Rxart Secure

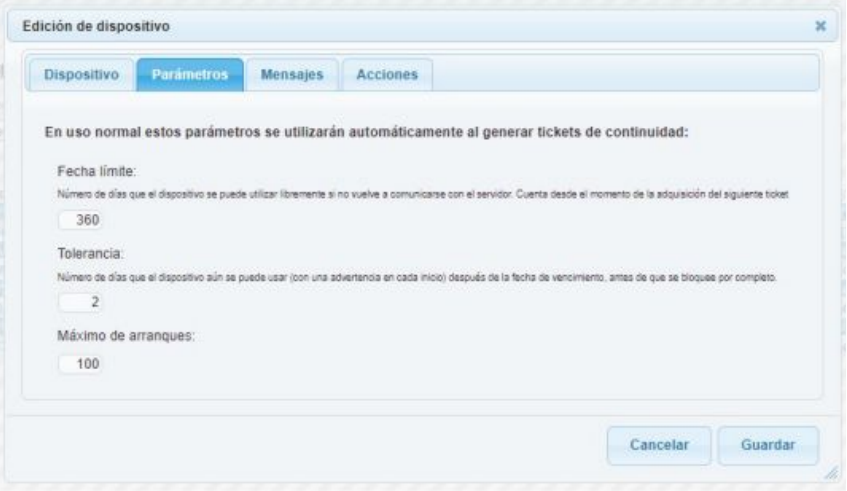
Rxart Secure - Control de la unidad central I

Rxart Secure es una tecnología de seguridad única para computadoras, que aprovecha el hardware, el firmware UEFI y los agentes de software para permitir que un dispositivo verifique el autocumplimiento, el bloqueo remoto automático o manual y el desbloqueo incluso antes de que el sistema operativo se esté ejecutando.

Rxart Secure permite una protección inteligente de dispositivos perdidos y robados, destinada a evitar el uso no autorizado de una computadora, que se ejecuta en todos los dispositivos x86 modernos *, desde una computadora portátil, estación de trabajo o servidor con las especificaciones más altas. Rxart Secure no requiere características de seguridad de chipset o CPU patentadas tradicionales, aprovechando el Modelo de seguridad de firmware UEFI y es independiente del software.

Rxart Secure - Control de la unidad central I

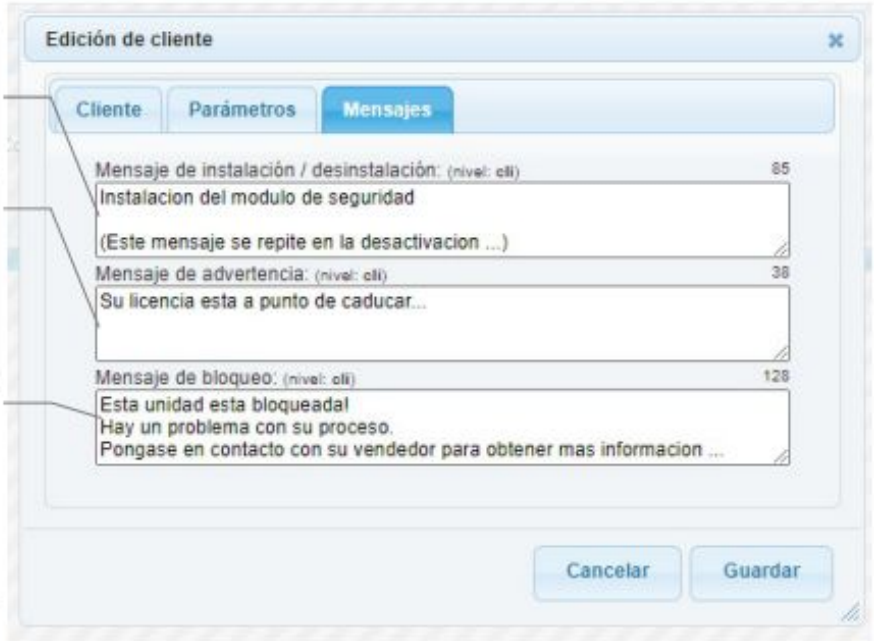
Rxart Secure mejora drásticamente las probabilidades de recuperación de hardware y cumplimiento de contratos, permitiendo proyectos inclusivos y no discriminatorios que de otro modo enfrentarían obstáculos económicamente insuperables. Es una verdadera clave de desbloqueo para los proyectos de Dispositivo como servicio, ya que resuelve el principal obstáculo de DaaS: el control del dispositivo por parte del propietario del proyecto mientras está bajo un contrato de servicio. Ahora, los grandes proyectos sobre educación, donde la inclusión y la no discriminación son prioridades primordiales, finalmente son posibles. Los estudiantes están protegidos contra abusos cuando portan un dispositivo con un candado de seguridad que evita completamente que cualquier ladrón se beneficie de un dispositivo robado que está bloqueado e inutilizable. La distribución del dispositivo al suscribirse a un servicio de Internet, finalmente puede suceder al mismo tiempo que la distribución tradicional del teléfono inteligente sobre la suscripción al servicio.



