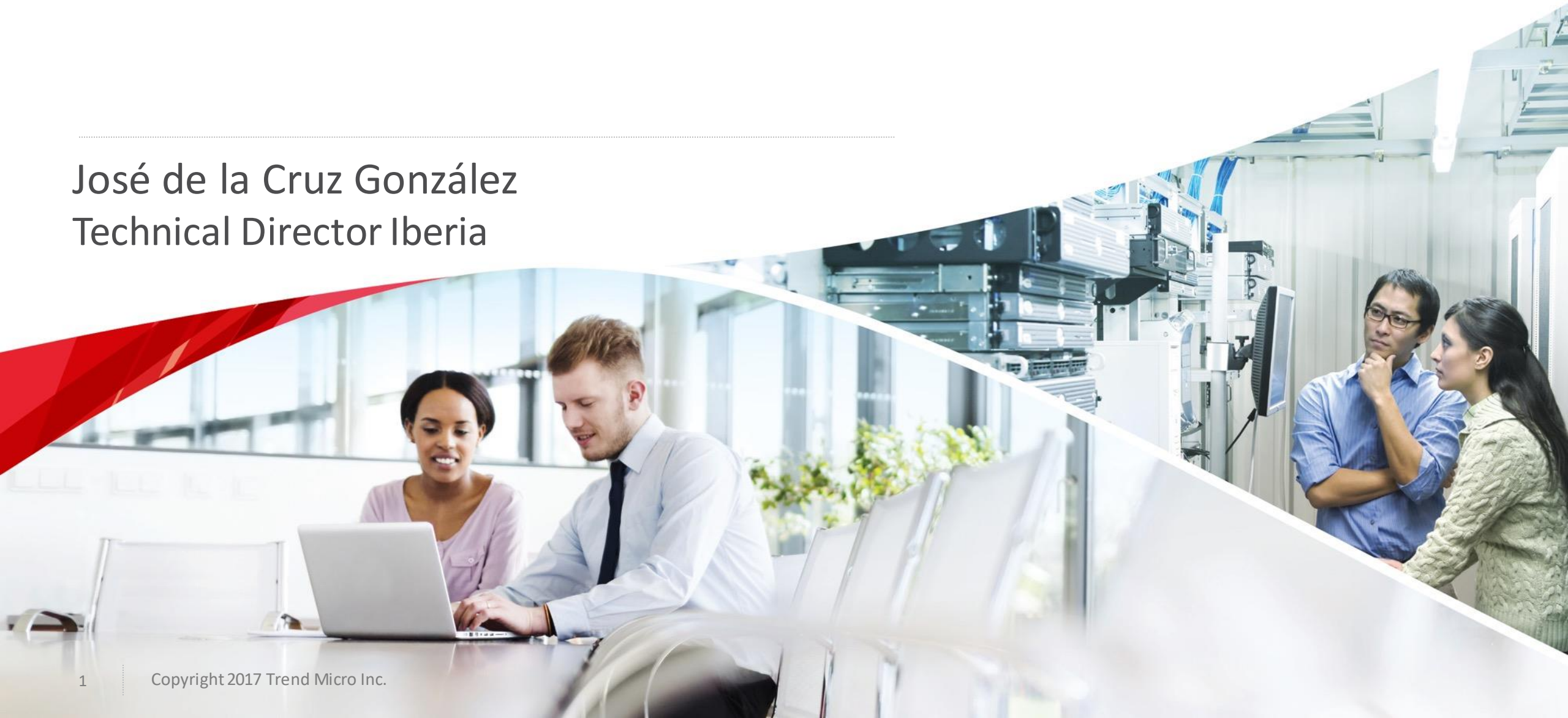
Seguridad Gestionada

José de la Cruz González
Technical Director Iberia



Copyright 2017 Trend Micro Inc.

O
P
L
Update
M
Shift

GDPR

Copyright 2017 Trend Micro Inc.

