CLOUD ACCESS CONTROLLER
SINOPSIS

Seguridad inteligente para aplicaciones web

Reduzca el riesgo del acceso con privilegios en todas sus aplicaciones basadas en la Web

A medida que las empresas transfieren sus aplicaciones locales a la nube e incrementan el uso de aplicaciones web, su habilidad para establecer controles de seguridad sólidos se reduce. Por lo general, la propia empresa define, implanta y gestiona los controles de seguridad. Pero puede que no sea posible obtener el grado de control deseado en aplicaciones web alojadas en proveedores externos. Por ejemplo, los sitios web de medios sociales y las aplicaciones web antiguas normalmente no disponen de un control de acceso basado en roles, o lo hacen solo a un nivel limitado. Thycotic Cloud Access Controller permite aplicar procedimientos sólidos de autenticación, autorización y monitorización en todas las aplicaciones y sitios web sin necesidad de implementar software, infraestructura o agentes adicionales.

Aumento de la seguridad sin fisuras

Integración con AD, Okta, Ping, YubiKey, y Duo.

Exija autenticación biométrica antes de conceder el acceso.

Añada integración MFA, SSO o AD a

aplicaciones web antiguas o personalizadas sin necesidad de escribir código.

Los usuarios remotos obtienen acceso a las aplicaciones web a través de un portal intuitivo para los usuarios.

Implemente controles de seguridad y reduzca el área expuesta a las amenazas

Limite el acceso a las aplicaciones basándose en la IP del usuario, su proximidad y ubicación geográficas y el tipo de navegador utilizado.

Reduzca el número de cuentas únicas con privilegios configuradas en aplicaciones web.

Cree cuentas compartidas basadas en directivas de seguridad detalladas.

Oculte o bloquee elementos específicos de la web para impedir que los usuarios los puedan leer o clicar.

Mayor conocimiento de las aplicaciones y del comportamiento de los usuarios

Registre sesiones sin desplegar ninguna infraestructura.

Vea cuándo se utilizan las aplicaciones y quién lo hace.

Establezca notificaciones adaptables para alertar de la detección de patrones de usuarios específicos.

Demuestre la conformidad normativa con informes listos para el uso.

Comience a utilizarlo de inmediato

Gestiónelo todo mediante controles centralizados de administración y directivas.

Elimine la necesidad de configurar agentes o infraestructura.

Incorpore a usuarios fácilmente a través de un portal simplificado.

Ventajas de Cloud Access Controller

Reducción del riesgo

Aplique controles de seguridad sólidos en todas las aplicaciones web

Aumento de la eficiencia

Equilibre la seguridad con la facilidad de uso y reduzca los inconvenientes para el usuario

Inicio rápido

Efectúe la implementación de inmediato sin necesidad de infraestructura o agentes adicionales

Conviértase en un defensor autosuficiente de la ciberseguridad

REMOTE ACCESS CONTROLLER

Imponga un modelo de confianza cero para teletrabajadores y terceros.

Acceso remoto seguro: Establezca permisos detallados, usuarios y una estructura de mapeado para su empresa.

Concesión de permisos a terceros: Permita que proveedores y contratistas puedan acceder a los recursos informáticos.

Protección ligera de entorno aislado: Efectúe el despliegue sin tener que abrir puertos RDP o SSH a la Internet pública.

Autenticación (MFA): Conceda a los teletrabajadores un acceso seguro con protección multifactor.

Monitorización de sesiones registradas: Informe de la actividad visible en un portal centralizado para garantizar que los trabajadores cumplan las directivas de la empresa.

CLOUD ACCESS CONTROLLER

Protección de sus activos en la nube.

Acceso remoto seguro: Garantice que cada usuario de IaaS y SaaS tenga los privilegios necesarios.

Control de acceso detallado basado en roles: Defina con exactitud qué puede clicar, leer o modificar cada usuario en una aplicación web.

Gestión de cuentas compartidas: Imponga fácilmente la separación de roles y obligaciones en cuentas estándar y compartidas.

Grabación de sesiones web: Vea las grabaciones de sesiones de vídeo de usuarios realizando acciones delicadas.

Bloqueo inteligente: Detecte comportamientos inusuales y bloquee cualquier acceso no autorizado.

DATABASE ACCESS CONTROLLER

Control detallado y autenticación multifactor (MFA) para bases de datos.

