Ajuste el nivel de seguridad del escritorio remoto

Cuando se trata de exponer el Protocolo de escritorio remoto a conexiones directas, necesita un servidor sólido y seguro para proteger sus sistemas contra los atacantes remotos. Debido a las técnicas innovadoras disponibles para los delincuentes cibernéticos modernos y una vulnerabilidad de uso después de la liberación en la solución de Microsoft, los **piratas informáticos de todo el mundo pueden acceder fácilmente a las credenciales de inicio de sesión en cualquier lugar, realizar ataques de ransomware y ejecutar código arbitrario en el objetivo. sistemas**
Mientras tanto, nuestro equipo de expertos calificados ha trabajado arduamente para asegurar su acceso de escritorio remoto . Nacido de la clara comprensión del problema,

RDS-Knight ofrece una funcionalidad avanzada y hace que el uso del acceso remoto en su rutina diaria sea lo más seguro posible. Ahora, con **RDS-Knight** puede administrar fácilmente toda la flota de estaciones de trabajo, incluso si se encuentra a mil millas de distancia.

Mantenga su servidor seguro

Si desea iniciar sesión en su computadora personal desde otra ubicación, **RDS-Knight** es su espada y escudo para proteger su entorno de servidor contra atacantes no autenticados. **Nuestro producto está diseñado para proteger el escritorio remoto, monitorear fallas de inicio de sesión, bloquear direcciones IP prohibidas o sospechosas y prevenir acciones no autorizadas.** Al revisar las opciones de acceso remoto de su computadora, **RDS-Knight le** brinda un excelente control sobre los usuarios conectados con acceso otorgado.

Acceda a su estación de trabajo de forma segura

Al utilizar el servicio Brute-Force Attacks Defender, puede crear una lista blanca con IP dedicadas que necesita para alcanzar el servidor y establecer el número esencial de intentos de contraseña incorrecta. Por lo general, establecer el máximo de intentos fallidos de inicio de sesión desde una sola IP es una medida efectiva para evitar ataques de fuerza bruta.

Si desea asegurar el inicio de sesión en el servidor y permitir conexiones solo desde países específicos, tenga la seguridad de que nuestro producto protegerá su sistema contra cualquier atacante extranjero. Además de eso, nuestro luchador contra delitos cibernéticos ofrece protección de puntos finales y control de dispositivos para la comprobación periódica de los nombres de dispositivos aprobados para cualquier sesión entrante.

Recuerde, los **hackers y las bolsas maléficas nunca duermen.** Con **RDS-Knight** , puede conectarse a su estación de trabajo en cualquier momento y en cualquier lugar sin temor a ataques externos. **Póngase en contacto con nosotros hoy, agregue esta herramienta excepcional a su arsenal y use el acceso remoto en todo su potencial.**

RDS-Knight existe en dos ediciones:

- **RDS-Knight *Security Essentials* es el mejor paquete para mantener segura su conexión a Escritorio remoto, con excelentes características de protección.** Es la solución de seguridad de bajo costo que incluso puede aplicar a todos los accesos RDP W7 / W10 Pro.
- **RDS-Knight *Ulti mate Protection* es la herramienta de seguridad que todo administrador de Windows Server debe tener:** debe proporcionar todo lo que necesita para proteger eficazmente los entornos de sus usuarios y prohibir las acciones maliciosas.

  Las características incluidas se detallan a continuación.

