



Trend Micro Apex One™ Endpoint Security Evolution

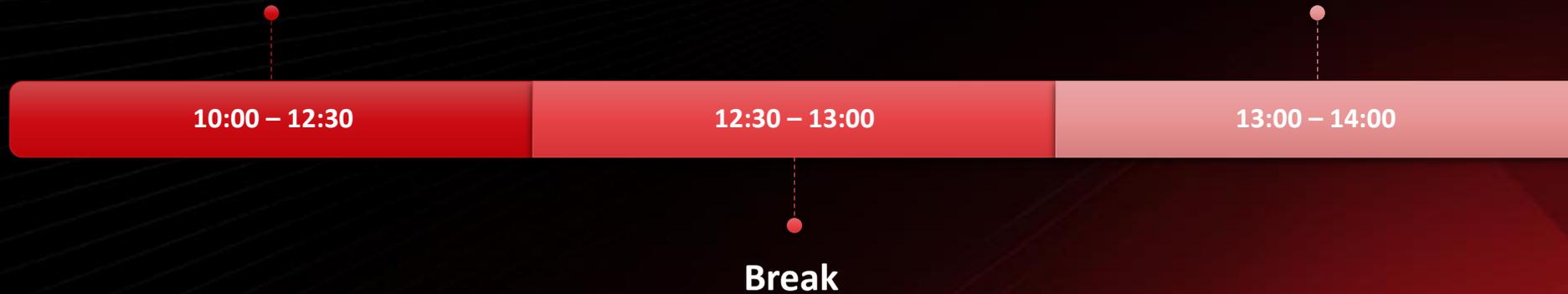
Agosto 2023



Dinámica del curso

Primer periodo: Presentación teórica y práctica

Segundo periodo: Ejercicios prácticos



Endpoint Security



Automatizada

Detección y Respuesta efectiva

Tecnología moderna para
bloquear ultimas amenazas

