ENTRUST

DATA PROTECTION SOLUTIONS

“PROTEGIENDO MÁS ALLÁ DEL PERÍMETRO”

Ricardo Hernández,
CISSP, CISM, CRISC
PreSales Engineer, Latin America
ricardo.hernandez@entrust.com

ENTRUST
SECURING A WORLD IN MOTION

AGENDA

- CUANDO VEAS LAS BARBAS DE TU VECINO……..
- ENTRUST: CIFRADO KEYCONTROL / DATACONTROL
- HISTORY SAD TIME
- ENTRUST: ADEMAS DE CIFRAR , HAY QUE SEGUIR PRESTANDO ATENCION AL PERIMETRO
- RETOS DEL CIFRADO EN LA NUBE Y DATOS EN REPOSO
- COMO PROTEGER CON CIFRADO
- CONCLUSIÓN

CUANDO VEAS LAS BARBAS DE TU VECINO…….

BANCO PICHINCHA

Comunicado oficial a nuestros clientes

En las últimas horas, hemos identificado un incidente de ciberseguridad en nuestros sistemas informáticos que ha inhabilitado parcialmente nuestros servicios. Hemos tomado acciones inmediatas como aislar los sistemas potencialmente afectados del resto de nuestra red y contar con expertos de ciberseguridad para asistir en la investigación.

Al momento, nuestra red de agencias, cajeros automáticos para retiros de efectivo y pagos con tarjetas de débito y crédito están operativos.

Este incidente tecnológico no afecta el desempeño financiero del banco. Reiteramos nuestro compromiso en precautelar los intereses de nuestros clientes y restablecer la atención normal a través de nuestros canales digitales en el menor tiempo posible.

Hacemos un llamado a la calma para no generar congestión y mantenerse informados a través de los canales oficiales de Banco Pichincha para evitar la propagación de rumores falsos.

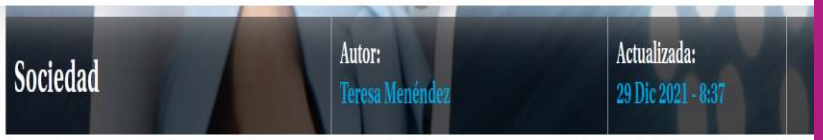
Quito, 11 de octubre de 2021

Antonio Acosta
Presidente

Santiago Bayas
Gerente General

PRIMICIAS

Home Política Economía Sociedad Tecnociencia En Exclusiva Lo último Firmas y Análisis Jugada



La ministra de Telecomunicaciones, Vianna Maino, durante el encendido del cable submarino Mistral, el 13 de agosto de 2021 en Guayaquil. Habla
- Foto: Mintel

#ciberseguridad #ciberseguridad en Ecuador #Ecuador #hackeos #Ministerio de Telecomunicaciones #Naomi Arcen

Ecuador registra un bajo índice de ciberseguridad

La ministra de Telecomunicaciones, Vianna Maino, se refirió al hackeo al sistema informático de la Policía, a propósito del caso de Naomi Arcentales. Ecuador trabaja en fortalecer su ciberseguridad.

LO M

01 Revi

buscando?

1 20:15

expreso

Las cifras acerca de las pérdidas económicas provocadas por la ciberdelincuencia son también elementos que faltan en los balances. **EFE**

Una vez más, aunque en esta oportunidad le tocó el turno a la Policía Nacional, que a causa de un supuesto **hackeo a su infraestructuras digital**, inició un operativo de captura contra Juan Carlos Izquierdo, el fiscal implicado en la muerte de su expareja Naomi Arcentales.

Tras descubrir que la orden de detención que constaba en el registro del sistema informático habría sido **subida de manera fraudulenta**, Izquierdo quedó libre luego de cinco horas.

No es la primera vez que las **seguridades informáticas** de entidades nacionales reportan ingresos irregulares a sus sistemas digitales. Este año ocurrió con la ANT, la CNT y hasta en una entidad financiera.

COMUNICADO OFICIAL

ACCESO NO CONSENTIDO AL SISTEMA INFORMÁTICO INTEGRAL DE LA POLICÍA NACIONAL "SIIPNE 3W", PARA EL REGISTRO DE ALERTAS DE ÓRDENES DE CAPTURA

La Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional, a través de su Departamento de Seguridades y Auditoría de las TIC, luego del análisis del supuesto hackeo, ha verificado mediante el análisis de las pistas de auditoría, el presunto **uso no consentido del usuario de un servidor policial asignado al subsistema investigativo** en el Sistema Informático Integral de la Policía Nacional del Ecuador (SIIPNE 3W). Se constató el ingreso al módulo de registro de Boletas de Captura, donde se activó fraudulentamente una presunta alerta de Boleta de Captura en contra del señor JUAN CARLOS I, con fecha 21-12-2021, sin la documentación y justificación legal de la autoridad competente. Cabe recalcar que el registro habría sido realizado utilizando métodos de evasión y suplantación de identidad mediante VPN/Proxi desde el exterior del país.

