Microsoft 365

Microsoft 365 Lighthouse

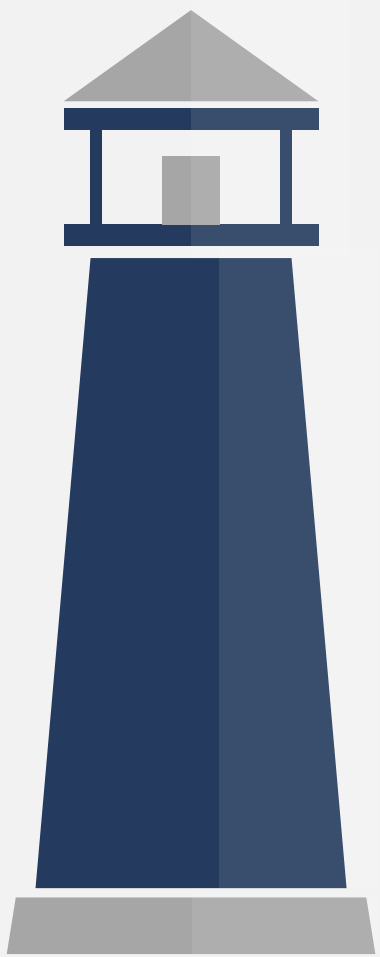
Manuel García González
Senior Security PSA in GPS – Microsoft Spain

Nuestro equipo se centra en la creación de soluciones para ayudar a los socios a tener éxito con Microsoft 365.

Queremos ayudarte a:

Escala tu negocio

Proteja y administre a los clientes de pymes y hágalos productivos en Microsoft 365



Le damos la bienvenida a Microsoft 365 Lighthouse

Microsoft 365 Lighthouse es un servicio gratuito que permite a los proveedores de servicios de administración proteger y administrar Microsoft 365 a escala en todos sus clientes de pymes

Managed Service Providers (MSPs)

Un MSP es un proveedor de servicios tecnológicos que actúa como un departamento de TI subcontratado, principalmente para pymes

Ganan dinero vendiendo Contratos de Servicios Gestionados

La mayoría en EE. UU. cobra entre $ 50 y $ 100 por dispositivo por mes

Por lo general, administra de 50 a 200 clientes

El tamaño medio de los asientos de los clientes es de < 50

Son pequeñas empresas en sí mismas

Los MSP que prestan servicios a las pymes tienden a ser proveedores regionales, muchos de los cuales son empresas de estilo de vida propiedad de sus fundadores con menos de 10 millones de dólares en ingresos anuales.

La mayoría de los MSP son generalistas de TI que realizan seguridad de línea de base

"EDR es ideal para los proveedores de seguridad especializados. Esos MSP que tienen su negocio allí. La mayoría de las veces no quiero investigarlo, solo quiero que se arregle. Quiero que se elimine. Quiero saber qué tan malo es. Quiero saber cuáles son mis próximos pasos".

Nathan Taylor, Director of Technical Services at machineLOGIC

La eficiencia operativa, la seguridad y la automatización son lo más importante, junto con la estandarización de su pila y la minimización del número de proveedores que hay que gestionar

Los MSP maduros utilizan varias herramientas para su eficiencia operativa

RMM (gestión y supervisión remotas)

PSA (Automatización de Servicios Profesionales)

Inicio de sesión remoto

Y más...

Los 5 principales proveedores de servicios gestionados generales

2021 GLOBAL MSP BENCHMARK SURVEY REPORT - KASEYA

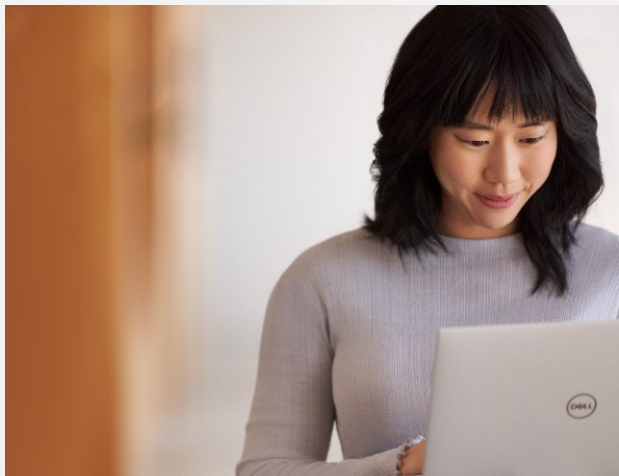
Microsoft 365 Business Premium es nuestra suscripción de héroe. Es una solución integral de seguridad y productividad, diseñada para empresas de 1 a 300 empleados

Colabora en tiempo real

Habilite el acceso remoto y proteja la identidad

Defiéndase de las amenazas cibernéticas y la pérdida de datos

Proteja y administre fácilmente los dispositivos



M365 Lighthouse Overview

Ayuda a los Proveedores de servicios gestionados para proteger los dispositivos, los datos y los usuarios de sus clientes

Gestión de clientes a escala

Supervise y gestione a los clientes de forma centralizada para identificar fácilmente las brechas en la configuración del cliente final, orientar las mejoras e impulsar la adopción

Estandarizar la configuración

Benefíciese de los planes de implementación para impulsar la estandarización, aumentar las ventas en toda la base de clientes y reducir el riesgo

Seguridad Mejorada

Asegure y proteja los dispositivos, los datos y los usuarios en todos los entornos de los clientes utilizando las mejores prácticas recomendadas

