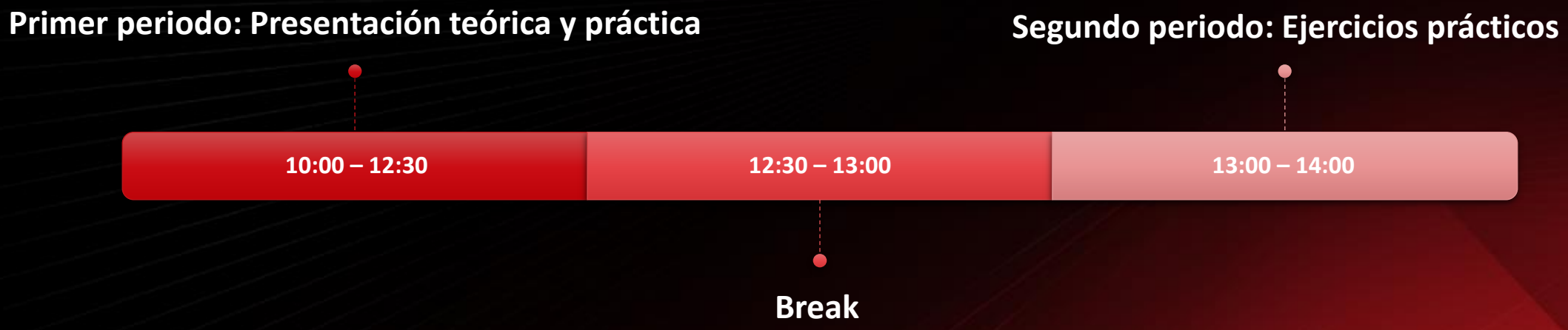
Trend Micro Cloud One Workload Security™