Las credenciales del usuario que tuvo acceso al Módulo de

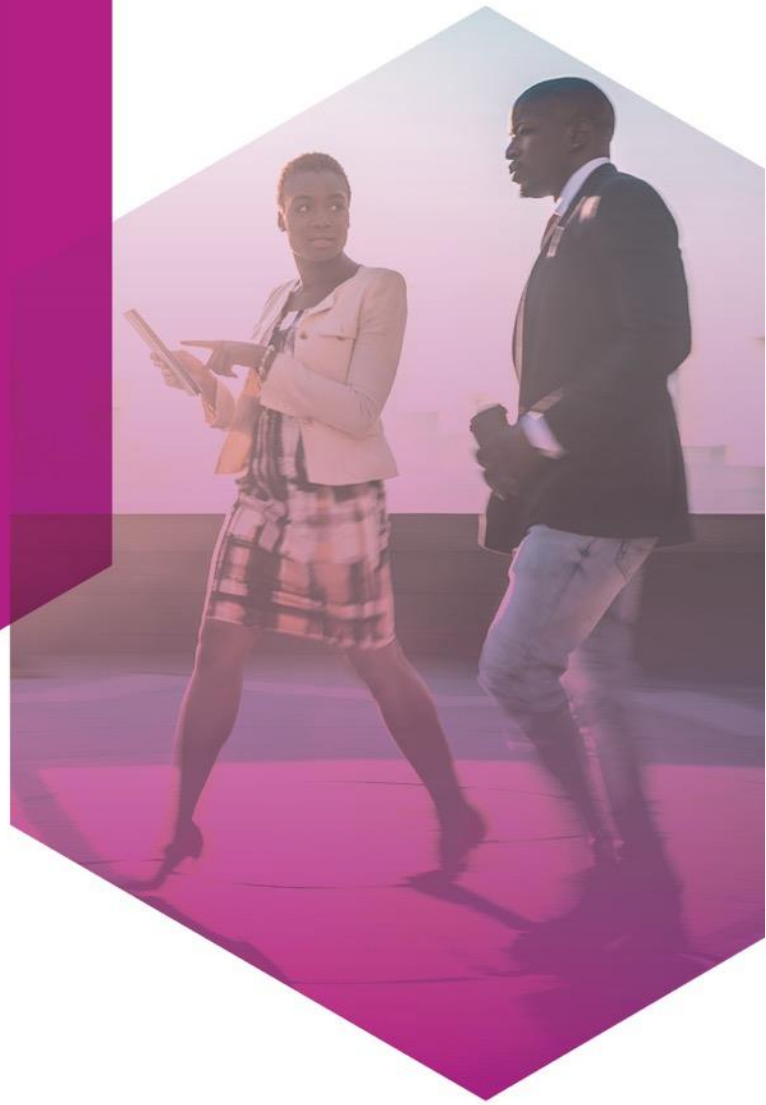
Un comentario,

No hay riesgo cero, con imaginación, tiempo y recursos, todo es posible…..

ENTRUST

- KEYCONTROL
- DATACONTROL
- HSM
- IDAAS

“EL CONTEXTO LO ES TODO”



History Cloud Sad Time

Habia una vez un administrador de un club de football infantil que **recolectaba**, **trataba** y **guardaba** información personal de sus jugadores en un servicio en la nube, por ser menores de edad necesitaba el **consentimiento** del padre o tutor.

En cierta ocasión se filtró que uno de los niños padecia de **diabetes juvenil**, y la aseguradora se entero, haciendo que el padre de familia pagara una prima extra por no informar de esta situación en el momento adecuado.

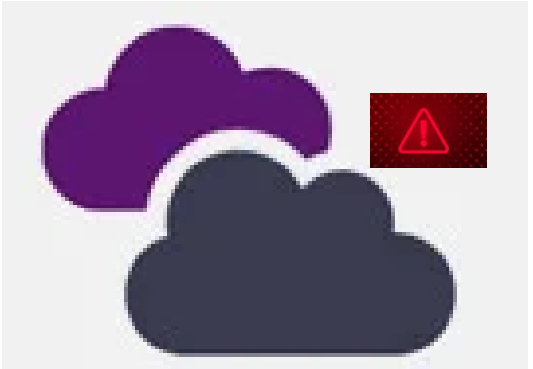
La pregunta es, ¿ cómo se filtro la información ?

Adivinaron, un servicio de almacenamiento en la nube, **sin cifrar =(**

© Entrust Corporation

Un poco de riesgos en los servicios de nube.

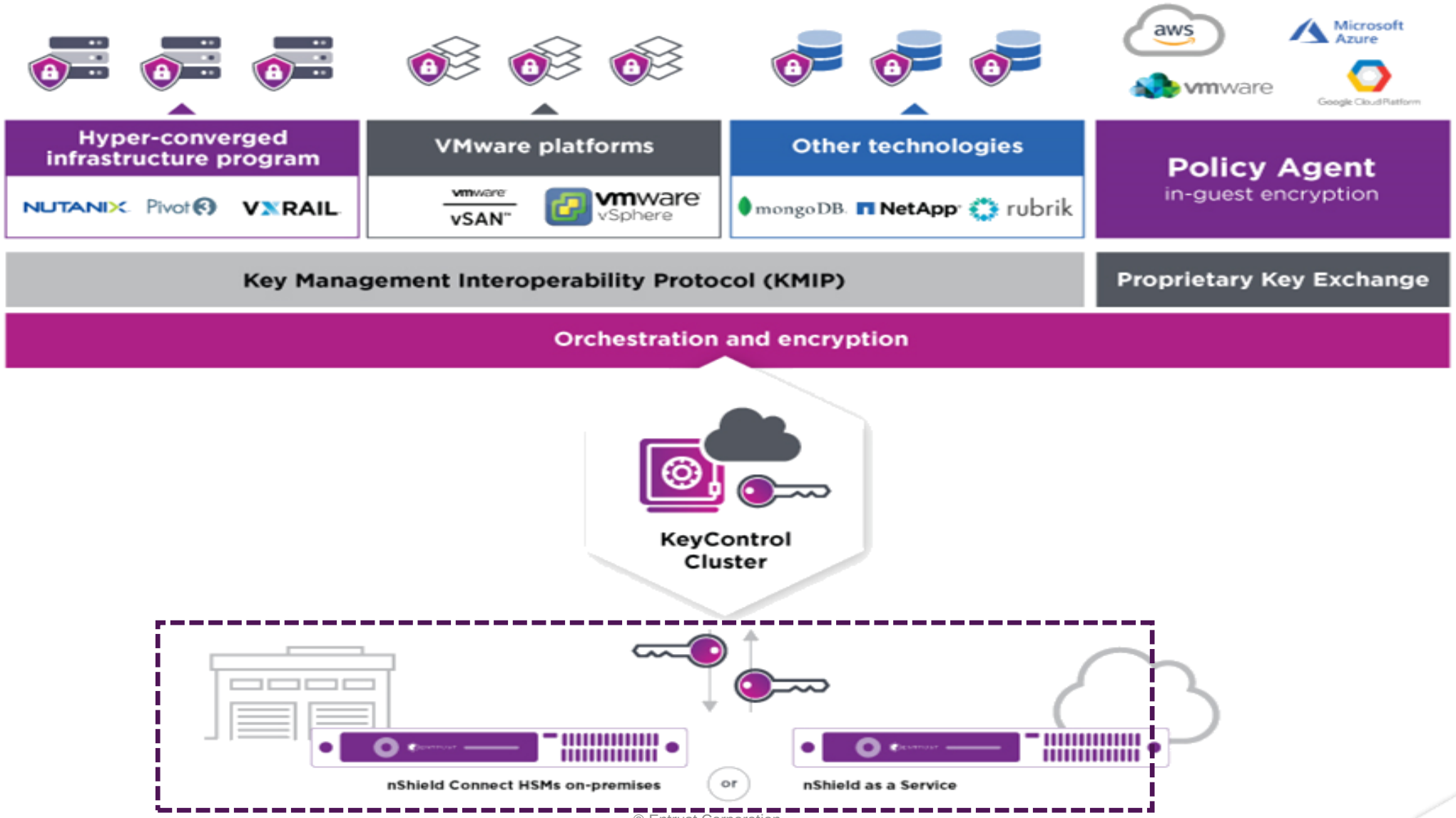
- **Brechas de información.**
- **Mala configuración y control de cambios.**
- **Falta de estrategia y arquitectura de seguridad para nube.**
- Vulnerabilidad de los sistemas.
- Gestion de identidad, gestion de llaves y accesos deficientes.
- Amenazas internas y abuso de privilegios.
- Robo de cuentas.
- API / interfaces inseguras
- Abuso y mal uso de los servicios de nube.



