Resumen de la Solución

Cinco Casos de Uso CASB que Necesita Conocer

De Deena Thomchick, Directora General de Gestión de Productos y Seguridad en la Nube

Nadie quiere una isla de seguridad que esté desconectada del resto de sus soluciones de seguridad. Este documento detalla cómo debe pensar para juntar las piezas.

El actual escenario es una desenfrenada carrera. Los funcionarios y las organizaciones adoptan a ritmo acelerado aplicaciones y servicios en la nube debido a la productividad, colaboración y conveniencia que ofrecen. ¿Y por qué actuarían de forma diferente?

Si tiene un problema, es posible que exista una aplicación en la nube que pueda solucionarlo. Así mismo, el movimiento a nivel corporativo que se distancia de licencias tradicionales de software hacia plataformas en la nube como Office 365, G Suite, Salesforce, etc., ofrece el beneficio adicional de un modelo financiero de Opex en lugar de Capex para sus costos de software.

Sin embargo, no todo es un mar de rosas. También existen riesgos.

El último año, las compañías descubrieron que sus funcionarios utilizaban, en promedio, 1.232 servicios diferentes en la nube y la mayoría de esas aplicaciones no estaban adecuadas para el uso corporativo. Para las aplicaciones autorizadas que se monitorean en la nube, 20% de los archivos en la nube estaban en riesgo de exposición debido al comportamiento de uso compartido de riesgo y muchos archivos contenían datos relacionados a la conformidad, como PII, PCI y PHI. 47% de las organizaciones identificaron comportamiento de alto riesgo de usuarios y 71% de esas instancias de comportamiento de alto riesgo indicaron tentativas de exfiltrar datos.

En este escenario han surgido los Agentes de Seguridad de Acceso a la Nube (CASBs - Cloud Access Security Brokers), que de acuerdo con Gartner es la categoría de seguridad que más crece. Los CASBs se proyectan específicamente para descubrir y monitorear el uso de aplicaciones en la nube, ofrecer protección contra la pérdida de datos (DLP - Data Loss Protection) para aplicaciones en la nube y proteger a las organizaciones contra amenazas que utilizan aplicaciones en la nube.

Una solución completa de CASB es una buena idea, sin embargo, Gartner recomienda que las empresas transciendan a una implantación independiente de CASB. La recomendación es que las organizaciones planeen integrar su CASB con su infraestructura de seguridad y procesos de SOC existentes.

Una excelente idea. Nadie quiere una isla de seguridad que esté desconectada del resto de sus soluciones de seguridad. Sin embargo, ¿cómo empezar a juntar las piezas?

Existen cinco casos de uso de integración que pueden aumentar drásticamente la eficacia de un CASB y, al mismo tiempo, disminuir la complejidad de la gestión de los riesgos asociados al uso de aplicaciones y servicios en la nube. A ese abordaje integrado de seguridad lo llamamos CASB 2.0.

1 Caso de Uso

La computación en la nube permite que los usuarios estén en prácticamente cualquier parte del mundo y aún sean productivos. En el modelo original de TI, proteger los dispositivos de un funcionario exigiría una conexión que regresara a un local centralizado.

Una solución más moderna aprovecha los agentes de seguridad de acceso basados en la nube y los métodos de autenticación de dos factores, y de ese modo permite que los usuarios traigan sus sistemas favoritos para portabilidad, mientras también ofrece al equipo de seguridad la capacidad de ver los datos y verificar a los usuarios que acceden a esos datos.

2 Caso de Uso

Integre su CASB a su solución corporativa de DLP en la nube. Sus datos en aplicaciones se inspeccionan en la nube, basandose en las mismas políticas de DLP utilizadas para todos los otros locales donde rastrea sus datos. Con este abordaje, su CASB es la conexión a todas sus aplicaciones y transacciones en la nube, y emplea un mecanismo de inspección DLP que está en la nube, pero su gestión centralizada de la solución corporativa de DLP es donde se pueden controlar las políticas de DLP y las acciones de respuesta para los datos en la nube. De esta forma, sus datos nunca salen de la nube. Y es posible aplicar las mismas políticas de DLP y acciones de respuesta a sus datos en la nube que ya utiliza para datos en los endpoints, en el datacenter o en la red. Su alternativa sería administrar dos sistemas DLP separados o intentar administrar un abordaje ICAP extremadamente complicado. Le sugerimos evitar esto al máximo, a menos que tenga mucho tiempo adicional a su alcance.

3 Caso de Uso

Integre su CASB con autenticación de usuario. Controle el acceso a aplicaciones en la nube, al integrar su CASB con soluciones de autenticación multifactor de usuario e Inicio de Sesión Único (SSO). En un nivel básico, la integración con SSO y MFA ayuda a su CASB a garantizar mejor seguridad de acceso a sus aplicaciones en la nube.

