inetum

Positive digital flow

Nuevos desafíos
Ciberseguridad

¿Qué ofrecemos?

Seguridad Física
Eventos del mundo físico, entornos industriales (OT) y de IoT

Seguridad Lógica
Perímetro, Red, Endpoints

Identidad Digital
DoB, Biometría, IAM, SSO

Cumplimiento Normativo
ISO 27000, GDPR, PSD2, ENS

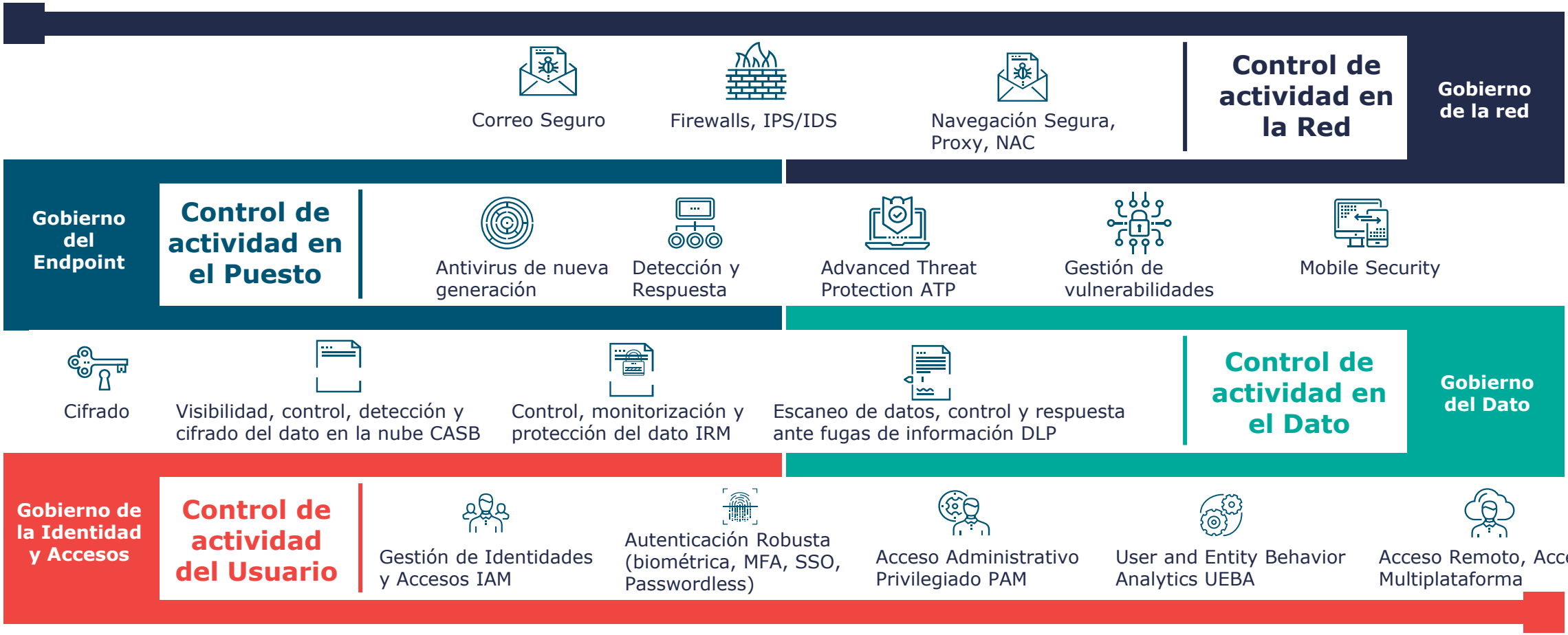
Blockchain

(Identidad soberana, trazabilidad, IoT, tokens…)

Algunos de nuestros clientes

Gerencia de Informática de la Seguridad Social · Aena · BBVA · Enel · FCC · IBERDROLA · icm · Junta de Andalucía · MAXAM Beyond Performance · Applus · Gobierno de Aragón · persán · Alimerka