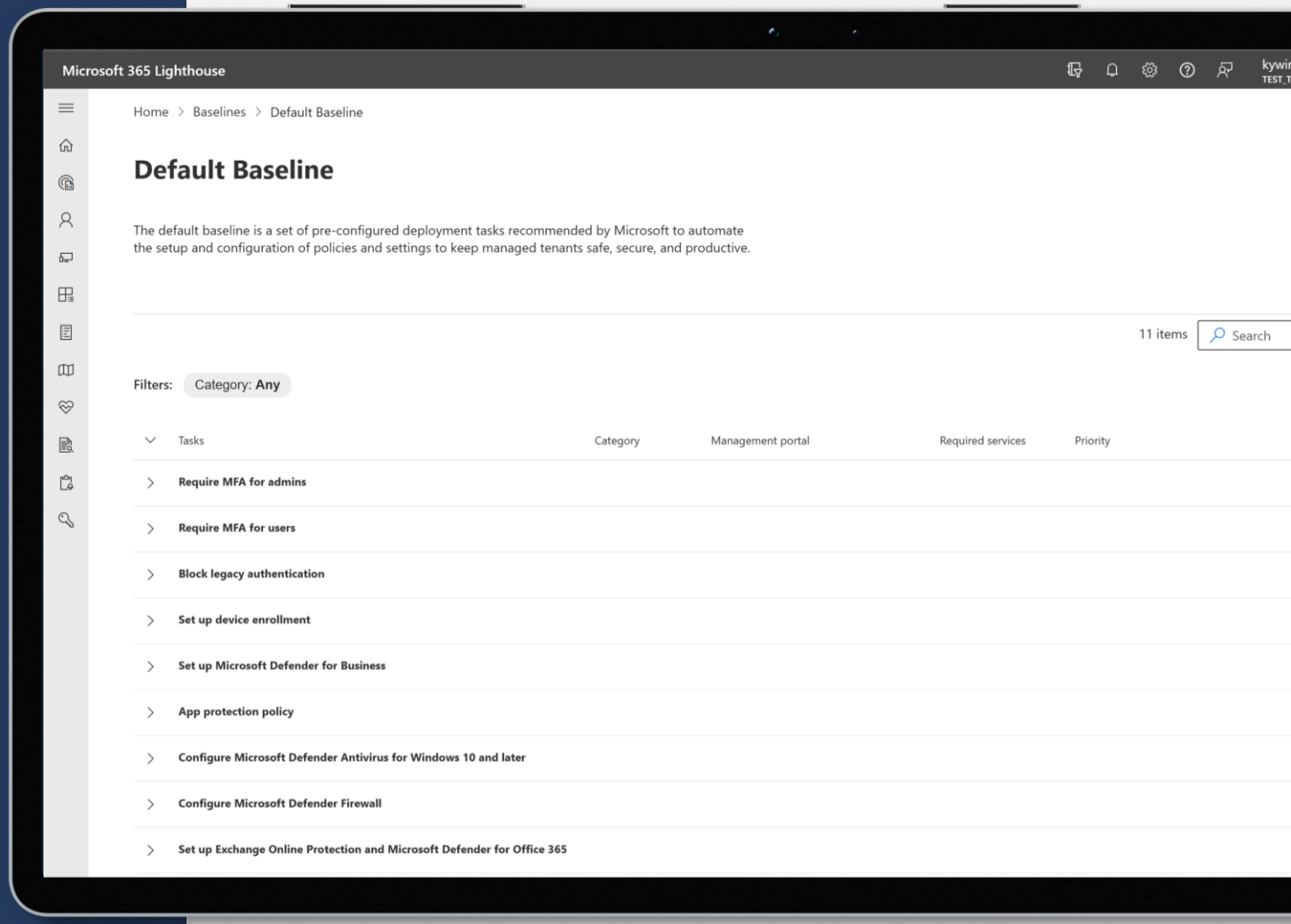
Gestión proactiva de riesgos

Logre eficiencias en la gestión de clientes para respaldar la escala y el crecimiento del negocio

Estandarizar la configuración con líneas de base

Ajustes recomendados: Las líneas base son las directivas y configuraciones recomendadas por Microsoft optimizadas para pequeñas y medianas empresas.

Implementación coherente: Vaya más allá de la supervisión mediante la implementación de estándares de seguridad coherentes en clientes nuevos y existentes mediante planes de implementación.



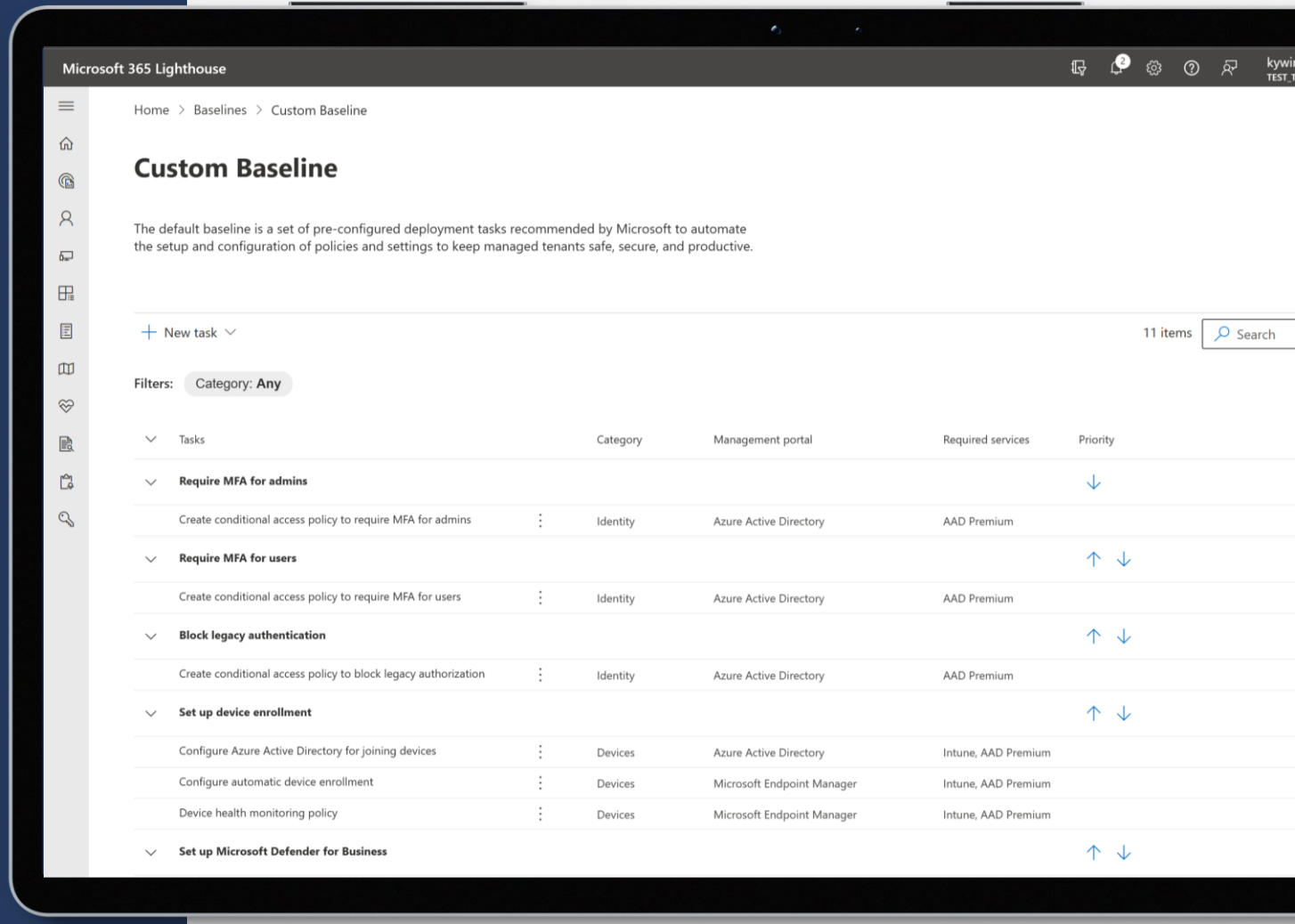
M365 Lighthouse
Custom Baseline Demo

Capacitar a los socios de CSP para que **estandaricen a sus clientes** en M365 al ofrecer un solo panel para asegurar **y la gestión de sus clientes a escala** en todos los servicios de M365.

La línea base predeterminada proporciona un conjunto de tareas "listas para usar" para que los asociados las completen. Las tareas incluidas en la línea base predeterminada son las tareas que creemos que los partners deben completar con cada uno de sus clientes.

Las líneas base personalizadas permiten al socio crear su propia lista de tareas que desea que sigan sus ingenieros de servicio. Las tareas se pueden clonar a partir de la línea base predeterminada o crearse a partir de directivas o configuraciones de un inquilino existente.

