THINMANAGER
A ROCKWELL AUTOMATION TECHNOLOGY

Seguridad de redes e infraestructura industriales con ThinManager

Informe oficial

CONEXIÓN DE LA EMPRESA: UNA TRANSFORMACIÓN DIGITAL

A medida que las empresas en una gran variedad de industrias adoptan tecnologías e infraestructuras que permiten dispositivos conectados, envío de datos específico y mejores experiencias del operador, existen riesgos crecientes de ciberseguridad en estas instalaciones que se deben tomar en cuenta. Ya sea que la iniciativa se describa como The Connected Enterprise, fabricación digital o Industria 4.0, hay que tomar decisiones para proteger la red de control industrial a medida que se introducen en estos ambientes redes a nivel empresarial. ThinManager de Rockwell Automation ha sido diseñado específicamente un entorno protegido y seguro para la gestión de dispositivos finales y el envío de contenido. También mitiga los riesgos presentes en un ambiente industrial conectado.

MITIGACIÓN DE RIESGOS

Tendencias industriales

La protección de redes industriales es una meta importante de todas las personas que trabajan en la industria y supone un enfoque cada vez más importante con respecto al tiempo de la transformación digital en el ámbito industrial. Las buenas practicas ampliamente aceptadas por la industria abarcan las redes, la supervisión de aplicaciones y los dispositivos finales. Los cortafuegos, la seguridad de puertos, la implementación de zonas desmilitarizadas industriales y las políticas inalámbricas contribuyen a reducir los riesgos de un ataque a la zona industrial desde el exterior. Las políticas exigentes respecto a contraseñas, la comunicación cifrada, el software antivirus, la elaboración de listas blancas de aplicaciones o la detección de anomalías pasiva ayudan a evitar la pérdida de datos o funcionalidad en la zona industrial. La restricción de acceso a aplicaciones, el cifrado del almacenamiento de datos local, la prevención de dispositivos de almacenamiento extraíbles y la concienciación relativa a los ataques de ingeniería social pueden dar lugar a un ambiente más seguro gracias a la protección de dispositivos de computación finales. Estos y otros conceptos se implementan con mayor facilidad cuando se envía contenido a los dispositivos finales gestionados ThinManager.

Gestión de dispositivos finales

ThinManager elimina la mayor parte (en muchos casos hasta en un 80%) de los sistemas operativos existentes en comparación con una metodología tradicional basada en PC en lo tocante a la arquitectura de plantas. ThinManager puede aprovechar el hardware existente compatible con PXE, PXE obsoleto, UEFI o UEFI PXE en el BIOS del dispositivo a fin de recibir un pequeño paquete de firmware enviado a través de la red. Cuando estos dispositivos se establezcan a la inicialización PXE\UEFI, solicitarán dos respuestas al encenderse: PXE\UEFI y DHCP. ThinManager puede responder a las dos solicitudes. Los dispositivos que reconocen ThinManager de forma nativa, como el cliente ligero industrial VersaView 5200, pueden recibir firmware mediante una respuesta TFTP y no necesitan una respuesta DHCP, a menos que se desee. Estos dispositivos contienen el nombre del archivo cargador de inicio que deben buscar en la red, la cual se puede configurar de forma estática.

Una vez que el hardware, independientemente su tipo, ha recibido el firmware ThinManager , este se desembala en la memoria en ejecución del dispositivo. No se requiere que un disco duro funcione como un cliente cero ThinManager y no se permite el almacenamiento local del firmware ni de datos accedidos por el cliente cero. Toda la información se almacena y se accede desde un lugar mediante una conexión RDP o VNC a un activo remoto y gestionado, tal como un servidor de escritorio remoto.