Protección de la bases de datos: Proteja su información más confidencial controlando el acceso web a las bases de datos.

Administración de usuarios con privilegios: Imponga niveles de acceso apropiados y ofrezca acceso con límite temporal.

Verificación de identidad: Vea quién accede a las bases de datos y controle su acceso.

Autenticación (MFA): Gestione la autorización y la monitorización en toda la sesión y el nivel con MFA.

Auditoría: Registre eventos de acceso a bases de datos, demuestre la conformidad normativa y genere notificaciones.

Thycotic se centra en el vector más vulnerable a los ataques: las cuentas con privilegios. Con Thycotic, podrá adoptar un enfoque multinivel capaz de satisfacer sus necesidades de seguridad en el ámbito de privilegios desde los puntos terminales hasta la nube, garantizando así una protección completa en toda el área de exposición a los ciberataques.

SECRET SERVER
INFORMACIÓN GENERAL

Administración de cuentas con privilegios a escala empresarial

Descubra, administre, proteja y audite los accesos a cuentas con privilegios en toda su organización

Dado que las amenazas cibernéticas siguen aumentando en volumen y sofisticación, la eficaz y ágil administración de cuentas con privilegios (PAM) se ha convertido en un aspecto fundamental para las organizaciones de todos los tamaños. Ahora usted puede adoptar una postura enérgica de seguridad de cuenta con privilegios con Secret Server, la única solución PAM totalmente equipada disponible tanto en las instalaciones como en la nube. Potencie su seguridad y sus equipos de operaciones de TI para proteger y administrar todos los tipos de cuentas con privilegios con rapidez y facilidad.

Proteja las contraseñas

Asegure el almacenamiento y la administración de contraseñas para las cuentas con privilegios en toda la infraestructura de su empresa.

Protección proactiva que incluye cambio de contraseñas automatizado,latidos y políticas configurables.

Un flujo de trabajo inteligente que incluye registro de salida, solicitud de acceso privilegiado, requisitos de justificación y aprobación por niveles.

Elimine las amenazas internas y externas

La detección busca cuentas de servicio en toda la red.

La secuencia de comandos personalizados ayuda a configurar dependencias, enlaces e integraciones en sus propios términos

La seguridad del flujo de trabajo de DevOps a través de Secret Server SDK amplía la protección de PAM a DevOps.

Actualizaciones de rotación de contraseña sin romper dependencias.

Audite e informe

Las características de auditoría, informes y alertas personalizadas o programadas ayudan de forma proactiva a cumplir con las obligaciones de conformidad.

El control de políticas granular se aplica en todos los dispositivos y equipos.

Detecte actividad sospechosa

El control y la supervisión de sesiones en tiempo real incluyen servidores proxy, grabación de sesiones y registro de pulsación de tecla.

Las integraciones con SIEM y los detectores de vulnerabilidades proporcionan visibilidad.

El análisis de comportamiento aprovecha el aprendizaje automático para identificar el comportamiento anormal del usuario.

Empiece rápidamente

La configuración y la implementación están basadas en asistente para una rápida puesta en marcha.

Fácilmente personalizable significa que no hay necesidad de gastar tiempo ni dinero extra.

Ventajas de Secret Server

Seguridad mejorada
Proteja las cuentas con privilegios para ajustar la superficie expuesta a ataques y generar resiliencia.

Equipos de TI sin carga de trabajo
Controle la administración de cuentas con privilegios (PAM) fácilmente con una interfaz simplificada y un diseño optimizado.

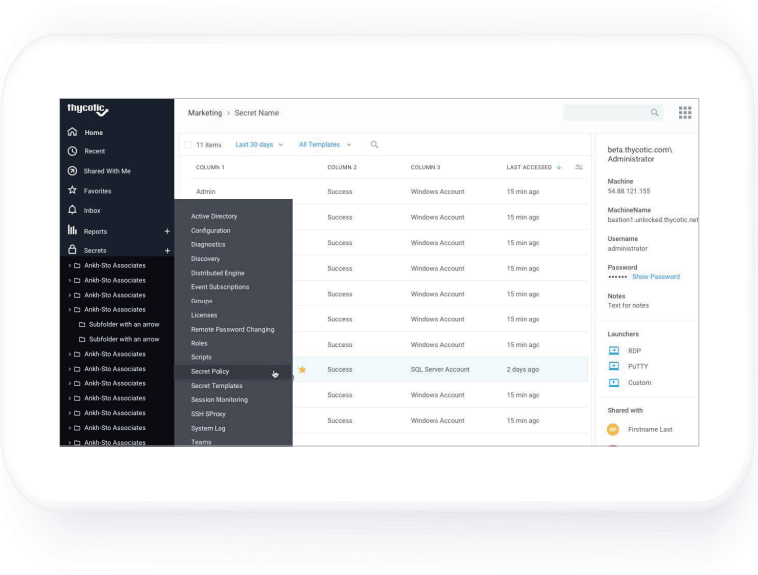
Cumplimiento de las exigencias normativas
Evite penalizaciones financieras significativas.

