Mast Backup Online

MBO End to End

Dispositivos endpoint

Actualmente los empleados de las empresas están acostumbrados a acceder a los datos corporativos en cualquier momento con sus propios dispositivos gracias a la cada vez mayor velocidad de la red inalámbrica. Los trabajadores crean, utilizan y guardan toda la información crítica para la empresa en sus dispositivos portátiles ya sean ordenadores, smartphones o tablets. A menudo, utilizan estos dispositivos del trabajo para su uso personal, con la cual cosa aumenta la vulnerabilidad de los datos corporativos que se mezclan con emails personales, fotografías y archivos.

Tal y como señaló Forrester Research, para evitar que los empleados operen en un entorno fuera del control de IT, muchas organizaciones llevan a cabo la política de Bring-your-own-device: BYOD aunque esta política implique problemas de seguridad. Permitir a los empleados utilizar su propio dispositivo puede beneficiarles, pero esta práctica sigue suponiendo que los datos empresariales sensibles se encuentren fuera de sus límites y control. A pesar de implementar políticas que regulen las aplicaciones que los empleados pueden utilizar en los dispositivos portátiles para acceder a los datos corporativos y configurarlos de manera que su memoria pueda borrarse, aun así, sigue sin existir un acceso a los datos si no se realiza el backup al propio centro autorizado. Imagine que el ordenador portátil o tablet con información crítica para su negocio se pierde o lo roban: en ese caso, podría borrar en remoto el dispositivo para prevenir que cualquier otra persona acceda a la información, pero, ¿qué pasaría si nunca ha realizado el backup de los datos? En ese caso, también perdería el acceso a los datos. Y, ¿cómo asegurar que los datos corporativos y la propiedad intelectual (IO) están protegidos? En ese caso, también perdería el acceso a los datos. Y, ¿cómo asegurar que los datos corporativos y la propiedad intelectual (IO) están protegidos?

Si su empresa no tiene una política de backup para los datos de este tipo de dispositivos endpoint; existe una alta probabilidad de que los propios empleados realicen el backup por su propia cuenta. Por ejemplo: un backup de los datos a un dispositivo USB, a un disco duro externo o a un servicio desprotegido en la nube como iCloud. En cualquier caso, corre el riesgo de que se produzca una fuga de datos fuera del propio firewall, esto significa que su IP puede quedar desprotegida en estos dispositivos, que pueden ser robados o que se comparten indiscriminadamente a personas que no deberían tener acceso a ellos.

Introducción

Con la creciente popularidad de tablets y smartphones, el fenómeno BYOD no va a desaparecer. Mientras los empleados sigan trayendo sus propios dispositivos a la oficina, la IP corporativa comparte ubicación con los mismos dispositivos donde se encuentran fotos familiares y mensajes personales. Se ha preguntado alguna vez ¿qué pasaría con los datos cuando un empleado suyo deje la organización? ¿Qué pasaría si este dispositivo se perdiese y acabase en manos de alguien que no debería acceder a esta información?

Para proteger los datos corporativos muchas empresas establecen un método que consiste en obtener el consentimiento de sus empleados para borrar definitivamente todos los datos en caso de pérdida, tanto si es un dispositivo corporativo o personal. Con este método sólo se induce a algunas empresas a la falsa sensación de que sus datos están seguros. La realidad es que una vez borrados los datos, nadie más tendrá acceso a ellos, incluido usted.

Según Gartner, en 2015 más del 60% de las empresas habrán sufrido la pérdida material de datos corporativos delicados a través de los dispositivos portátiles.

Si no tiene una política de backup de datos para dispositivos endpoint, posiblemente sus empleados utilicen métodos propios para crear otras copias de los datos, incluyendo USBs de baja seguridad, sincronizaciones y/o softwares de compartición de datos. Desafortunadamente, esto deja sin control a los datos corporativos y potencialmente los pone en manos de personas que no deberían acceder a su IP corporativa. Imagine que la información sensible de su negocio llegase a manos de su competencia o se filtrase en los medios de comunicación. Piense el caso en que se filtraran datos corporativos altamente sensibles en sectores regularizados como la sanidad o los servicios financieros. Estas circunstancias no sólo representarían el fin para esa empresa sino que además incurriría en graves consecuencias legales.