Mensaje de configuración predeterminado.

Mensaje de advertencia predeterminado. Ocurre cuando se alcanza el límite de días y durante el periodo de tolerancia.

Mensaje de bloqueo predeterminado. Este es el mensaje que ven los usuarios cuando sus dispositivos están bloqueados por Rxart



Rxart Secure - Sistemas operativos soportados

- ➔ Ubuntu (a partir de la versión 12.04.2)
- ➔ Fedora (a partir de la versión 18)
- ➔ Debian (a partir de la versión7.0)
- ➔ FreeBSD (a partir de la versión 10.0)
- ➔ OpenBSD (a partir de la versión 5.8)

- ➔ Windows 11 (64 bit)
- ➔ Windows 10 (32 & 64-bit)
- ➔ Windows 8.1 (32 & 64-bit)
- ➔ macOS 10.15, 11, 12 and 13 (Intel and Apple M1, M2 based Mac devices)

Rxart Secure - Control de la unidad central II

Esta tecnología de seguridad única ha sido verificada y garantizada contra ataques de vulnerabilidad. El "motor de reglas" interno de **Rxart Secure** tiene umbrales, intervalos de temporizador y acciones a tomar, independientemente del estado de conectividad de la red del dispositivo. **Rxart Secure** proporciona protección local, a prueba de manipulaciones y basada en políticas que funciona incluso si el sistema operativo se vuelve a crear desde una imagen o se instala un nuevo disco duro. Desarrollado y patentado* por Pixart y un equipo de ingenieros de investigación especializados en seguridad, está disponible en una variedad de hardware basado en x86. La última versión está optimizada para las familias Intel IceLake®, CometLake® y GeminiLake®, y aprovecha el modelo de seguridad estándar UEFI para el desarrollo futuro. La mayoría de los principales fabricantes de computadoras ya han obtenido licencias y han validado dispositivos compatibles con Rxart Secure, como Acer, ASUS, Classmate, Clevo, Dell, Dynabook, ECS, INSYS, Lenovo, MSI, etc. Rxart Secure está disponible para licencia por ODM, MNC, hardware Los SI, los IDH y los gobiernos, las escuelas, las universidades, los operadores de telecomunicaciones, las empresas de arrendamiento y los propietarios de proyectos de DaaS pueden activarlos en muchos escenarios. El componente del servidor para controlar el dispositivo puede ser compartido en la nube o instalado localmente por el propietario del proyecto DaaS, dependiendo del tamaño del proyecto. El lado del servidor se puede implementar en Microsoft Azure y opcionalmente ** se conecta a las funciones de Microsoft Intune MDM. Rxart Secure Firmware Security también proporciona información segura de hardware de bajo nivel para funciones MDM que es fundamental para administrar grandes redes de dispositivos heterogéneos. * Actualmente desarrollado para x86, pero ARM en desarrollo y se espera que esté disponible en el primer trimestre de 2024. Debido a las limitaciones tecnológicas de la arquitectura ARM, no todas las defensas de seguridad se implementan en ARM. ** En desarrollo**

Seguridad real

Comprobación de autocumplimiento, bloqueo remoto basado en reglas

• Protección del dispositivo
• Disuasión contra robos
• Bloqueo previo al arranque no destructivo
• Evitar que el sistema operativo se inicie
• Interfaz personalizable
• Desbloquear la recuperación a través del portal web o el teléfono
• Reinstalación del sistema operativo
• Reemplazo de disco duro
• Ataques de vulnerabilidad de ROM
• BIOS re-flash Rxart Secure se activa a través de suscripciones de proveedores de servicios con licencia y socios de Pixart en hardware compatible con x86 pre-aprovisionado (*). Los dispositivos preparados para Rxart Secure son completamente probados y depurados por el equipo de ingeniería de Pixart antes de su introducción en el mercado. Los proveedores de servicios pueden brindar el servicio a través de un acceso web seguro basado en la nube o instalando los servidores de autorización en las instalaciones del cliente (generalmente, operadores gubernamentales o de telecomunicaciones).

