



Thycotic adquiere Onion ID para fortalecer su liderazgo en tecnología PAM en la nube

Con esta adquisición, Thycotic añade a su portfolio soluciones orientadas a proteger el acceso a las aplicaciones SaaS, infraestructuras IaaS y a los teletrabajadores

Thycotic, proveedor de soluciones de gestión de acceso privilegiado (PAM) para más de 10.000 organizaciones, incluyendo 25 de las 100 de Fortune, ha anunciado la adquisición del proveedor de soluciones PAM Onion ID. Con esta operación, Thycotic incluye tres nuevos productos a su portfolio de soluciones PAM: Thycotic Remote Access Controller, Thycotic Cloud Access Controller y Thycotic Database Access Controller. Thycotic fortalece así su liderazgo en la industria emergente de tecnología PAM al añadir soluciones orientadas a proteger el acceso a las aplicaciones SaaS e infraestructura IaaS y asegurar que los trabajadores en remoto se mantienen productivos y seguros a la vez.

“Con el repentino crecimiento del teletrabajo en todo el mundo, los controles de seguridad de acceso privilegiado deben tener en cuenta tanto a los usuarios del departamento comercial, como al financiero o de marketing, que ahora pueden acceder a datos corporativos privilegiados y sensibles desde dispositivos o redes no seguras. Con la adquisición de Onion ID, podemos implementar controles de acceso que se ajustan a los roles de los usuarios en cualquier aplicación web, consola IaaS y base de datos alojada en la nube, a la vez que proporcionamos autenticación flexible multifactor. Esto permite a los responsables de seguridad de las organizaciones garantizar de forma más fácil las rutas de acceso seguras a los empleados remotos”, comenta James Legg, Presidente y CEO de Thycotic.

Por su parte, Anirban Banerjee, CEO y Fundador de Onion ID, señala que: “Gracias a esta unión con Thycotic, aumentamos nuestro compromiso de ofrecer autenticación, autorización y auditoría a servidores cloud, bases de datos y aplicaciones. Además, lanzamos al mercado un conjunto de

ofertas PAM 2.0 de próxima generación que permitirá a las organizaciones elevar sus controles de seguridad más allá de las soluciones actuales y reducir los costes relacionados con un acceso remoto seguro”.

Implementación de Zero Trust para teletrabajadores y acceso de terceros

El teletrabajo ha llevado a las empresas a adoptar una estrategia de seguridad Zero Trust para empleados que trabajan en remoto y terceros que necesitan acceder a recursos corporativos. El principio del menor privilegio debería guiar todos los canales de acceso remoto, asegurando que personas ajenas a la empresa tengan acceso sólo a los recursos que necesitan para hacer su trabajo. El equipo de seguridad debe tener el control de quién puede acceder, a qué y cuándo, a fin de proteger los recursos corporativos y cumplir con las normativas.

Thycotic Remote Access Controller resuelve esta situación simplificando y automatizando la gestión de los trabajadores en remoto que acceden a recursos IT. El controlador utiliza autenticación de multifactor (MFA) y grabación de las sesiones, sin necesidad de ningún software o extensión de navegador adicional. Asimismo, proporciona un nivel de seguridad avanzado que permite cumplir con las normas y las políticas corporativas en este sentido. Y gracias a que el conjunto de APIs puede integrarse en los flujos de trabajo automatizados y en los sistemas de ticketing, Remote Access Controller agiliza las concesiones de acceso a terceros dentro de un portal web centralizado.

Activos cloud de las empresas protegidos

Con el 80% de los presupuestos IT destinados ya a soluciones cloud, Gartner advierte que el paso a la nube es un reto para la tecnología PAM, ya que estas soluciones son inmanejables para las organizaciones sin procesos automatizados o herramientas especializadas.

Thycotic Cloud Access Controller asegura que los administradores que acceden a plataformas IaaS como Amazon Web Services (AWS) y a aplicaciones SaaS como Salesforce o Twitter mantengan los Controles de Acceso Basados en Roles (RBAC, por sus siglas en inglés). Dichos controles imponen lo que cada usuario puede clicar, leer o modificar dentro de cualquier aplicación web. Los administradores cuentan también con un dashboard centralizado que muestra a qué aplicaciones ha accedido cada usuario y permite la eliminación del acceso y la producción de informes, entre otros aspectos, para una seguridad más estricta y un cumplimiento más eficiente.

Martin Kuppinger, fundador y principal analista de KuppingerCole, afirma que: “Las consolas de

gestión cloud, como Azure, AWS y GCP, plantean importantes riesgos de seguridad para todas las compañías. Los excesos de privilegios son un hecho común y la mayoría de las organizaciones carecen de una visibilidad granular sobre si los usuarios privilegiados tienen derechos innecesarios”.

Control del acceso a las bases de datos

La creciente adopción de bases de datos alojadas en la nube ha complicado aún más a los equipos de seguridad los requisitos de acceso privilegiado y de cumplimiento. Las bases de datos que contienen información confidencial de empleados y clientes son un área de atención cada vez mayor para los auditores y principal objetivo de los ciberdelincuentes.

Thycotic Database Access Controller permite a las empresas adoptar bases de datos cloud modernas de AWS (RDS), Google, Azure, Oracle, Redis y otros, al mismo tiempo que se aplican los niveles de acceso adecuados, MFA y flujos de trabajo completos de información y auditoría. Ahora los clientes pueden grabar las sesiones de acceso a la base de datos, proporcionar acceso justo a tiempo, informar y registrar acciones, generar alertas y cortar conexiones de manera automatizada. Así, la gestión del acceso a bases de datos ya no requiere de procedimientos manuales intensos ni complicados.

“La reciente ola de teletrabajadores ha acelerado la adopción por parte de las empresas de aplicaciones y plataformas cloud, lo que ha hecho que más recursos corporativos estén expuestos a un Internet público. Estas condiciones han creado un entorno de mayor riesgo para cualquier equipo de InfoSec. Implementar el menor privilegio para trabajadores en remoto con BYOD que necesitan acceso privilegiado a cientos de aplicaciones SaaS es un gran desafío que la unión de Onion ID y Thycotic puede resolver”, apunta Lamont Orange, CISO de Netskope, actual cliente de Onion ID.

Finalmente, Jai Dargan, Vicepresidente de Gestión de Producto de Thycotic, concluye que: “La propia definición de acceso privilegiado ha sufrido un cambio de paradigma debido al panorama actual de teletrabajo –cambiando el perímetro de las oficinas a las residencias personales–. Las soluciones PAM basadas en dispositivos legacy no han sido efectivas para extender los controles de acceso privilegiado a los entornos cloud. Con esta adquisición, Thycotic amplía la seguridad a todos los usuarios, aplicaciones y secretos, asegurando los recursos de más alto riesgo alojados en la nube que históricamente han sido dominio de los proveedores convencionales de IAM”.

Los términos financieros del acuerdo de Onion ID no se han revelado. Como parte de la transacción, Onion ID operará bajo la marca y liderazgo de Thycotic.



Contacto de prensa:

JAVIER MODUBAR ALVAREZ

info@ingecom.net

944395678

<http://www.ingecom.net>