Data Sheet

Active Directory Solution Suite

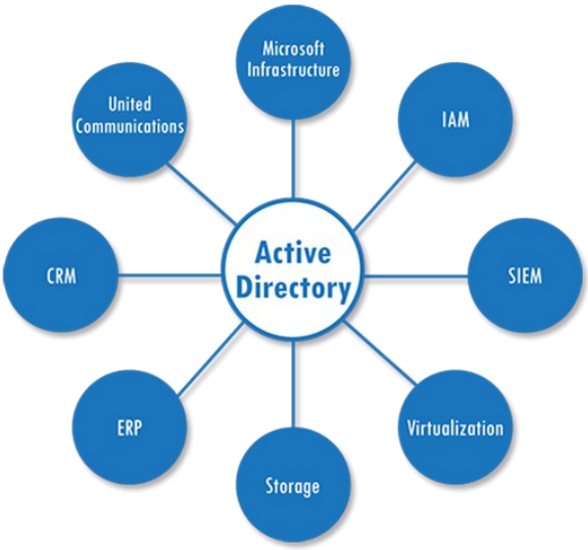
Insight. Automation. Control.

El Directorio Activo (AD) es el centro de autenticación y autorización para la infraestructura de TI en una organización, y necesita un poco de ayuda. Debido a la resistencia dentro del AD y el trabajo duro de los astutos administradores, el negocio no puede visualizar el problema que existe en el AD. El Directorio Activo es un desastre para la mayoría debido al crecimiento, los cambios que ha experimentado, y las complejidades que se han presentado en más de una década. Todo lo que el negocio ve es cuando inician sesión en su ordenador en la mañana. Cuando navegan a su recurso compartido de archivos favorito, tienen el acceso que necesitan. Pero las personas que realmente saben del AD son conscientes que es una fachada ...

Sus Inversiones

¿Qué tienen en común todas sus inversiones? El Directorio Activo controla quién se puede conectar a su entorno (autenticación), quién puede acceder a sus aplicaciones, datos y sistemas (autorización), y hasta qué nivel de acceso reciben. El Directorio Activo hace que todo funcione.

Las organizaciones confían en el AD para llevar a cabo las funciones más críticas que necesitan para operar de manera eficiente y segura, pero no se dan cuenta qué tan significativo es el impacto que tiene el AD a una mayor escala.



El Directorio Activo es:

- **Obstáculo para el éxito de sus nuevas inversiones**
  - ⇒ Su IAM, CRM, SIEM, ERP, UC, y otras inversiones en tecnología todas dependen del Directorio Activo, de alguna manera. Si el AD no está saludable, sus inversiones no lo estarán tampoco.
- **Poner sus operaciones en riesgo**
  - ⇒ En el extremo inferior de la escala, las condiciones tóxicas como bucles anidados de grupos causan que los usuarios tengan que esperar más tiempo para autenticarse en los dominios y recursos. Sin embargo, en el extremo superior de la escala, la misma condición hace aplicaciones para suspender, una espiral fuera debido a bucles infinitos. Esto no tiene que suceder, y es sólo una de las muchas condiciones que las organizaciones pueden de forma rápida y fácil hacer frente para mitigar el riesgo operacional.
- **Poniendo en peligro sus datos**
  - ⇒ Los grupos de seguridad son el principal mecanismo por el cual se aprovisiona el acceso a los sistemas, aplicaciones y datos. Sin un control estricto en la visibilidad de Usuarios de Grupos y donde los grupos han tenido acceso, el riesgo no se puede mitigar con eficacia con la preocupación de que exista violación de los datos y se otorgue el acceso inadecuado.
- **Le cuesta dinero que no es necesario gastar**
  - ⇒ La combinación de las dificultades experimentadas en la aplicación de nuevas tecnologías, frente a los cortes, las cuestiones operacionales y la protección de datos que sufren como consecuencia trae un costo de dinero superior al que en realidad la organización necesita gastar.

STEALTHbits protege sus inversiones

A través de un conjunto de soluciones integradas de Active Directory, a escala empresarial, STEALTHbits proporciona la perspectiva, la automatización y controles necesarios para producir un Active Directory de seguro, que cumple, altamente organizado y estructurado que funciona a los costos más bajos, mayor rendimiento, y se coloca para crecimiento futuro.

Informes y flujos de trabajo

Obtener los conocimientos necesarios para limpiar y optimizar el Directorio Activo. Informes sobre los riesgos de seguridad y operativos, como objetos obsoletos, condiciones de anidación de grupos tóxicos (es decir anidación circular, anidación profunda, anidamiento de dominios cruzados, etc.) y la pertenencia a grupos de seguridad sensibles; proporcionan la supervisión global que el Directorio Activo carece de forma nativa. Automatización incorporada para la limpieza de AD automatiza las tareas comunes y ayuda a garantizar la recuperación segura de objetos obsoletos.

Gobernanza

Facultar a la empresa a través de la simplificación y automatización de los cambios de pertenencia de grupo y la propiedad. Muchas veces, los grupos se asignan directamente a las líneas de negocio, por lo que los propietarios de negocios más adecuados para determinar la pertenencia al grupo de TI a pesar de ser los que físicamente pueden manejarlos. El grupo de Gobierno AD cierra la brecha entre TI y el negocio para asegurar que la pertenencia al grupo está actualizada y correcta, protegiendo así que los usuarios tengan un acceso inadecuado.

Monitoreo y Control

Comprender todos los cambios que se producen en la EA y establecer políticas para prevenir cambios no deseados. Con una visibilidad completa de todos los detalles del cambio (no sólo los registros de seguridad que se suministran de forma nativa en el Directorio Activo) Los administradores están habilitados para crear controles preventivos de seguridad y el cumplimiento a normativas, al mismo tiempo que el suministrado por otras tecnologías (por ejemplo, aplicaciones SIEM) con datos contextuales en tiempo real, que ayuda a mejorar la capacidad de una organización para identificar y prevenir las violaciones de datos y actividades nefastas.

Sobre STEALTHbits Technologies

Identificar las amenazas. Asegurar los datos. Reducir el riesgo.

STEALTHbits es una compañía de software de seguridad de los datos. Ayudamos a las organizaciones a garantizar que las personas adecuadas tienen acceso a la información correcta. Al dar nuestra visión a los clientes de quién tiene acceso y propiedad de sus datos no estructurados además de la protección contra el acceso malintencionado, reducimos los riesgos de seguridad, otorgamos cumplimiento total a los requisitos y ayudamos a disminuir los gastos operativos.

STEALTHbits Technologies, Inc.
200 Central Avenue
Hawthorne, NJ 07506
P: 1.201.447.9300 | F: 1.201.447.1818
sales@stealthbits.com | support@stealthbits.com
www.stealthbits.com