Impementación Zero Trust 4 semanas

Identity Protection / Device Management / Access Management
WDATP / WDSG / AAD / MDM
KS - Consulting Services

Este es el núcleo de Zero Trust. En lugar de creer que todo lo que hay detrás del firewall corporativo es seguro, el modelo de confianza cero asume la infracción y verifica cada solicitud como si se originara de una red no controlada. Independientemente de dónde se origine la solicitud o a qué recurso acceda, el modelo de confianza cero nos enseña a "nunca confiar, verificar siempre".

Implementar un modelo Zero Trust requiere que todos los componentes (identidades, dispositivos, redes y aplicaciones) sean validados y provean confianza.

KS Consulting realizará las siguientes tareas como parte del ofertamiento Zero Trust:

1. Microsoft Intune

- Workshop de 16 horas para:
  - Evagelizar funcionalidades de MDM/MAM.
  - Definir y documentar alcance MDM/MAM.
- Configuración de Consola con alcance MDM (para 5 dispositivos):
  - Reglas, Configuraciones, Políticas.
  - Enrolamiento de dispositivos Android i/o IOS.
- Configuración de Consola con alcance MAM (para 5 aplicaciones):
  - Asignación de aplicaciones móviles a grupos de usuarios y dispositivos.
  - Consulta de informes sobre las aplicaciones que se usan.
  - Borrado selectivo eliminando solo los datos de la organización de las aplicaciones.
- Transferencia de Conocimiento en cada alcance para administración y autosuficiencia.

2. Azure Active Directory

- Workshop de 8 horas para:
  - Evagelizar funcionalidades de AAD.
  - Definir y documentar alcance AAD.
- Azure Active Directory Identity Protection (5 políticas).
  - Configuración de decisiones de control de acceso dinámico basadas en el riesgo de usuario, dispositivo, ubicación y sesión para cada solicitud de recursos.
  - Consideraciones para decidir si (1) permitir el acceso, (2) denegar el acceso o (3) controlar el acceso con desafíos de autenticación adicionales (por ejemplo, autenticación multifactor), Términos de uso o restricciones de acceso.
  - Access Management:
    - Single Sign-On.
    - Multi-Factor Authentication.

        - Acceso Condicional.
- Transferencia de Conocimiento en cada alcance para administración y autosuficiencia.

3. Microsoft Defender for End-Point

- Advanced Threat Protection / System Guard.
- Workshop de 8 horas para:
    - Evagelizar funcionalidades de WDATP y WDSG.
    - Definir y documentar alcance WDATP y WDSG.
- Configuración 10 políticas.
- Transferencia de Conocimiento en cada alcance para administración y autosuficiencia.

Timeline Operativo

- Semana 1:
    - Evangelización, Definición y Documentación
        - Alcance 1 y 2.
- Semana 2:
    - Evangelización, Definición y Documentación
        - Alcance 3 y 4.
    - Configuración de Plataforma y Pruebas.
        - Alcance 1 y 2.
- Semana 3:
    - Configuración de Plataforma y Pruebas.
        - Alcance 3 y 4.
- Semana 4:
    - Capacitación y Cierre.
        - Alcances 1, 2, 3 y 4.

Mayor Información:

Zero Trust con Microsoft 365

Un modelo de red Zero Trust (Figura 1) normalmente comprende lo siguiente:

1. Proveedor de identidades para realizar un seguimiento de los usuarios y la información relacionada con el usuario.
2. Directorio de dispositivos para mantener una lista de dispositivos que tienen acceso a los recursos corporativos, junto con su información de dispositivo correspondiente (por ejemplo, tipo de dispositivo, integridad, etc.).
3. Servicio de evaluación de políticas para determinar si un usuario o dispositivo cumple con la política establecida por los administradores de seguridad.
4. Proxy de acceso que utiliza las señales anteriores para conceder o denegar el acceso a un recurso organizativo.