Con modelos comunes de integración, esto funciona principalmente para controlar el inicio de la sesión de aplicación en la nube de un usuario. Sin embargo, si tiene una integración más profunda entre CASB y MFA, donde CASB puede enviar comandos a su MFA y recibir respuestas incluso después que se inicia una sesión de nube, su seguridad es mejorada al bloquear las actividades malintencionadas en la nube sin bloquear las actividades legítimas en la nube.

En este escenario, imagine que posee un usuario que ya ha sido autenticado en Office 365, pero de repente comienza a cargar o descargar muchos archivos extraños, o acceden desde una ubicación inusual. ¿Qué es lo que su solución de CASB puede hacer? De forma aislada, puede bloquear esa actividad anormal o permitir que se produzca, sin embargo, con un MFA integrado es posible exigir una ronda adicional de autenticación en el medio de la sesión para garantizar que sea realmente el usuario autorizado que intenta realizar esas acciones. Si el usuario concluye la autenticación, la acción podrá ser permitida, caso contrario, la acción será bloqueada. De esa forma, se habilitan las acciones legítimas mientras se niegan las acciones activadas por malware o hackers.

4 Caso de Uso

Integre su CASB con cifrado, DLP y autenticación del usuario. Proteja los datos y administre los derechos digitales para visualización de datos en aplicaciones en la nube como parte de una solución que protege sus datos en cualquier lugar. Considere una solución con la que sus datos sus datos confidenciales sean automáticamente cifrados con base en una clasificación DLP automática en el momento en el que un usuario envía los datos hacia una cuenta en la nube. A continuación, cualquier usuario que desee visualizar o descargar ese archivo debe efectuar una verificación de autenticación del usuario para garantizar que posea permiso para ver esos datos. Y ese requisito de cifrado y autenticación permanece con el archivo incluso después de haber sido descargado de una cuenta en la nube y enviado a otro usuario (colega, colaborador, proveedor, cliente, etc.). Finalmente, su solución mantiene un registro de quien tiene acceso a ese archivo en cualquier lugar y ofrece la capacidad de revocarlo en cualquier momento en el futuro.

5 Caso de Uso

Integre su CASB con protección avanzada contra amenazas. Impida que los ataques avanzados de malware utilicen sus cuentas en la nube, al integrar CASB con protección contra las amenazas de clase empresarial. Proteja sus cuentas en la nube con el mismo nivel de protección que utiliza actualmente en sus endpoints para detectar y mitigar infecciones avanzadas de malware. Ponga a disposición la protección avanzada contra las amenazas con sandbox en la nube para detectar las amenazas avanzadas que pueden intentar propagarse a través de uploads, descargas, sincronizaciones de cuentas y usos compartidos de aplicaciones en la nube.

No todas las soluciones de CASB ofrecen actualmente todas esas opciones de integración y no todas las soluciones de seguridad corporativa pueden soportar este nivel de integración CASB. Las soluciones de Symantec son proyectadas para proporcionar una ciberdefensa integrada a las organizaciones que desean optimizar el uso de soluciones integradas. Aparecen aquí algunos enlaces para ayudarlo a obtener más información:

Secure Web Gateway (SWG) for the Cloud Generation
CloudSOC Security for Cloud Apps – Securlets | Symantec
Symantec Shadow Data Report

Acerca de Deena Thomchick

Deena es una entusiasta de seguridad y profesional de tecnología con 25 años de experiencia, una ejecutiva senior del grupo de productos CASB de Symantec. Además de su objetivo actual en la seguridad en la nube, su historial incluye trabajo con cifrado, ATP, seguridad de red y seguridad de endpoints.

Acerca de Symantec

Symantec Corporation (NASDAQ: SYMC) es líder mundial en soluciones de ciberseguridad y ayuda a las compañías, gobiernos e individuos a proteger sus datos más importantes en cualquier lugar. Compañías en todo el mundo buscan a Symantec para soluciones estratégicas e integradas para defenderse contra ataques sofisticados en endpoints, en la nube e infraestructura. De la misma forma, una comunidad global de más de 50 millones de personas y familias dependen de la suite de productos Norton y LifeLock de Symantec para proteger sus vidas digitales en casa y en todos sus dispositivos. Symantec opera una de las redes civiles de ciberinteligencia más grande del mundo, lo que le permite ver y proteger contra las amenazas más avanzadas. Para más información, visite **www.symantec.com** o síganos en **Facebook**, **Twitter** y **LinkedIn**.

Symantec™ 350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**

SYMC_ 5_CASB_Use_Cases_You_Should_Know_v1a