El riesgo de no proteger los datos que se albergan en los dispositivos endpoint

Los ejecutivos que toman decisiones de negocio conocen la importancia de protejer los datos de los dispositivos tanto como los datos de las instalaciones que residen en la red LAN. Pero muchos departamentos de IT son lentos a la hora de llevar a cabo este tipo de protección por culpa de la resistencia de los usuarios.

Los trabajadores que se conectan a la red de la empresa se oponen a la instalación de cualquier política de backup en sus ordenadores portátiles al temer que este tipo de procesos empeorarán el rendimiento de sus dispositivos. De hecho, en lo que concierne a dispositivos personales, ya sean laptops u otros dispositivos portátiles, los usuarios finales son muy precavidos a la hora de instalar cualquier aplicación que provenga del departamento de IT. Después de todo, sostienen que se trata de su dispositivo y tienen el derecho de rechazar la instalación de cualquier software que pueda dañarlo.

Los departamentos de IT suelen decantarse por ignorar la problemática a la hora de tratar el backup de dispositivos endpoint y así controlar que el coste del ancho de banda no se les dispara. Probablemente, quieran ahorrarse el backup en dispositivos portátiles porque reduce el potencial de la red en las redes ya congestionadas. Cuando los dispositivos portátiles se reconectan al LAN después de un tiempo largo, el tiempo de duración que consume la copia entra en acción y pone en evidencia esta problemática con el ancho de banda. A los departamentos de IT también les preocupa la gestión del backup que estos dispositivos requieren al realizarse con herramientas específicas y que pueden requerir un soporte muy diverso.

De todas formas, no implementar una política de backup en este tipo de dispositivos deja a la corporación expuesta a las amenazas de perder información confidencial.

Soporte múltiple OS

La protección de datos para dispositivos endpoint debe generalizarse e incluir soporte para múltiples sistemas operativos y plataformas, así como organizaciones y usuarios individuales que sean fieles a sus propias marcas o dispositivos. MBO End to End Cloud Backup es un hardware y software agnóstico y soporta la mayoría de sistemas operativos. Tanto si hablamos de usuarios de desktop o laptop que utilicen Windows, Linux o Mac OS, nuestro software puede proteger los datos de sus PC's, dispositivos Apple iOS y dispositivos Android, cubrimos la mayoría de las tablets y smartphones que se están utilizando hoy en día en los entornos empresariales, tanto si son dispositivos de los empleados como si son otorgados por la compañía.

Uso intuitivo y seguro

MBO End to End presenta una interface sencilla y user-friendly, que incluso permite a los empleados realizar el backup y recuperar tareas de sus dispositivos cuando sea necesario.

App certificada disponible para descargar

Esta aplicación para tablets y smartphones está disponible para descargar desde Apple App Store y desde Google Play; sus empleados pueden descargarla gratuitamente ayudará a combatir cualquier abyección por parte de sus empleados acerca de no querer instalar una aplicación sospechosa en sus propios dispositivos.

MBO End to End una solución integral para la protección de todo tipo y fuentes de datos incluyendo máquinas virtuales y físicas, aplicaciones empresariales, dispositivos end-point y datos en el cloud como Office 365, Google Apps, Salesforce, Amazon Web Services y Microsoft Azure.

Sobre Mast Storage & Asigra

Fundada en Barcelona en 1999, **Mast Storage**, es una compañía que se crea como especialista en soluciones de copia de seguridad para el entorno profesional: backup a cinta & backup a disco. **En 2007**, lanzamos el servicio de copia externalizada, **Mast Backup Online**, que se convierte en líder en España, y que actualmente cuenta con un canal de **más de 950 distribuidores en España**.

En 2017, Mast Storage firma un acuerdo con Asigra para incorporar esta solución de software a sus servicios y posicionarse como proveedor de soluciones Enterprise de backup y disaster recovery.

Desde 1986, Asigra, líder en cloud backup, proporciona a organizaciones de todo el mundo la solución de software más avanzada del mercado. La primera empresa con un software de recuperación sin agentes que permite realizar el backup y recuperación de servidores, máquinas virtuales, dispositivos endpoint, bases de datos y aplicaciones basadas en SaaS y IaaS. Una única solución para todo tipo de entornos y empresas.

T. 935 045 330 | mbo@mastbackuponline.com

Parc Tecnològic del Vallès | Ronda Can Fatjó 8
E-08290 Cerdanyola del Vallès | Barcelona

mastbackuponline.com | blog@mastcloud.net