Planteamientos

Detección en la Red

+ Monitoriza protocolos de red.
+ Análisis de comportamiento y detección de ataques.

- Complejo.
- Múltiples eventos y alertas.
- Es dificil determinar el origen,

Endpoint Detection & Response (EDR)

+ Registra actividades de Endpoint: Análisis de raíz.
+ Detección avanzada: Análisis de comportamiento, Machine Learning, etc.

- Requiere personal especializado.
- Complejo.
- Requiere tiempo e implica un coste elevado.

Copyright 2017 Trend Micro Inc.

Detección y Respuesta

PROTECT

Web/URL reputation
Exploit prevention
Brand new PE files
Sandbox analysis
DLP violation

DETECT

Machine learning
Behavioral analysis
Application control
Hunting rules
Census

RESPOND

Network isolation
Threat quarantine
Remediation
Rollback
C&C blocking
Rapid response pattern

INVESTIGATE

Behavior modeling
Root cause analysis
Sweeping
Memory assessment
Impact assessment
Snapshot
Retrospective search
Disk scan

- La mayoría de las empresas necesitan esto
- Automatizado
- Requiere menos conocimientos

- Alto conocimiento
- Mucho tiempo
- Poco solicitado

Copyright 2017 Trend Micro Inc.

Fabricantes EDR

PROTECT

Web/URL reputation
Exploit prevention
Brand new PE files
Sandbox analysis
DLP violation

DETECT

Machine learning
Behavioral analysis
Application control
Hunting rules
Census

RESPOND

Network isolation
Threat quarantine
Remediation
Rollback
C&C blocking
Rapid response pattern

INVESTIGATE

Behavior modeling
Root cause analysis
Sweeping
Memory assessment
Impact assessment
Snapshot
Retrospective search
Disk scan

- La mayoría de las empresas necesitan esto
- Automatizado
- Requiere menos conocimientos

- Alto conocimiento
- Mucho tiempo
- Poco solicitado

Copyright 2017 Trend Micro Inc.

Trend Micro

PROTECT

Web/URL reputation
Exploit prevention
Brand new PE files
Sandbox analysis
DLP violation

DETECT

Machine learning
Behavioral analysis
Application control
Hunting rules
Census

RESPOND

Network isolation
Threat quarantine
Remediation
Rollback
C&C blocking
Rapid response pattern