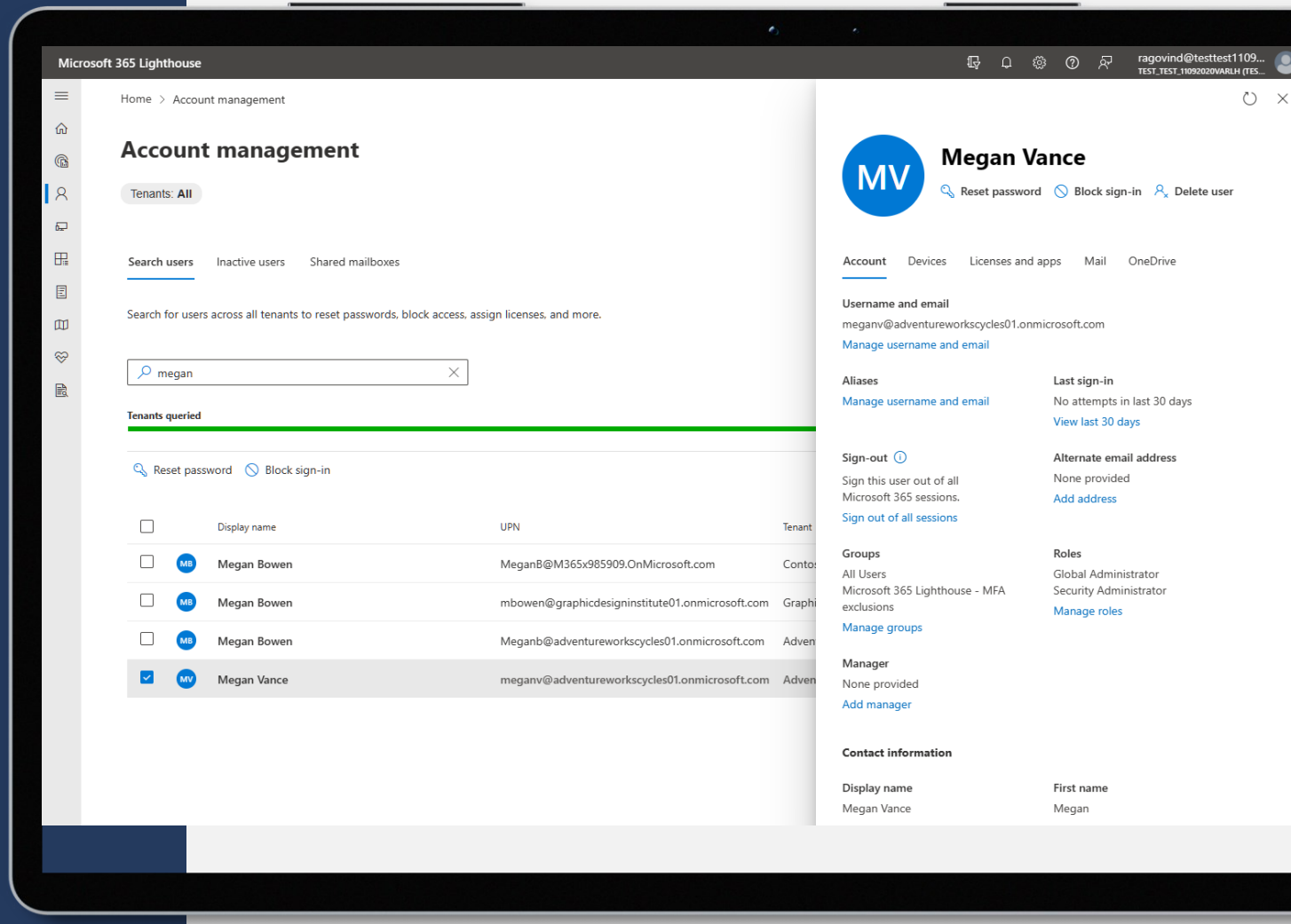
Las líneas base se materializan como planes de implementación para cada inquilino y proporcionan un conjunto de tareas para que los ingenieros de servicio las sigan de forma coherente con cada cliente.



Usuarios

Gestión de cuentas

Administre los usuarios de todos los inquilinos con tareas comunes, como buscar, restablecer contraseña, asignar licencias y bloquear el inicio de sesión. Supervise fácilmente a los usuarios de riesgo que no tienen configurada la autenticación multifactor junto con los usuarios inactivos y los buzones compartidos seguros.



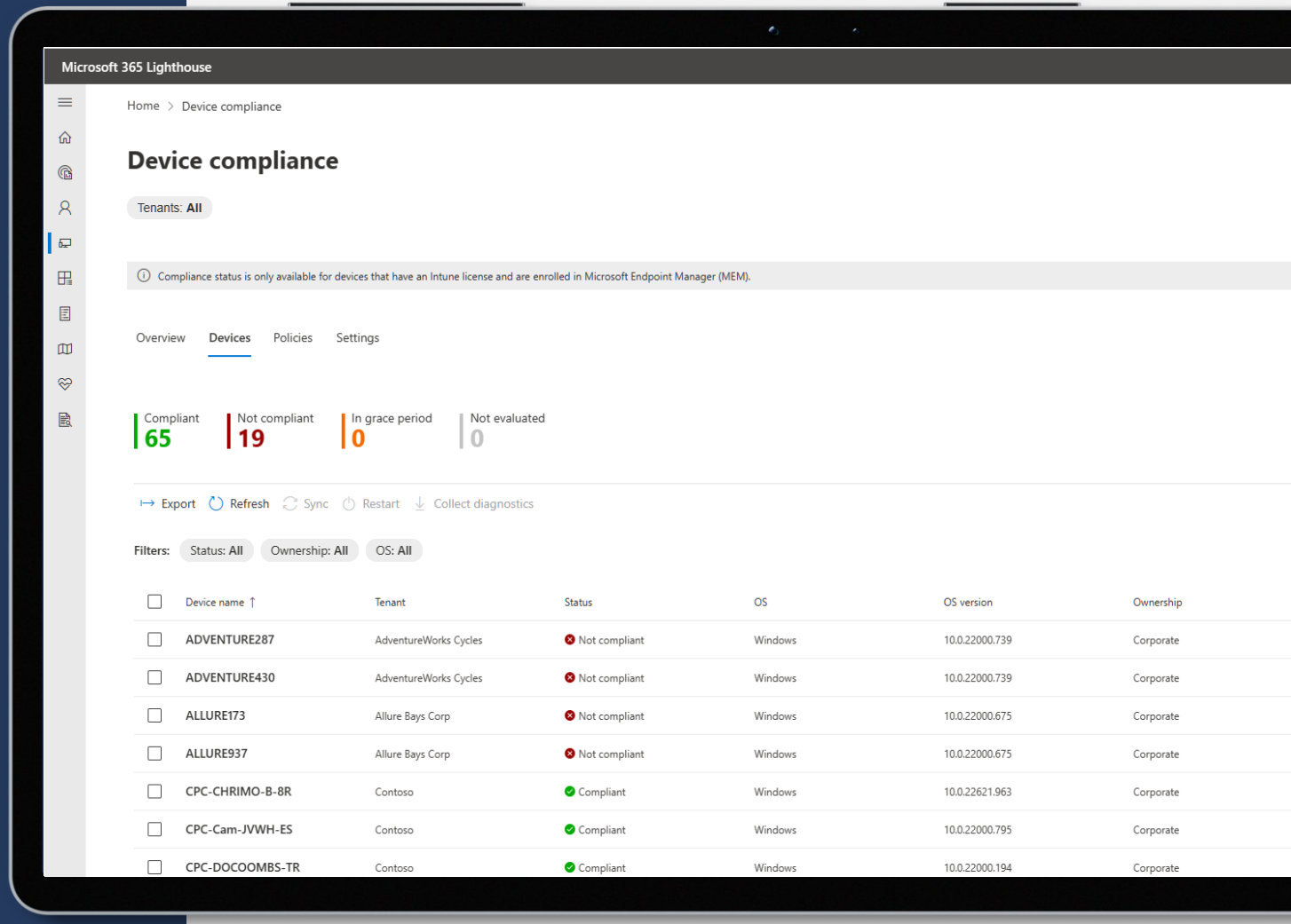
Dispositivos

Lista de dispositivos multi-tenant

Vea la lista de dispositivos administrados en sus inquilinos en un único panel con la capacidad de realizar acciones comunes como reiniciar y recopilar diagnósticos.