Fuente: Top Threats to cloud computing, The Cloud Security Alliance (CSA)

© Entrust Corporation

Gestionar el problema, con acciones…… entonces, protegamos los servicios de nube con una estrategia clara utilizando claves de cifrado.

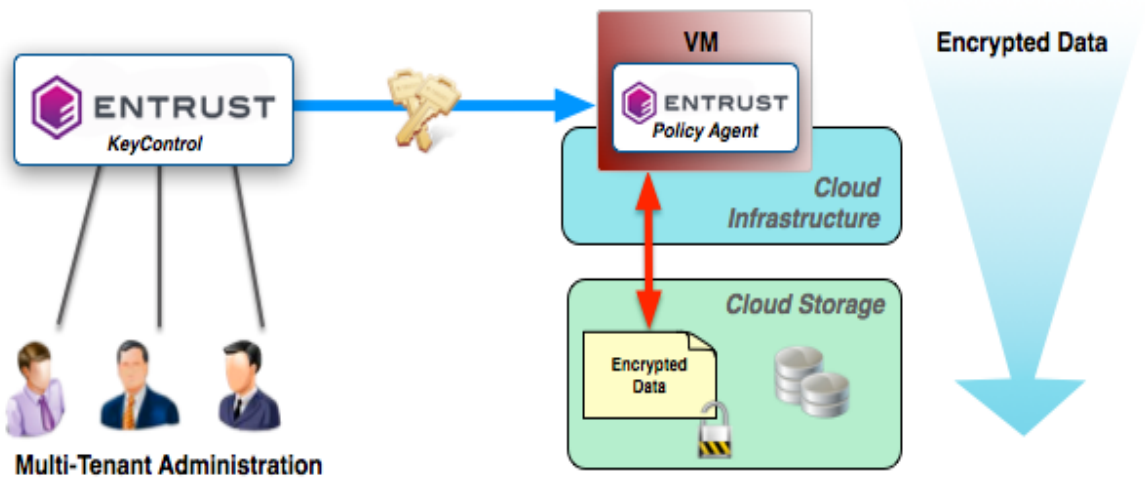


© Entrust Corporation

Descarga la prueba de KeyControl directamente de: https://go.entrust.com/HyTrust_KeyControl

Entrust **KeyControl** & Entrust **Datacontrol**

Necesidad	Solución
Proteger directorios / particiones / ACL en servidores virtualizados(Windows / Linux) on-premise o en la nube.	DataControl
Cumplir con estandares de seguridad y cumplimiento.	Idem
Integrar un gestor de llaves	Idem



Necesidad	Solución
Cifrar máquinas virtuales (vmdk / RAM) en la nube u on-premise	KeyControl
Cumplir con estandares de seguridad y cumplimiento.	Idem
Integrar un gestor de llaves	Idem
BYOK	Idem

ENTRUST
KeyControl

© Entrust Corporation

Descarga la prueba de KeyControl directamente de: https://go.entrust.com/HyTrust_KeyControl

ENTRUST

Entrust **KeyControl**, & **BYOK**, 3 pasos para gestionar tus claves en la nube.

01.

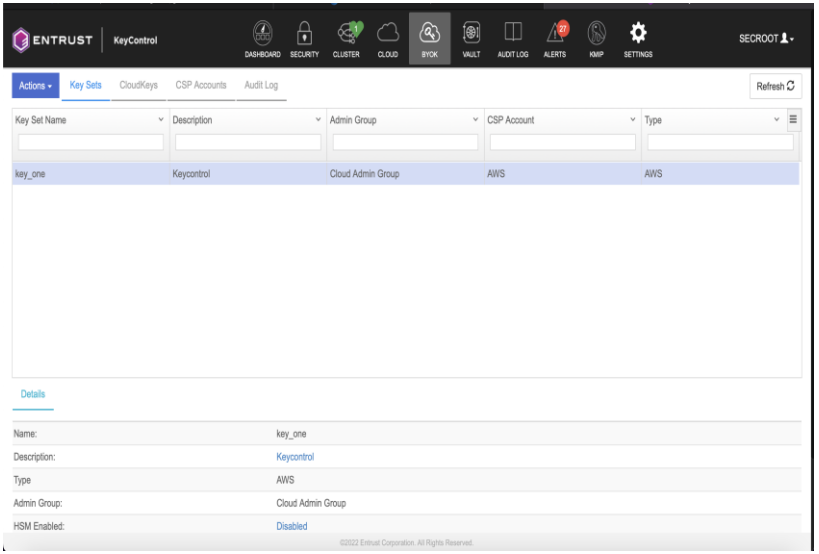
Entrust: Configura proveedor de nube y permisos de acceso