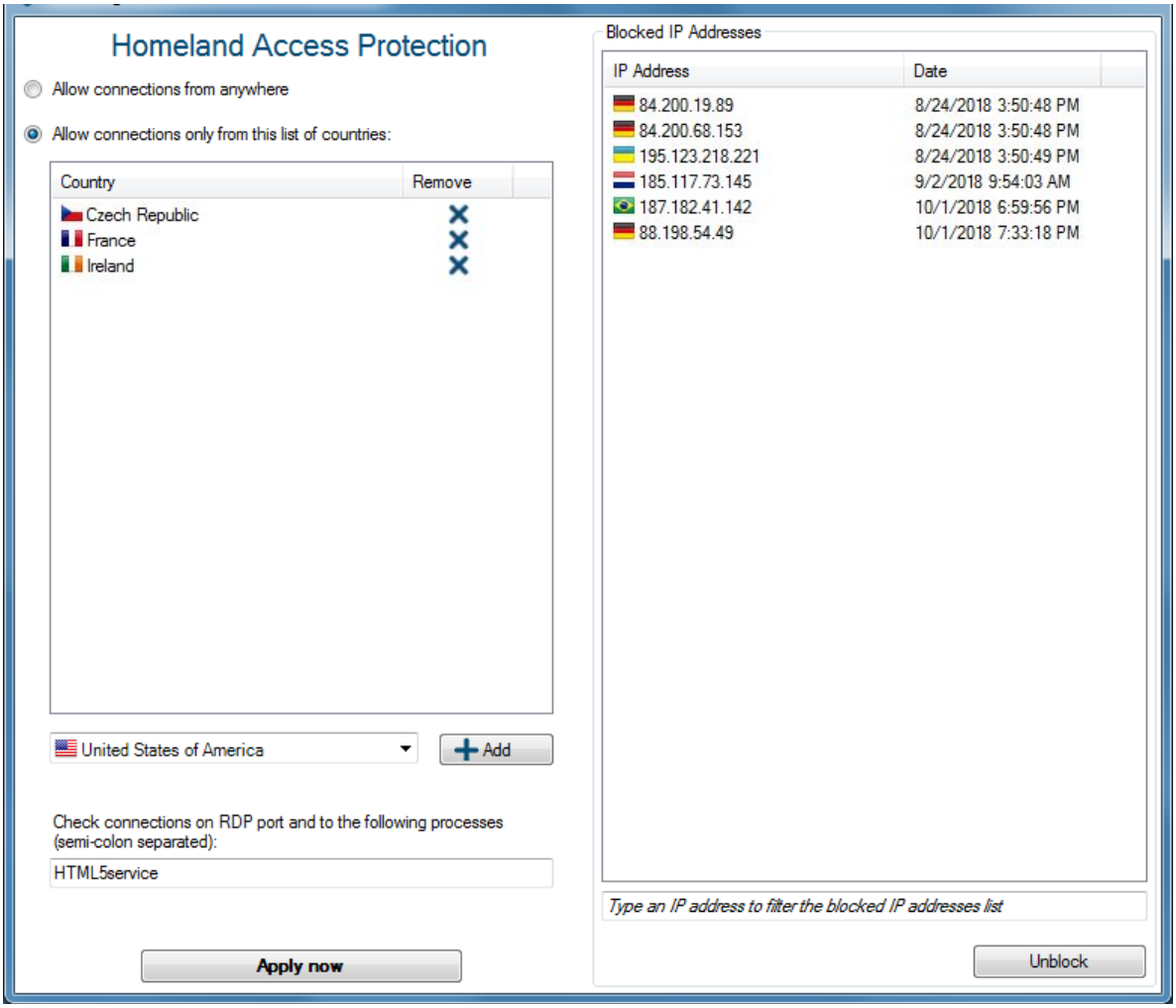
El enfoque de 360 grados a la seguridad

RDS-Knight Security Essentials proporciona tres protecciones principales:

- Protección de la patria: evita que los atacantes extranjeros abran una sesión.
- Previene los ataques de fuerza bruta: enlista las direcciones IP ofensivas.
- Restricción de horas de trabajo: prohíbe a los usuarios conectarse por la noche (para todos los usuarios).

RDS-Knight Ultimate Protection proporciona todas las protecciones que necesita:

- Protección de la patria: evita que los atacantes extranjeros abran una sesión.
- Previene los ataques de fuerza bruta: enlista las direcciones IP ofensivas.
- Restricción de horas de trabajo: prohíbe a los usuarios conectarse por la noche (por usuarios o por grupos).
- One Click to Secure Desktop: proporciona un entorno de usuario altamente seguro (por usuarios o por grupos).
- Protección de dispositivos de punto final: restringe el acceso por dispositivo (por usuarios).
- Protección contra ransomware: detenga inmediatamente el cifrado de datos durante un ataque de ransomware.
-