Dispositivos que necesitan atención

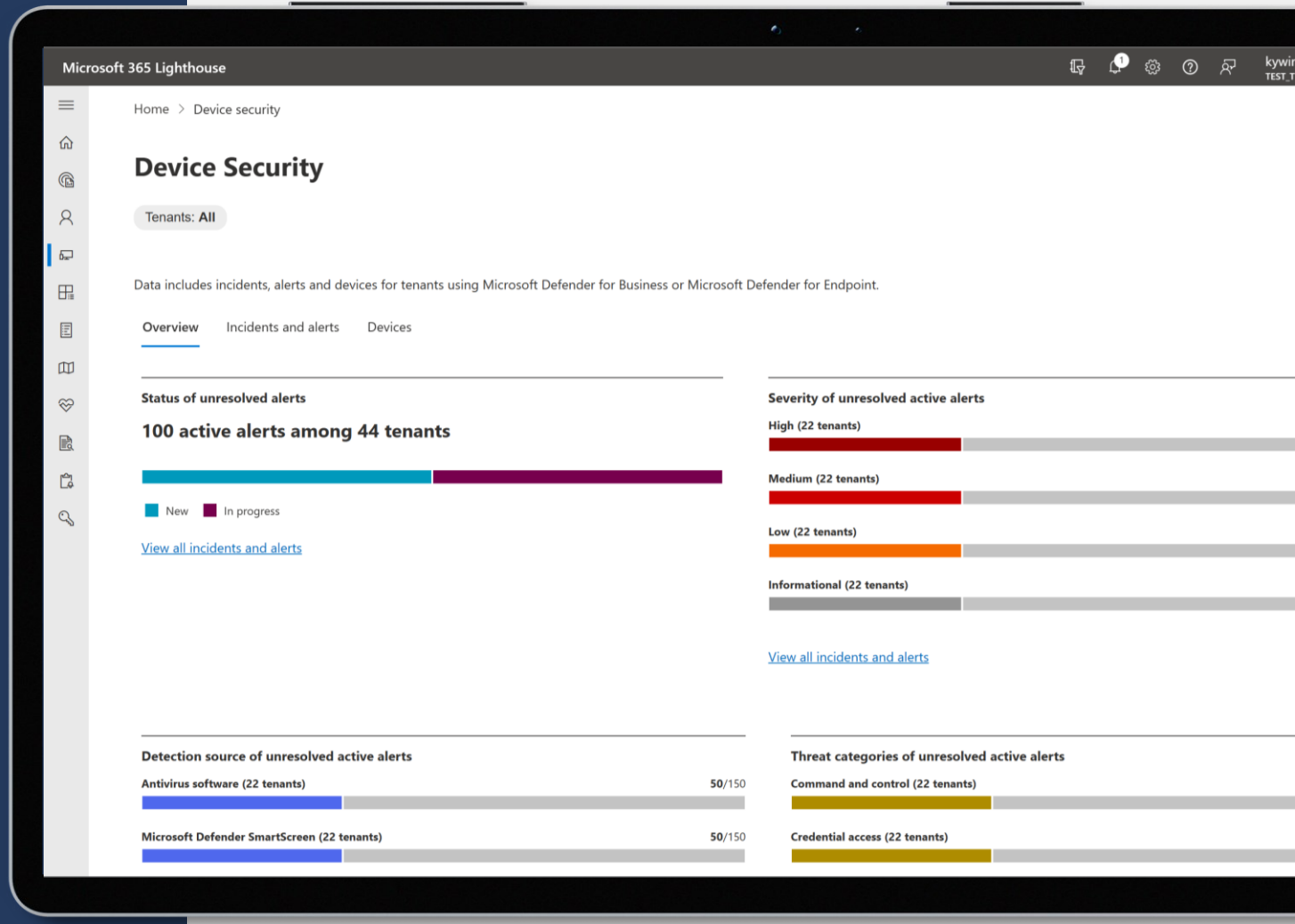
Identifique fácilmente los dispositivos que no se adhieren a las políticas de la empresa o los dispositivos en los que los usuarios finales experimentan problemas para devolverlos a un estado compatible y saludable.



Seguridad del dispositivo

Información multi-tenant
Supervise rápida y fácilmente los incidentes y las alertas de los endpoints para todos los dispositivos de sus clientes administrados en una vista multiinquilino

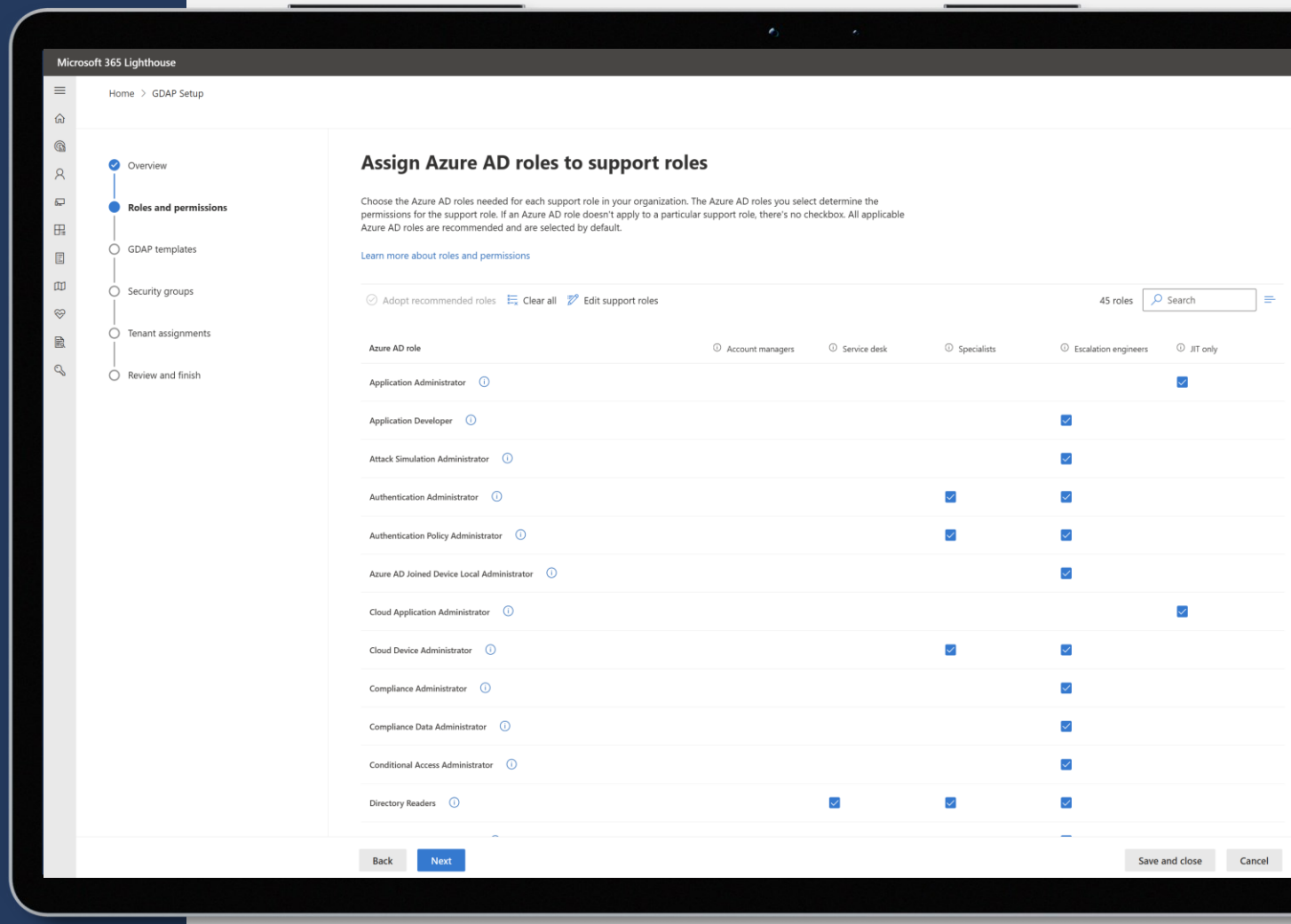
Gestión de dispositivos
En el caso de los inquilinos que se han incorporado a Defender para punto de conexión o Defender para empresas, puede ver y corregir alertas e incidentes, así como ver todos los dispositivos que tiene actualmente bajo administración.