Luego de recibirse, ThinManager se convierte en el sistema operativo del dispositivo y seguirá siéndolo siempre que el dispositivo esté energizado. Si se desenergiza el dispositivo, el sistema operativo (en este

caso ThinManager) se elimina de la memoria del dispositivo y no guardará propiedad intelectual ni otra información. De manera predeterminada, cualquier dispositivo gestionado por ThinManager restringirá el acceso de cualquier dispositivo periférico en todos los puertos USB excepto un mouse o teclado. Si se desea que un dispositivo de almacenamiento externo, incluyendo USB/CD/DVD/disco flexible u otros dispositivos como un escáner o escala, se comunique con una sesión de escritorio remoto enviada al cliente gestionado, hay que brindarle permiso al dispositivo de forma explícita añadiendo un módulo a la configuración de dicho dispositivo en ThinManager. Además de la restricción de acceso a dispositivos periféricos, los módulos como el módulo de bloque clave se pueden configurar para evitar que las combinaciones de pulsaciones de teclas no deseadas tales como CTRL+ALT+DEL o ALT+F4 pasen del teclado del dispositivo a la sesión en ejecución en el servidor gestionado de manera central.

Cuando se desconecta y se vuelve a conectar la alimentación eléctrica del dispositivo, el servidor ThinManager contiene la dirección MAC del dispositivo y la asocia con un perfil de terminal, que es una prescripción de lo que se debe visualizar en esa parte física del hardware. En caso de un fallo de hardware de un dispositivo final, se puede iniciar un proceso denominado reemplazo de terminal. Este proceso reemplaza al hardware fallado por un cliente funcional. Cuando el dispositivo reciba su firmware y lo desembale en el sistema operativo ThinManager, el servidor ThinManager no reconocerá la dirección MAC del dispositivo nuevo. El operador apenas tiene que saber el nombre del dispositivo según su denominación en ThinManager. Este proceso permite el reemplazo rápido del hardware antiguo y no sujeta el hardware nuevo a un proceso de validación riguroso puesto que no hay sistemas operativos o aplicaciones locales instalados. Para incrementar la seguridad, es posible proteger este proceso con contraseña, requerir el mismo hardware de modelo o apagar el proceso entero.

Envío seguro de contenido y centralización de aplicaciones

ThinManager suministra la plataforma para enviar contenido a un dispositivo final, tal como un dispositivo móvil o cliente cero sin que estos dispositivos finales o terminales hospeden localmente las aplicaciones o datos.. La reducción de la cantidad de sistemas operativos implican la reducción de la cantidad de aplicaciones que se deben mantener y revisar. ThinManager centraliza la implementación de las aplicaciones a dispositivos finales y protege y cifra la comunicación proveniente de los hosts de la aplicación (servidores de escritorio remoto, servidores VNC, cámaras IP y estaciones de trabajo) a los dispositivos finales. Las comunicaciones RDP cifradas, si las permiten los servidores host (Sever 2008 o posterior), negociarán el nivel de seguridad hasta el protocolo TLS 1.2. ThinManager utiliza un conteo de puerto bajo para las implementaciones, lo cual incrementa aún más la protección del sistema. Esto reduce, a su vez, el número total de reglas de cortafuego que se deben crear a través de los servidores y capas de red. La lista de puertos siguiente muestra los puertos utilizados para la implementación de un sistema gestionado ThinManager. Los puertos con O son opcionales y no son necesarios para la funcionalidad principal, y los puertos con C son configurables dentro del producto.

Puerto	Protocolo	Descripción
UDP 67	DHCP	Usado por el servidor PXE (si se usa el hardware de inicialización PXE).
UDP 69	TFTP	Se usa para ejecutar el TFTP del firmware y de los módulos a los clientes ligeros compatibles con ThinManager.
TCP 443[O]	HTTPS	Se usa para establecer túneles HTTPS SSL al gateway RD.
TCP 1494[O]	ICA	Usado por el protocolo ICA (si se usa Citrix ICA en vez de RDP).
UDP 1758[C]	Multidifusión TFTP	Se usa si ThinManager habilita la multidifusión.
TCP 2031	Propiedad	Se usa para pasar la configuración desde el servidor ThinManager al terminal, y se usa para la sincronización automática entre los servidores ThinManager.
TCP 3268	LDAP	Se usa para la autenticación de dominio mediante Lightweight Directory Access Protocol.

