Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

INTELIGENCIA DE SEGURIDAD COOPERATIVA

PARA LAS ESTRATEGIAS DE GOBIERNO ABIERTO

Maydeli Solorio

Account Manager Gobierno

Octubre 2014

ALIANZA PARA EL GOBIERNO ABIERTO
MÉXICO

Responsabilidad del Gobierno Abierto Materia TIC

- **Alineación con Estrategia Digital Nacional**
- **Habilitador alcanzar las metas de conectividad Nacional**
- **Homologar Sistemas/ Nuevas Tecnologías**
- **Lograr Transparencia**
- **Interacción**
- **Indicadores Claros**

PLAN DE ACCIÓN
2013—2015
MÉXICO
UNA NUEVA RELACIÓN ENTRE SOCIEDAD Y GOBIERNO

Alcances

Lineamientos - Publicación Datos Abiertos

Medios Acceso Públicos a los Datos Abiertos

Mecanismos de Retroalimentación y Participación

Iniciativas de fomento al uso de Datos Sociedad y Gob.

Garantías a la privacidad de quien aporta, usa y reutiliza

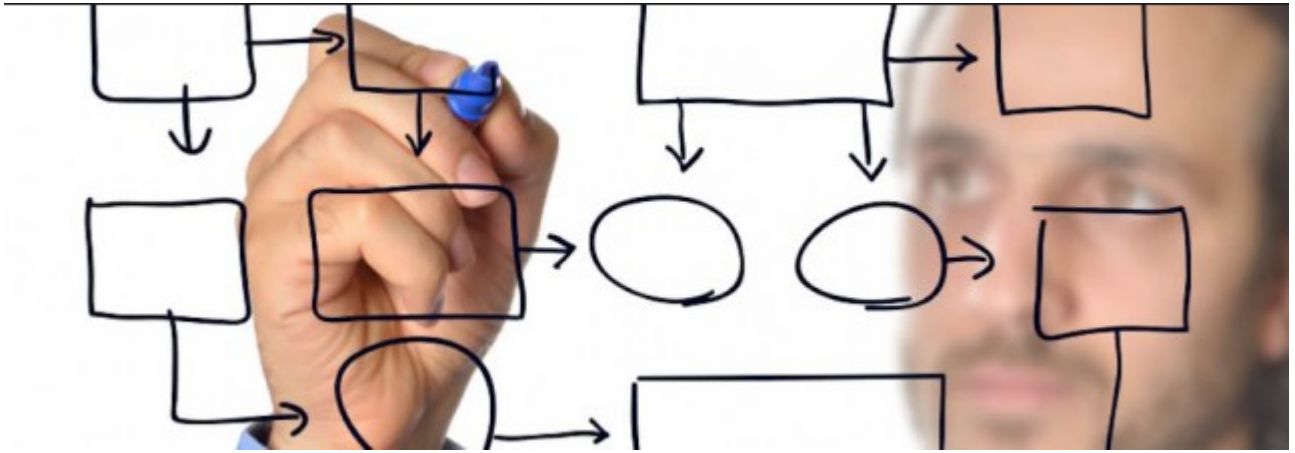
Alineación Estrategia Digital Nacional

POLÍTICA TIC

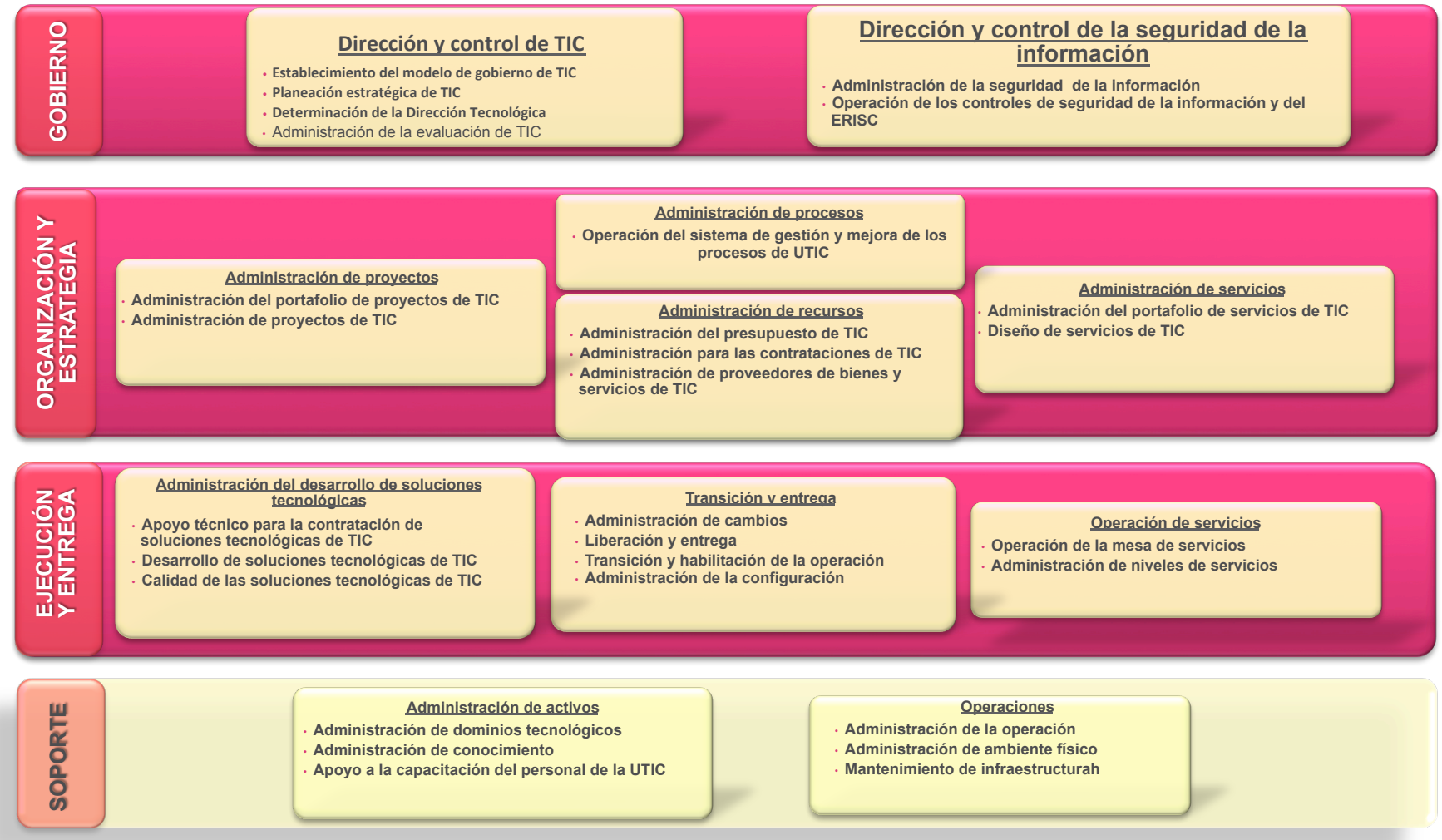
Las Instituciones deberán **compartir** servicios e infraestructura en todos los dominios tecnológicos, favoreciendo la **consolidación** y considerando la **seguridad** de la información de manera transversal.