Seguridad de los socios

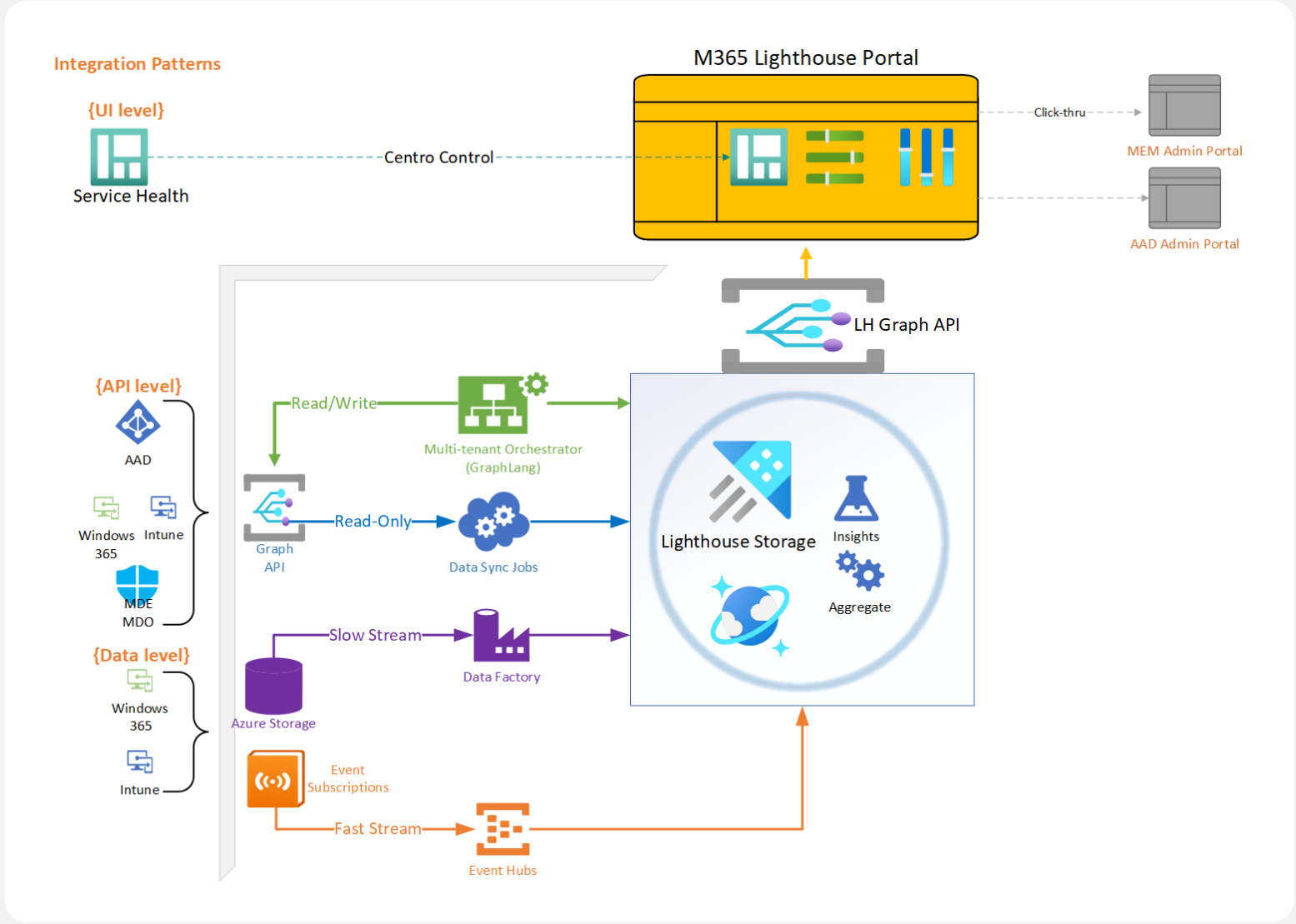
Configuración y administración de relaciones de privilegios de administrador delegado granular (GDAP)

Diseñado para que los MSP configuren sus relaciones GDAP con sus clientes. Roles de soporte recomendados para proporcionar a los ingenieros los permisos basados en el tiempo adecuados. Experiencia guiada para simplificar la complejidad.

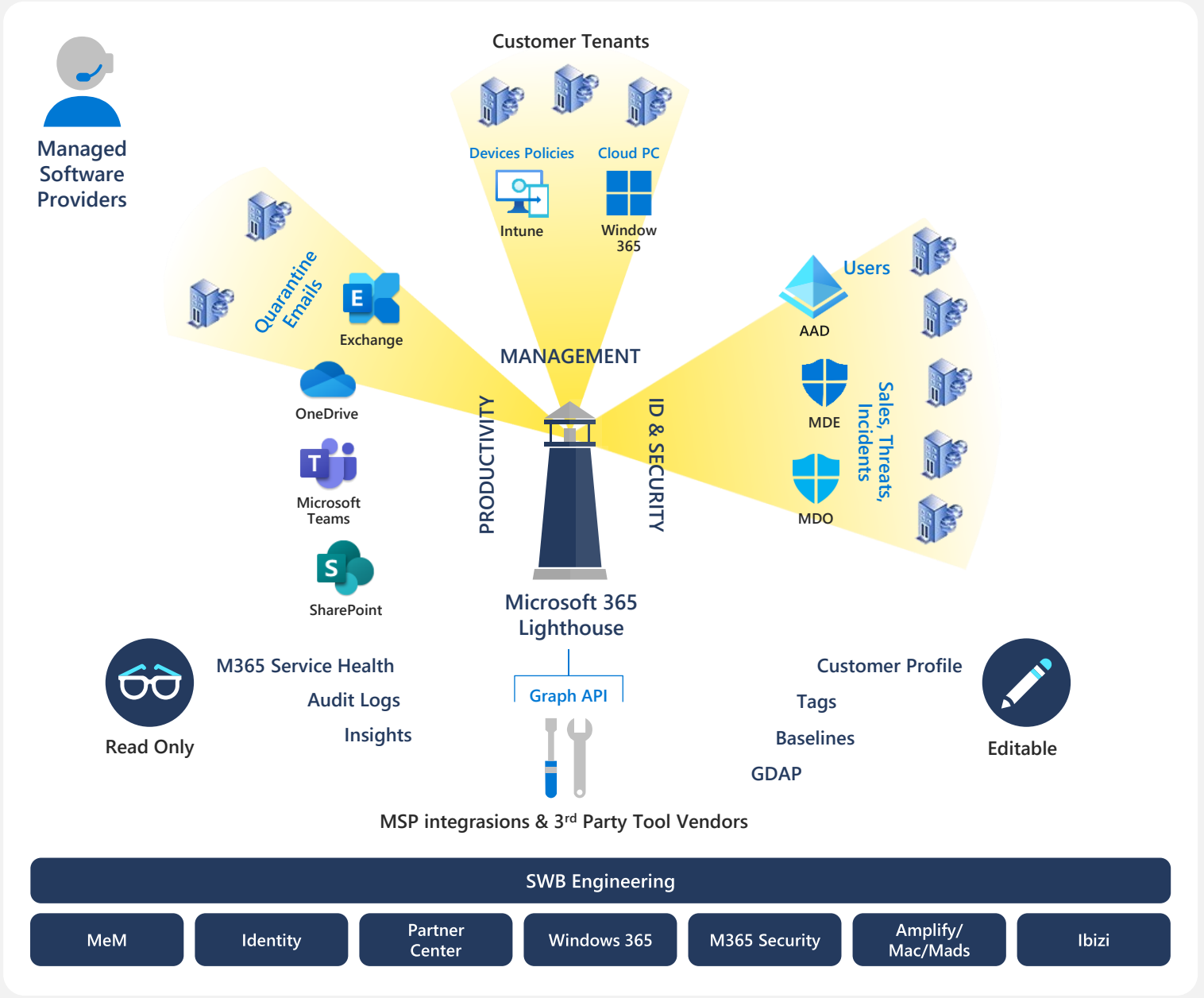


Microsoft 365 Lighthouse – Enfoques y tecnologías

- Una plataforma de ingesta de datos
- Alojado en Graph
- Multi-Tenant: las API están en el contexto del socio, pero exponen los datos de sus clientes Inquilinos, por lo que son **"Multi-Tenant"**
- Integrado con el Centro de partners/AAD para las relaciones entre socios y clientes
- Tiene un modelo de inserción y extracción para la ingesta de datos



Microsoft 365 Lighthouse y sus equipos de asociados o requisitos previos



Q4 2022

Se actualizó la línea base predeterminada para incluir directivas de protección de aplicaciones y supervisión del estado del dispositivo.

