

Resolviendo el puzzle de GDPR

José de la Cruz González
Technical Director Iberia





Se acerca el GDPR

Armonizar
reglamento



Protección de
datos personales

Aplica a quien
procese datos de
ciudadanos de la
UE

DE OBLIGATORIO CUMPLIMIENTO

Puntos Clave



Protección por diseño



Procesamiento de datos seguro.



La fuga de datos debe ser comunicada



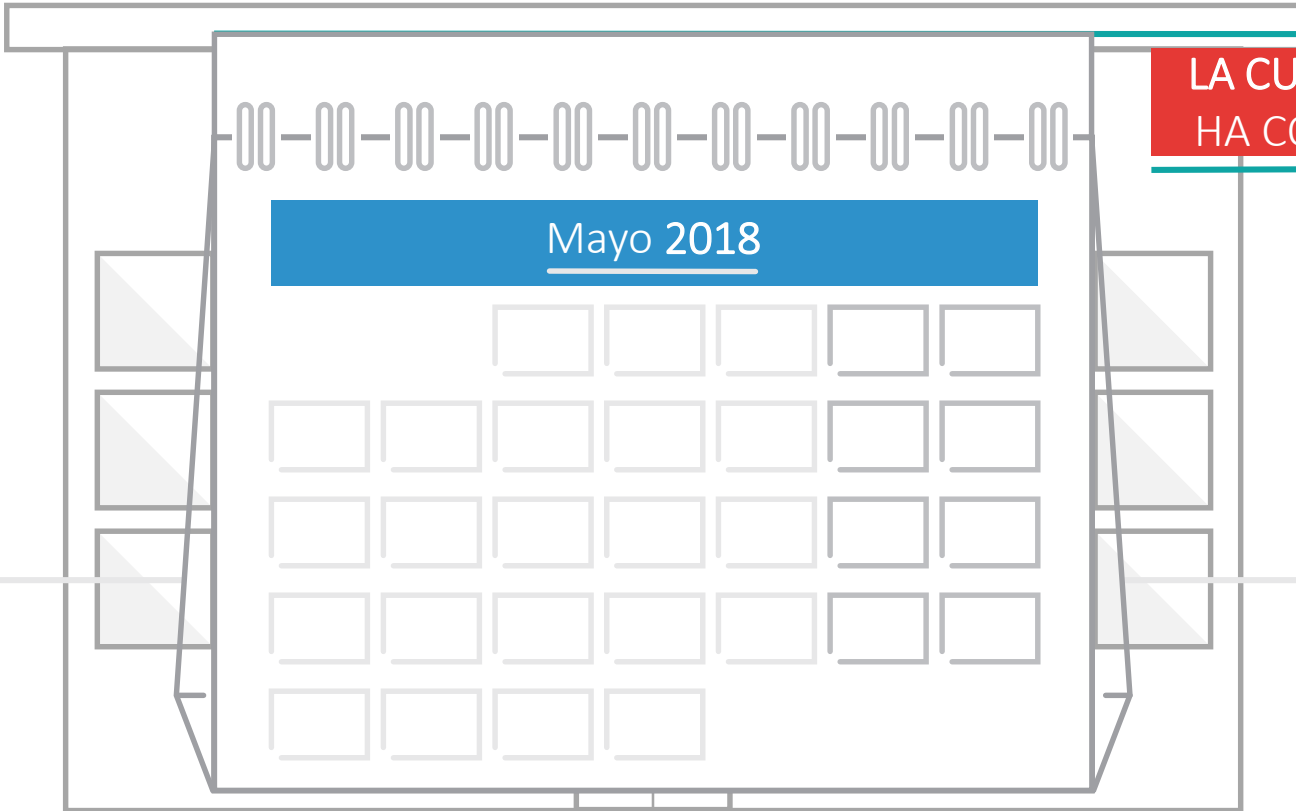
La seguridad debe ser evaluada

Consecuencias del GDPR





Retos



LA CUENTA ATRÁS
HA COMENZADO

Mayo 2018



Preparación para el GDPR

¿Qué estoy **procesando**?

¿Cómo **gestiono** el riesgo?

¿Puedo **detectar** una filtración y notificarla en 72 horas?