MAAGTIC-SI

Directiva a nivel gobierno, enfoque a homologar Gestión y Gobernabilidad de las TIC´s en la Administración pública



Marco Rector del MAAGTIC-SI



4 Niveles de gestión, 11 grupos de procesos y 29 procesos

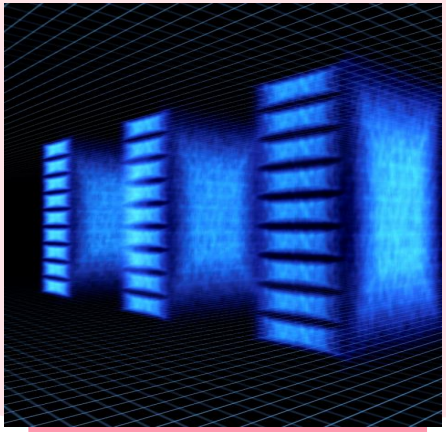
MAAGTIC – SI: Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información

TIC: Tecnologías de la Información y Comunicaciones

UTIC: Unidad Administrativa de TIC (Responsable de proveer de infraestructura y servicios de TIC a las demás áreas del RAN)

ERISC: Equipo de Respuesta a Incidentes de la Seguridad en TIC

La tecnología…



Virtualización

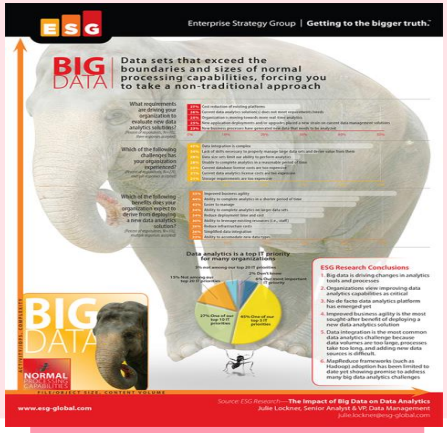
de Servers, Networking & Storage llegará a un 75%*

*IDC Predictions 2013

Consideración de Servicios en la nube

80% Aplic. serán etregadas por esa vía en 2015*

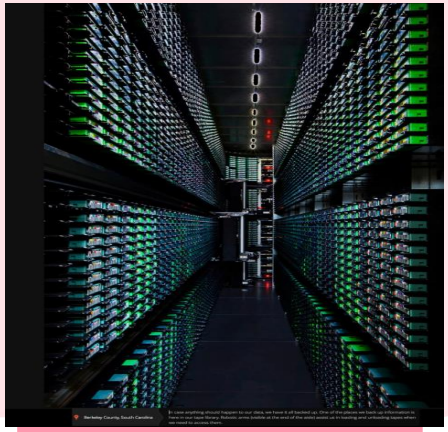
*Gartner 2013 Predictions



Aplicabilidad del Big Data

Crecimiciento 72% *

*ESG: Impact of Big Data on Analytics



Datacenter

Componentes bajo el concepto Software-Defined*

*VMware CTO Keynote 2012

La Importancia de la Seguridad de la información en el Desarrollo Económico

- Las tecnologías de Información en las últimas décadas han ido cambiando constantemente la dinámica operación, derivado de la creación de nuevos modelos, lo que ha requerido un constante flujo de información entre usuarios y entidades.

INFORMACIÓN

- Crea la necesidad de contar con nuevos procesos y flujos dependientes de la identificación de los mismos a través de la transferencia de datos globalmente para consultar, proveer o adquirir un servicio.

Integridad, Confidencialidad y Protección de Datos

Titular

La persona física a quien corresponden los datos personales.

Datos Personales

Cualquier información concerniente a una persona física identificada o identificable.

Datos Personales Sensibles

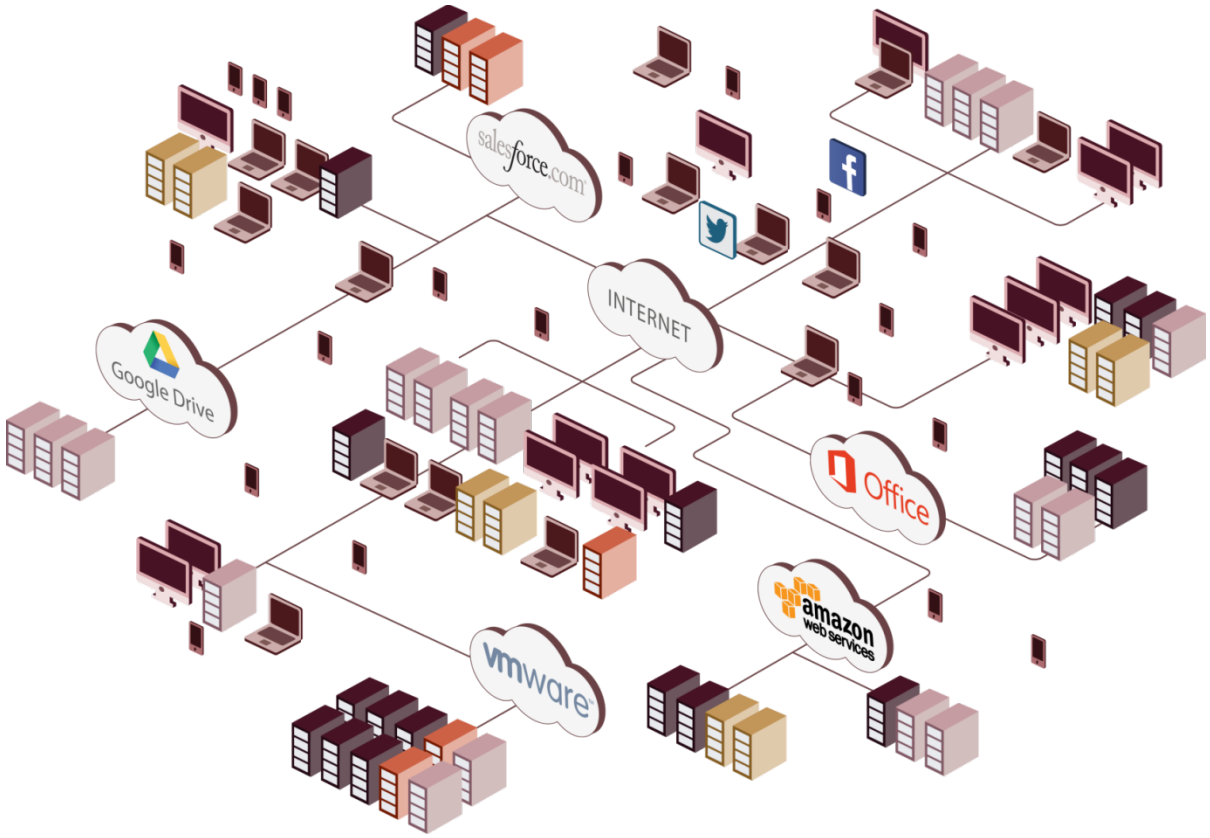
Aquellos Datos Personales que afecten a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