Administrar buzones compartidos

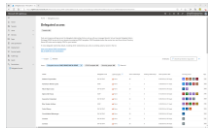
Asistente de configuración de GDAP

Información de implementación

Update to Defender Firewall Task

Q1 2023

Línea base predeterminada ampliada con la inscripción automatizada de dispositivos y la tarea de OneDrive



Información sobre la implementación multiinquilino e identificación de tareas con regresión

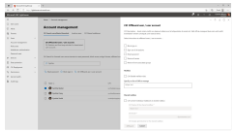
Acceso delegado

Resumen de MDE: Insights y TVM

Custom Baselines

Alertas y notificaciones

Usuarios de Offboarding



Q2 2023

Lighthouse RBAC

Ampliación de historias existentes

Vista de inquilinos de M360 con información de Lighthouse y Orland

5x5: Registro simplificado y expansión de clientes elegibles, incluido el valor agregado de WoW

Microsoft 365 Lighthouse Roadmap

Permitir que los partners protejan y gestionen a sus clientes pymes (SMB)

NFW	Q1 2023	Q2 2023
Mantener el servicio en buen estado	• Compatibilidad con Intune go-local • Plan Regional de Conmutación Condicional de la UE - Proyecto Umatilla • Registro de la información del inquilino del cliente en la telemetría de Lighthouse	• Límite de cumplimiento (M365) • Aumente la automatización de pruebas • Demostraciones externas • Automatice las actualizaciones de OKR (cobertura de pruebas, SLA/SLO)
Pasar de Intune/EMX	• ADO / Wiki migración • Privacidad / Reseñas de gráficos / Accesibilidad • Entrada de árbol de servicio y • Gestión del código fuente	• Revisiones de seguridad • Información e infraestructura de telemetría • Registro de clústeres de Kusto • Biblioteca de registro de MDS • Migración de toros

Q1 2023

Análisis de endpoints
- Estado del dispositivo y de la aplicación

Planes de implementación
- Tarjeta de página de inicio
- Vistas de MT
- Información sobre licencias
- Progreso del usuario

Líneas de base ampliadas
- OneDrive

MDE/MDB
- TVM y puntuación de exposición
- Información sobre la seguridad de los dispositivos

Q2 2023

GDAP
- Gestión de acceso delegado
- Paso de implementación

Alertas y notificaciones

Planes de despliegue
- Detección de estado

Baselines
- Líneas base personalizadas
- Windows Update y ASR

H2 2023 y más allá

Gestión de usuarios
- Incorporación
- Offboarding

Productividad
- Equipos, SPO, EXO
-

Amplíe los escenarios existentes, entre los que se incluyen:
- Planes de implementación
- Líneas base predeterminadas
- MDE/MDB
- RBAC para Lighthouse

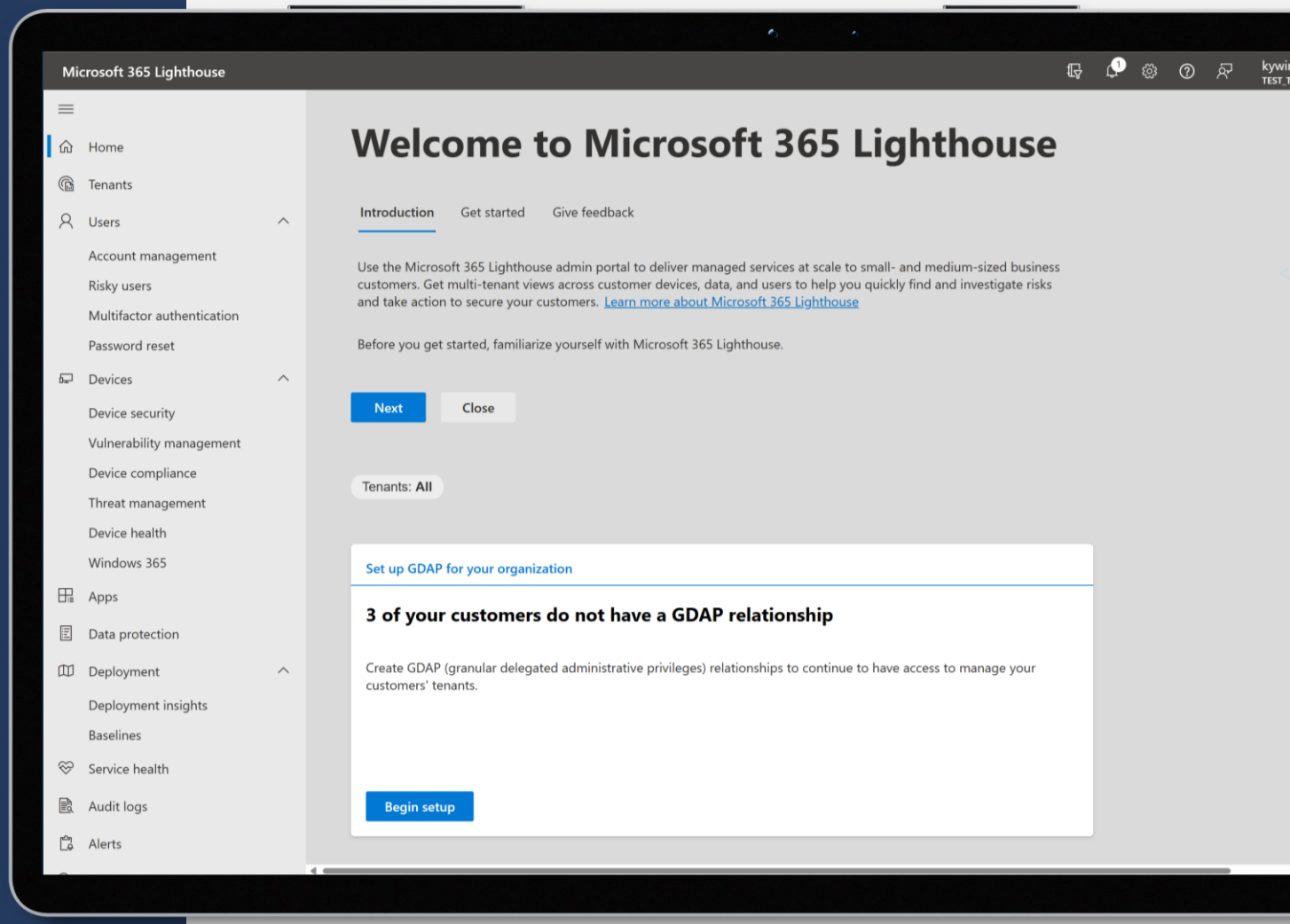
Microsoft 365 Lighthouse Roadmap

Enabling partners to secure and manage their SMB customers

Siguientes pasos

Comenzar:

aka.ms/M365Lighthouseonboard



Requirementos

Partner Tenant

Los MSP deben estar inscritos en el ***programa Proveedor de soluciones en la nube (CSP)*** como ***revendedor indirecto*** o ***socio de facturación directa*** para usar Lighthouse.

