulnerabilidades fue un aspecto clave del proyecto. La solución anterior, presentaba limitaciones que fueron completadas con Microsoft Defender. La nueva solución permitió identificar más vulnerabilidades y proporcionó un valor diferencial en su gestión.

Un aspecto destacable fue la configuración de directivas de acceso condicional basado en riesgo. Para ello se implementaron de estas directivas tanto para User Risk como para Sign-In Risk, esto incluyó la revisión de usuarios en riesgo, notificaciones por correo electrónico, monitoreo y operación.

Adicionalmente, se configuró el método de enrollment mediante policies EDR de Intune, que se implementó para lograr visibilidad y políticas de seguridad para dispositivos personales que acceden a recursos corporativos, algo que el cliente no disponía de manera previa y que ayudó a ampliar la maduración de seguridad de cara a los requisitos de la norma ISO 27001.

Por su parte, se estableció la conexión con el servicio de Defender for Endpoint y la integración con el módulo de operación Defender XDR y se configuró la reducción de la superficie de ataque y el espacio de trabajo en Defender. La implementación de Microsoft Defender permitió una integración total con las políticas de Intune, lo que llevó a una gestión más eficiente de los dispositivos. Esta integración no solo ofreció beneficios económicos al unificar las suscripciones, sino que también mejoró la visibilidad y el monitoreo de los dispositivos.

Se verificaron las conexiones de los Endpoints enrolados contra el servicio de Defender for Identity siguiendo el método de enrollment mediante sensores instalados en los DCs y se realizó el sizing para gestionar el ancho de banda, la instalación de los sensores y el armado del workspace en Defender XDR.

Estos desafíos técnicos fueron abordados con una planificación cuidadosa y una ejecución meticulosa, asegurando que todas las soluciones implementadas cumplieran con los requisitos del proyecto y mejoraran la seguridad y gestión de dispositivos en la empresa.

RESULTADOS Y BENEFICIOS

Cumplimiento de estándares de seguridad: La implementación de herramientas de seguridad colaboró con el compromiso del cliente respecto de la norma internacional que establece los requisitos para la gestión de la seguridad de la información ISO 27001. Asimismo, durante el proceso de certificación, se realizó un ejercicio de pentesting que ayudó a identificar debilidades y mejorar la seguridad. La implementación de Defender y la gestión de identidades ayudaron a detectar movimientos laterales y ataques de fuerza bruta durante dicho test de manera exitosa.

Beneficios Económicos y de Integración:

La unificación de las suscripciones y la integración total con Microsoft Defender ofrecieron beneficios económicos significativos. Al consolidar las licencias en una sola suscripción, se logró una reducción de costos, ya que se evitó el pago por productos separados. Además, la integración permitió una gestión más eficiente y una mejor visibilidad de los dispositivos, lo que se tradujo en ahorros operativos y una optimización de recursos.

Consolidación de Licencias: Al unificar las licencias de seguridad en una sola suscripción de Microsoft Defender, se eliminó la necesidad de mantener suscripciones separadas para diferentes soluciones de seguridad. Esto resultó en una reducción directa de los costos de licenciamiento.

Optimización de Recursos: La integración de Microsoft Defender con Intune permitió una gestión centralizada y más eficiente de los dispositivos. Esto redujo la carga administrativa y operativa, permitiendo al equipo de TI enfocarse en tareas más estratégicas.

Reducción de Costos de Monitoreo: La capacidad de Microsoft Defender para proporcionar una visibilidad completa y un monitoreo continuo de los dispositivos eliminó la necesidad de soluciones de monitoreo adicionales. Esto no solo redujo los costos de software, sino también los costos asociados con la gestión y el mantenimiento de múltiples plataformas.

Beneficios Económicos de la Suscripción Única: Al pagar una única suscripción por usuario que cubre múltiples funcionalidades, se logró una mayor eficiencia en el gasto de TI. Esto permitió a la empresa aprovechar al máximo su inversión en tecnología sin incurrir en costos adicionales por funcionalidades redundantes.

CONCLUSIONES

El proyecto de transformación digital en Marval O'Farrell Mairal, apoyado por las tecnologías de Microsoft, no solo mejoró la seguridad y gestión de dispositivos, sino que también permitió a la empresa cumplir con los requisitos de la certificación ISO 27001. La colaboración entre los diferentes departamentos y la implementación de soluciones avanzadas como Defender for Endpoint e Intune, demostraron ser fundamentales para el éxito del proyecto.

Estos servicios permitieron clarificar todavía más su estrategia futura de gestión de identidades y la posibilidad de reemplazar el proxy reverso de terceros con la tecnología de Microsoft Global Secure y destacar la importancia de continuar explorando y aprovechando las tecnologías disponibles en Microsoft E5 para mejorar la seguridad y gestión de dispositivos en la empresa.