Seguridad Microsoft, en resultados de negocio.

Ingeniería sobre Entra ID · Intune · Defender · Purview — más monitoreo de superficie de ataque y pruebas de intrusión.

1 DIAGNÓSTICO · *empiece sabiendo dónde está parado*

Radiografía de Seguridad

Sepa exactamente dónde está parado. Revisamos su infraestructura Microsoft y le entregamos un reporte claro con lo que ya está bien y lo que conviene mejorar — para decidir con orden, no con corazonadas.

Plan de Remediación

Llegue al consejo con un plan que se defiende solo. Hoja de ruta por etapas con riesgo, costo y prioridad de cada fase, más el caso de negocio de licenciamiento (¿E5 o add-ons?) ya resuelto.

2 IDENTIDAD · *Microsoft Entra ID*

Blindaje de Identidad

Que una contraseña robada deje de ser una crisis. Verificación en dos pasos y reglas de acceso por contexto para toda la empresa; y cuando alguien se va, pierde todos sus accesos el mismo día.

Privilegios Bajo Control

Elimine el riesgo del administrador todopoderoso. Los permisos delicados se activan solo cuando se necesitan, por tiempo limitado y con registro de todo.

Un Solo Login (SSO)

Un solo acceso para todas sus aplicaciones. Menos contraseñas que robar y altas y bajas automáticas — cero accesos huérfanos cuando alguien deja la empresa.

Acceso Remoto sin VPN

Sus aplicaciones internas seguras desde cualquier lugar, sin abrir la red. Publicamos cada aplicación con verificación de identidad, sin exponer todo lo demás.

3 DISPOSITIVOS · *Microsoft Intune*

Endpoint Moderno (Windows)

El equipo nuevo listo al encenderlo; el robado, solo un fierro perdido. Configuración automática, cifrado y borrado a distancia — las horas de soporte por equipo se vuelven minutos.

Catálogo de Aplicaciones

Las apps que su gente necesita, al día en toda la flota — sin tickets. Instalación y actualización automáticas, con portal de autoservicio para el usuario.

Móviles Protegidos (iOS/Android)

La información de la empresa protegida en cualquier celular, incluso personal. Si la persona se va, lo corporativo se borra; sus fotos y lo suyo, intacto.

4 AMENAZAS · *Microsoft Defender*

Detección y Respuesta en Equipos (EDR)

Detenga el ransomware en minutos, no en días de operación caída. Detección y respuesta en toda la flota, validada con una simulación de ataque real.

Correo Blindado

Que nadie de su equipo transfiera dinero a una cuenta falsa. Freno al phishing y a la suplantación de su dominio antes de que lleguen a la bandeja.

Consolidación Defender XDR

Todas sus alertas de seguridad en un solo lugar, con respuesta automatizada. Menos ruido y menos silos — listo para que lo opere su equipo o su SOC.

Protección de Aplicaciones en la Nube (Cloud Apps)

Recupere el control del shadow IT. Descubrimos qué servicios en la nube usa de verdad su gente, bloqueamos los de riesgo e impedimos que su información salga a equipos no administrados.

Protección de Cargas en Azure (Defender for Cloud)

Sus servidores en Azure con gobierno de seguridad, no a la deriva. Postura priorizada y protección de cargas — con el costo dimensionado antes de encender nada.

5 DATOS · *Microsoft Purview*

Mapa de Datos Sensibles

Sepa dónde vive su información crítica y quién la toca. Descubrimos y etiquetamos clientes, nómina y contratos — porque no se puede proteger lo que no se ve.

Anti-Fuga de Información (DLP)

Que lo que vale su negocio no salga con quien renuncia. Bloqueo de fuga de datos por correo, Teams y USB — por fases, sin frenar la operación.

Cumplimiento y Retención

Cuando un auditor o un juicio pidan evidencia, aparece en horas, no en semanas. Retención de lo que exige la ley y búsqueda legal lista para responder.

6 CONTINUIDAD · *que la inversión no se degrade*

Consultoría Mensual de Seguridad

Un experto pendiente de su seguridad cada mes, sin sumar una plaza. Bolsa de horas mensual para revisiones de configuración, ajustes, asesoría y atención de dudas — usted decide en qué se usan, con un reporte de lo trabajado.

7 SUPERFICIE DE ATAQUE · *servicio propio · monitoreo continuo*

Monitoreo de Superficie de Ataque Externa

Vea su empresa como la ve un atacante — antes de que la ataquen. Monitoreo continuo de dominios, puertos, fugas y suplantaciones de marca, priorizado por lo que de verdad se explota. Planes Basic · Business · Enterprise.

8 PRUEBAS DE PENETRACIÓN · *servicio propio · pentesting*

Pruebas de Penetración

Demuestre que su seguridad aguanta — con evidencia para auditoría y ciberseguro. Ataque controlado y autorizado que expone lo explotable en la práctica, con plan de remediación y re-test de verificación incluido.

Modular · a precio fijo por alcance. Contrate solo los servicios que necesita. Todo se construye sobre las herramientas de su suscripción Microsoft 365 — no vendemos licencias, hacemos que rinda lo que ya paga. Si necesita licencias adicionales, nuestros partners se las proveen sin complicaciones.