Monitorización y correlación (SIEM) | Threat Hunting | SOC | Visibilidad IT

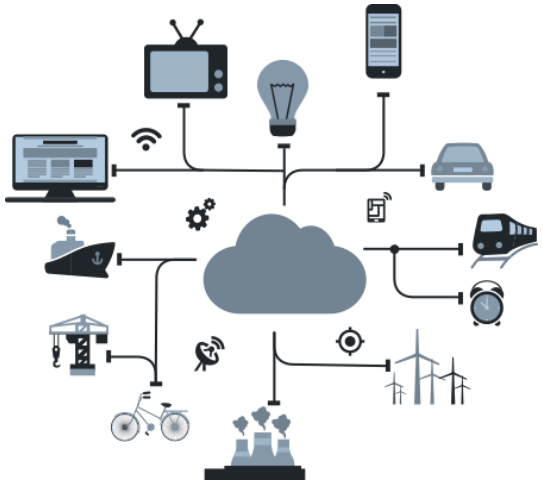


Gobierno | Riesgo | Cumplimiento | Auditorías

Sector Público

Entorno

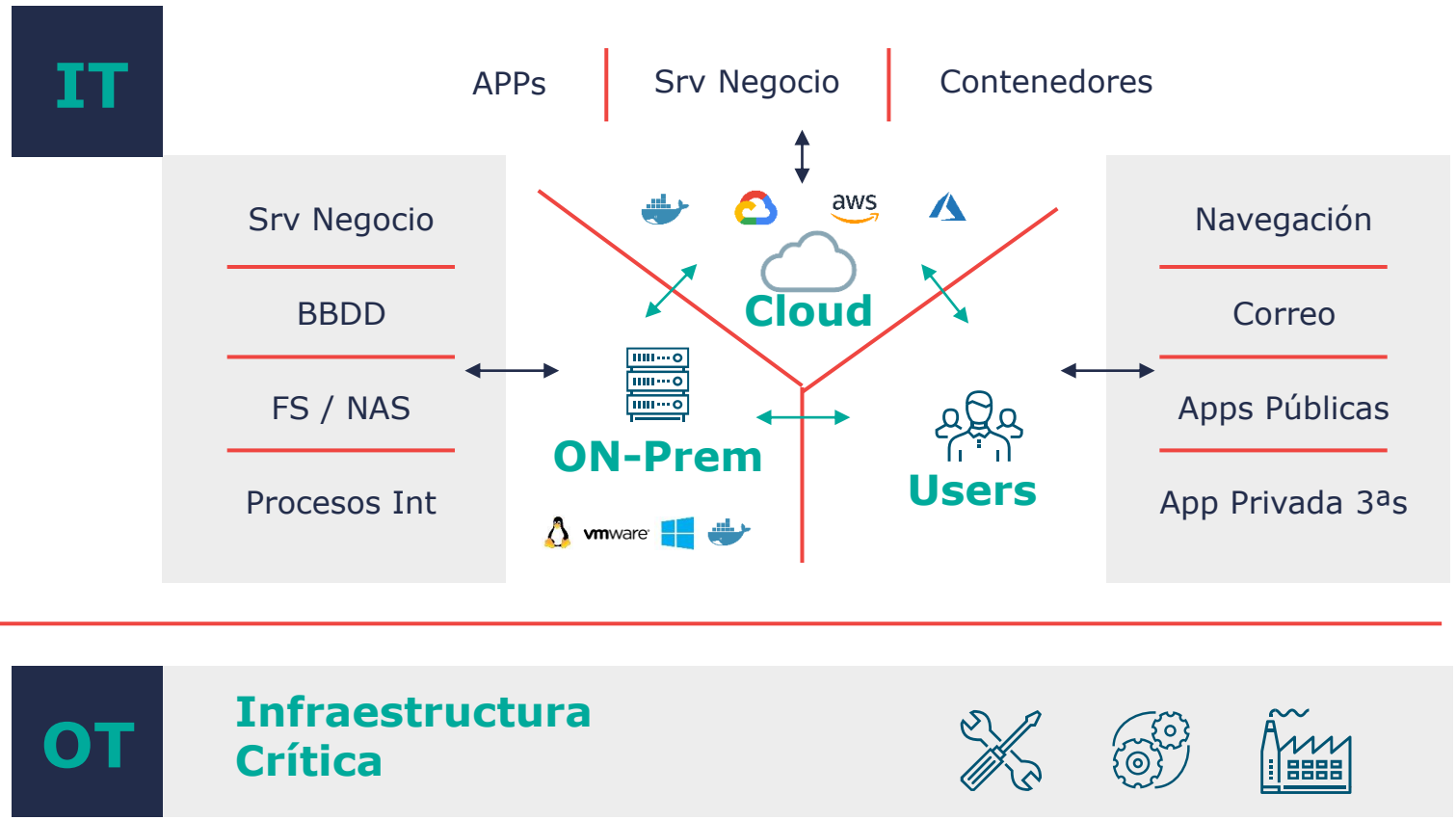
- Arquitecturas Heterogéneas y de Amplio Espectro (Legacy & OT)
- Manejo información Sensible - Alto Impacto Normativo
- Distintos Entornos / Niveles Seguridad Distintos
- Usuarios Heterogéneos
- Personal Poco Concienciado En Ciberseguridad
- Necesidad Alta De Monitorización Servicios