Lista de características

Lista de características Firmware basado en UEFI

• Modelo de seguridad UEFI estándar (foro www.uefi.org)
• Ejecución completa del firmware UEFI, independiente del software
• Independiente del software, compatible con Windows, Linux.
• Comprobaciones de firmware UEFI de autocumplimiento, independientes del sistema operativo
• Bloqueo remoto basado en reglas, independiente del estado de conectividad
• Bloqueo previo al arranque no destructivo
• Protección contra el reinicio del BIOS que no es Rxart Secure cuando Rxart Secure está en estado activo
• Evita que el sistema operativo se inicie cuando está en estado de bloqueo
• Desbloquear la recuperación a través del portal web, teléfono o llamada API remota
• El firmware detecta fallas del agente de software (autorreparación) y notifica al usuario.
• Si TPM está presente, Rxart Secure opcionalmente usa la generación de claves TPM para asegurar la comunicación basada en tickets con el servidor. Agente de software
• Las reglas de bloqueo del dispositivo y la función de trabajo sobreviven a la reinstalación del sistema operativo, reemplazo de almacenamiento, ataques de vulnerabilidad de ROM y actualización de BIOS

Lista de características

• Comunicación de usuario final (firmware y software) basada en varios idiomas
• Soporte de firmware para acceso de software de bajo nivel para funciones "Rxart Secure MDM" Plataforma e integración en la nube
• Servidor basado en la nube y opcionalmente compatible con Microsoft Azure
• API abierta para integrarse con plataformas de administración de dispositivos de terceros
• Integración de Microsoft Intune MDM (en desarrollo*)
• Integración de MDM de código abierto (en desarrollo*)
• Compatible y certificado con la mayoría de las marcas de computadoras (consulte la lista en línea*)

Escenario típico: aprovisionamiento

Los dispositivos habilitados para Rxart Secure se aprovisionan con reglas de contrato

• Cada organización propietaria de dispositivos (por ejemplo: un operador de telecomunicaciones; una empresa de alquiler / arrendamiento; una unidad gubernamental; un distrito escolar) define con el proveedor de servicios Rxart Secure un conjunto de reglas de contrato para suministrar cada dispositivo.
• Los mensajes para el dispositivo específico o el propietario de la organización se definen en el momento del aprovisionamiento.

Los mensajes de advertencia del estado de Rxart Secure y los mensajes de "bloqueo" se muestran cuando un dispositivo se bloquea automáticamente. Debido a las leyes de muchos países, el mecanismo Rxart Secure fue diseñado para ser auto automatizado, es decir, el dispositivo nunca recibe una “orden remota” para que se bloquee. El dispositivo verifica su propio estado y actúa de acuerdo con las reglas establecidas en el momento del aprovisionamiento, independientemente de su propio agente de software, ya que el bloqueo se produce en el prearranque.

Escenario típico: Bloqueo

Las reglas del dispositivo detectan el uso por incumplimiento, el informe de robo / pérdida, el vencimiento del temporizador o el intento de piratería y ejecutan automáticamente un bloqueo del dispositivo.

• El usuario final recibe un mensaje de "bloqueo" (personalizable), un código de evento único y, por lo general, un número de devolución de llamada para buscar ayuda para desbloquear su dispositivo.

- A solicitud del propietario del dispositivo, el usuario final puede desbloquear automáticamente mediante un sitio de soporte web en caso de que el dispositivo no esté en estado de "orden de bloqueo".

- Si se denuncia la pérdida o el robo de una computadora, se inicia una señalización de ubicación y se crea un registro de dirección IP para uso forense y recuperación del dispositivo

- Se crearon múltiples defensas autorreparables, utilizando los métodos de criptografía más avanzados, para proteger el mecanismo Rxart Secure contra ataques de piratería. La tecnología Rxart Secure no está destinada a proteger los datos que residen en los discos duros, solo el hardware en sí al "bloquearlo" temporalmente.