Escale su PAM
Implemente con elasticidad dentro la arquitectura segura para la empresa de Thycotic.

Determine un ROI rápido
Configure rápidamente con el asistente para instalación y configuración

Controles de seguridad integral para proteger su infraestructura y su red

Secret Server otorga a los equipos de seguridad un potente control necesario para proteger proactivamente su infraestructura y su red, sin la complejidad ni la carga de gestión de soluciones de PAM heredadas. Secret Server simplifica la potente PAM.



Seguridad utilizable

Nuestro equipo de interacción hombre-máquina. Los expertos en interacción diseñaron Secret Server teniendo en cuenta los usuarios finales para:

- Mitigar el riesgo de error humano con una interfaz intuitiva y simplificada.
- Abordar simultáneamente la facilidad de uso y las inquietudes sobre seguridad para construir sistemas verdaderamente seguros.
- Minimizar la complejidad para mantener a sus equipos productivos y controlados.

Una edición diseñada para cada organización, disponible en las instalaciones o en la nube.

La flexibilidad y la agilidad para escalar los controles de seguridad de PAM en sus propios términos.

SECRET SERVER
Vault Edition

Protección de PAM asequible y fácil de usar para su empresa.

SECRET SERVER
Professional Edition

Automatización inteligente de PAM para cumplir con las mejores prácticas de seguridad cibernética y las obligaciones de conformidad.

SECRET SERVER
Platinum Edition

PAM de última generación para lograr máxima seguridad y agilidad.

Prueba gratuita de 30 días y demostraciones de productos en thycotic.com

Thycotic está enfocada en el vector de ataque más vulnerable: el privilegio. Con Thycotic puede adoptar un enfoque multicapa que cubre sus necesidades de seguridad de los privilegios desde los dispositivos terminales hasta las credenciales, y así asegurar la protección en cada paso de la cadena de un atacante.

thycotic.com | sales@thycotic.com

ACCESS CONTROLLER SINOPSIS

Control detallado del acceso con privilegios

Autenticación, autorización y monitorización de accesos en toda la red no perimetral

Los departamentos de IT y ciberseguridad tienen dificultades a la hora de proteger sus redes a medida que la gestión del acceso con privilegios (PAM) tradicional evoluciona para englobar a usuarios normales y a usuarios con privilegios, quienes ahora requieren controles de acceso para aplicaciones y sistemas potencialmente sensibles. Ya no basta con controlar solamente el acceso con privilegios: todo el acceso debe ser controlado y gestionado en un entorno de confianza cero. **Thycotic Cloud Access Controller, Thycotic Remote Access Controller y Thycotic Database Access Controller** permiten a las empresas ampliar su control a un nivel más detallado. Estas soluciones amplían la capacidad de los departamentos informáticos para hacer frente a desafíos de PAM, protegiendo el acceso a aplicaciones de SaaS y a la infraestructura de la nube y garantizando que los teletrabajadores puedan llevar a cabo sus tareas de manera productiva y segura.

Obtenga una completa visibilidad

Vea qué servidores, aplicaciones y sitios web están siendo utilizados.

Detecte comportamientos de riesgo.

Asegúrese de que solo los empleados y terceros de confianza obtengan el acceso necesario.

Proteja la infraestructura y las aplicaciones

Conceda y anule el acceso fácilmente y controle las acciones complejas.

Reduzca el riesgo de amenazas internas, el abuso de derechos y la filtración de datos hacia el exterior por infracciones de seguridad.

Olvídese de tener que gestionar claves SSH en sus servidores.

Gestione el mínimo privilegio

Administre las identidades y los accesos de empleados y terceros.

Imponga la directiva de la empresa para todos los usuarios.