INVESTIGATE

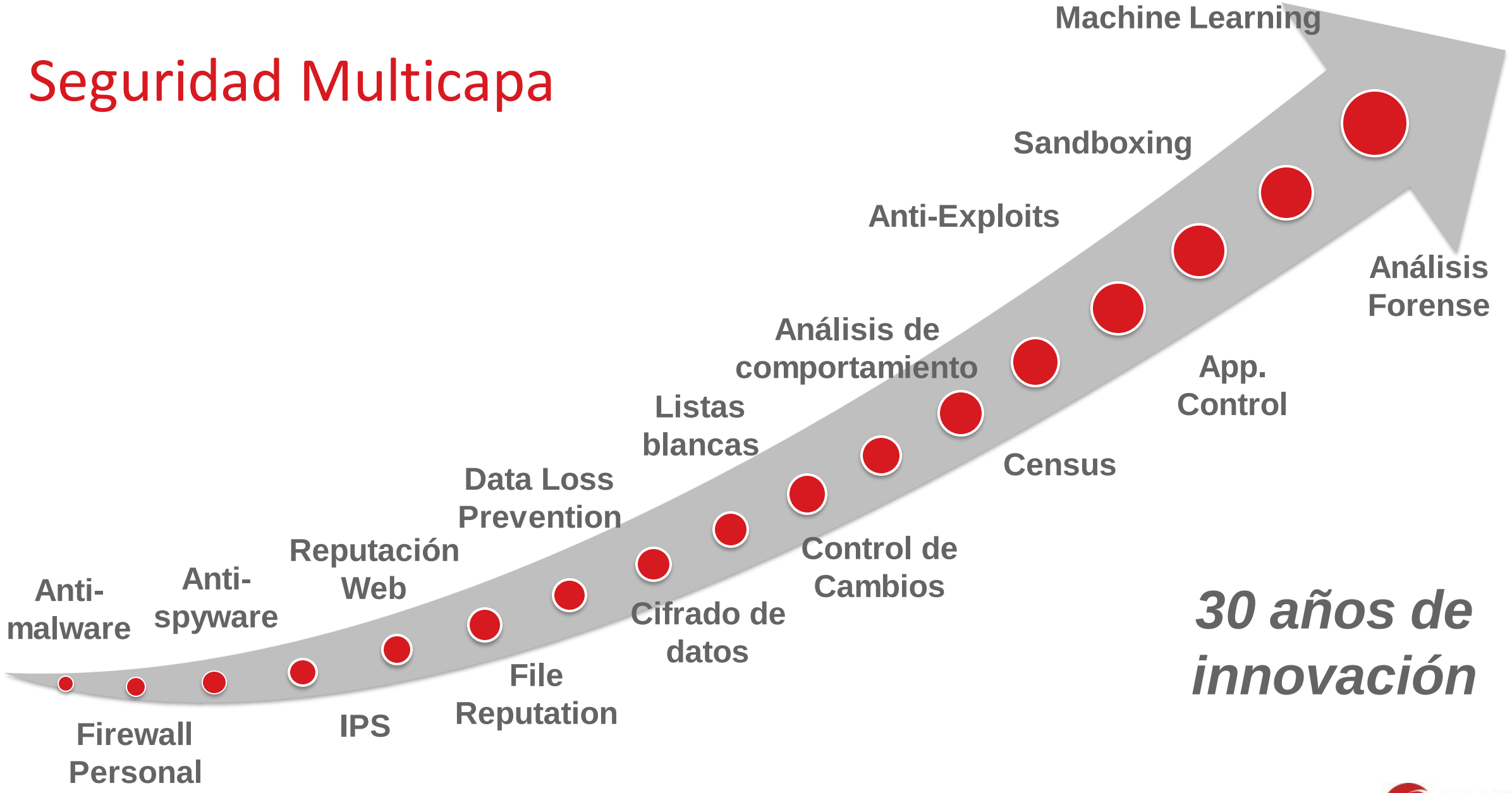
Behavior modeling
Root cause analysis
Sweeping
Memory assessment
Impact assessment
Snapshot
Retrospective search
Disk scan

- La mayoría de las empresas necesitan esto
- Automatizado
- Requiere menos conocimientos

- Alto conocimiento
- Mucho tiempo
- Poco solicitado

Copyright 2017 Trend Micro Inc.