Noviembre 2023

Dinámica del curso



Contenido

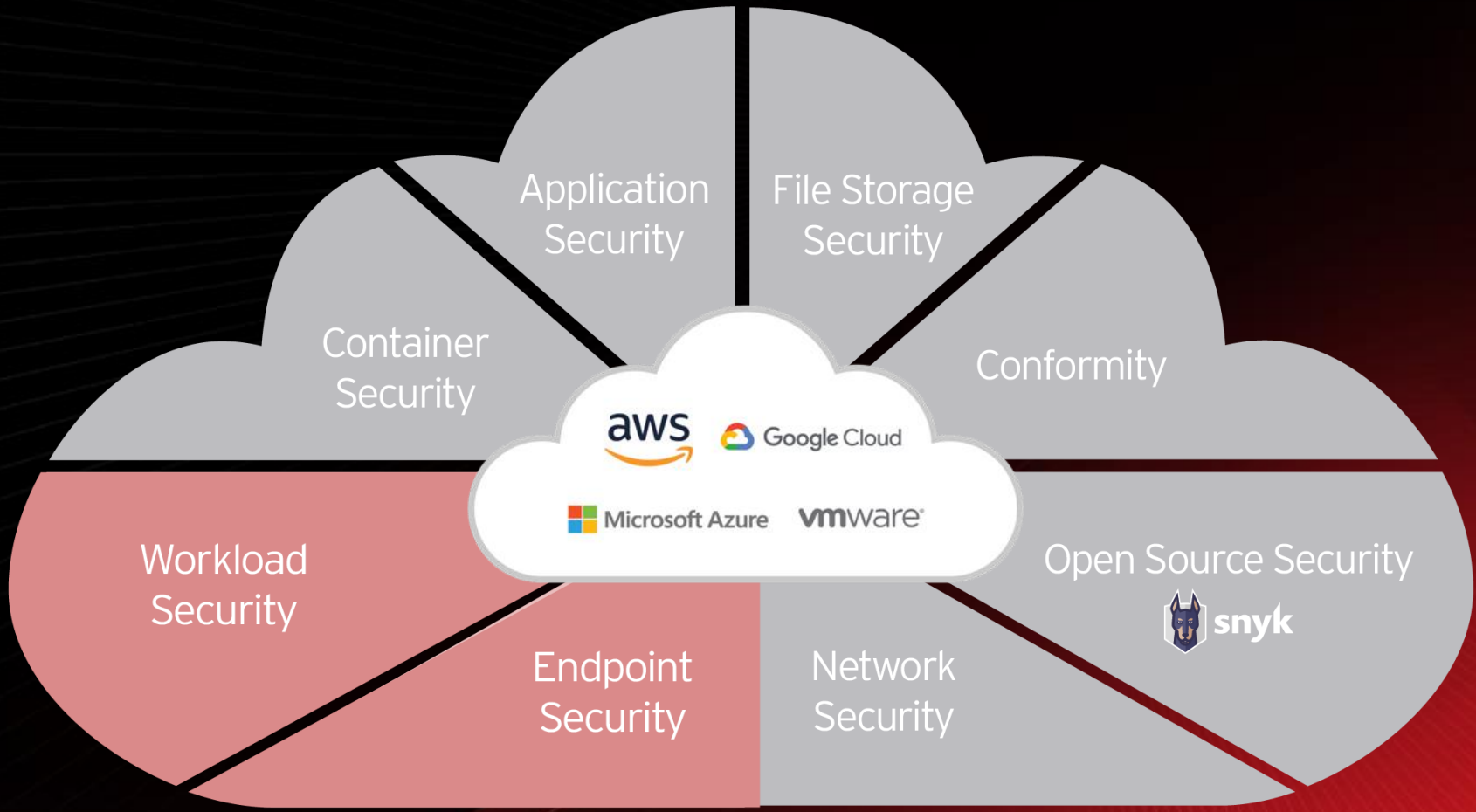
Presentación

- ¿Qué es Workload Security?
- ¿Qué es Vision One?
- Modelo Compartido
- Integraciones
- Arquitectura
- Módulos de Protección

Consola

- Dashboard
- Actions & Alerts
- Politicas y sus módulos
- Instalación de agente
- Generación de reportes
- Administración

Cloud One – Endpoint & Workload Security



Licenciamiento

La forma de licenciamiento pasa de ser:

Cloud One Workload Security ➡ **Vision One Endpoint Security Pro**

Esta nueva forma de licencia se puede cargar como creditos dentro de la consola de Vision One o por usuario, incluye el sensor XDR.

TREND MICRO™ Vision One

Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Managed Services

Ecosystem Integration

Extended Detection and Response (XDR)

Email Security | **Endpoint Security** | **Cloud Security** | **Network Security** | **OT Security**

Orchestration and Automation

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research | AI/ML | Big Data Analytics