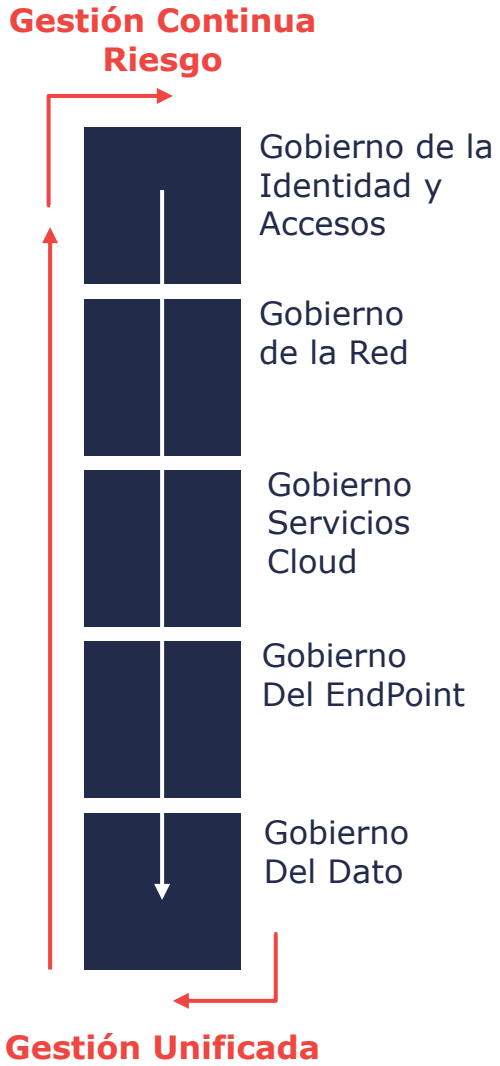


Retos

- Mejora de sus procedimientos y servicios
- Digitalización procesos (IoT & BigData)
- Cumplimiento de regulación (new&old)
- "Apertura" redes operativas
- Gestión nuevo riego: ciberseguridad
- Crear e implantar cultura ciberseguridad
- Mayor Inter-relación varios servicios y redes

Contexto de Clientes





Contexto Usuario Digital

Problemática

- USUARIO ACTIVO MAYOR RIESGO (people centry security)
- Endpoint primer punto de entrada ataques
- Cambio continuo técnicas ataque (add & modify)
- Aumento uso dispositivos móviles
- Ataques dirigidos
- Aumento ingeniería social
- EPP insuficiente para proteger
- Movilidad del ususario

Amenazas

- Malware infection and propagation
- Business email compromise (BEC)
- Ransomware attacks
- Leak personally identifiable information (pii)
- Phishing

Funcionalidades

- Cubrir tanto entorno endpoint como server
- Bien posicionada en informes externos
- Transparente para usuario
- Soporte en 24x7
- Fácil integración con terceros
- Agente único
- Variedad de SO soportados