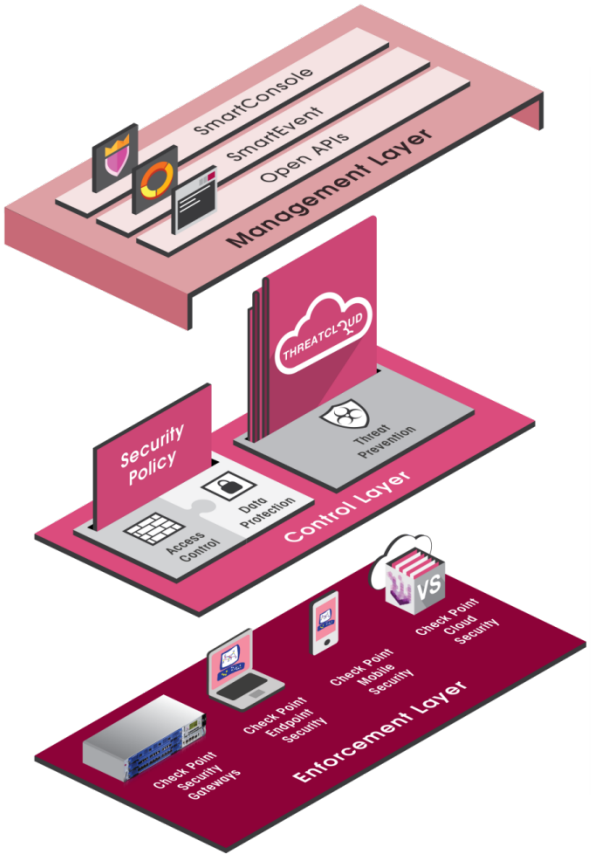
La información de la entidad, de los usuarios y la personal, es el *ACTIVO MAS* importante y por ende hay que protegerlo.

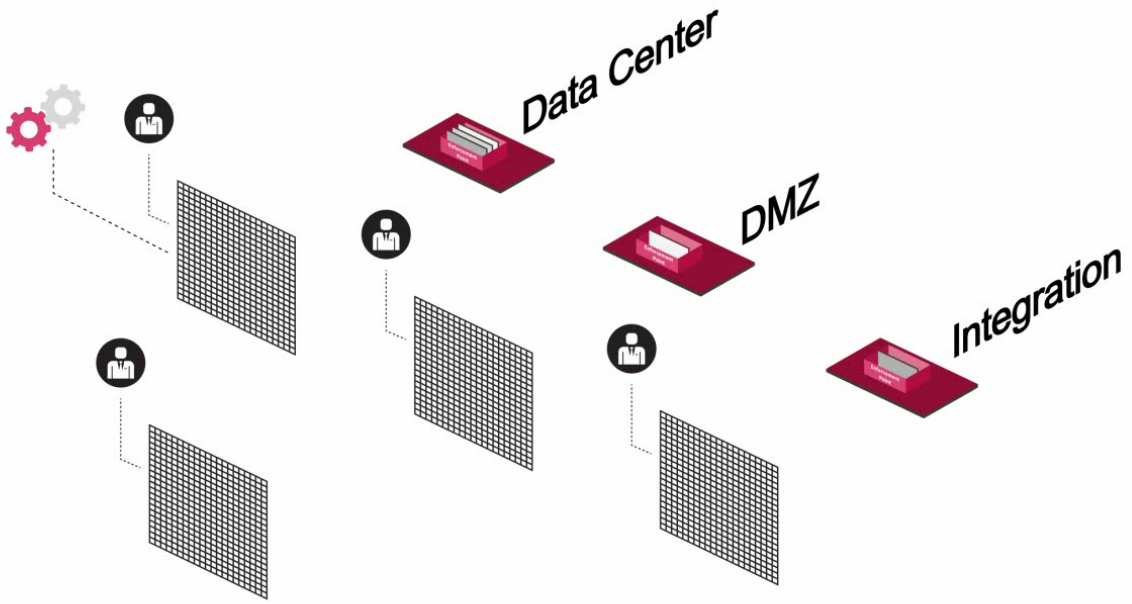
"La *Clasificación de la Información* es clave para cualquier entidad"

¿Como brindar un escenario a entidades y usuarios con enfoque en seguridad?

¿Como proteger ambientes sin fronteras bien definidas?







Software Defined Protection sugiere que los ambientes estén: **Segmentados**

LA SEGMENTACION ES EL NUEVO PERIMETRO

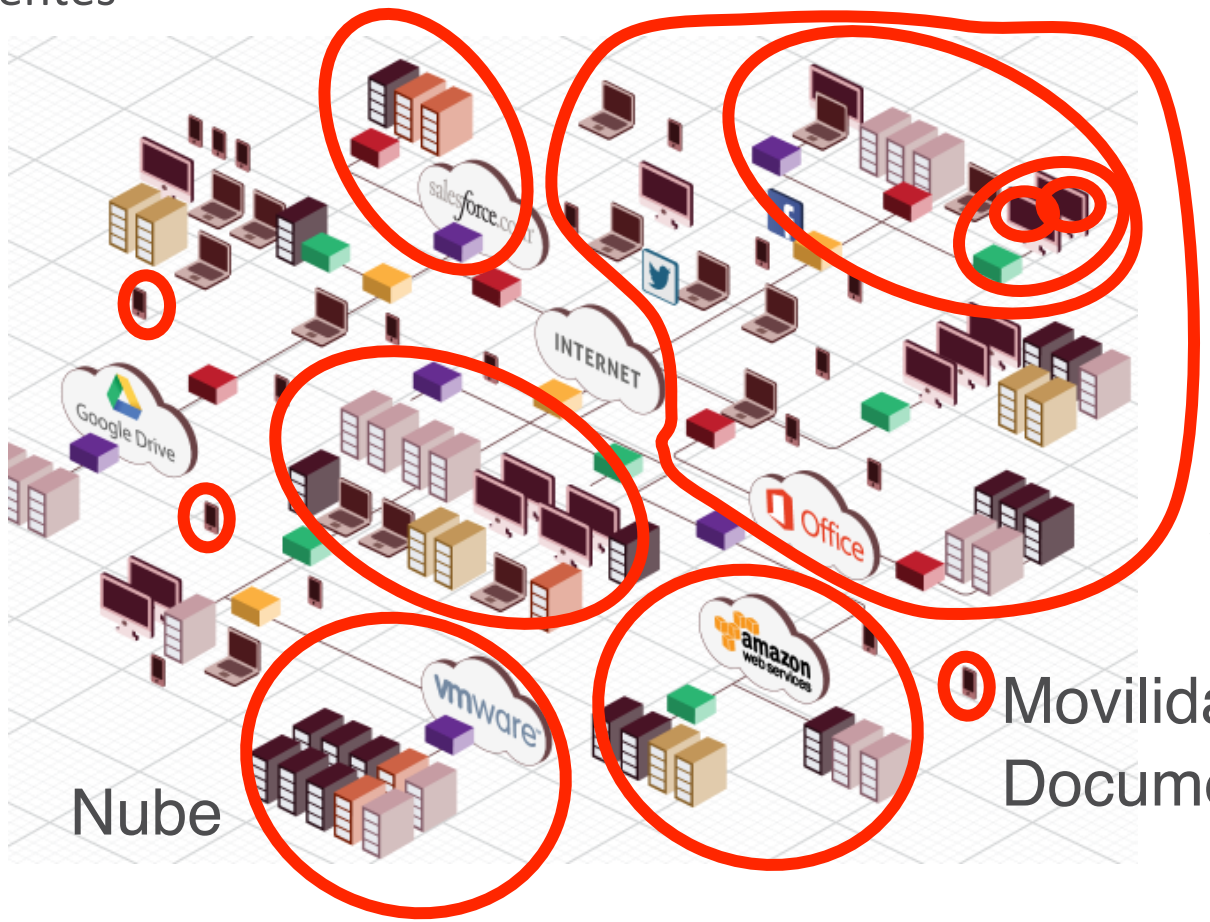
En las **REDES DE HOY**, no se presenta un perímetro como lo conocíamos anteriormente.