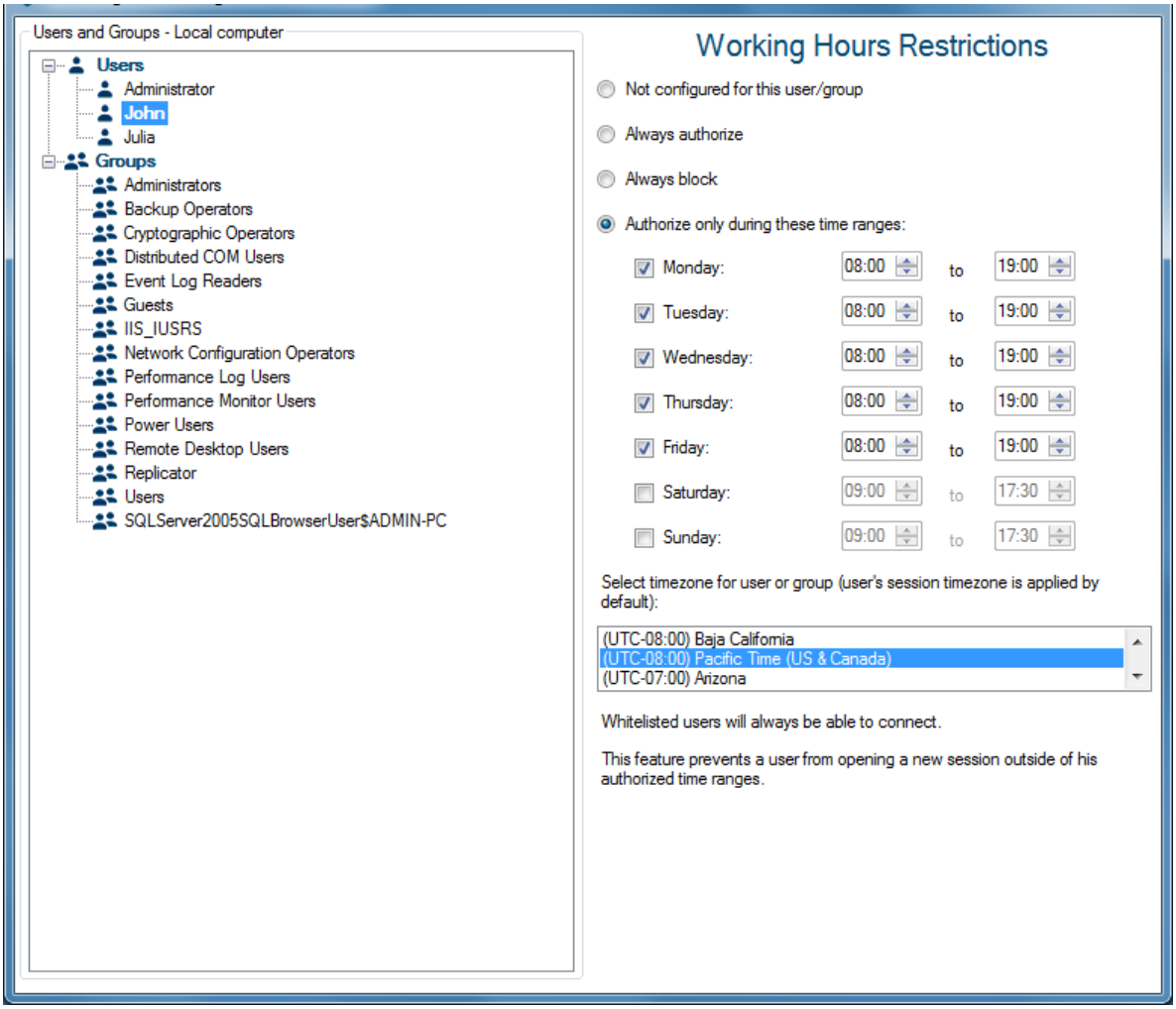


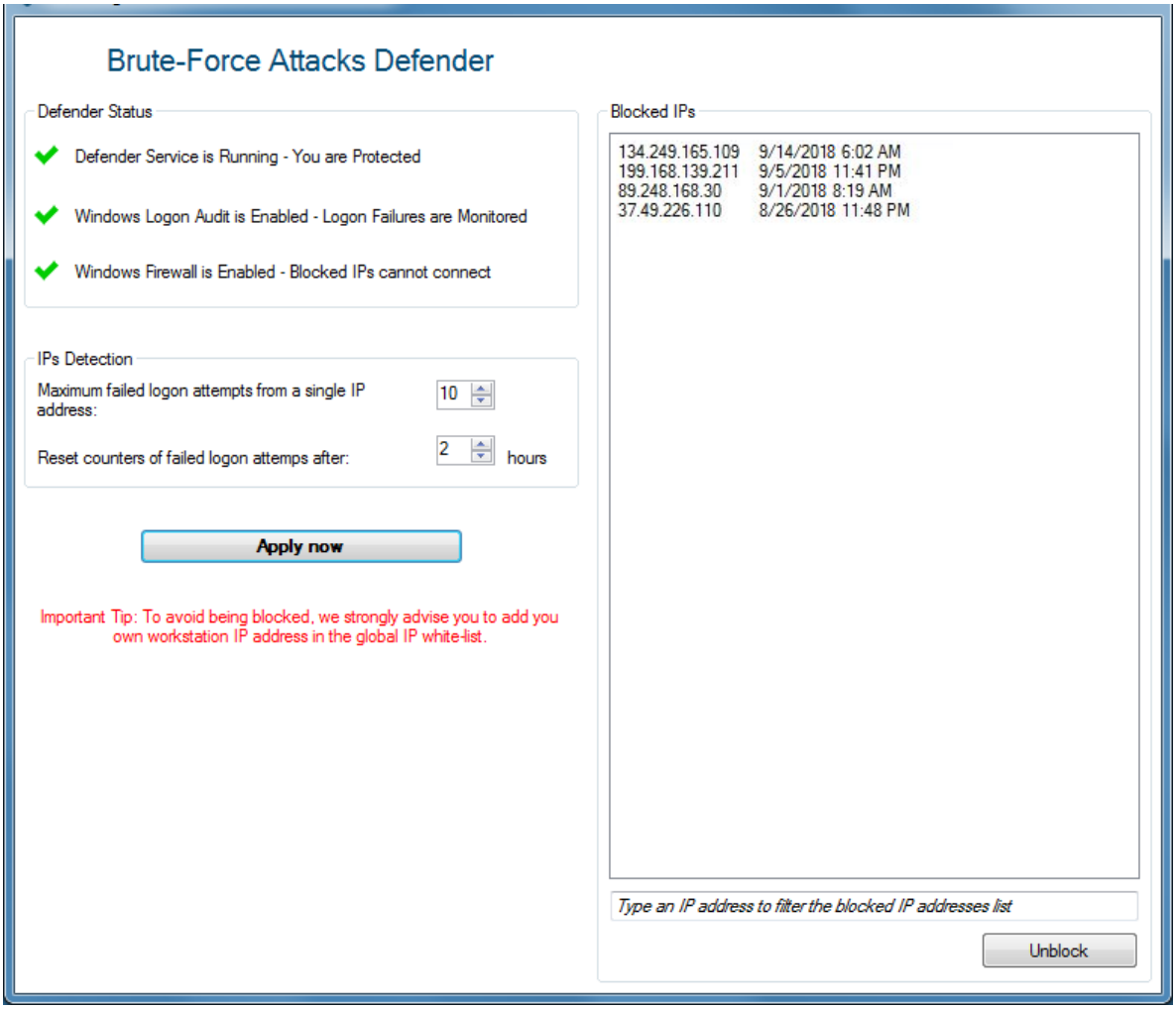
Geo-restricción para RDP

Sus usuarios se encuentran en las oficinas de Estados Unidos, Reino Unido y Canadá. **¿Por qué alguien debería poder abrir una sesión** desde China, India, Irán o Alemania?
En un instante con **RDS-Knight** , protege sus servidores RDS de cualquier atacante que intente abrir una sesión desde un país extranjero. Esto es extremadamente simple y muy poderoso.¡Simplemente hazlo!

Proteja sus servidores en la noche

Por supuesto, sus usuarios deben tener la libertad de conectarse y trabajar cuando están en sus escritorios. Sin embargo, ¿por qué se les permitiría abrir una sesión a la medianoche?
Con **RDS-Knight** , puede **especificar la hora de trabajo del día y la zona horaria en la que sus usuarios o grupos pueden abrir sesiones** dependiendo de las horas de trabajo del empleado y la ubicación de la oficina.
Será tan fácil e increíblemente agradable mejorar sus políticas de seguridad.





Bloquear ataques de fuerza bruta

Si su servidor Windows está disponible públicamente en Internet, existe una probabilidad del 100% de que **piratas informáticos, escáneres de red y robots de fuerza bruta** estén tratando de adivinar el nombre de usuario y la contraseña de su administrador, en estos momentos . Usando inicios de sesión y diccionarios de contraseña actuales, intentarán iniciar sesión en su servidor cientos de personas paramilesveces cada minuto. No solo esto es **malo para la seguridad de su servidor** , sino que también puede **consumir muchos de sus recursos** (CPU y ancho de banda).