Cambio Paradigma

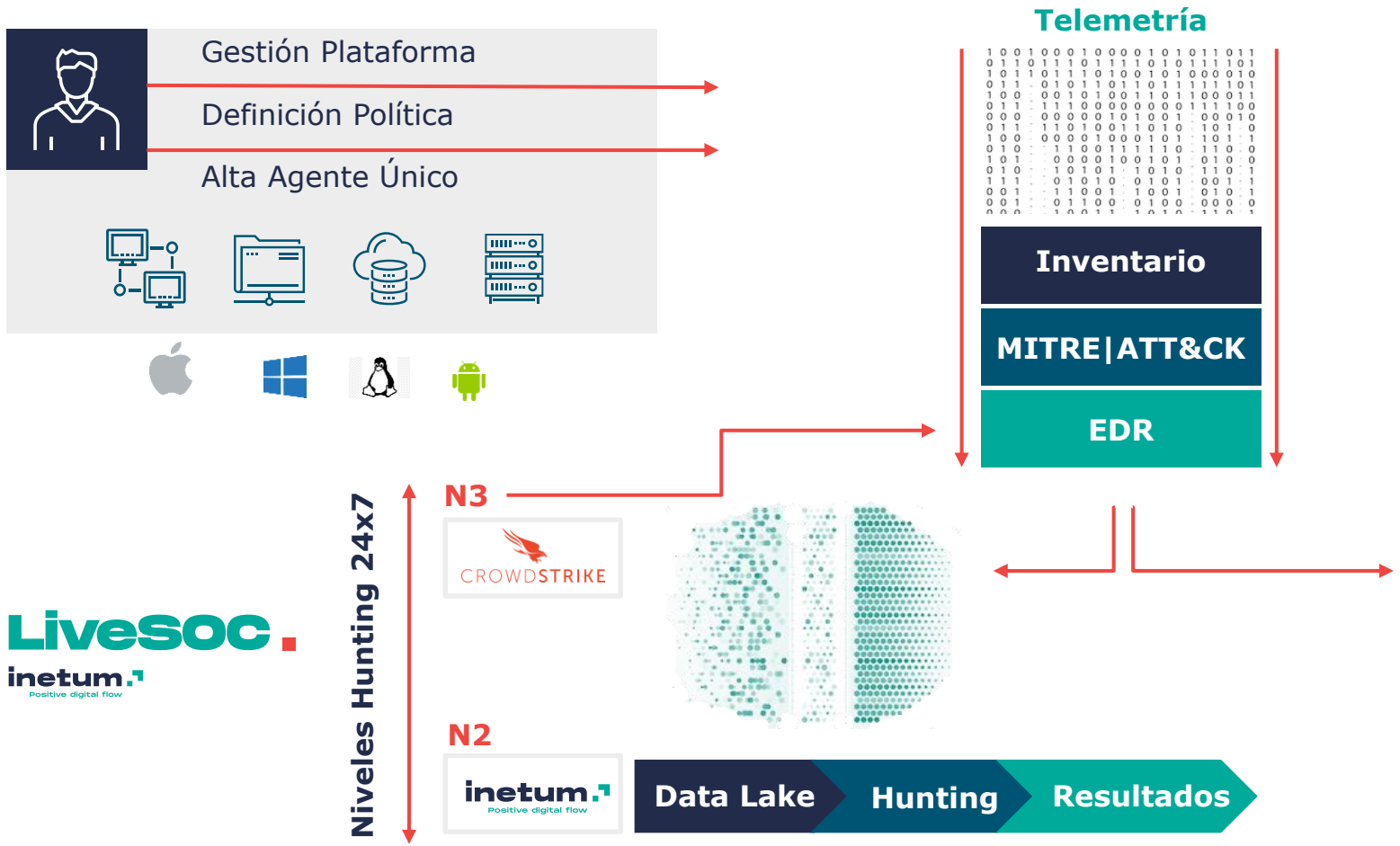
EDR + MDR

- Agente único
- Analítica en cloud
  Modular

Awareness

- Correo
- Cultura Interna

Servicio EDR + Threat Hunting



1 Funcionalidades

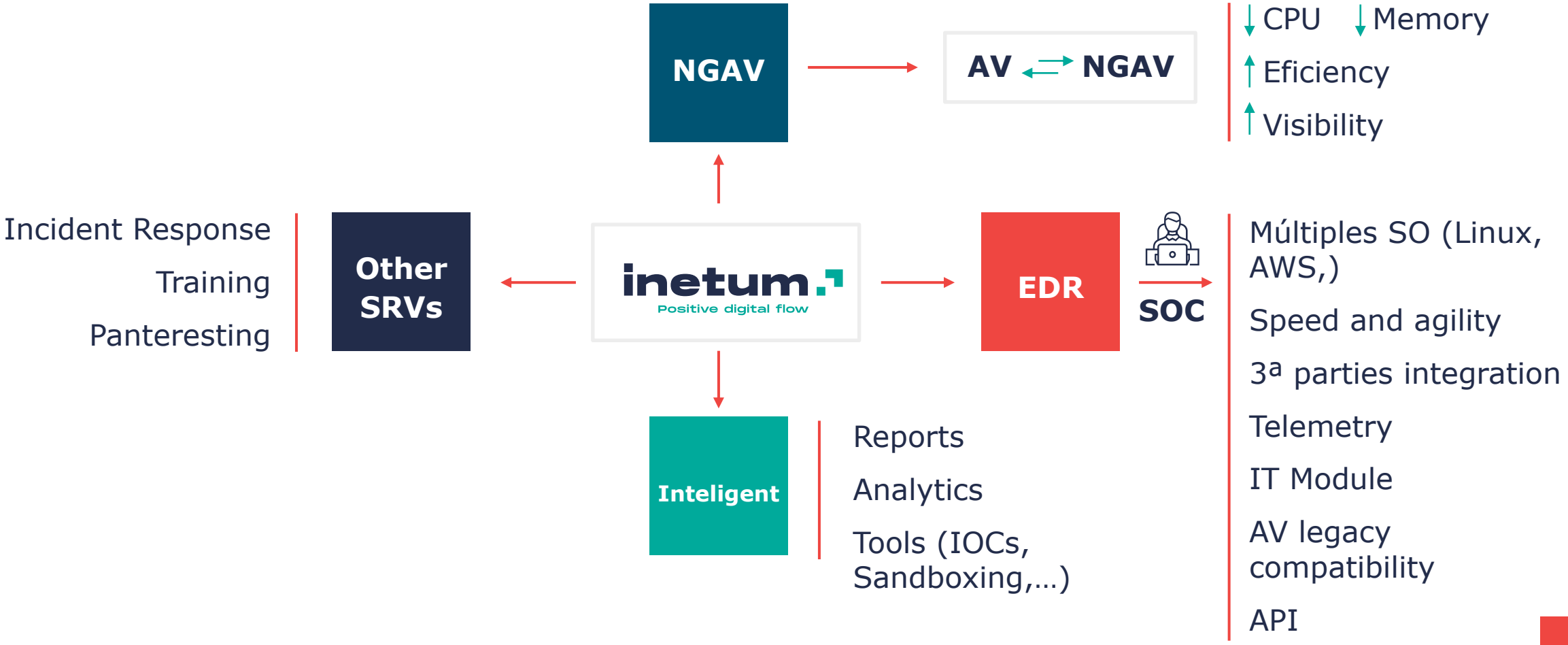
- Protección Amenazas Avanzadas (motor ML – no firmas)
  - Búsqueda de Malware
  - Análisis de Malware
- Sandboxing
- Uso Indicadores de Ataque (IOA)

2 Servicios

- Monitorización de la Seguridad
- Detección de Incidentes de Seguridad
- Capacitación Respuesta a Incidentes
- Escalado y Comunicación Incidentes