¿Tengo una **seguridad adecuada**?



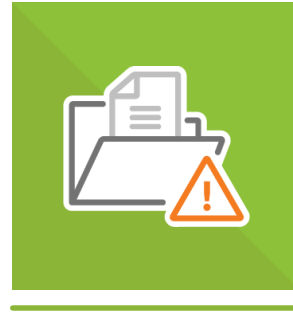
Requisitos técnicos del GDPR



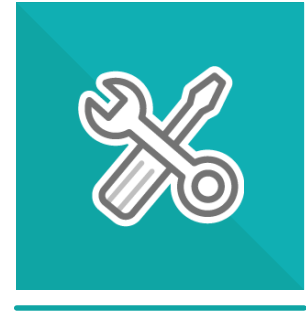
Proteger
datos personales



Resistencia a código
malicioso y ataques
cibernéticos

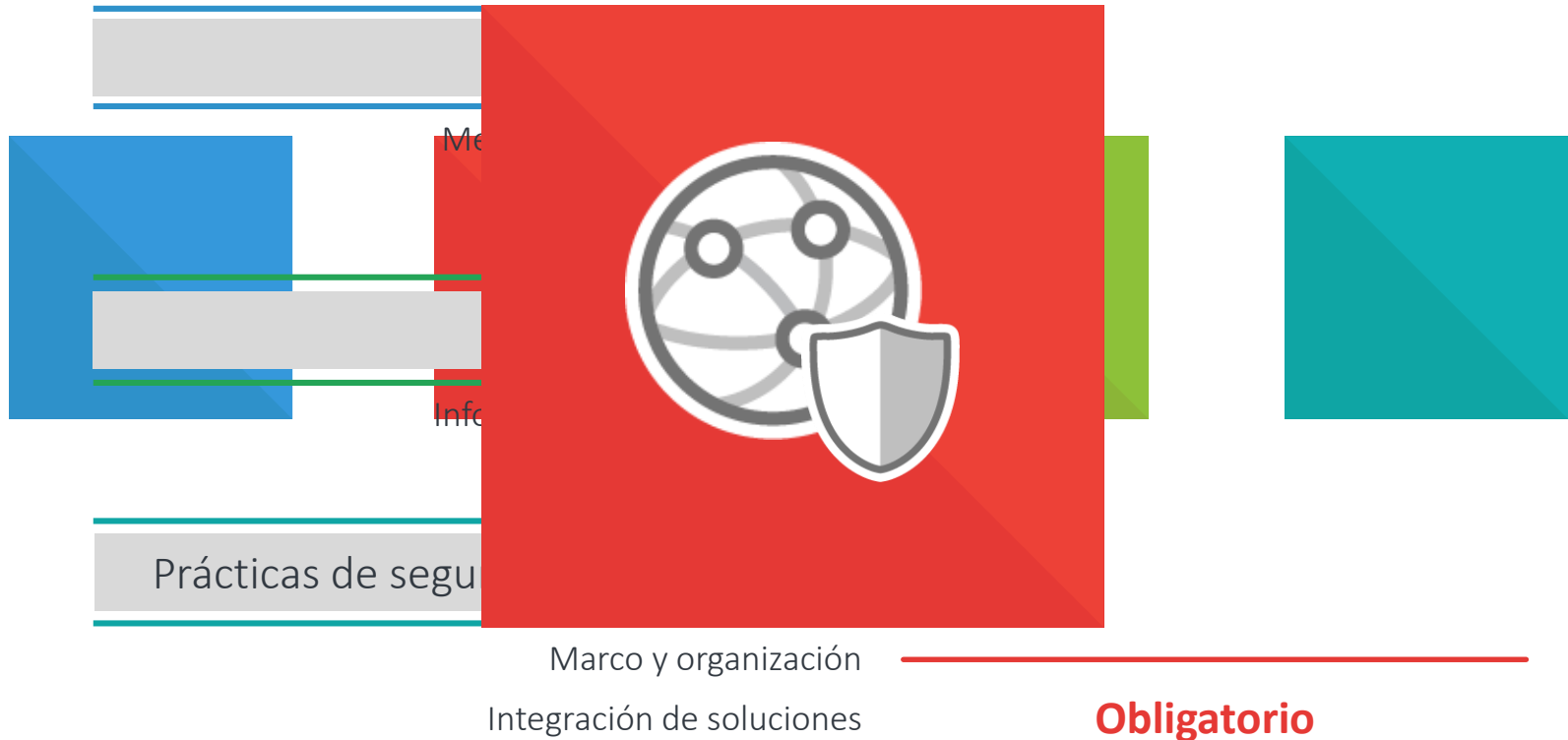


Evaluar los
riesgos de los
datos personales