Mejores tiempos de virtual
patching de la industria



Intuitiva

Visibilidad y control a traves de
todas las funciones

Opción para investigación EDR
de root cause y amenazas

Opción de servicio MDR/equipos
SOC



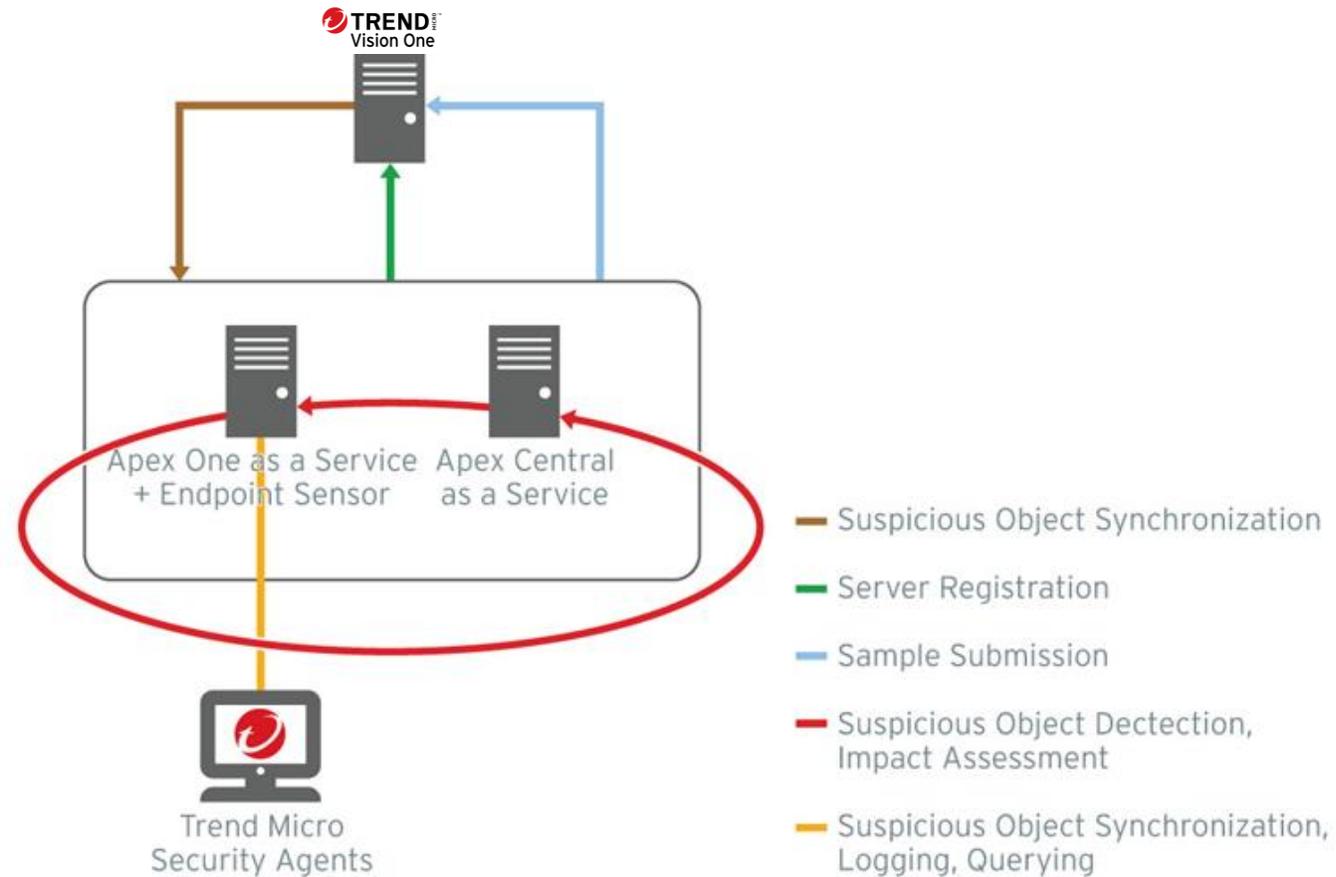
Flexible

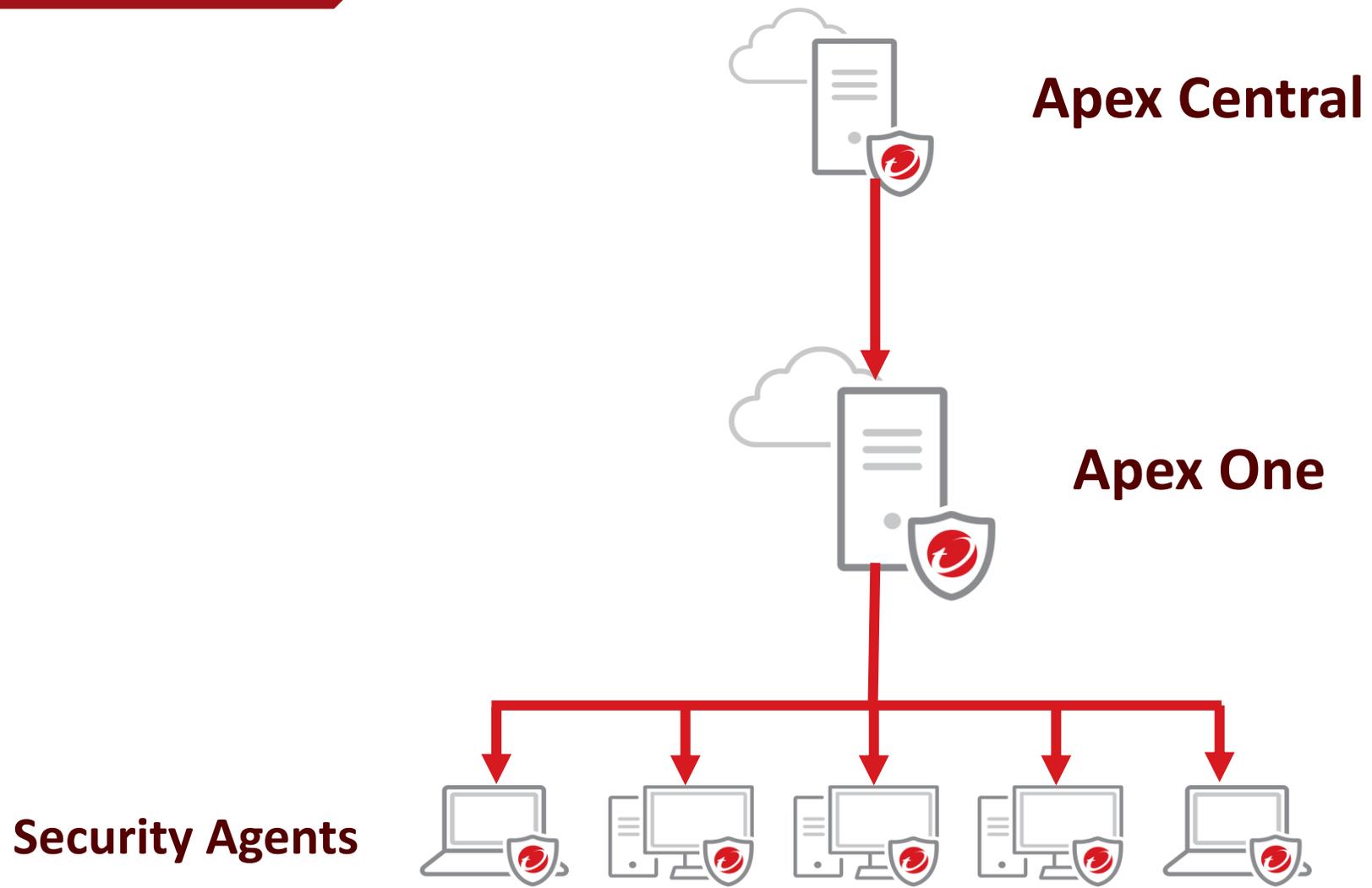
EDR y seguridad de Endpoint en
un agente