Smartphones, la Nube y el movimiento de **DATOS** en la NUBE en Redes bajo múltiples ambientes de cómputo sin fronteras.

SOFTWARE DEFINED PROTECTION

Check Point SOFTWARE TECHNOLOGIES LTD.

"Establecer líneas jerárquicas de defensa que proporcionan protecciones para datos y los sistemas alojados dentro de los límites de los segmentos correspondientes"



METODOLOGIA PARA LA SEGMENTACION

PASO 1

ATOMIZACION DE SEGMENTOS

Elementos que comparten la misma política y necesidades de protección

PASO 2

AGRUPAMIENTO DE SEGMENTOS

Agrupamiento de Segmentos que permiten una protección modular

PASO 3

CONSOLIDACIÓN

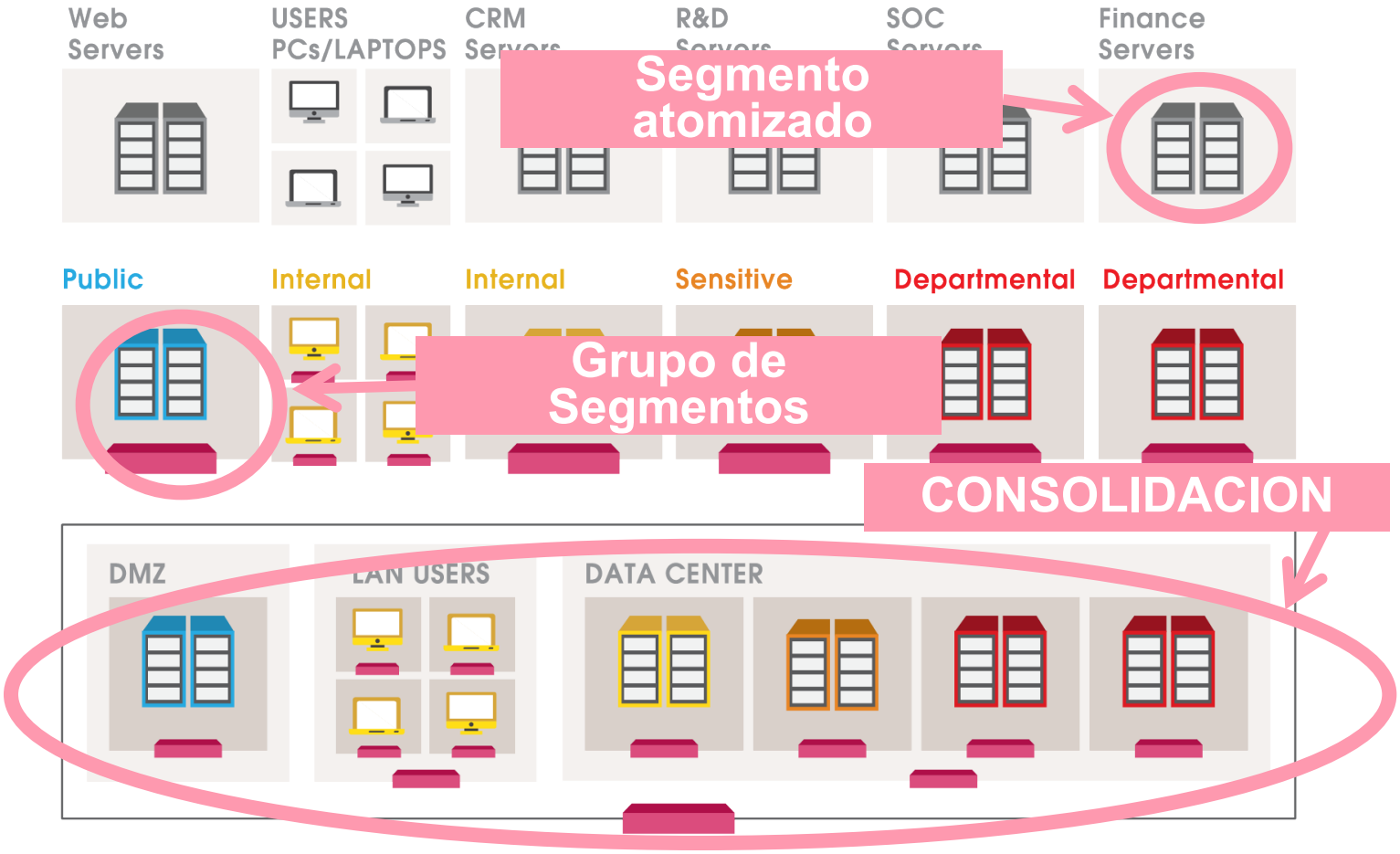
Proteger las interacciones y flujos de datos entre los segmentos

PASO 4

CANALES CONFIABLES

De los componentes físicos y virtuales

SEGMENTANDO LA RED



Segmentos: su objetivo

Cuando se determina segmentar las fronteras en un ambiente virtual o nube privada, hay que hacerse estas preguntas:

- ¿Las entidades tienen las **mismas autorizaciones**?
- ¿Soportan los mismos **procesos de negocio**?
- ¿Se manejan **activos similares**?
- ¿Reciben el **mismo nivel de protecciones** de seguridad?