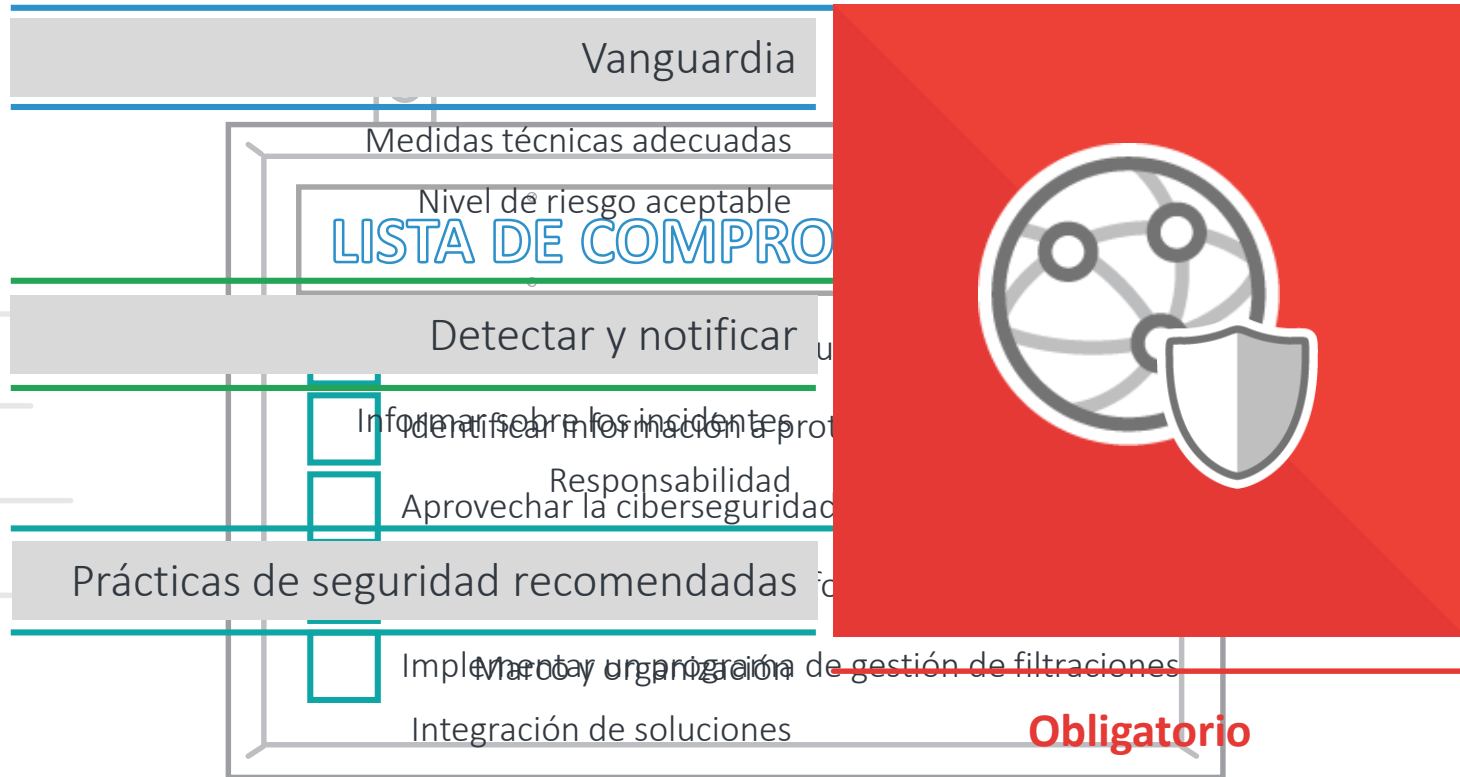


Desarrollar
una protección
de datos **a medida**

El GDPR exige una ciberseguridad eficaz



El camino al cumplimiento del GDPR



Cómo podemos ayudar



Proteger la
infraestructura
de procesamiento
de datos



Detectar y
responder
a las filtraciones
de datos
personales

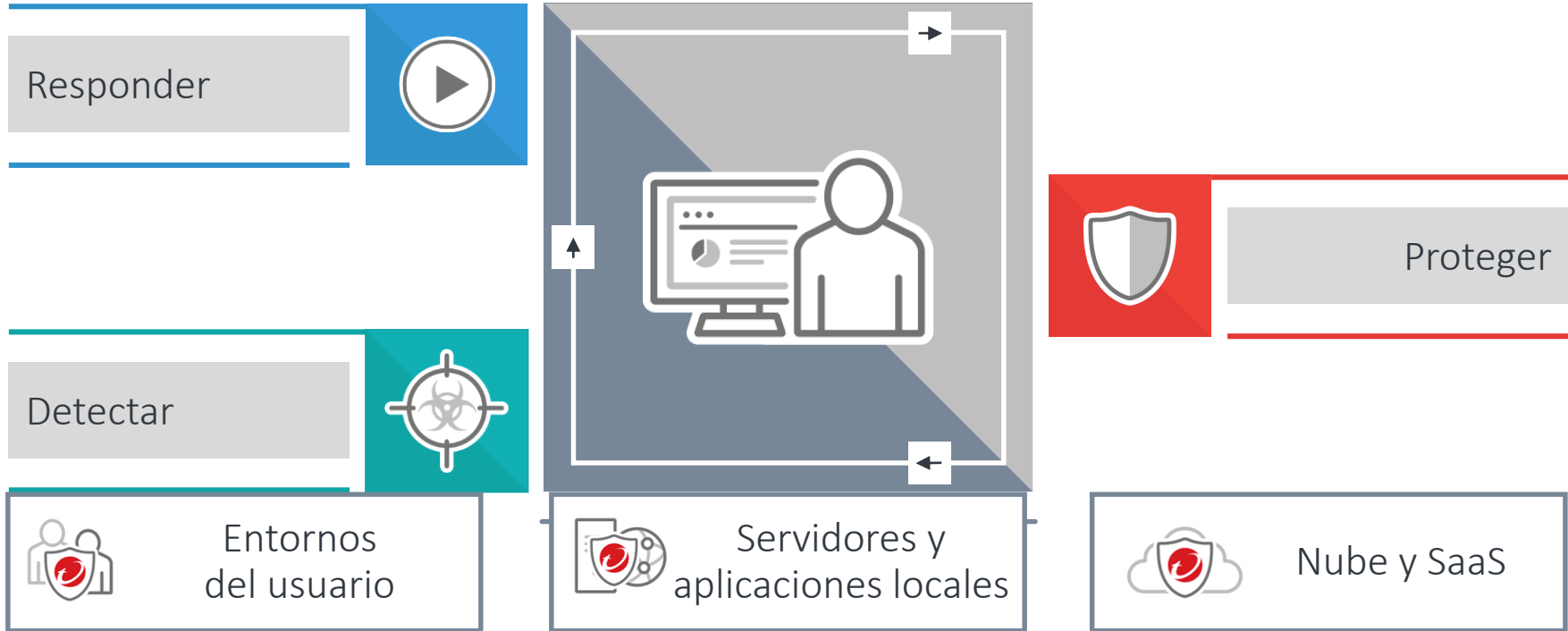


Evaluar riesgos

Cómo podemos ayudar



Cómo podemos ayudar



Motivos para usar Trend Micro



Inteligente

Vanguardia
Intergeneracional
Seguridad multicapa



Optimizado

Multiplataforma
Integrado en la nube
Impacto operativo bajo



Conectado

Informa sobre amenazas
en tiempo real
Identifica filtraciones de seguridad
Aísla y bloquea ataques