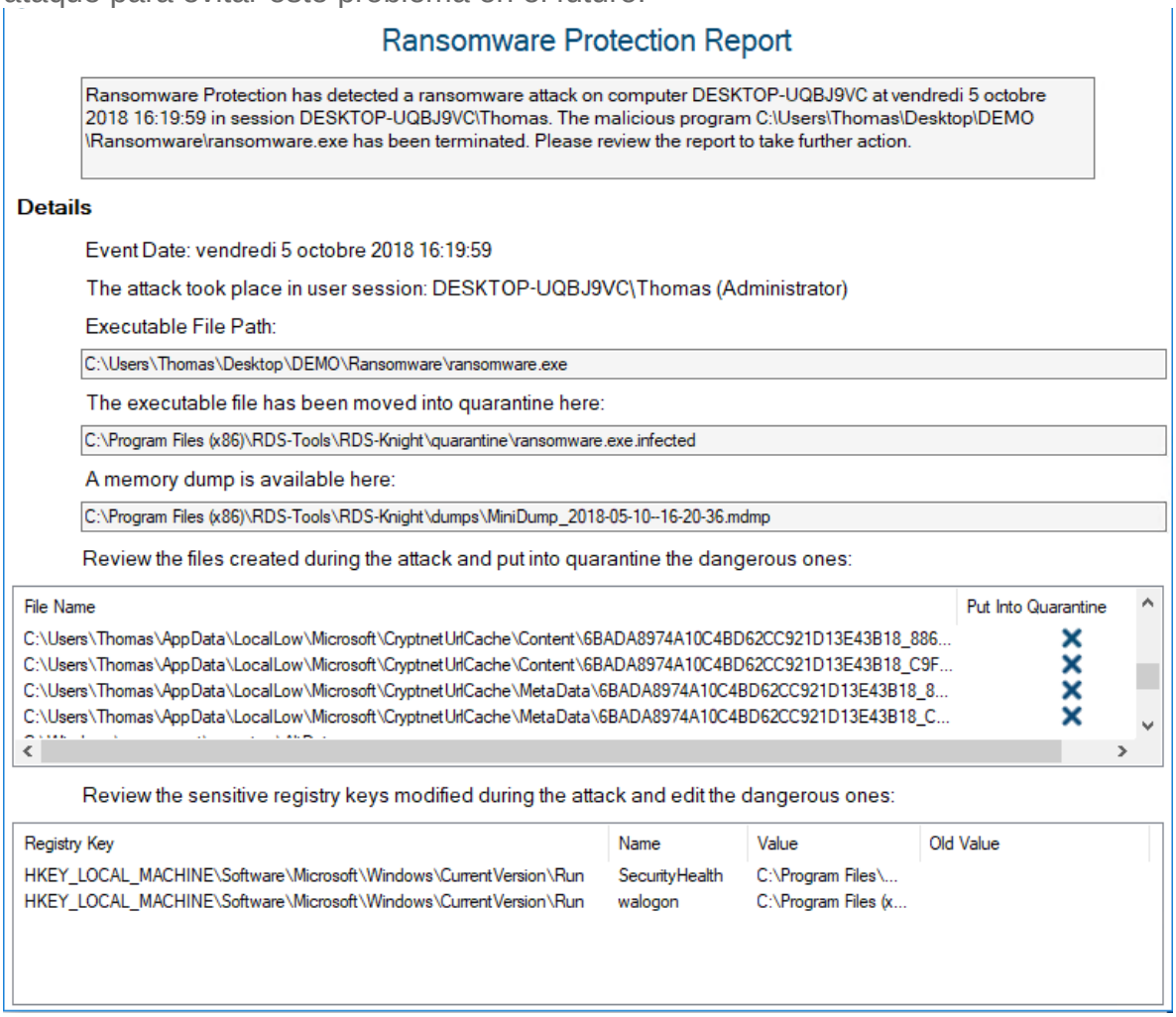
Detén los ataques constantes en este momento con el defensor de los ataques de fuerza bruta **RDS-Knight** . Se **protegerá al instante su servidor** mediante el control de Windows intentos fallidos de inicio de sesión y automáticamente la lista negra las direcciones IP infractor después de varios fracasos. Además, puede, por supuesto, configurarlo para que se ajuste a sus necesidades.