TCP 3389[c]	RDP	Usado por el protocolo RDP. El cliente ligero inicia la conexión al servidor RD
UDP 3391[o]	Datagrama	Permite que el transporte cree una conexión al gateway RD (solo se requiere si está habilitado el RDP a través de UDP; de lo contrario, regresa de forma predeterminada a TCP 443).
UDP 4011	DHCP	Usado por ThinManager PXE Service cuando se instala un servidor DHCP estándar en el mismo ordenador que ThinManager. Se usa este puerto al inicializar los clientes ligeros de inicialización PXE compatibles con ThinManager mediante el BIOS de la UEFI (Unified Extensible Firmware Interface). (ThinManager 11)
UDP 4900	TFTP	Se usa para ejecutar el TFTP del firmware a los clientes ligeros listos ThinManager
TCP 5900[c]	Propiedad, VNC	Propriety Shadow Protocol, VNC inicializado por el cliente ligero al servidor VNC.

El uso de la funcionalidad ApplicationLink de ThinManager restringe el acceso a todo en el dispositivo final que no sea la aplicación requerida por el usuario final para ejecutar el trabajo requerido. Se sugiere la entrega de aplicaciones, en lugar de experiencias de escritorio. La entrega es compatible con ThinManager y reduce el acceso del operador a las aplicaciones tales como File Explorer, navegadores web u otra información del sistema. Esto también impedirá que los operadores establezcan conexiones RDP de un servidor al otro. ApplicationLink se puede configurar en un servidor de escritorio remoto publicando RemoteApps como parte de una colección de sesiones en la implementación de servicios del escritorio remoto o bien cambiando la política de grupo del host del escritorio remoto a fin de permitir el inicio remoto de las aplicaciones no listadas. De todos modos, los terminales del operador suministrarán acceso solo al conjunto de aplicaciones permitidas por al administrador ThinManager. Cuando se ejecuta una aplicación FactoryTalk View SE en un terminal gestionado por ThinManager, existe funcionalidad nativa denominada Authentication Pass-Through, lo cual permitirá acceso a cualquier usuario designado que inicia sesión en el dispositivo. Cuando el usuario inicia sesión en un dispositivo, la cuenta de servicio utilizada para el inicio de sesión automático cierra sesión del cliente FactoryTalk View SE e inicia sesión para el usuario designado, independientemente del método de autenticación que emplea dicho usuario. Esto constituye la integración nativa entre los productos que valida la entrada y la salida del testigo de seguridad RNA como parte de FactoryTalk Security. Tome en cuenta que Authentication Pass-Through requiere el uso de usuarios de dominio.

ThinManager puede seguir incrementando la seguridad del sistema aumentando el nivel de autenticación al sistema por medio de requerir múltiples factores de autenticación que no necesitan actualmente más de una forma de autenticación. La autenticación de inicio de sesión adicional puede implicar el escán de una credencial, números secretos, bandas inteligentes o la biometría. Cualquiera de los métodos de autenticación también se puede utilizar como alternativa al uso de credenciales Windows. Para emplear otro método de inicio de sesión, es necesario que el nombre del usuario y la contraseña Windows se almacenen en la base de datos cifrados ThinManager o se puedan almacenar en caché durante un plazo de tiempo configurable. El caché de contraseñas le pedirá al usuario que introduzca sus credenciales una vez durante el plazo de tiempo configurado y permitirá otro método de iniciar sesión a fin de establecer una conexión a las aplicaciones Windows durante dicho plazo.