Liderazgo en el mercado



El **líder del mercado** en seguridad de servidores por **7.º año consecutivo**



- Fuente: IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, enero de 2017 #US41867116



Sistema de detección de filtraciones **recomendado** por **tercer año consecutivo**, y IPS de nueva generación **recomendado**



Líder en el Cuadrante mágico Gartner para sistemas de detección y prevención, enero 2017

- Resultados de las pruebas de detección de filtraciones de NSS Labs (2014-2016); Resultados de las pruebas de NSS NGIPS, 2016
- <http://www.trendmicro.com/us/business/cyber-security/gartner-idps-report/>



En el **primer puesto y completamente a la derecha** en el cuadrante de liderazgo del cuadrante mágico Gartner sobre plataformas de protección de endpoints (EPP), enero 2017



N.º 1 en protección y rendimiento

- <https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html>
- av-test.org (de enero de 2014 a diciembre de 2016)



Proteger datos personales



- Pérdida accidental
- Mal uso por parte de las personas
- Revelación ilegal y accidentada



La prevención de pérdida de datos (DLP) integrada ayuda a identificar y proteger los datos personales



Endpoint Encryption protege los datos personales frente a la pérdida de dispositivos

Proteger los dispositivos de los empleados



- Robo de identidad a través del phishing y la ingeniería social
- Malware distribuido por correo electrónico o vulnerabilidad web
- Código malicioso distribuido por configuración poco segura o vulnerable



Email Security bloquea correos maliciosos



Web Security protege las actividades de navegación web



Endpoint Security protege los dispositivos de los usuarios frente a amenazas conocidas y desconocidas (ransomware)



Network Security bloquea la vulnerabilidad de la red y detecta posibles filtraciones

Proteger su infraestructura corporativa



- Infección de los servidores y las aplicaciones por configuración poco segura o vulnerable
- Acceso no autorizado a servidores que procesan datos personales
- Propagación de amenazas a través de la infraestructura corporativa



Hybrid Cloud Security protege los servidores y las aplicaciones en el centro de datos y la nube



Network Security (a través de IPS) protege la infraestructura local de vulnerabilidades conocidas y desconocidas

Proteger datos en la nube



- Asumir la responsabilidad de seguridad compartida para las descargas en la nube
- Proteger datos personales a través de implementaciones de varias nubes
- Los proyectos de transformación de la nube permiten la protección de datos a medida



Hybrid Cloud Security automatiza la seguridad de la carga de trabajo a través de implementaciones de varias nubes



Cloud App Security protege los entornos SaaS como Office 365 de ransomware y phishing

Detectar y responder a las filtraciones de seguridad

- Supervisar el tráfico de la red en busca de posibles indicadores de amenaza
- Detectar las filtraciones causadas por dispositivos no revisados/no corporativos
- Informes procesables sobre las actividades de resolución iniciales/en curso

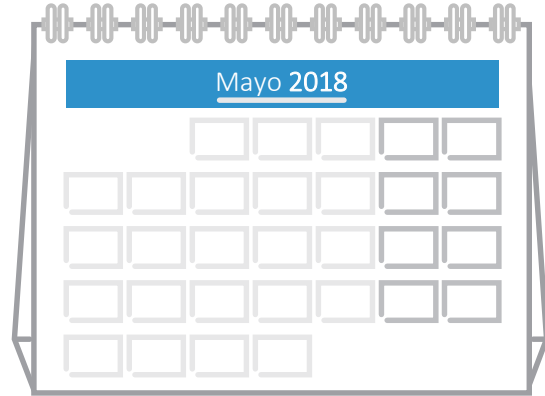


Breach Detection System identifica actividades sospechosas que pueden conllevar un riesgo de pérdida de datos



Las soluciones de **Connected Trend Micro** permiten una respuesta rápida y la resolución de las filtraciones

El camino al cumplimiento del GDPR



LISTA DE COMPROBACIONES

- Sigue las directrices de la autoridad de control
- Utiliza un marco de seguridad de la información
- Aprovecha la ciberseguridad de vanguardia
- Limitar riesgos
- Implementa un programa de gestión de filtraciones

GRACIAS

<http://www.trendmicro.es/campaigns/gdpr-compliance/>