Seguridad Multicapa

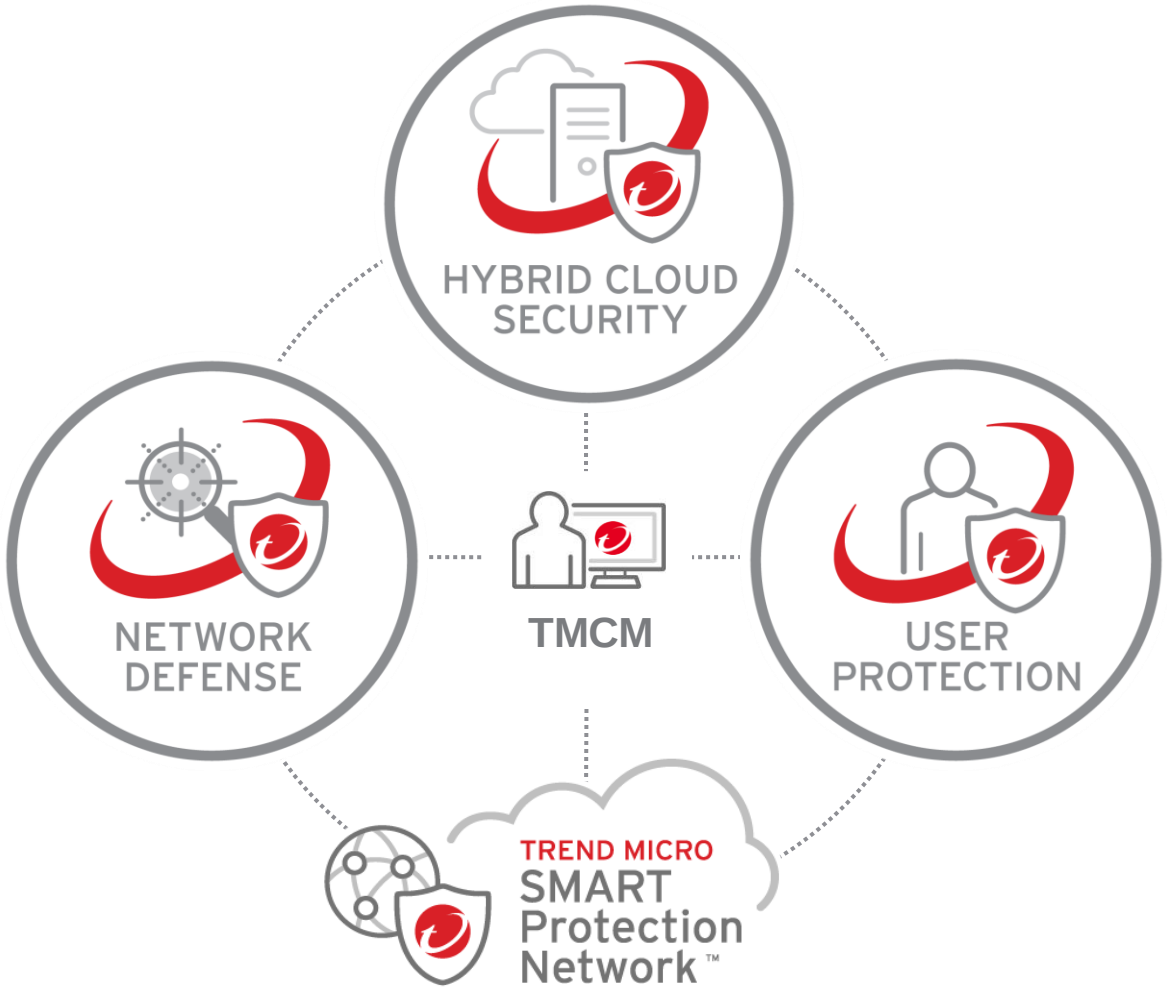


30 años de innovación

Copyright 2017 Trend Micro Inc.

Copyright 2014 Trend Micro Inc.

Seguridad Conectada



Copyright 2017 Trend Micro Inc.

Problema Persiste

Tiempo y Coste

Gran volumen de Alertas

Falta de Conocimiento

No sólo el endpoint

Servidores

Red

IIoT

Nuevo Planteamiento

Automatización

Correlación y priorización de alertas

Tecnicas avanzadas de IA

Reduce el trabajo manual

Servicios Gestionados

Expertos en Seguridad

Respuesta a incidentes

Ofrecido desde Trend Micro

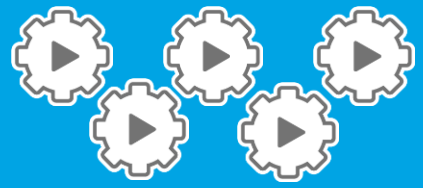
TREND MICRO MANAGED DETECTION AND RESPONSE

Copyright 2017 Trend Micro Inc.

Managed Detection and Response

SENSORS

- Integrated Endpoint Protection
- Deep Discovery Inspector
- Deep Security



THREAT INVESTIGATION CENTER

Threat Intelligence

Expert Rules

Machine Learning

TREND MICRO ANALYSTS

RESPONSE

- Delivered to management console

Copyright 2017 Trend Micro Inc.

¡Muchas Gracias!

Copyright 2017 Trend Micro Inc.