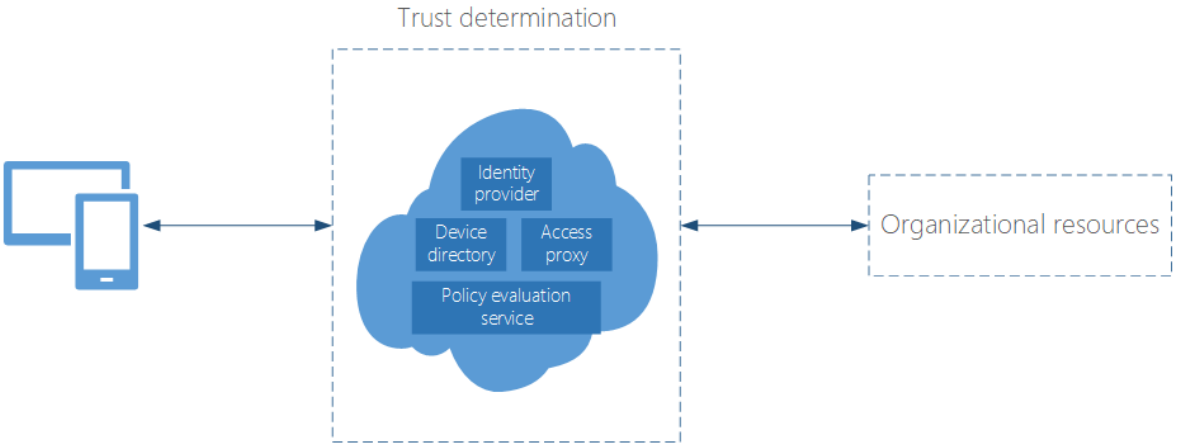

Figura 1. Componentes básicos de un modelo de red general de Zero Trust

Zero Trust es la siguiente evolución en seguridad de red. El estado de los ciberataques impulsa a las organizaciones a adoptar la mentalidad de "asumir la violación", pero este enfoque no debería ser limitante. Las redes de Zero Trust protegen los datos y recursos corporativos, a la vez que se aseguran de que las organizaciones puedan construir un lugar de trabajo moderno utilizando tecnologías que capaciten a los empleados a ser productivos en cualquier momento, en cualquier lugar y de cualquier manera.

Azure AD – Conditional Access

Es el pilar fundamental de cómo los clientes pueden implementar un enfoque de red de Zero Trust. **Conditional access** y **Azure Active Directory Identity Protection** toman decisiones dinámicas de control de acceso basadas en el **riesgo de usuario**, **dispositivo**, **ubicación** y **sesión** para cada **solicitud de recursos**.

El acceso condicional proporciona un conjunto de directivas que se pueden configurar para controlar las circunstancias en las que los usuarios pueden acceder a los recursos corporativos. Las consideraciones para el acceso incluyen el rol de usuario, la pertenencia a grupos, el estado y el cumplimiento del dispositivo, las aplicaciones móviles, la ubicación y el riesgo de inicio de sesión. Estas consideraciones se utilizan para decidir si (1) permitir el acceso, (2) denegar el acceso o (3) controlar el acceso con desafíos de autenticación adicionales Azure Active Directory.