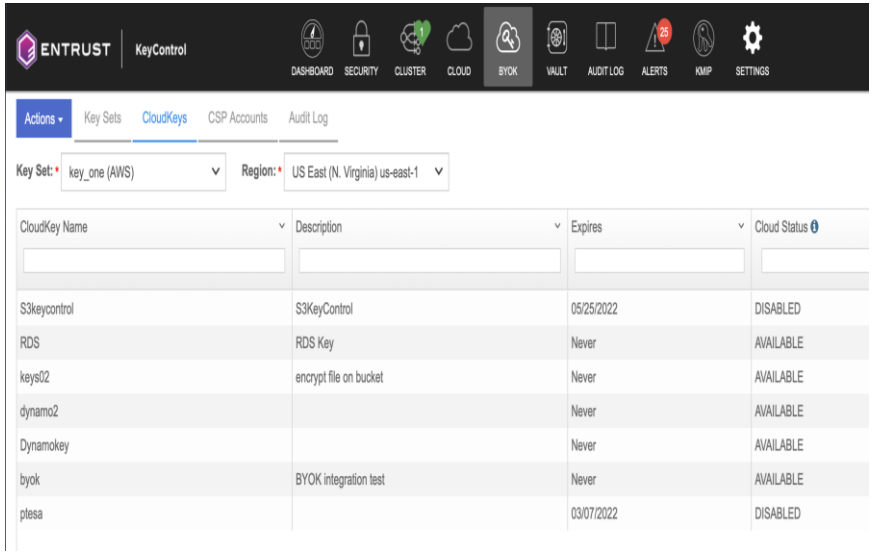
02.

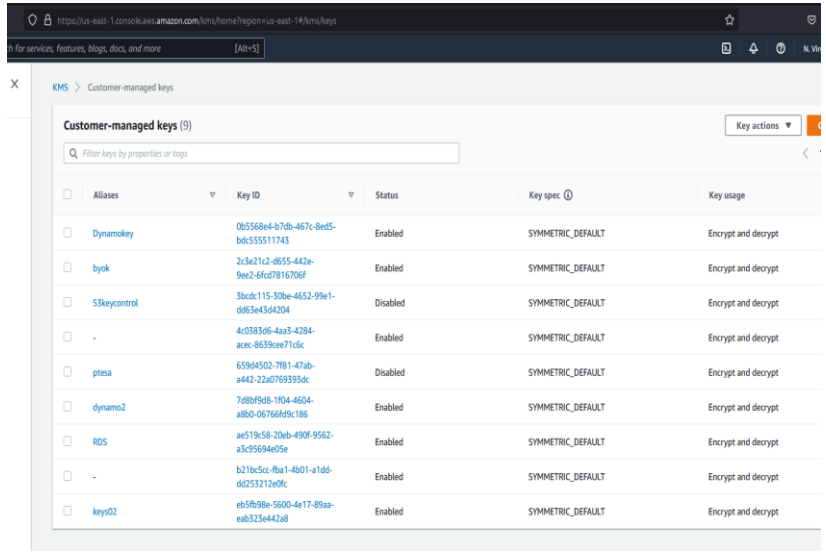
Entrust: Crea tus llaves.

03.

Entrust: Utiliza las llaves compartidas en el KMS







© Entrust Corporation

Descarga la prueba de KeyControl directamente de: https://go.entrust.com/HyTrust_KeyControl

ENTRUST

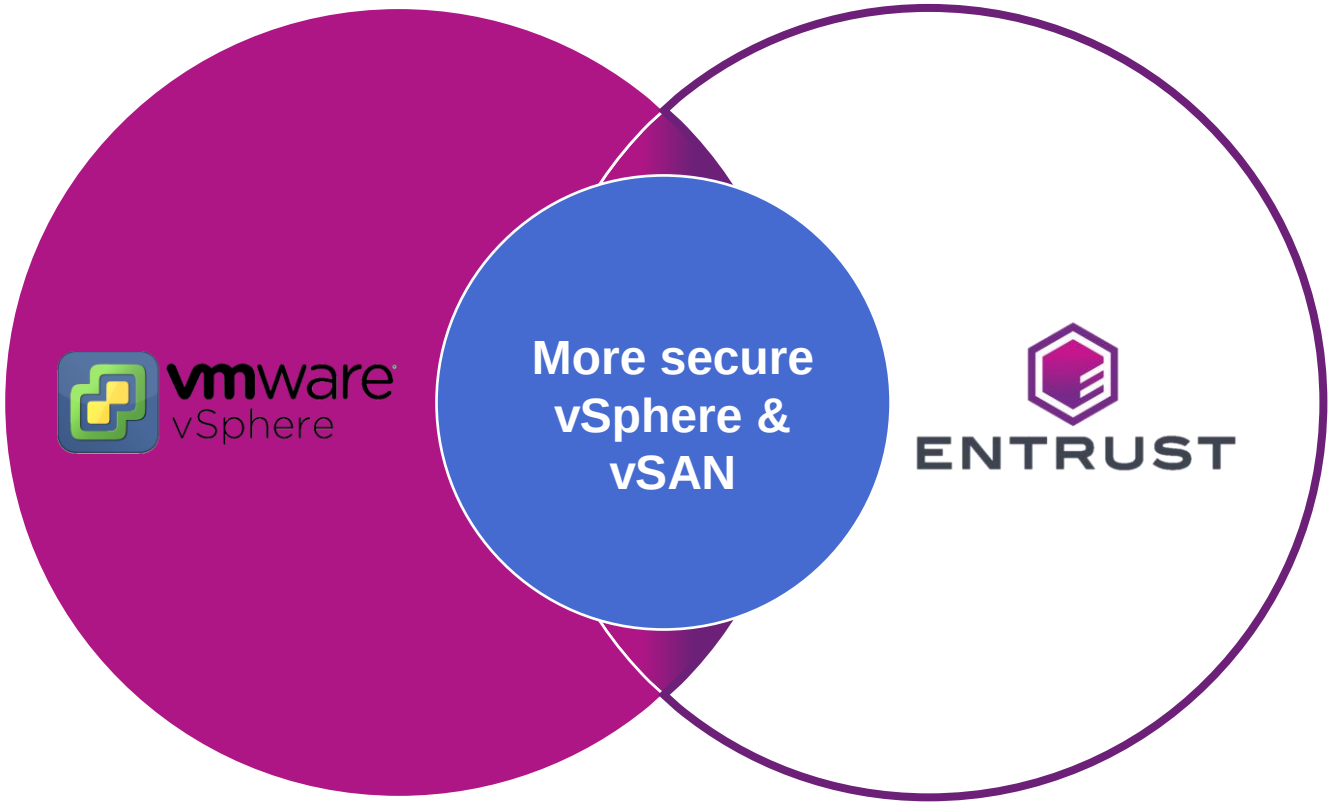
Entrust **KeyControl** / **KMS** para vCenter