Implemente la separación de obligaciones.

Simplifique la autenticación

Centralice la autenticación multifactor.

Utilice geoperimetraje, geoproximidad y biometría para que la experiencia de acceso sea agradable.

Equilibre la seguridad con la facilidad de uso y reduzca los inconvenientes para el usuario

Automatice los recursos de auditoría

Reduzca el tiempo y el esfuerzo empleados en actividades relacionadas con la conformidad normativa.

Genere los informes necesarios en un solo paso.

Comience a utilizarlo de inmediato

Efectúe la implementación con rapidez sin necesidad de agentes.

Elimine la necesidad de modificar los servidores.

Fácil incorporación de usuarios con un panel de control simplificado.

Ventajas de Access Controller

Consolidación de la tecnología de ciberseguridad

Implemente controles de seguridad eficaces con menos proveedores

Menos trabajo para los equipos de IT

Controle fácilmente el acceso de todos los usuarios mediante una interfaz simplificada y un sencillo diseño

Cumplimiento de la conformidad normativa

Evite multas económicas considerables

Conviértase en un defensor autosuficiente de la ciberseguridad

CLOUD ACCESS CONTROLLER

Seguridad inteligente para aplicaciones web

Mínimo privilegio: Defina e implemente directivas de seguridad sólidas y centralizadas que rijan la concesión de privilegios y acceso a los usuarios en todas las aplicaciones web.

Mayor seguridad: Proteja las aplicaciones web antiguas o personalizadas con técnicas modernas de autenticación. Integre soluciones de SSO, MFA y directorios sin tener que escribir ni una línea de código.

Controles detallados: Limite con exactitud qué datos u objetos pueden ser leídos o utilizados por los usuarios. Exija una aprobación antes de que los usuarios puedan acceder a elementos importantes de la web. Restringa el acceso según el sistema operativo, el tipo de navegador, la dirección IP y otros factores.

Confianza cero: Implemente técnicas modernas de autenticación multifactor (MFA) y controles de acceso "justo a tiempo" antes de permitir el acceso a aplicaciones web fundamentales y datos delicados. Registre, examine y monitorice todas las sesiones.

REMOTE ACCESS CONTROLLER

Imponga un modelo de confianza cero para teletrabajadores

Acceso remoto seguro: Registre, examine y monitorice todas las sesiones de acceso remoto RDP y SSH en servidores y contenedores basados en Windows y Unix. Conceda tranquilamente acceso temporal con caducidad automática.

Acceso centralizado: El portal intuitivo para usuarios se integra a la perfección con las técnicas de autenticación SSO y MFA existentes con el fin de simplificar y asegurar el acceso a los servidores y contenedores.

Inicio rápido: Sin necesidad de desplegar agentes o instalar software en puntos terminales o servidores. Localice e importe las cuentas existentes en servidores y contenedores de Windows y Unix.

Notificación de riesgos: Los paneles de control analíticos señalan los riesgos existentes para usuarios y para servidores y contenedores. Los informes listos para el uso, el registro de eventos y la puntuación de riesgos ofrecen información importante para valorar el rendimiento de las medidas de seguridad y conformidad normativa.

DATABASE ACCESS CONTROLLER

Seguridad de conexión centralizada para bases de datos

Seguridad unificada: Proteja la información más delicada con una seguridad centralizada para todas las bases de datos modernas.

Acceso seguro: Integre soluciones de SSO y MFA con toda garantía e imponga el acceso según el método "justo a tiempo".

Reducción del riesgo: Acceso a bases de datos por proxy mediante un portal web para usuarios centralizado.

Mayor conocimiento: Aprovéchese de informes listos para el uso, el registro y la monitorización de la actividad de acceso, y configure alertas y notificaciones para eventos críticos.

Thycotic se centra en el vector más vulnerable a los ataques: los privilegios. Con Thycotic, podrá adoptar un enfoque multinivel capaz de satisfacer sus necesidades de seguridad en el ámbito de privilegios desde los puntos terminales hasta las credenciales, garantizando así una protección completa en cada eslabón de la cadena de ciberataque.

thycotic.com | sales@thycotic.com

IDENTITY BRIDGE SINOPSIS

Gestión de usuarios para Unix/Linux

Simplifique la administración, reduzca el área de exposición a los ciberataques y mejore la seguridad.