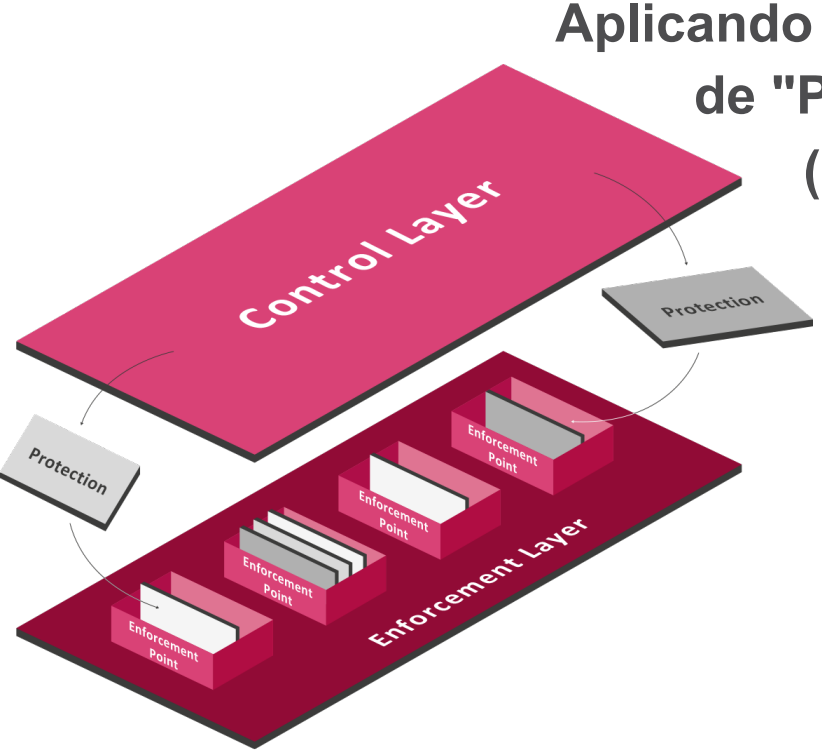
CONTROL LAYER

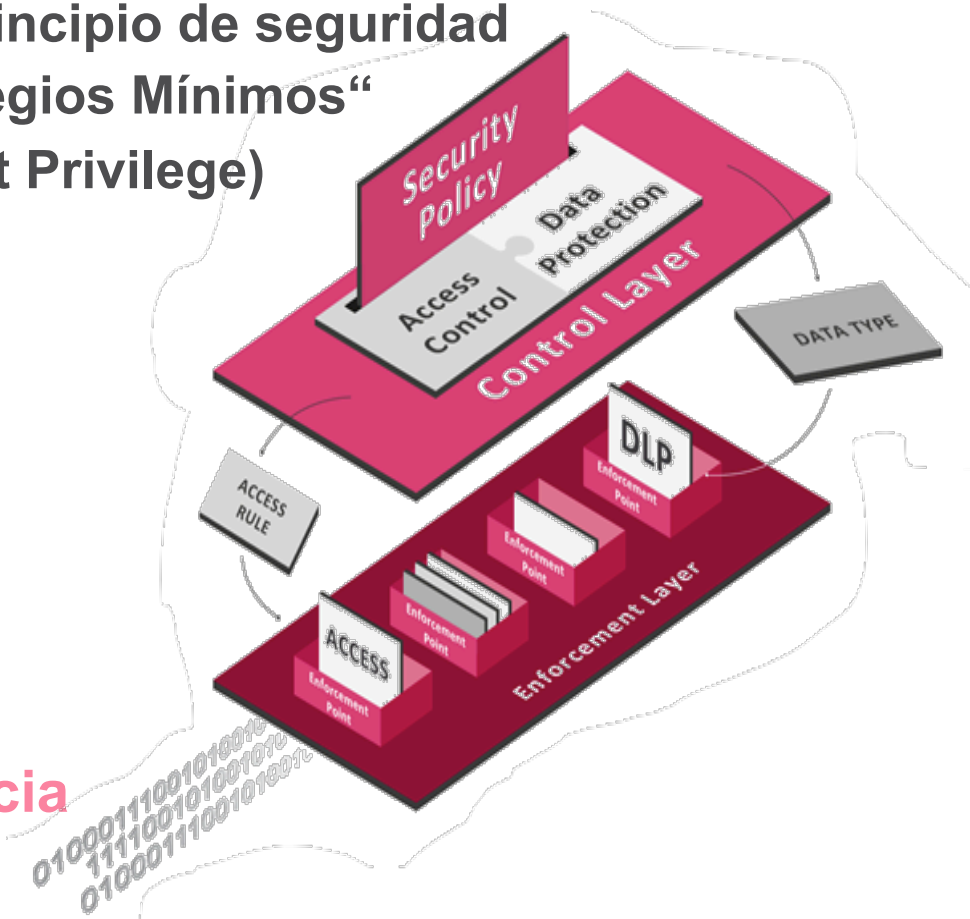
Genera protecciones **DEFINIDAS EN SOFTWARE** y las implementa en una forma apropiada en los puntos de **ENFORCEMENT**.

Capa de Control
Protecciones inteligentes basadas en el contexto

Controla la interacción entre usuarios, activos, datos e información

Aplicando el principio de seguridad de "Privilegios Mínimos“ (Least Privilege)