Actualización para GDAP.

Customer Tenants

1. Tener una configuración de acceso delegado (DAP o GDAP)
    1. Incluida la no relación de reventa
2. **Tener al menos una de las siguientes suscripciones:**
    - **Microsoft 365 Business Premium**
    - Microsoft 365 E3/E5
    - Windows Microsoft 365 Business
    - Microsoft Defender for Business
3. **No más de 2500 usuarios con licencia**
4. El inquilino y el asociado del cliente deben residir en la **misma región geográfica**

¿Cuál es la diferencia entre Microsoft 365 Lighthouse y las capacidades de organización multiinquilino en Microsoft 365 Defender? Si administro servicios para LASB, ¿qué debo usar?

Las funcionalidades multi-inquilino de Microsoft 365 Defender proporcionan a las organizaciones grandes la capacidad de proteger y administrar varios inquilinos desde un único portal, con un enfoque en los flujos de investigación del Centro de operaciones de seguridad global (SOC), incluida una vista unificada de incidentes entre inquilinos y la capacidad de realizar búsquedas avanzadas en los datos contenidos en varios inquilinos. Las funcionalidades también ayudan a los proveedores de servicios de seguridad administrados (MSSP) empresariales a ejecutar de forma eficaz su SOC.

Para los MSP que administran servicios para clientes SMB y que necesitan un conjunto completo de funcionalidades que abarcan la ***seguridad, la identidad y la administración de aplicaciones de Microsoft 365*** en una experiencia unificada en un único portal, seguimos recomendando ***Microsoft 365 Lighthouse***. Lighthouse incluye un conjunto más amplio de funcionalidades optimizadas para los CSP, especialmente las que usan Microsoft 365 Empresa Premium y Defender para empresas.

	Microsoft 365 Lighthouse	Funcionalidades de organización multiinquilino en Microsoft 365 Defender
Enfoque de audiencia y solución	Los csp inscritos en el programa CSP, especialmente los que se centran en soluciones SMB como Defender para la empresa y Microsoft 365 Empresa Premium Incluye un conjunto completo de funcionalidades que abarcan la seguridad, la identidad y la administración de aplicaciones de Microsoft 365 en una experiencia unificada en un único portal	Grandes organizaciones de clientes y MSSP centrados en clientes empresariales Ayuda a los CSP a administrar de forma eficaz sus operaciones de seguridad Microsoft 365 Defender proporcionando la capacidad de ver incidentes y alertas, buscar amenazas y abordar escenarios de seguridad avanzada desde un único portal.
Requisitos de idoneidad	Los CSP deben inscribirse en el programa CSP. Requiere una relación de acceso delegado con el cliente Consulte la lista completa de requisitos	Requiere una relación GDAP con el cliente Clientes que usan la colaboración B2B de Azure Active Directory
Gorra de asiento	Hasta 2500 puestos por inquilino administrado	Ilimitado
Límite de inquilino	Ilimitado	Hasta 50 inquilinos por cliente o asociado
Aprovisionamiento de inquilinos en Defender para empresas o Defender para punto de conexión	Iniciado mediante el aprovisionamiento con un solo clic en la línea base predeterminada en Lighthouse	Iniciado seleccionando Dispositivos activos> en el portal de Microsoft 365 Defender del cliente
Incorporación a Defender para empresas o Defender para punto de conexión	Se realiza a través de la línea base predeterminada en Lighthouse para dispositivos inscritos en Intune	Los dispositivos se pueden incorporar en el portal de Microsoft 365 Defender de cada cliente o mediante Intune
Capacidad de ver el estado de licencia	Visible a través de la línea base predeterminada en Lighthouse	Visible en el portal de Microsoft 365 Defender de cada cliente
Inventario de dispositivos	Ver todos los dispositivos (todas las plataformas) inscritos en Intune o dispositivos Windows incorporados a Defender para empresas o Defender para punto de conexión	Ver una lista de inquilinos e información sobre dispositivos (Windows, iOS, Android, Mac, Linux) incorporados a Defender para empresas o Defender para punto de conexión
Administración de configuración entre puntos de conexión, correo electrónico, Intune, identidad, protección de datos	Implemente las configuraciones recomendadas en los inquilinos a través de la línea base predeterminada, incluidas las directivas de reducción de superficie expuesta a ataques, firewall y antivirus, así como correo electrónico, Intune, etc. Detectar configuraciones que ya están presentes en el inquilino y variaciones de la configuración recomendada Informes multiinquilino sobre implementaciones entre inquilinos	Planeada para una versión futura
Administración de amenazas y vulnerabilidades	Vista agregada de la puntuación de exposición, la mayoría de los dispositivos expuestos y las recomendaciones entre inquilinos	Vista agregada de la puntuación de exposición y la mayoría de los dispositivos expuestos

	Microsoft 365 Lighthouse	Funcionalidades de organización multiinquilino en Microsoft 365 Defender
Incidentes y alertas	Visualización de incidentes y alertas, con vínculos a inquilinos individuales para ver detalles y realizar acciones Acciones masivas para asignar o resolver un incidente o una alerta Notificaciones automatizadas por correo electrónico de incidentes y alertas basadas en reglas personalizables	Visualización de incidentes y alertas, con vínculos a inquilinos individuales para ver detalles y realizar acciones Acciones masivas para asignar o resolver un incidente o una alerta
Búsqueda avanzada de amenazas	No disponible	Búsqueda de amenazas en varios inquilinos simultáneamente Nota: La búsqueda avanzada solo está disponible en Microsoft Defender para punto de conexión P2
Búsqueda global	Búsqueda global de usuarios y dispositivos administrados entre inquilinos	Búsqueda global de archivos, usuarios y dispositivos entre inquilinos
Puntuación de seguridad de Microsoft	Vista comparativa de puntuación segura en todos los inquilinos administrados	No disponible
Identity	Usuarios marcados por Protección de id. de Microsoft Entra para un comportamiento de riesgo entre inquilinos, incluida la capacidad de corregir riesgos de forma masiva Cuentas de usuario inactivas y cuentas de buzón compartido desprotegidas, incluida la capacidad de bloquearlas Habilitación de la autenticación multifactor y finalización del registro entre inquilinos Habilitación del autoservicio de restablecimiento de contraseña y finalización del registro entre inquilinos	No disponible
Administración	Lista de todos los dispositivos inscritos en Intune y su estado de cumplimiento de dispositivos Información de estado de dispositivos y aplicaciones para dispositivos inscritos en Intune de Análisis de puntos de conexión Lista de dispositivos PC en la nube Windows 365 y acciones básicas de administración	No disponible

	Microsoft 365 Lighthouse	Funcionalidades de organización multiinquilino en Microsoft 365 Defender
Otras funcionalidades de seguridad	Lista de dispositivos inscritos en Intune que están vencidos por exámenes o que no tienen Microsoft Defender Antivirus o las últimas actualizaciones Microsoft Defender Antivirus Información sobre los correos electrónicos en cuarentena entre inquilinos Vista agregada de incidentes y avisos de mantenimiento del servicio entre inquilinos	No disponible
Asesor de ventas	Conclusiones, recomendaciones e instrucciones basadas en IA para ayudar a los CSP a adquirir, conservar y aumentar los clientes	No disponible

Configurar playbooks para responder de manera automática a los incidentes de Microsoft 365 Defender sin necesidad de Sentinel

Microsoft Power Automate se integra con Microsoft 365 Defender para proporcionar guías de orquestación y automatización para alertas personalizadas. Mediante el uso de los conectores disponibles en Power Automate, ***puede automatizar la activación de playbooks cuando Microsoft 365 Defender genera alertas***. Por ejemplo, puede crear automáticamente una incidencia en los sistemas de tickets mediante el conector de ServiceNow o enviar un correo electrónico de aprobación para ejecutar una acción de gobierno personalizada cuando se active una alerta en Microsoft 365 Defender.