Los administradores de Unix y Linux a menudo pasan muchas horas gestionando usuarios y grupos localmente y en múltiples directorios separados. Las auditorías son dolorosas debido a la existencia de distintas directivas de contraseñas y la imposibilidad de controlar el acceso de identidades consolidadas en varios sistemas.

Thycotic Identity Bridge proporciona autenticación centralizada y autorización para sistemas Unix y Linux. El sistema utiliza un servicio de directorios de la empresa –como Active Directory– para lograr coherencia en las identidades en toda la compañía, independientemente de la plataforma y del sistema operativo utilizados. Esto permite mejorar la eficiencia de la protección de identidades, reducir el área de exposición a ciberataques y simplificar la administración del control de acceso.

Control de acceso centralizado

Deje de gestionar usuarios en servidores y estaciones de trabajo Unix/Linux de manera aislada

Utilice un solo punto de control para todos los usuarios y grupos con una autenticación y autorización centralizadas

Menor riesgo

Reduzca la propagación de cuentas para reforzar el área de exposición a ciberataques

Anule inmediatamente el acceso a todos los sistemas cuando un usuario abandone la empresa

Reducción de costes

Simplifique la gestión de usuarios, grupos y ordenadores con tecnología económica

Garantice un despliegue rápido y sencillo para acelerar la implantación

Pierda menos tiempo y recursos comprobando múltiples ubicaciones y estructuras de directorios

Mejore la eficiencia del soporte técnico y reduzca la complejidad al realizar servicios relacionados con cuentas

Ventajas de Identity Bridge

Menos trabajo para los equipos de IT

Implemente un proceso simplificado para gestionar accesos e identidades

Incremento de la seguridad y del cumplimiento normativo

Verifique las identidades de los usuarios y la integridad de las sesiones con un control centralizado

Mejora del servicio para los usuarios finales

Los usuarios solo deben recordar una clave de usuario y una contraseña

Administración de usuarios sencilla y segura para diversas compañías

Ahora, las empresas en crecimiento pueden conceder y gestionar el acceso de usuarios en cientos o miles de cuentas distintas y en diversos sistemas y plataformas. No hay necesidad de gestionar manualmente cuentas de usuario dispersas en múltiples entornos ni de crear cuentas compartidas genéricas que infrinjan directivas de mínimo privilegio.

Características principales

Identity Bridge impone una autenticación y autorización centralizadas para Unix y Linux con:

- Integración entre servicios de directorio existentes, tales como Active Directory
- Autenticación Kerberos completa
- Generación automática de peticiones en estaciones de trabajo y servidores
- Sin necesidad de cambios de esquema en Active Directory o requisitos para usar directivas de grupo
- Aprovisionamiento flexible de usuarios y un agente combinado para identidades y privilegios
- Solución de alta rentabilidad

Thycotic ofrece una gestión potente e integral del acceso con privilegios a la escala y la velocidad de la nube.

Localización, protección y monitorización de cuentas con privilegios

Elevación de privilegios de puntos terminales y control de aplicaciones

Gestión de secretos de alta velocidad para aplicaciones, DevOps y automatización robotizada de procesos

Prueba gratuita disponible en thycotic.com

Thycotic se centra en el vector más vulnerable a los ataques: los privilegios. Con Thycotic, podrá adoptar un enfoque multinivel capaz de satisfacer sus necesidades de seguridad en el ámbito de privilegios desde los puntos terminales hasta las credenciales, garantizando así una protección completa en cada eslabón de la cadena de ciberataque.

thycotic.com | sales@thycotic.com

REMOTE ACCESS CONTROLLER
SINOPSIS

Acceso remoto seguro a la infraestructura fundamental

Reduzca los riesgos al conceder acceso remoto con el método de mínimo privilegio

Las compañías deben poder ofrecer un acceso remoto seguro a sus servidores, contenedores e infraestructura sin tener que perder tiempo en implementar agentes y conexiones VPN o solucionar problemas de acceso. También deben ser capaces de extender ese mismo acceso a sus contratistas y proveedores externos, a menudo para poder administrar y facilitar soporte técnico relacionado con los servidores, contenedores e infraestructura utilizados por sus empleados. A medida que el volumen de usuarios aumenta, también lo hace el área de exposición a los ciberataques. Remote Access Controller de Thycotic centraliza la autenticación, el registro y la monitorización de sesiones en conexiones RDP y SSH e implementa controles de acceso privilegiado según el método "justo a tiempo".