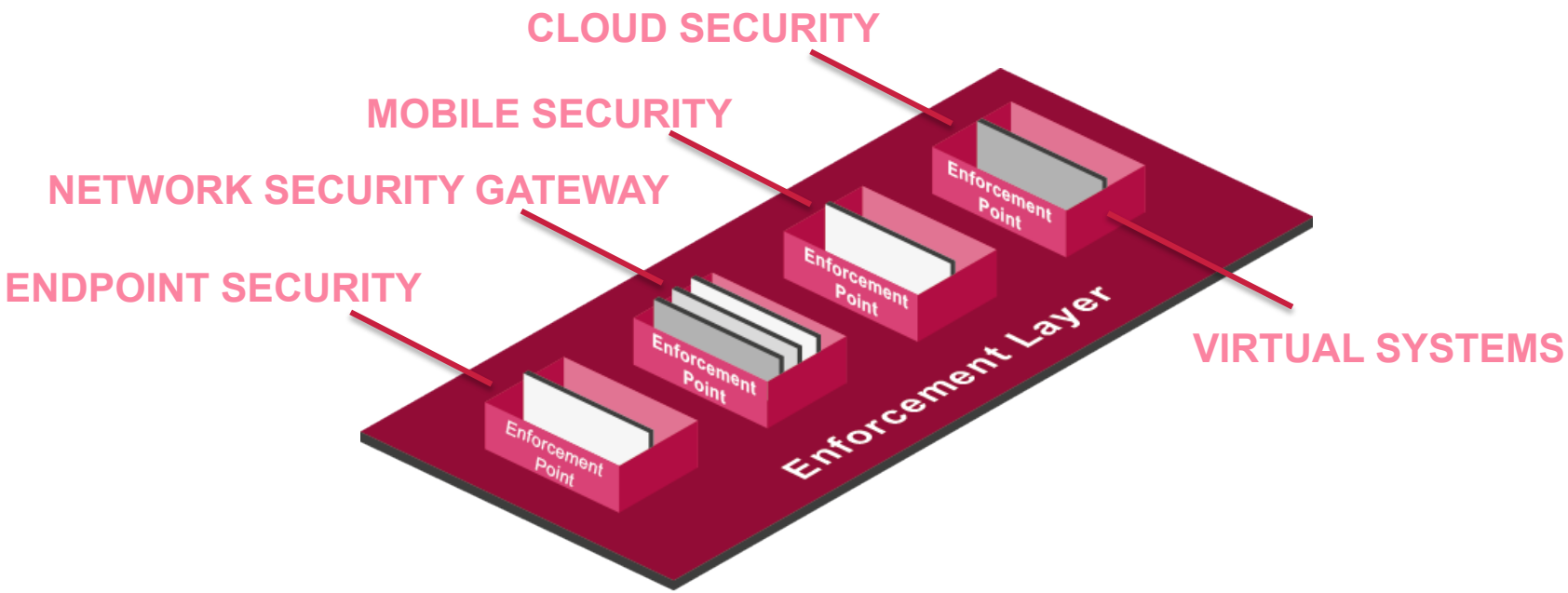




Protege los datos en transferencia y almacenamiento

Capa de Enforcement

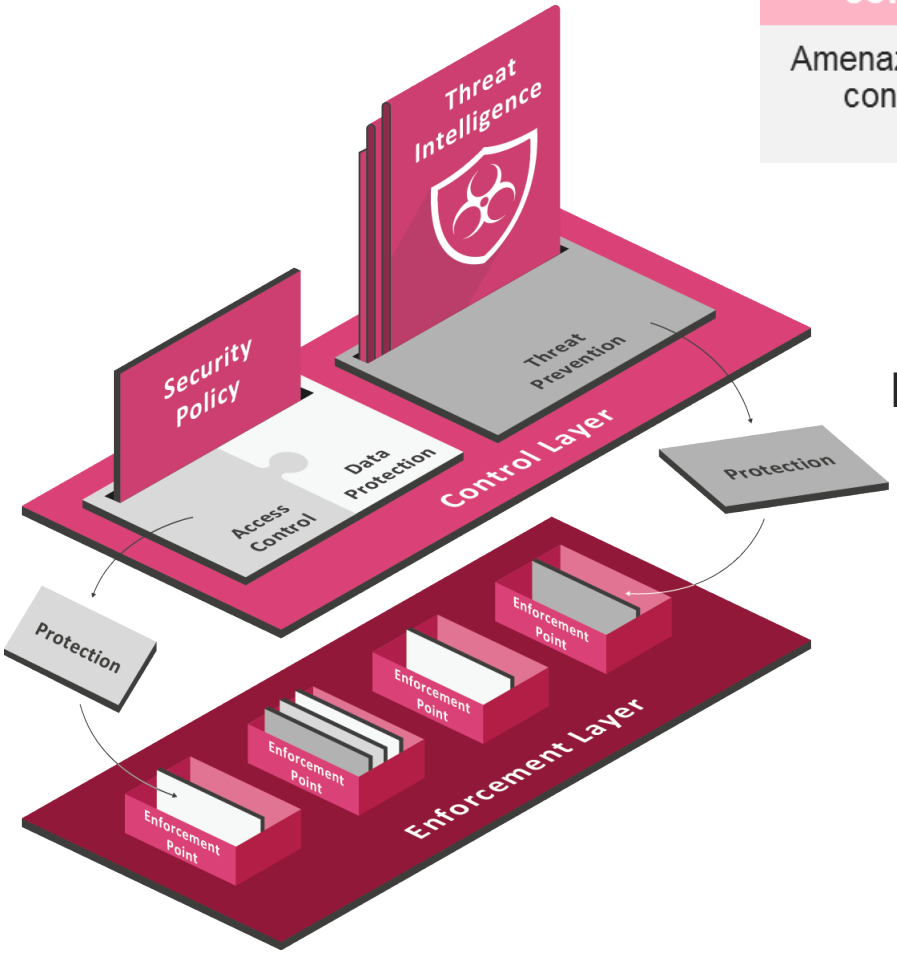
Los puntos de Enforcement son **MEDIADORES** en las interaccciones entre usuarios y sistemas **EJECUTANDO** protecciones



¿Qué hay respecto de las AMENAZAS?

LAS NUEVAS AMENAZAS QUE NECESITAMOS PREVENIR

Conozco lo conocido	Conozco lo desconocido	Desconozco lo no conocido
Amenazas que las conocemos	Amenazas que aún no conocemos	Amenazas que no no sabemos de su existencia



Protecciones actualizadas en **TIEMPO-REAL**

Utilizando los mismos puntos de enforcement para protecciones dinámicas contra amenazas

Vulnerabilidades Día-Cero

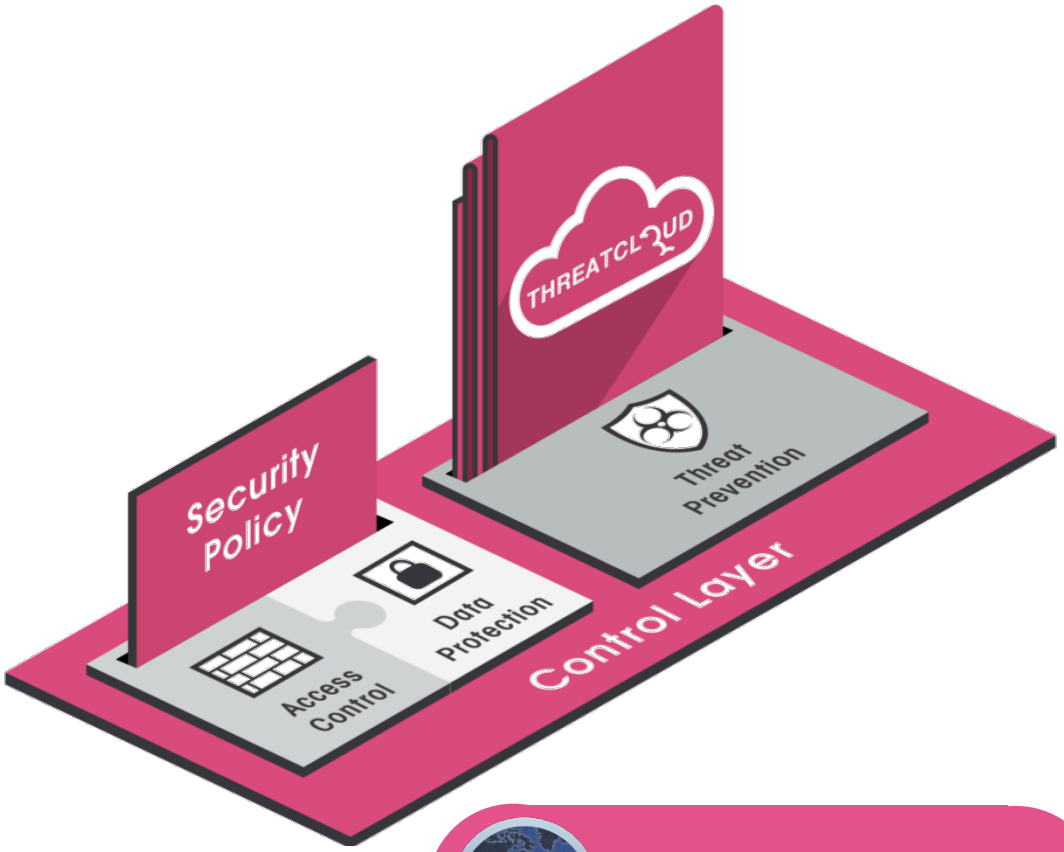
Nuevas Vulnerabilidades

Miles de nuevas variantes

"Cerca de 200,000 nuevas variantes de Malware aparecen en forma global cada día"