La oferta

- **BYOK**, trae tu propia llave a la nube.
- Entrust KeyControl para vSphere & cifrado vSAN (**KMIP**)
- Incluye soporte para multiples nodos, clustered key, (para alta availability), admin/API interface.
- **Licenciamiento** perpetuo.

Casos de uso para el cifrado

- VM, estáticas, (no hay movimiento)
- Ambientes regulados (datos en reposo donde el cifrado es un requerimiento)



© Entrust Corporation

Descarga la prueba de KeyControl directamente de: https://go.entrust.com/HyTrust_KeyControl

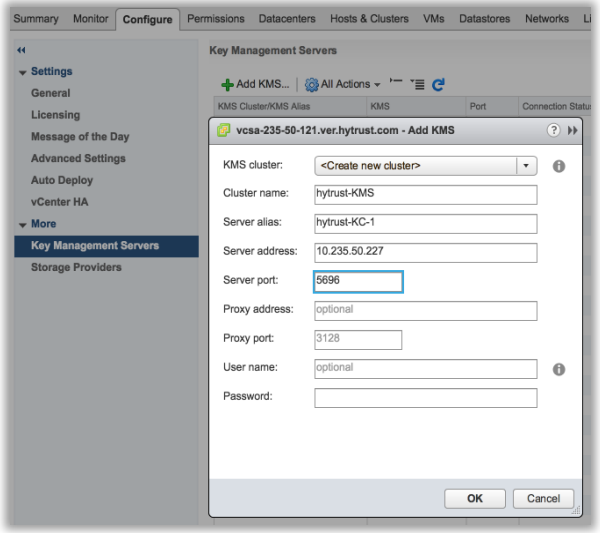
ENTRUST

Entrust **KeyControl** Time to Value con VMware, sólo 3 pasos !!!

01.

Entrust: Instala la imagen Entrust KeyControl OVA

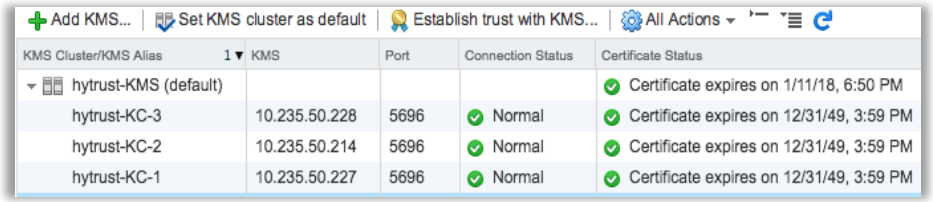
STEP 1



02.

VMware: Agrega Entrust KeyControl en el vCenter config

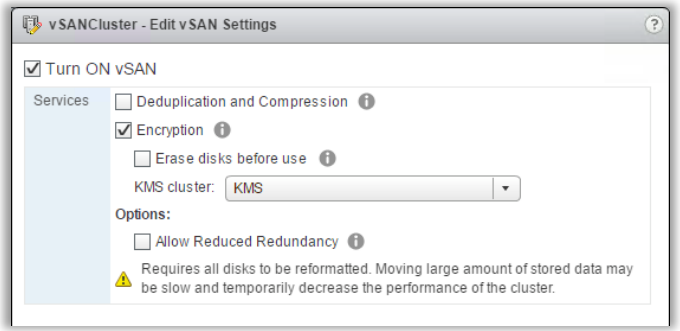
STEP 2



03.

VMware: Habillitar cifrado vSAN & cifrado para vSphere

STEP 3



© Entrust Corporation

Descarga la prueba de KeyControl directamente de: https://go.entrust.com/HyTrust_KeyControl

ENTRUST

Entrust Datacontrol para VMware

Habia una vez una partición en el servidor corporativo en la cual el CFO también guardaba la llave privada empresarial, alguién copio la partición completa del servidor, en un USB drive de 1 TB y sin querer, se llevo también la llave privada.