Análisis competitivo

- Análisis de Rxart Secure frente a los 3 principales competidores
- Plataforma abierta, basada en estándares UEFI, compatible con múltiples marcas de dispositivos de punto final (licencia abierta para ODM)
- Bloqueo remoto de nivel de firmware de propósito único, control automático del dispositivo, bloqueo previo al inicio del sistema operativo.
- Sin acceso a los datos del usuario en el dispositivo por el administrador de la plataforma (compatible con RGPD)
- Reactivar el dispositivo de forma remota después del evento de bloqueo (no depende del software, sino únicamente del bloqueo del hardware / firmware)
- Autoprotección contra intentos de piratería para desactivar la seguridad en el dispositivo
- Funcionamiento regular de ancho de banda bajo y sin conectividad durante un período definido Compatibilidad con varios sistemas operativos, incluidos Windows, Linux, Android, Chrome. Bloqueo por firmware.
- Concéntrese en la seguridad de "solo hardware". Independiente de los datos y el contenido.
- Ticket remoto permanente de "libertad" para desactivar permanentemente el mecanismo de seguridad

Casos comerciales I

Los datos estadísticos mostraron, después de ejecutar el programa durante más de 2 años, que el 27,9% de los usuarios dejaron de pagar las cuotas mensuales en algún momento. El sistema de seguridad Rxart Secure en las computadoras portátiles detectó el incumplimiento y bloqueó automáticamente el dispositivo. Tras el mensaje personalizado "perdido y encontrado / bloqueado", el 98,6% de los usuarios se puso en contacto con nuestro centro de atención telefónica, pagaron las cuotas vencidas y obtuvieron un código único para desbloquear el dispositivo y reactivarlo. Rxart Secure proporcionó una reducción masiva de los pagos predeterminados al bloquear las unidades que no cumplen. También se confirmó que el 3% de las unidades han estado fuera de línea durante más de 2 meses, y el sistema Rxart Secure basado en reglas las bloqueó incluso sin conectividad de red. Durante el período, el 2% de las unidades han sido reportadas por los usuarios como robadas o extraviadas, pero dada su “huella digital” al contactar con el servidor Rxart Secure, la mayoría fueron recuperadas y devueltas al usuario o denunciadas a las autoridades. Al final del período del contrato, todas las unidades en cumplimiento fueron liberadas del control de Rxart Secure. En este escenario, la mayoría de las cuotas en mora se habrían perdido o el costo de recuperarlas a través de los agentes de recuperación tradicionales o el sistema legal sería demasiado alto y, por lo tanto, el sistema de seguridad Rxart Secure demostró ahorrar más del 20% del precio de venta por unidad. Si no fuera por la solución Rxart Secure, los grandes proyectos de implementación basados en flujos financieros futuros no serían viables. Rxart Secure es un verdadero facilitador del modelo HaaS en educación.

Casos comerciales II

Alquiler y arrendamiento de dispositivos El modelo DaaS (dispositivo como servicio) se está convirtiendo en la forma líder de negocios de todos los tamaños y profesionales independientes para satisfacer sus necesidades de computación. Normalmente, cuanto menor es el tamaño de la empresa, mayor es el riesgo de cobranza de crédito y la recuperación del hardware. Sin la solución de seguridad Rxart Secure, una gran parte del negocio se pierde debido a los clientes de verificación de crédito "rechazados", a los contratos que entran en incumplimiento y no se pagan, al hardware que no se devuelve, a los altos costos de las verificaciones de antecedentes crediticios, a honorarios legales para recuperar contratos en mora o para servicios de recuperación de crédito. Una vez que Rxart Secure bloquea una computadora portátil, una estación de trabajo o un servidor, el usuario o la empresa infractores se toman solo unos minutos para liquidar los alquileres vencidos. Además, la detección del paradero del hardware alquilado es muy importante en la industria del alquiler. Rxart Secure, puede habilitar ese mecanismo de recuperación de manera mucho más eficiente que las soluciones patentadas y costosas actualmente disponibles que solo están disponibles para un conjunto limitado de dispositivos de gama alta y están diseñadas principalmente para proteger los datos en el dispositivo que el dispositivo en sí. Los avances tecnológicos permitieron el cifrado completo del disco duro y, por lo tanto, la protección de datos del usuario sin costo, pero aún dejaron el hardware desprotegido. ¡Rxart Secure protege ese hardware! Rxart Secure ROI (retorno de la inversión) es casi instantáneo dadas las reducciones de costos y las capacidades de "habilitación de proyectos" que presenta. Ahora es posible alquilar a pequeñas empresas o profesionales sin un buen historial crediticio con la seguridad de Rxart Secure. Actualmente se están iniciando varios proyectos piloto, basados en el alquiler de dispositivos con Rxart Secure habilitado. Estos proyectos no hubieran sido posibles sin un mecanismo de bloqueo y seguridad.

T: +54 11 43005900/+54 11 21817445 E: inf @pixartargentina.com.ar D: Ing Huergo 1437, 1°Piso B, Buenos Aires, Argentina