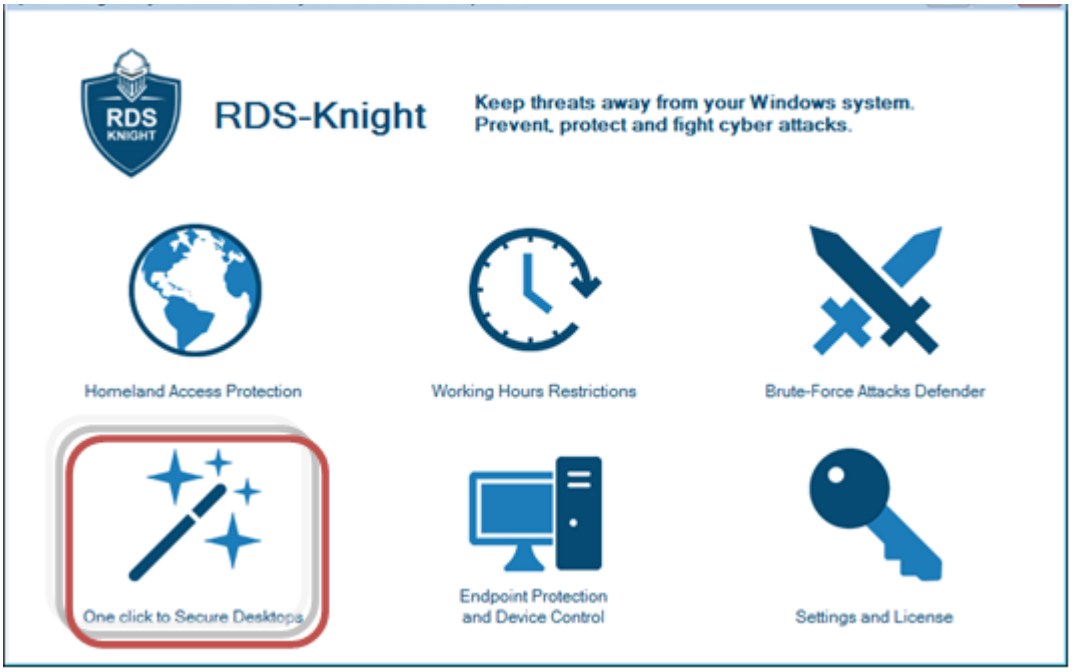
Detener los ataques de ransomware

Ransomware sonLas amenazas cibernéticas más significativas de hoy. Sus acciones en sus sistemas bloquearán completamente su acceso o cifrarán la mayoría de sus archivos hasta que pague la solicitud de rescate de los delincuentes cibernéticos. Sin embargo, esto no garantiza la restitución de sus datos y puede paralizar sus actividades comerciales.

La protección RDS-Knight Anti-Ransomware DETECTARÁ, BLOQUEARÁ y PREVENIRÁ eficientemente los ataques de ransomware. Evitará que su negocio tenga consecuencias catastróficas al eliminar el ransomware en una etapa temprana.

RDS-Knight le avisa instantáneamente tan pronto como detecta una actividad de ransomware en su sistema, proporcionándole la lista de los elementos infectados para poner en cuarentena. Obtendrá información detallada sobre la fuente del ataque para evitar este problema en el futuro.





Un clic para establecer políticas de derechos de usuario

Windows proporciona muchos GPO potentes, pero le costará varios días hacer cumplir las reglas de seguridad esperadas. La mayoría de nosotros no estamos lo suficientemente cómodos con este tipo de políticas de restricción del sistema; como resultado, renunciamos a él o seleccionamos solo algunos de ellos.

Con un solo clic, RDS-Knight aplicará las mejores prácticas de seguridad. En pocos minutos, obtendrá el mejor nivel de seguridad que espera alcanzar para el entorno de usuario de su Escritorio remoto. Es tan fácil hacerlo **"usuario por usuario",** o configurarlo **"por grupo"** . Más que un ahorro de tiempo para proteger su servidor, RDS-Knight le brinda más seguridad sin complejidad.

Protección del dispositivo

¿Por qué un pirata informático debería poder usar una credencial de Windows robada para abrir una sesión desde cualquier dispositivo? Esto debe evitarse. La **protección de EndPoint** es la respuesta correcta. Enlazará la credencial del usuario al propio dispositivo del usuario.

¿Cómo funciona? **RDS-Knight** grabará el nombre del dispositivo del usuario en su primera conexión. El administrador puede decidir**restringir el acceso para este inicio** de **sesión** al nombre de ese dispositivo grabado. Al hacerlo, cualquier intento de conectarse desde otro dispositivo se detectará y rechazará automáticamente.