- net-security.org, June 2014

Protección Multicapa y Holística



- Antivirus
- IPS
- Anti-Bot
- Threat Emulation (Sandboxing)
- Movilidad
- Seguridad en Documentos

Multi-Layer Threat Prevention

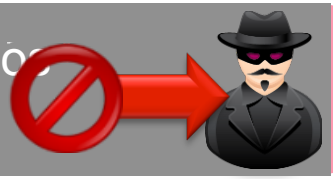
CONOCIDO

DESCONOCIDO

Antivirus — Bloqueo de archivos infectados con código malicioso conocido

IPS — Virtual Patching & contención contra Exploits

Anti-Bot — Prevención de daños provocados por Bots en equipos infectados

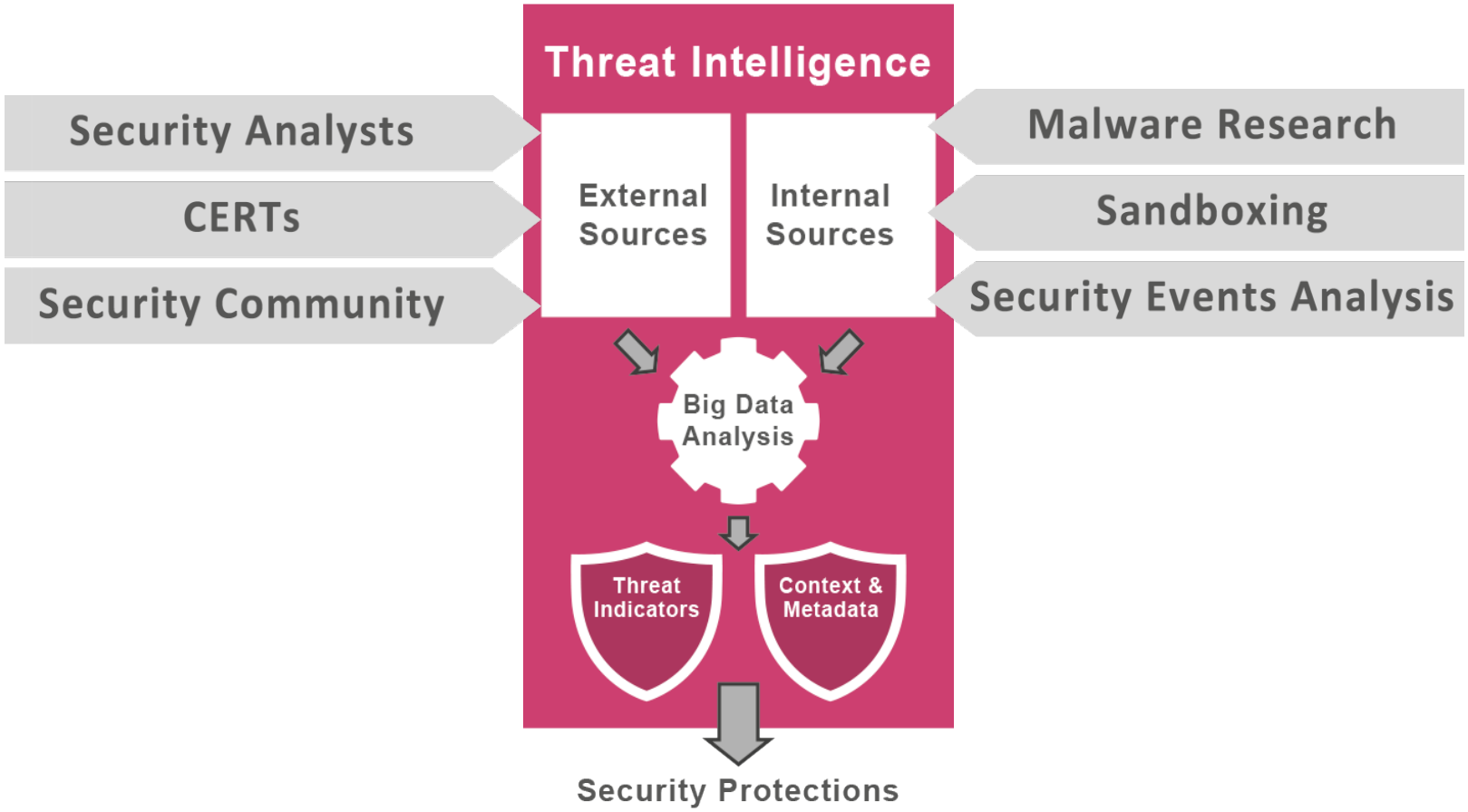


Threat Emulation — Detiene codigo malicioso y sus variantes vs ataques dia cero.

UNA EFECTIVA PREVENCION DE AMENAZAS ESTA BASADA EN LA INTELIGENCIA

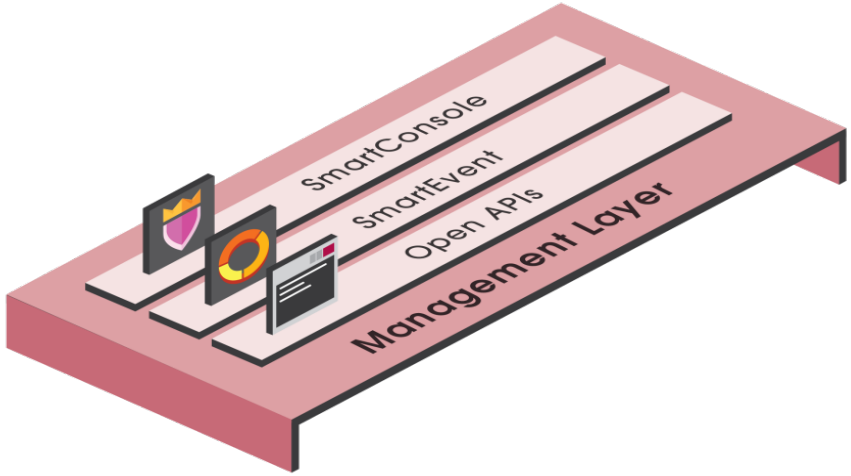
INTELIGENCIA CONTRA AMENAZAS

INTELIGENCIA abierta y colaborativa en **TIEMPO REAL** que permite la generacion de distintas protecciones de **SEGURIDAD**.