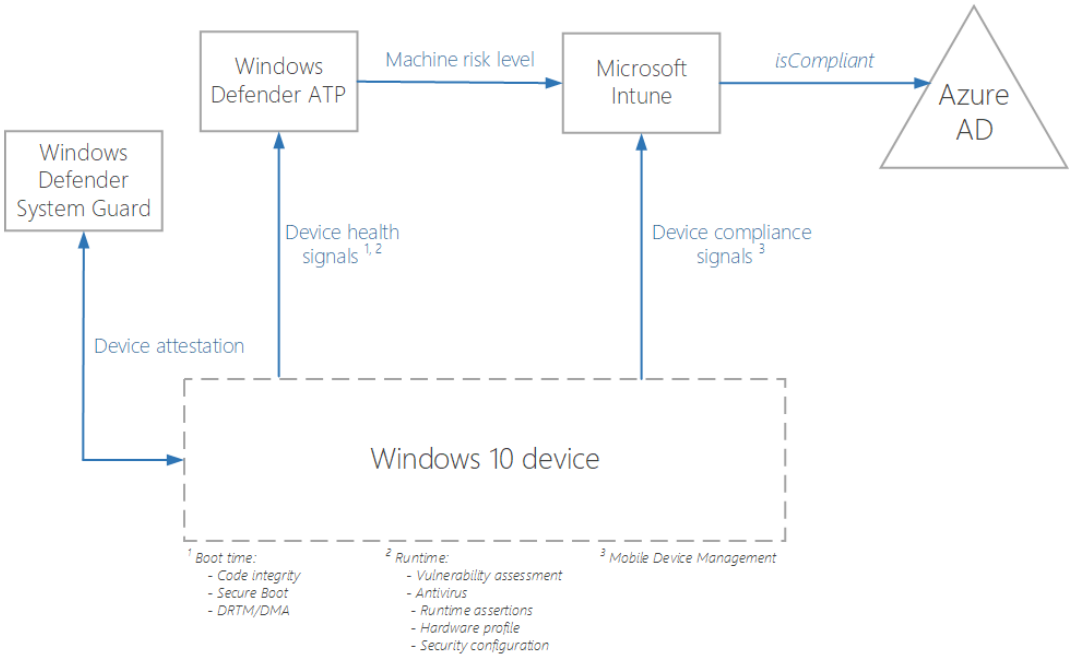

Figura 2. Enfoque de alto nivel de Microsoft para realizar redes de confianza cero mediante el acceso condicional.

Para lograr el modelo Zero Trust, Microsoft integra varios componentes y capacidades en Microsoft 365:

1. Windows Defender Advanced Threat Protection.
2. Windows Defender System Guard.
3. Azure Active Directory.
4. Microsoft Intune.

Windows Defender Advanced Threat Protection (ATP)

(ATP) es una Plataforma de Protección de Endpoint (EPP) y una Tecnología de Respuesta de Detección de Endpoint (EDR) que proporciona protección basada en inteligencia, detección posterior a la violación, investigación y capacidades de respuesta automática. Combina sensores de comportamiento integrados, aprendizaje automático y análisis de seguridad para monitorear continuamente el estado de los dispositivos y tomar medidas correctivas si es necesario. Una de las formas únicas en que ATP de Windows Defender mitiga las infracciones es aislando automáticamente a las máquinas y usuarios comprometidos de un mayor acceso a los recursos en la nube.

Windows Defender System Guard

Windows Defender System Guard protege y mantiene la integridad de un sistema a medida que arranca y continúa funcionando. En la mentalidad de "asumir la violación", es importante que los administradores de seguridad tengan la capacidad de dar fe remotamente del estado de seguridad de un dispositivo. Contribuye a establecer la integridad del dispositivo. Hace aserciones de tiempo de arranque y tiempo de ejecución con

raíz de hardware sobre el estado del dispositivo. Estas mediciones son consumidas por ATP de Windows Defender y contribuyen al nivel de riesgo de la máquina asignado al dispositivo.

El único objetivo más importante de Protección del sistema de Windows Defender es validar que no se ha infringido la integridad del sistema. Este marco de confianza de alta integridad respaldado por hardware permite a los clientes solicitar un informe firmado que pueda certificar (dentro de las garantías especificadas por las promesas de seguridad) que no se ha producido ninguna manipulación del estado de seguridad del dispositivo. Los clientes de ATP de Windows Defender pueden ver el estado de seguridad de todos sus dispositivos mediante el portal de ATP de Windows Defender, lo que permite la detección y corrección de cualquier infracción de seguridad.

La atestación de tiempo de ejecución de Protección del sistema de Windows Defender aprovecha las tecnologías de seguridad basadas en hardware en seguridad basada en virtualización (VBS) para detectar ataques. En dispositivos virtuales habilitados para modo seguro, la atestación de tiempo de ejecución de Protección del sistema de Windows Defender se ejecuta en un entorno aislado, lo que la hace resistente incluso a un adversario a nivel de kernel.

La atestación en tiempo de ejecución de Protección del sistema de Windows Defender afirma continuamente la postura de seguridad del sistema en tiempo de ejecución. Estas afirmaciones están dirigidas a capturar infracciones de las promesas de seguridad de Windows, como deshabilitar la protección de procesos.