Para ello, debe tener un plan válido de Microsoft Power Automate. Puede crear flujos de trabajo para habilitar opciones de gobierno personalizadas para sus políticas creando un libro de jugadas en Power Automate mediante un conector de Microsoft 365 Defender. Una vez creado el playbook en Power Automate, se sincroniza automáticamente con Microsoft 365 Defender. A continuación, puede asociarlo con una política en Microsoft 365 Defender para enviar alertas a Power Automate.

El conector de Microsoft 365 Defender en Power Automate admite acciones y activadores automatizados. ***Power Automate se activa automáticamente cuando Microsoft 365 Defender genera una alerta***. Las acciones incluyen el cambio del estado de la alerta en Microsoft 365 Defender.

Para crear playbooks de Power Automate para Microsoft 365 Defender, debe crear un token de API en Microsoft 365 Defender. A continuación, vaya al portal de Power Automate, seleccione "Mis flujos", "Nuevo flujo" y, en el menú desplegable, seleccione "Flujo automatizado en la nube". Proporcione un nombre para el flujo y en "Elija el desencadenante de su flujo", escriba "Microsoft 365 Defender" y seleccione "Cuando se genera una alerta".

Links de interés:
Cómo conectar una aplicación de un Partner asociada con el api de Microsoft 365 Defender
Integración con Microsoft Power Automate para la automatización de alertas personalizada - Microsoft Defender for Cloud Apps | Microsoft Learn
Ampliación de la gobernanza a la corrección de puntos de conexión - Microsoft Defender for Cloud Apps | Microsoft Learn
Integración con Microsoft Power Automate para la automatización de alertas personalizada - Microsoft Defender for Cloud Apps | Microsoft Learn

Acceso vía Microsoft 365 Ligthouse vía API

La API de Microsoft 365 Lighthouse está disponible en Microsoft Graph. Como MSP, puede utilizar la API de Microsoft 365 Lighthouse en Microsoft Graph para obtener información sobre los riesgos identificados y tomar medidas para ayudar a que sus clientes se encuentren en un estado saludable y seguro.

Puede utilizar la API Lighthouse para realizar las siguientes tareas:

Dispositivos: Analizar las tendencias de cumplimiento de dispositivos para comprender mejor cómo evoluciona el cumplimiento de dispositivos de sus clientes a lo largo del tiempo. Comprenda qué directivas de conformidad de dispositivos se han creado en sus clientes y el estado de las directivas.
Gestión de amenazas: Obtenga información sobre el estado del malware presente en los dispositivos Windows registrados para su gestión en todos sus clientes. Vea el estado de protección de los dispositivos Windows registrados para su gestión en todos sus clientes para asegurarse de que los que utilizan Windows Defender se encuentran en buen estado.
Usuarios: Descubra los usuarios de riesgo en todos sus clientes. Vea el resumen del registro de usuarios de credenciales para comprender qué usuarios de sus clientes se han registrado para la autenticación multifactor y el restablecimiento de contraseñas de autoservicio.

Hasta donde hemos investigado, ***el API de M365 Lighthouse no soporta la gestión de los incidentes ni de las alertas***: Microsoft 365 Lighthouse API in Microsoft Graph (preview). Se tendría que hacer cliente a cliente mediante power automation pero se puede desplegar como IaaC mediante pipeline para automatizar las configuraciones.

Enlaces de interés:
Administración de varios inquilinos de clientes mediante la API de Microsoft 365 Lighthouse - Microsoft Graph | Microsoft Learn
Tipo de recurso managedTenant - Microsoft Graph beta | Microsoft Learn

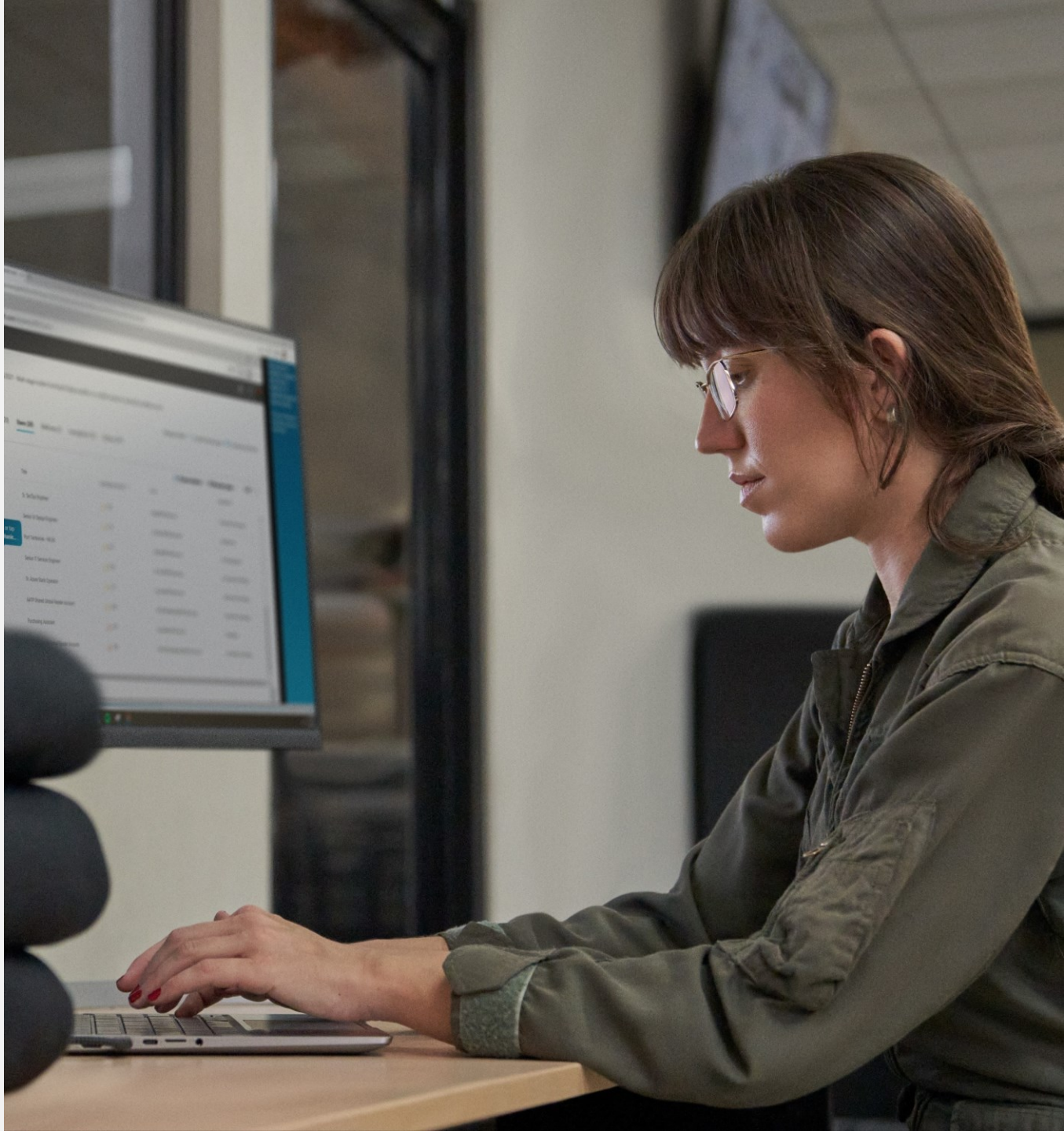
Recursos

Demostración de Microsoft 365 Lighthouse:
aka.ms/M365Lighthouse-OverviewGuide

Acceda a la documentación técnica:
aka.ms/M365LighthouseDocs

Aprende más:
aka.ms/M365Lighthouse

Comparte tus comentarios:
aka.ms/M365Lighthousefeedback



Thank you.