HYTRUST

ENTRUST
SECURING A WORLD IN MOTION

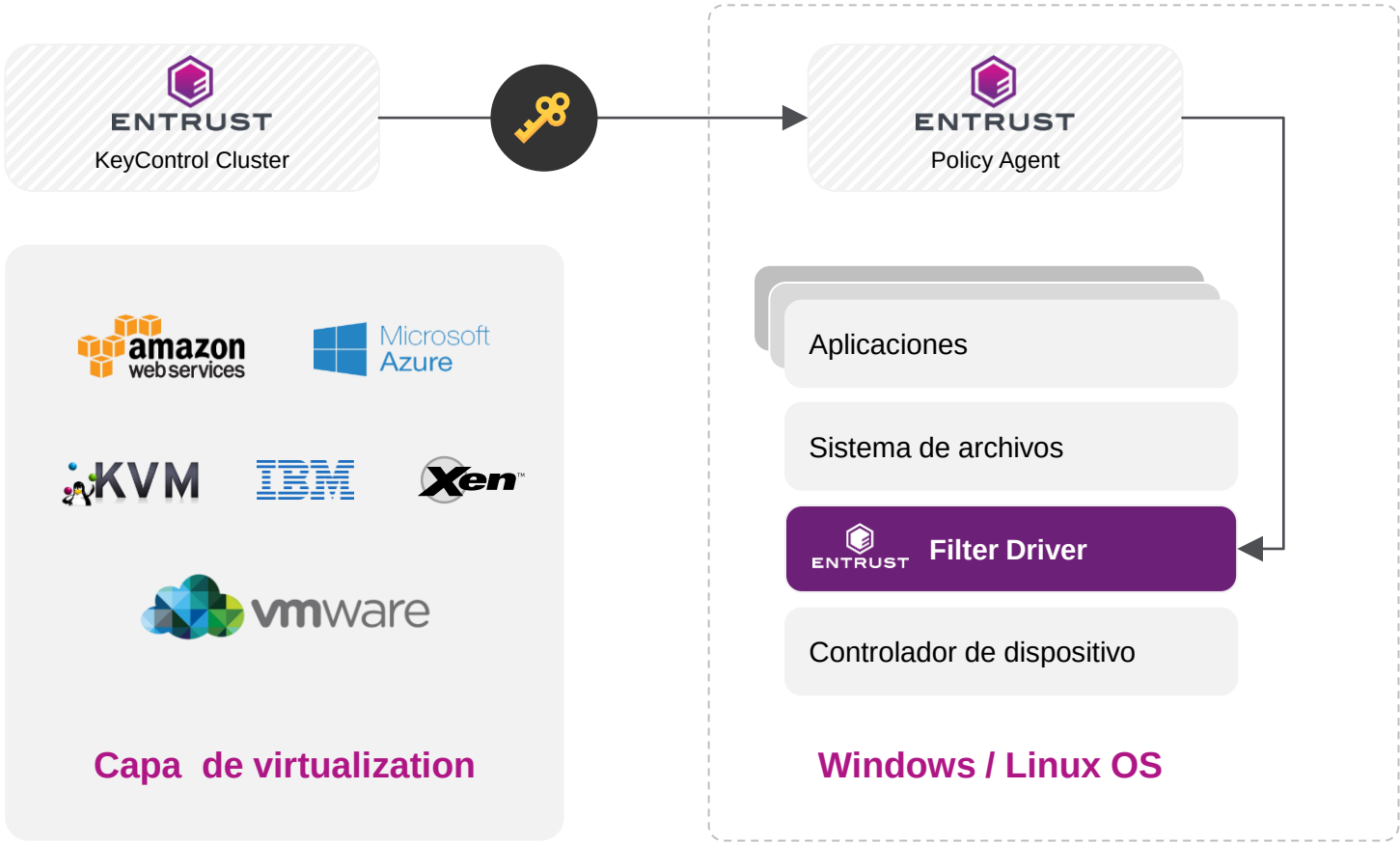
Entrust **DataControl**, Cómo funciona ?

KeyControl

- Gestor de claves empresarial
- KMIP Server

PolicyAgent

- Cifrado de discos y archivos para Linux y Windows



© Entrust Corporation

Descarga la prueba de KeyControl directamente de: https://go.entrust.com/HyTrust_KeyControl

ENTRUST

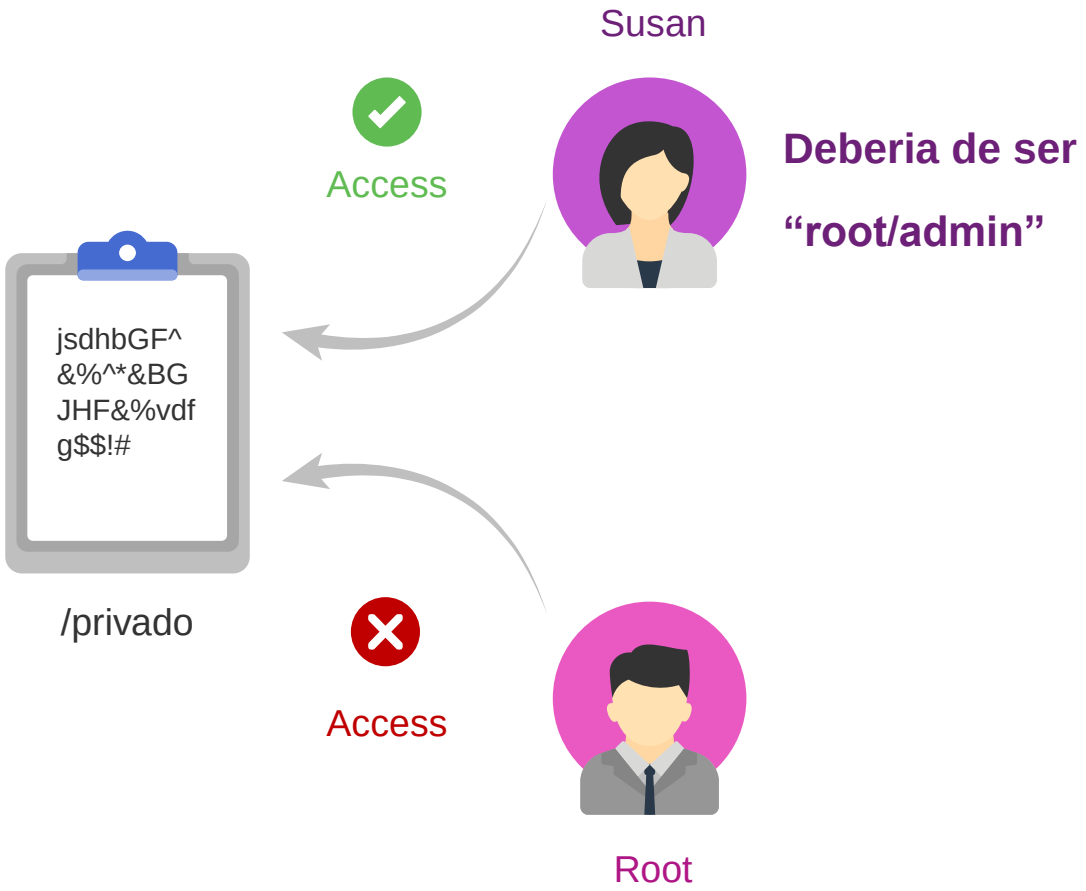
Entrust **DataControl** asignando control de acceso a directorios / particiones