Platform Foundations

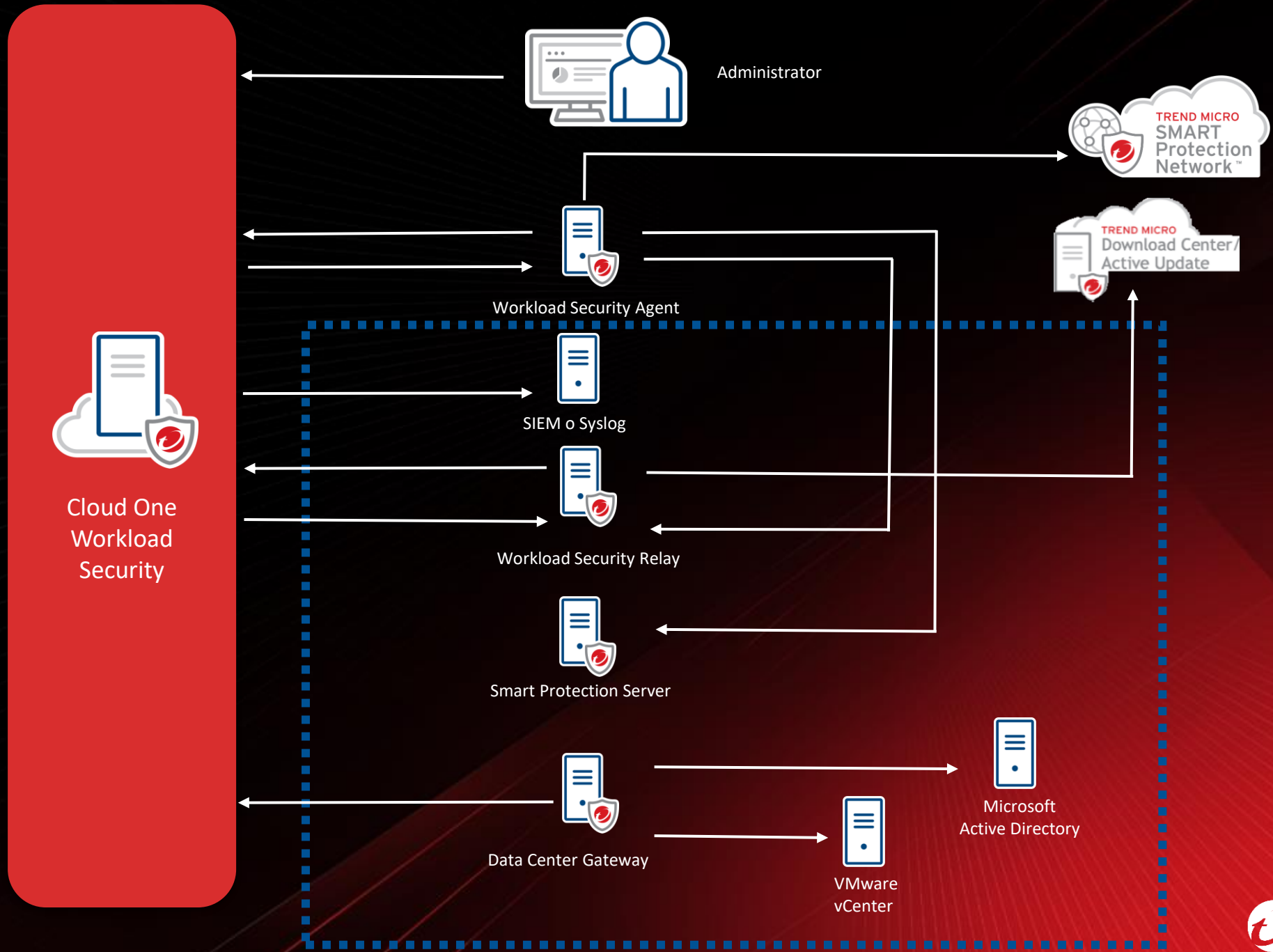
Multi-Tenancy | Role-Based Access Control | Single Sign-On | Policy Decision Point

TREND MICRO™

Trend Micro Vision One Workload Security

La seguridad es una responsabilidad compartida

Workload Security: Arquitectura


Cloud One
Workload
Security
Administrator
TREND MICRO
SMART
Protection
Network™
TREND MICRO
Download Center/
Active Update
Workload Security Agent
SIEM o Syslog
Workload Security Relay
Smart Protection Server
Data Center Gateway
VMware
vCenter
Microsoft
Active Directory

Workload Security: Protección

Cloud One – Workload Security

Módulos de Protección & D&R

Network Security

Intrusion Prevention | Firewall | Vulnerability Scanning

System Security

Application Control | Integrity Monitoring | Log Inspection

Malware Prevention

Anti-Malware | Behavioral Analysis | Machine Learning

Detection & Response (activity monitoring)

Detect | Respond | Investigate

TREND MICRO

Reduce los impactos operacionales

Virtual Patching (IPS) – Protección contra exploits de Sistema Operativo y Aplicaciones

Protege sistemas antes de que esten disponibles los parches del vendor

Protege sistemas operativos fuera de soporte

Detiene el Ransomware

Usa seguridad por capas:

- Detiene el ransomware en los servidores con protección avanzada contra malware que incluye analisis del comportamiento y machine learning
- Lock down de servidores Windows & Linux servers con application control
- Protege de ataques de red con IPS, incuyendo proteccion de SMB
- Detiene el movimiento lateral y tráfico de Command & Control (C&C)

Etapa II:
Demostración de Consola Web

Etapa III:
Ejercicios Prácticos

- Deteccion de Eicar.
- Excepción de Eicar.
- Web Reputation en acción
- Virtual Patching (IPS)

Etapa IV:
Multiple Choice

Muchas gracias!