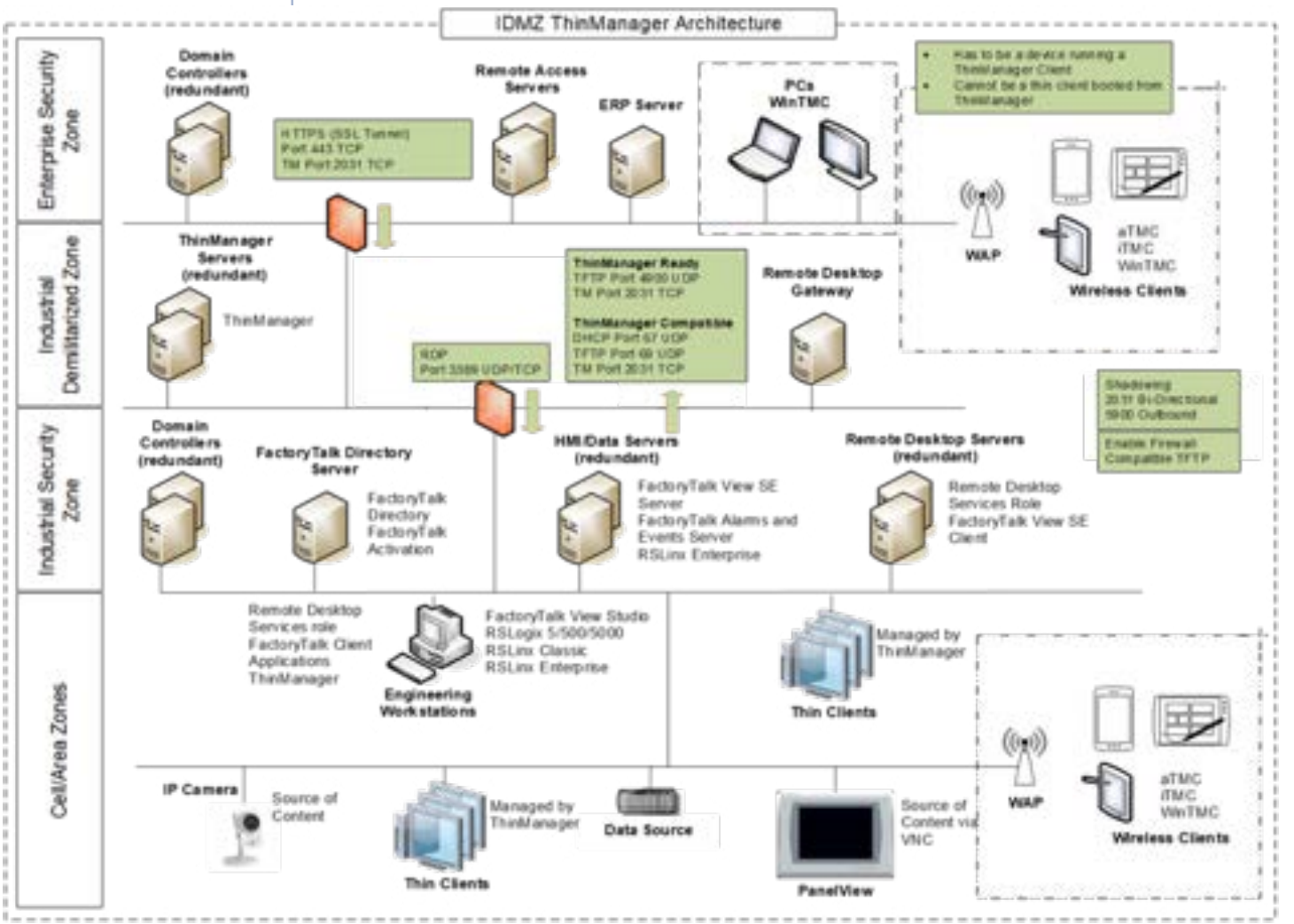
ThinManager permite que los usuarios sean miembros de Active Directory Group u Organizational Unit en Active Directory. Las cuentas que se utilizarían habitualmente como cuentas de servicio o cuentas de dispositivo genéricas, si se almacenan en la base de datos cifrados para permitir el inicio de sesión automático de las aplicaciones en los dispositivos finales, se pueden sincronizar de modo que ThinManager las actualice y las mantenga. La habilitación de Enabling Active Directory Synchronization en ThinManager garantiza que todas las cuentas de servicio utilizadas en las aplicaciones de inicio de sesión automático de los dispositivos se actualicen con regularidad en Active Directory y vuelvan a sincronizarse con ThinManager para que dichas cuentas acaten todas políticas de retención de contraseñas estipuladas por TI.