Previene el acceso de administradores a particiones cifradas

Define específicamente quién puede y quién no puede **acceder a los datos de texto claro**

Las politicas pueden ser **actualizadas fácilmente**

Soporte para Windows & Linux



© Entrust Corporation

ENTRUST

El cifrado en la practica…..

Cifrado de Base de Datos

Cifrado de archivos

Firmas Digitales / certificados

Dispositivos IoT

Blockchain

Pagos digitales

SSL

PKI

TODAS ESTAS SOLUCIONES UTILIZAN Al MENOS UNA CLAVE !!

© Entrust Corporation

ENTRUST

A todo esto, cómo puedes crear y proteger tus claves de cifrado?

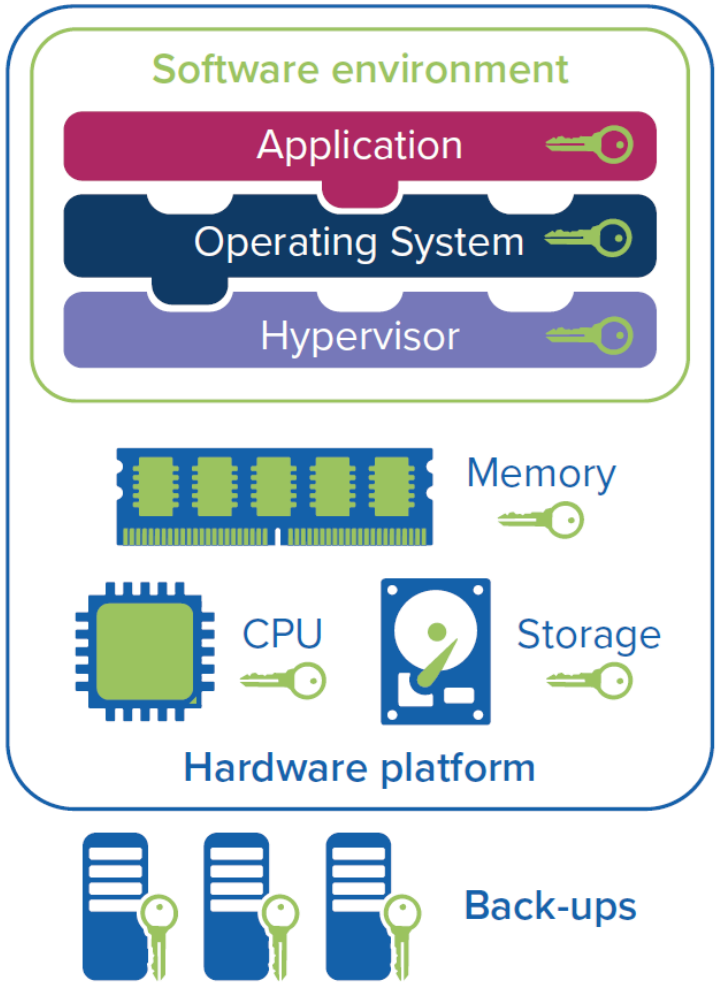
Crea y protege tus claves en un HSM, el cuál es un dispositivo especificamente diseñado y certificado para crear y proteger claves de cifrado.