Azure Active Directory

Azure Active Directory es una solución de administración de acceso e identidad en la nube que las empresas usan para administrar el acceso a las aplicaciones y proteger las identidades de usuario tanto en la nube como en el entorno local. Además de sus capacidades de administración de directorios e identidades, como motor de control de acceso, Azure AD ofrece:

- Experiencia de inicio de sesión único: cada usuario tiene una única identidad para acceder a los recursos de toda la empresa para garantizar una mayor productividad. Los usuarios pueden usar la misma cuenta profesional o educativa para el inicio de sesión único en servicios en la nube y aplicaciones web locales. La autenticación Multifactor ayuda a proporcionar un nivel adicional de validación del usuario.
- Aprovisionamiento automático de Acceso a Aplicación: el acceso de usuario a aplicaciones se pueden aprovisionar automaticamente o de-provisionar basados en sus membresías de grupos, geo-localización, y estado de empleado.

Como motor de administración de acceso, Azure AD toma una decisión bien informada sobre la concesión de acceso a los recursos de la organización mediante información sobre:

- Permisos de grupo y de usuario.
- Aplicación a la que se accede.
- Dispositivo utilizado para iniciar sesión (por ejemplo, información de cumplimiento de dispositivos de Intune).
- Sistema operativo del dispositivo que se utiliza para iniciar sesión.
- Ubicación o rangos IP de inicio de sesión.
- Aplicación cliente utilizada para iniciar sesión.

- Hora de inicio de sesión.
- Riesgo de inicio de sesión, que representa la probabilidad de que el propietario de la identidad no autorice un inicio de sesión determinado (calculado por Azure AD Identity Protection, con múltiples detecciones heurísticas o de aprendizaje automático).
- Riesgo de usuario, que representa la probabilidad de que un actor malo haya comprometido a un usuario determinado (calculado por el aprendizaje automático avanzado de Azure AD Identity Protection que aprovecha numerosos orígenes internos y externos para que los datos de etiquetas mejoren continuamente).

Las directivas de acceso condicional se evalúan en tiempo real y se aplican cuando un usuario intenta acceder a cualquier aplicación conectada a Azure AD, por ejemplo, aplicaciones SaaS, aplicaciones personalizadas que se ejecutan en la nube o aplicaciones web locales. Cuando se detecta actividad sospechosa, Azure AD ayuda a realizar acciones de corrección, como bloquear usuarios de alto riesgo, restablecer contraseñas de usuario si las credenciales se ven comprometidas, aplicar términos de uso y otros.

La decisión de conceder acceso a una aplicación corporativa se da a los dispositivos cliente en forma de token de acceso. Esta decisión se centra en el cumplimiento de la directiva de acceso condicional de Azure AD. Si una solicitud cumple los requisitos, se concede un token a un cliente. La directiva puede requerir que la solicitud proporcione acceso limitado (por ejemplo, no se permite la descarga) o incluso pasarse a través de Microsoft Cloud App Security para la supervisión en sesión.

Microsoft Intune

Microsoft Intune se usa para administrar dispositivos móviles, equipos y aplicaciones en una organización. Microsoft Intune y Azure tienen administración y visibilidad de activos y datos valiosos para la organización y tienen la capacidad de inferir automáticamente los requisitos de confianza basados en construcciones como Azure Information Protection, Etiquetado de activos o Microsoft Cloud App Security.

Microsoft Intune es responsable de la inscripción, el registro y la administración de los dispositivos cliente. Es compatible con una amplia gama de tipos de dispositivos: dispositivos móviles (Android e iOS), portátiles (Windows y macOS) y dispositivos BYOD de los empleados. Intune combina el nivel de riesgo de máquina proporcionado por ATP de Windows Defender con otras señales de cumplimiento para determinar el estado de cumplimiento (*"isCompliant"*) del dispositivo. Azure AD aprovecha este estado de cumplimiento para bloquear o permitir el acceso a los recursos corporativos. Las directivas de acceso condicional se pueden configurar en Intune de dos maneras:

- Basado en aplicaciones: solo las aplicaciones administradas pueden acceder a los recursos corporativos.
- Basado en dispositivos: solo los dispositivos administrados y compatibles pueden acceder a los recursos corporativos.