Para gestionar el acceso a la interface de usuario de ThinManager, se pueden configurar ThinManager Security Groups para permitir accesos diferentes a la aplicación para diferentes grupos de seguridad Windows. De manera predeterminada, todos los administradores tienen pleno acceso a la interface de usuario de ThinManager. Sería posible configurar un grupo de ingeniería que contaría con un subconjunto de dichos permisos, por ej., permisos para modificar el terminal, pero sin permiso para gestionar los servidores del escritorio remoto que son miembros de la implementación.

ARQUITECTURAS SEGURAS

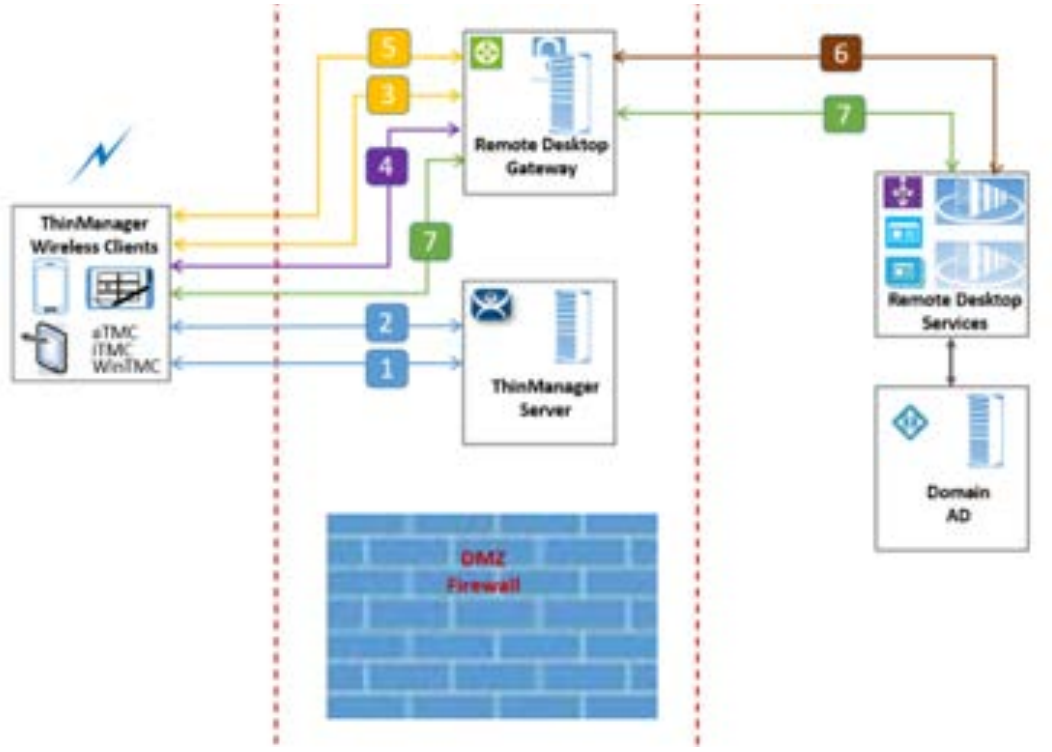
Segmentación de la red

La segmentación de la red es una faceta de gran importancia relativa al mantenimiento de un ambiente seguro a través múltiples capas de una red de control. Con la implementación actual de ThinManager, el servidor de este se debe colocar en el interior de la zona desmilitarizada industrial (IDMZ). Esto separa la zona de seguridad industrial y la zona de seguridad empresarial, y no permite por una regla que el tráfico en la red se transmita a través de la zona sin que algún tipo de proxy lo redirija. Puesto que ThinManager se coloca en el interior de la zona desmilitarizada industrial, no es necesario que el tráfico se transmita directamente a través de dicha zona a fin de enviar perfiles de terminal o firmware desde el servidor ThinManager a los clientes cero o dispositivos móviles