Sin necesidad de agentes de
múltiples Vendors

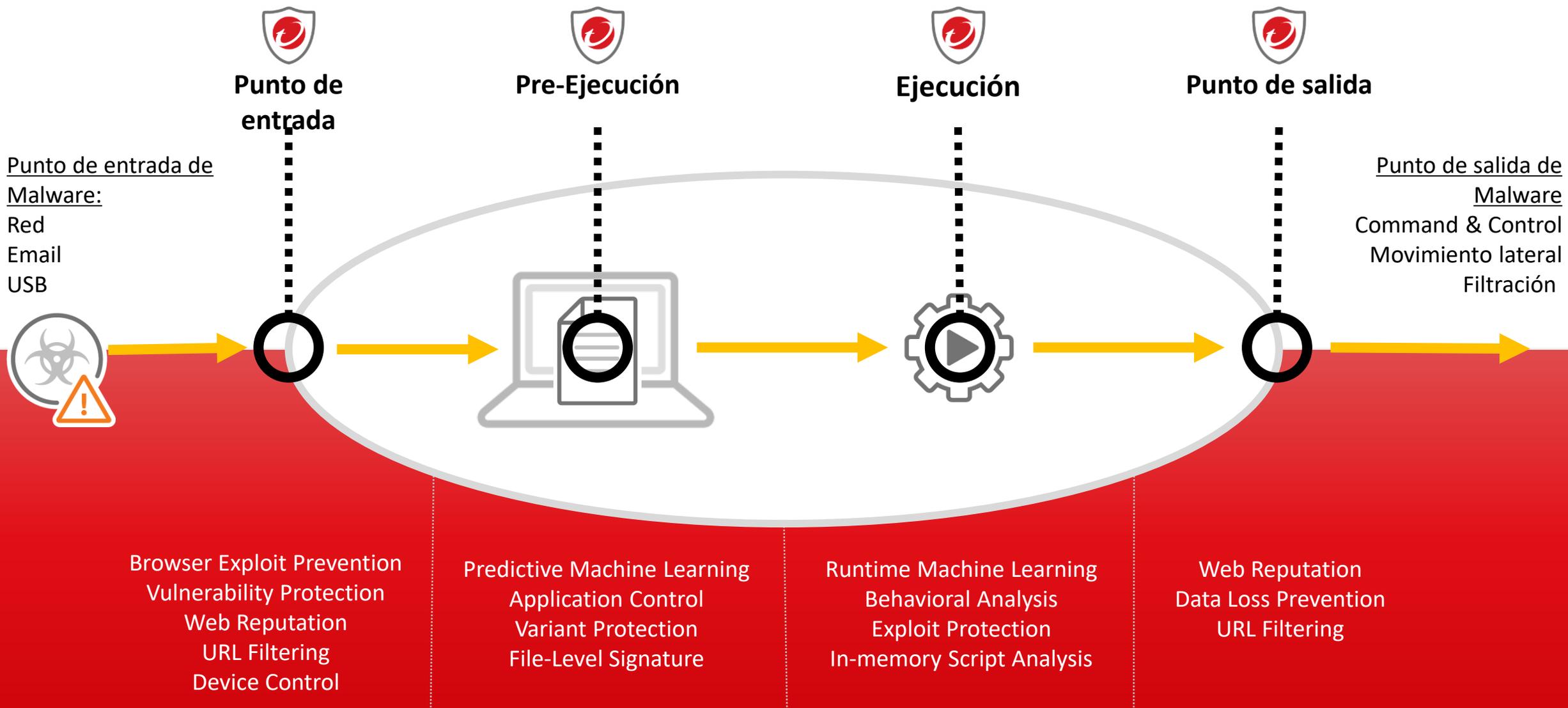
Opciones SaaS y On-premise
(enfoque en Saas)

Arquitectura Apex One/Central





Ciclo de vida y protección de amenazas



Apex One™: Agente único

Prevención



Virtual Patching



Device Control



Firewall



App. Control



Exploit Prevention

Detección



Machine Learning



Behavioral Analysis



Malicious CLI



Network Fingerprinting



Known Threats

Respuesta



DLP



Kill & Quarantine



Restore Encrypted Files



Connected Threat Defense



Investigate In Depth

* Requiere licencia adicional

Etapa II: Demostración de Consola Web

Etapa III: Ejercicios Prácticos

- Web Reputation en acción.
- Detección de Eicar.
- Excepción de Eicar.
- Creación de una regla de Application Control.

Etapa IV: Juego de Trivia



¡Muchas gracias!