Centralice y asegure el acceso y la administración remotos

Establezca conexiones RDP y SSH seguras.

Registre, examine y monitorice toda la actividad de los usuarios de todas las conexiones.

Establezca directivas de privilegios SSH que limiten el uso de comandos específicos.

Aprovéchese de inmediato del soporte de contenedores para Docker y Kubernetes.

Traiga su propia SSO/MFA

Integración con AD, Okta, Ping, YubiKey, y Duo.

Exija autenticación biométrica antes de conceder el acceso.

Implemente controles de seguridad y reduzca el área expuesta a las amenazas

Limite el acceso a los servidores basándose en la IP de los usuarios, su proximidad y ubicación geográficas y el tipo de navegador utilizado.

Reduzca el número de cuentas únicas con privilegios y pares de claves SSH.

Cree cuentas compartidas basadas en un rol con directivas comunes.

Limite el tiempo de conexión de una sesión.

Mayor conocimiento de las aplicaciones y del comportamiento de los usuarios

Monitorice cuándo se accede a los servidores y quién lo hace.

Establezca notificaciones adaptables para alertar de la detección de patrones de usuarios específicos.

Identifique fácilmente cuentas inactivas o huérfanas que deban eliminarse.

Demuestre la conformidad normativa con informes listos para el uso.

Comience a utilizarlo de inmediato

Gestiónelo todo mediante controles centralizados de administración y directivas.

Elimine la necesidad de configurar agentes o infraestructura.

Incorpore a usuarios fácilmente a través de un portal simplificado.

Ventajas de Remote Access Controller

Acceso seguro
Nivel en autenticación MFA, SSO y biométrica

Diseño intuitivo
Equilibre la seguridad con la facilidad de uso y reduzca los inconvenientes para el usuario

Inicio rápido
Efectúe la implementación de inmediato sin necesidad de infraestructura o agentes adicionales

Conviértase en un defensor autosuficiente de la ciberseguridad

REMOTE ACCESS CONTROLLER

Imponga un modelo de confianza cero para teletrabajadores y terceros.

Acceso remoto seguro: Establezca permisos detallados, usuarios y una estructura de mapeado para su empresa.

Concesión de permisos a terceros: Permita que proveedores y contratistas puedan acceder a los recursos informáticos.

Protección ligera de entorno aislado: Efectúe el despliegue sin tener que abrir puertos RDP o SSH a la Internet pública.

Autenticación (MFA): Conceda a los teletrabajadores un acceso seguro con protección multifactor.

Monitorización de sesiones registradas: Informe de actividad visible en un portal centralizado para garantizar que los trabajadores cumplan las directivas de la empresa.

CLOUD ACCESS CONTROLLER

Protección de sus activos en la nube.

Acceso remoto seguro: Garantice que cada usuario de IaaS y SaaS tenga los privilegios necesarios.

Control de acceso detallado basado en roles: Defina con exactitud qué puede clicar, leer o modificar cada usuario en una aplicación web.

Gestión de cuentas compartidas: Imponga fácilmente la separación de roles y obligaciones en cuentas estándar y compartidas.

Grabación de sesiones web: Vea las grabaciones de sesiones de vídeo de usuarios realizando acciones delicadas.

Bloqueo inteligente: Detecte comportamientos inusuales y bloquee cualquier acceso no autorizado.

DATABASE ACCESS CONTROLLER

Control detallado y autenticación multifactor (MFA) para bases de datos.

Protección de bases de datos: Proteja su información más confidencial controlando el acceso web a las bases de datos.

Administración de usuarios con privilegios: Imponga niveles de acceso apropiados y ofrezca acceso con límite temporal.

Verificación de identidad: Vea quién accede a las bases de datos y controle su acceso.

Autenticación (MFA): Gestione la autorización y la monitorización en toda la sesión y el nivel con MFA.

Auditoría: Registre eventos de acceso a bases de datos, demuestre la conformidad normativa y genere notificaciones.

Thycotic se centra en el vector más vulnerable a los ataques: las cuentas con privilegios. Con Thycotic, podrá adoptar un enfoque multinivel capaz de satisfacer sus necesidades de seguridad en el ámbito de privilegios desde los puntos terminales hasta la nube, garantizando así una protección completa en toda el área de exposición a los ciberataques.

thycotic.com | sales@thycotic.com