Desarrollo de la arquitectura de red

El desarrollo actual del producto permite que el firmware utilice un cliente RD no compatible con el gateway RD. El gateway RD será un elemento crítico de la implementación que va a requerirse para enviar contenido desde la zona de seguridad industrial a la zona de seguridad empresarial. En el caso de contenido que se debe visualizar en esta dirección desde un servidor del escritorio remoto que contiene datos o aplicaciones industriales, se deben utilizar clientes ThinManager (WinTMC, aTMC o iTMC). Esto se describirá de forma más detallada en la sección a continuación. El gateway del escritorio remoto (RDG) constituye un componente muy importante relativo a la protección de una implementación RDS; RDG es un servidor que se encuentra habitualmente en una zona desmilitarizada y sirve de intermediario. Cuando un cliente inicia una conexión, RDG primero establece túneles SSL entre sí mismo y el cliente externo. Luego, el RDG examina las credenciales del usuario (y como opción de la computadora) del cliente a fin de asegurar que el usuario/la computadora cuenten con la autorización de conectarse con el RDG. Después, el RDG asegura que el cliente tenga permiso para conectarse con el recurso solicitado. Si se autoriza la solicitud, el RDG establece una conexión RDP entre sí y el recurso interno. Toda la comunicación entre el cliente externo y el punto final interno pasa a través del RDG.



Número de flujo de la red	Puertos usados
1	TCP 2031: conexión inicializada por ThinClient al servidor ThinManager
2	TCP 2031: se usa para pasar la configuración (perfil de terminal) desde el servidor ThinManager al terminal (conexión inicializada de ThinClient)
3	TCP 443: el gateway RD establece los túneles HTTPS SSL, (permite el tráfico HTTPS al gateway RD)
4	El gateway RD autentica el usuario del cliente
5	UDP 3391: permite que el transporte cree esa conexión (solo se requiere si está habilitado RDP a través de UDP; de lo contrario, regresa de manera predeterminada a TCP 443).
6	TCP 3389: permite que el gateway RD envíe paquetes RDP
7	Comunicaciones entre el cliente ligero y el servidor RDS

1. Perfil de terminal de solicitud TMC desde el servidor ThinManager (puerto 2031 TCP).
2. ThinManager ordena al TMC que utilice el gateway RD para el contenido de pantalla solicitado del punto de conexión.
3. El gateway RD establece los túneles (puerto 443 TCP) entre sí y el cliente externo (uno para los datos de entrada y otro para los datos de salida).
4. Luego, el gateway RD autentica las credenciales del usuario (y como opción de la computadora) del cliente para asegurar que el usuario/la computadora cuenten con la autorización de conectarse con el gateway RD. Una vez establecidos los túneles, el cliente y el gateway RD establecen un canal principal a través de cada túnel.
5. Una vez que los canales de transporte HTTPS se habilitan para optimizar el transporte de datos, el UDP establece dos canales laterales (puerto 3391 UDP) a fin de proporcionar la entrega fiable (RDP-UDP-R) y de mejor esfuerzo (RDP-UDP-L) de los datos. El túnel UDP utiliza DTLS para proteger sus comunicaciones y también utiliza el certificado SSL en el servidor del gateway RD.
6. Después, el gateway RD asegura que el cliente tenga permiso de conectarse con el recurso solicitado. Se se autoriza la solicitud, el gateway RD establece una conexión RDP (puerto 3389 TCP) entre sí y el recurso interno. Toda la comunicación entre el cliente externo y el punto final interno pasa a través del gateway RD.
7. El TMC se inicia mediante el gateway RD al servidor RDS/ThinManager y el contenido se entrega al TMC.