Preferiblemente uno fabricado por Entrust

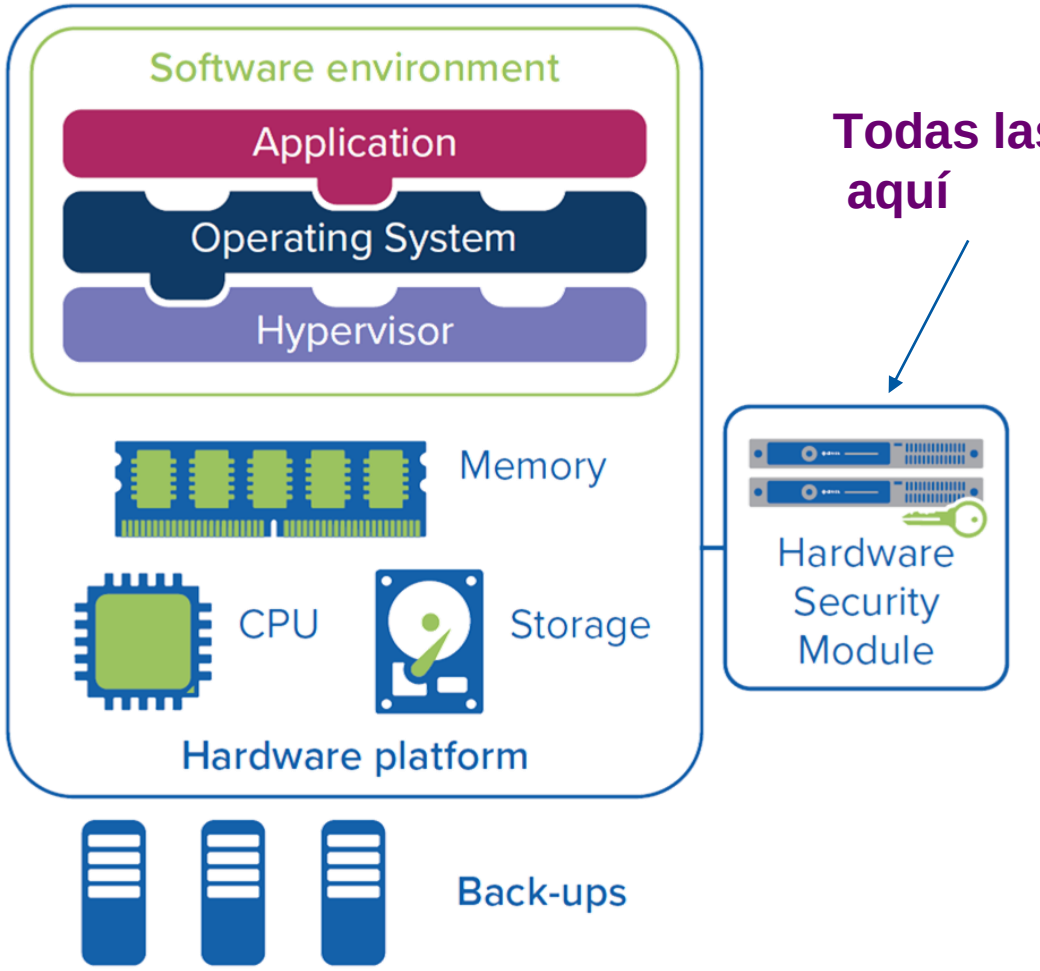
© Entrust Corporation

Y la clave….la clave….donde está la CLAVE?

Sin un HSM



Con un HSM

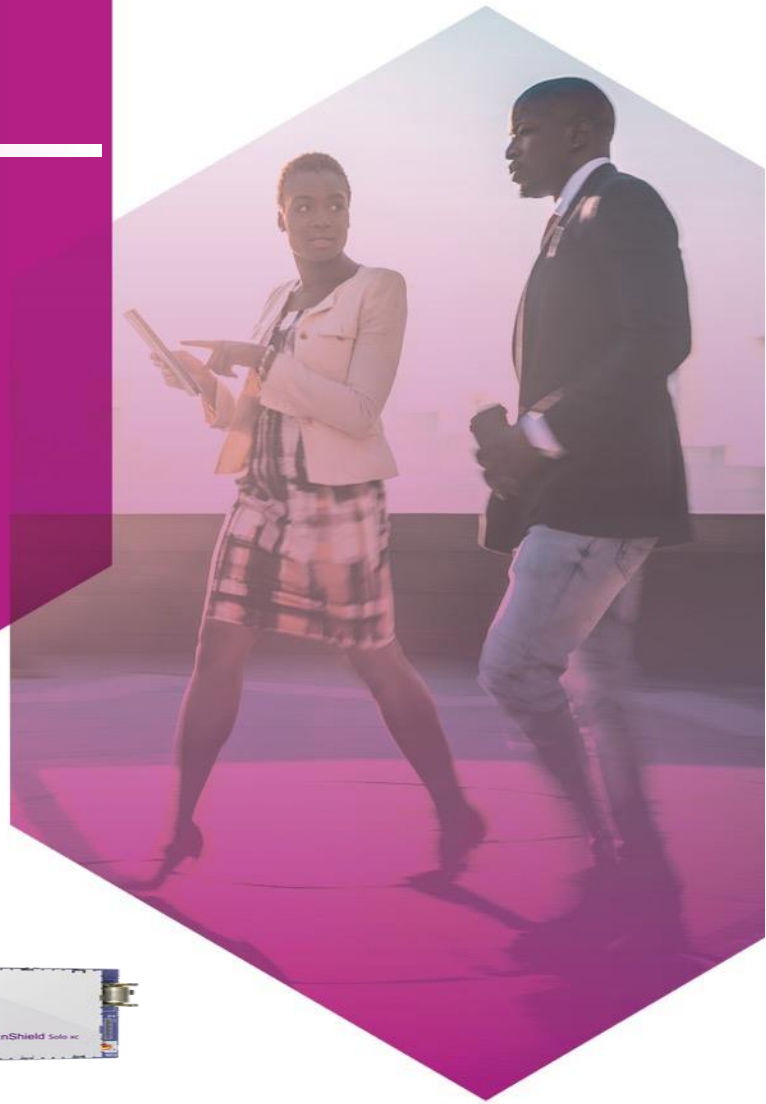


Todas las CLAVES viven aquí

© Entrust Corporation

A TODO ESTO, CÓMO PUEDES PROTEGER TUS CLAVES…… ?

Securing a world in motion



nShield Connect

nShield Edge

Low cost, portable

nShield Solo

Preferiblemente uno fabricado por Entrust

Sencilles y flexibilidad, recuerdan K.I.S.S. ?

- Protección y creación de llaves práctivamente ilimitada.
- Integración sencilla con PKCS11, JCE, OpenSSL, etc
- Separación de roles, privilegios y segregación de claves para los aplicativos.
- Bajo costo de mantenimiento.
- API / Interface para consumo de servicios web
- Codesafe, tú código corriendo directamente en el HSM

© Entrust Corporation

Portafolio de productos de protección de datos

Intellitrust

IdentityGuard

Identity Essentials

Hardware Security Modules (HSMs)

Public Key Infrastructure (PKI)

Internet of Things (IoT) Security

Identity and Access Management

Digital Certificates and Signing

ENTRUST

CONCLUSION:

EL CIFRADO NO DEBE DE SER COMPLICADO, EN ENTRUST TENEMOS UN CONJUNTO DE SOLUCIONES COMPLETAS INTEGRADAS, QUE VAN MAS ALLÁ DE OFRECER PKI, AUTENTICACIÓN Y HSMS.

ENTRUST
SECURING A WORLD IN MOTION