Capa de Gestión y Administración

Brinda a la arquitectura de SDP la **gestión** haciendo la integración de la seguridad con los procesos de negocio



MODULARIDAD

Soporta la segmentacion y segregacion de los roles de administración

AUTOMATIZACION

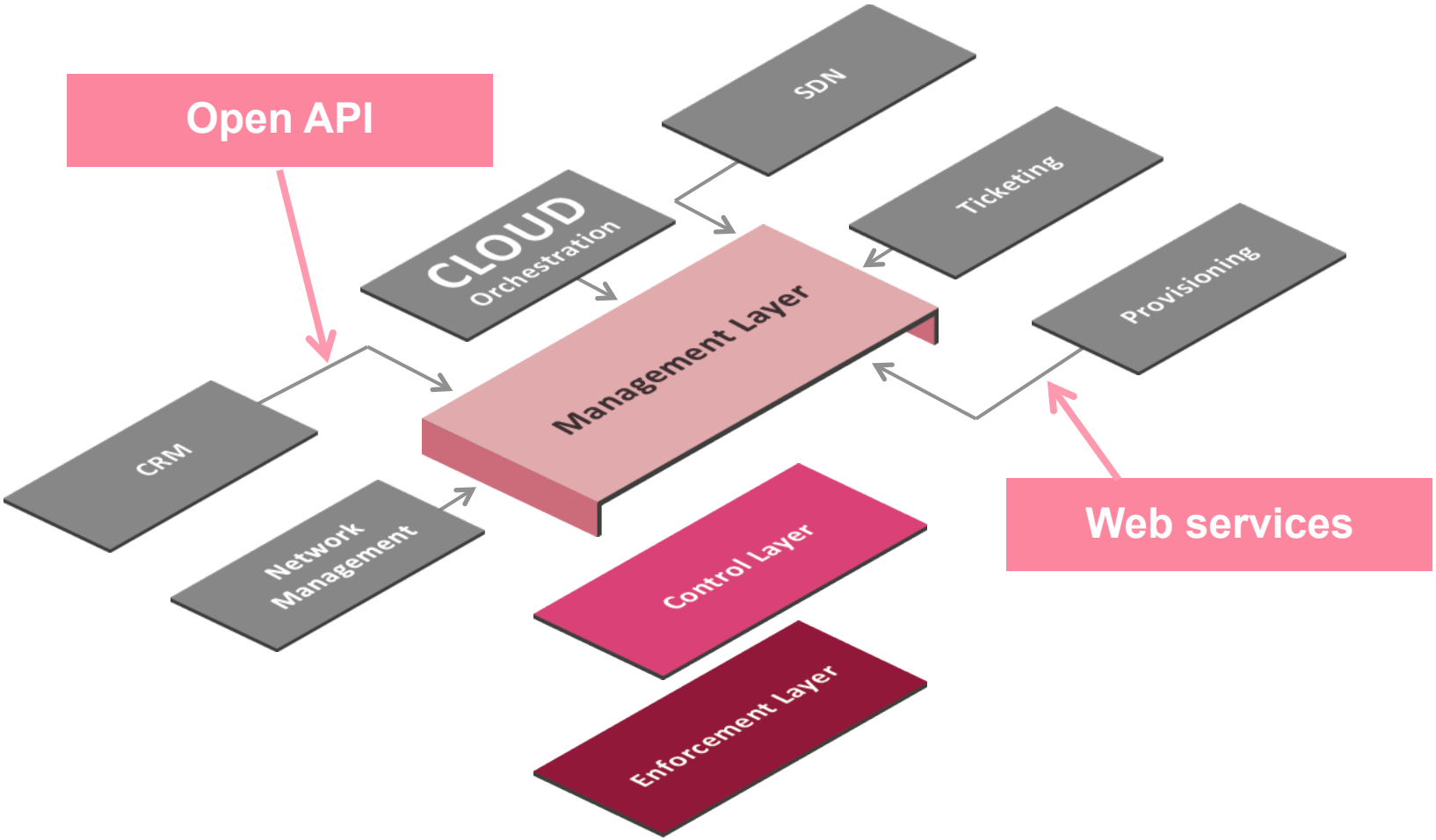
Automatiza la administración de las políticas de seguridad y sincroniza con los demás sistemas

VISIBILIDAD

360 grados de conocimiento de la situación y postura de seguridad

Automatización y Orquestación

INTERFACES ABIERTAS para soportar procesos y cambios de negocios (API/CLI)



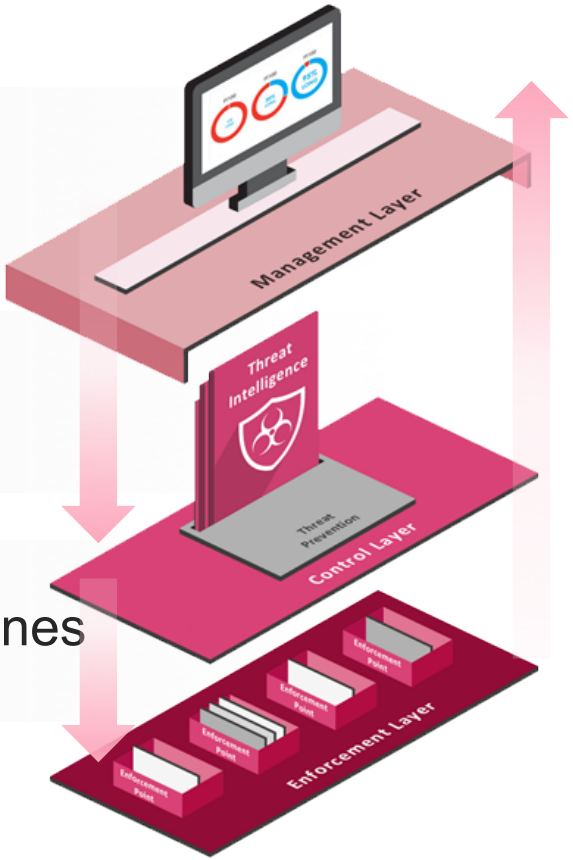
VISIBILIDAD

CONOCIMIENTO DE LA SITUACION & RESPUESTA AL INCIDENTE

Colecta informacion desde cada punto de enforcement

Percepción de la situación

Generación de nuevas protecciones



SOFTWARE – DEFINED PROTECTION

ARUITECTURA DE SEGURIDAD
MODULAR Y DINAMICA

APLICACION E INTEGRACION RAPIDA Y CONFIABLE CON
INTELIGENCIA EN TIEMPO REAL

ARQUITECTURA DE SEGURIDAD DEL HOY PARA
LAS AMENAZAS DEL MAÑANA

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

¡Muchas Gracias!

www.checkpoint.com