Movilidad segura

Relevance es la terminología comercial utilizada por el producto que incluye la entrega de contenido a usuarios y lugares. Relevance entrega contenido basado en el usuario y/o el lugar que promueve una rectilínea al control de máquinas que se habilitará en un dispositivo móvil, colocará la seguridad en torno al acceso a aplicaciones y podrá transferir la propiedad de una aplicación desde un terminal al otro. Los servicios de usuario y lugar Relevance no sustituyen la necesidad de hardware tradicional para fines de seguridad, pero sí pueden ayudar a mejorar la experiencia y la productividad del usuario. Existen tres aplicaciones diferentes que se pueden utilizar para convertir un dispositivo móvil o PC en un terminal ThinManager: iTMC (cliente iOS ThinManager), aTMC (Android) y WinTMC (Windows). En el caso de los dispositivos móviles, no se envía el firmware para reemplazar o servir del sistema operativo local, sino que se instala una aplicación desde la tienda en línea respectiva y se utiliza para conectar el servidor ThinManager mediante la especificación del nombre DNS o de la dirección IP del servidor ThinManager.

Cuando se envía contenido a un dispositivo móvil mediante el uso de ThinManager, no hay instalación ni gestión locales de las aplicaciones deseadas. Las aplicaciones se entregan al dispositivo cuando se inicia la aplicación y se conecta con la red apropiada. Si el dispositivo móvil no se autentica correctamente en la red, ninguna de las aplicaciones cliente podrá establecer conexiones al dispositivo.

Se puede colocar la seguridad en torno a las aplicaciones conectadas con la red mediante el requisito de que un usuario o miembro específico de un grupo de usuarios se haya iniciado sesión en el dispositivo móvil para acceder a una aplicación. Si el usuario no ha iniciado sesión, la aplicación no será visible.

El uso de dispositivos de resolución de lugar o identificadores de lugar permite que la solución incluya seguridad. Existen cuatro maneras en las que ThinManager puede identificar o resolver un lugar: códigos QR, señales Bluetooth, puntos de acceso inalámbricos y GPS. Cuando un dispositivo móvil entra en el rango configurable de uno de los dispositivos de resolución, se entrega el contenido al dispositivo. Cuando el dispositivo de resolución se encuentra fuera de rango, se elimina el contenido del dispositivo.

La integración de los conceptos de la entrega simultánea de contenido de usuario y lugar completa la oferta de soluciones Relevance y garantiza que el contenido esté disponible solo a la persona adecuada en el lugar adecuado. Si una aplicación fuera visible solo a un ingeniero, un operador no podría escanear un código QR a fin de recibir ese contenido. Si el contenido representa alguna cosa relativa al control de máquinas, se debe

mantener la rectilínea al proceso del que el ingeniero tiene control. Se podrían utilizar múltiples dispositivos de resolución de lugar para llevar a cabo esta acción. Por ejemplo, el ingeniero podría iniciar sesión en el cliente móvil, escanear un código QR cerca de una señal Bluetooth a fin de recibir una aplicación de control de máquinas. Luego, si el ingeniero moviera el cliente móvil fuera del rango Bluetooth configurado, perdería el contenido, lo cual le impediría realizar actividades peligrosas sin tener la rectilínea al equipo que controla.

La integración de contenido entregado de dispositivo, usuario y lugar desde ThinManager de forma segura y protegida permite la gestión de dispositivos y la gestión y la entrega centralizadas del contenido.

THINMANAGER
A ROCKWELL AUTOMATION TECHNOLOGY

TM-WP001A-ES-P

ThinManager
1220 Old Alpharetta Rd
Suite 390
Alpharetta, GA 30005

www.thinmanager.com
1-877-239-4282
sales@thinmanager.com