- Informes Periódicos
  - Elementos Bloqueados
  - Elementos Permitidos
  - Investigaciones Realizadas
  - Ejecución PUP (potentially Unwanted Programs)

Modelo Servicios

Matutity Model



Protección Usuario

93% Ataques son dirigidos

96% Vector ataque correo

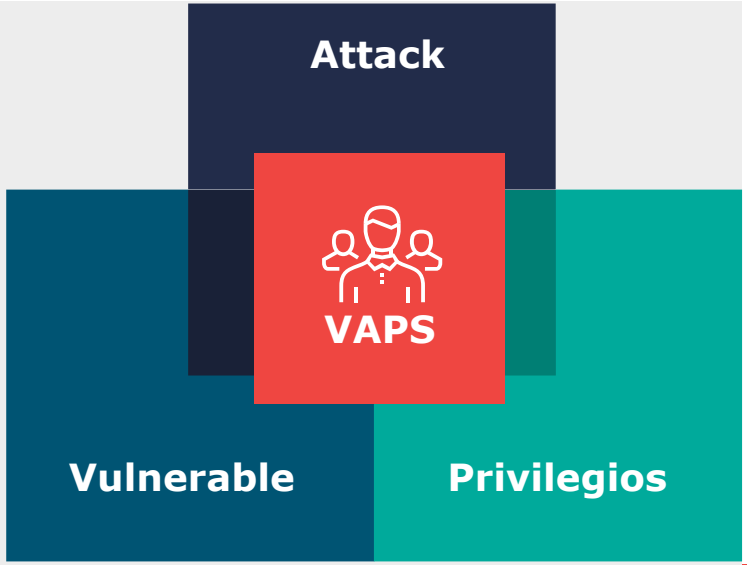
proofpoint

Phising BEC

VAP

- **Ataques**: son el objetivo ataques
- **Vulnerable**: ejecutan contenido malicioso
- **Privilegios**: acceden datos sensibles

Formación Continua



Contexto Cloud

Concepto cloud first enterprise

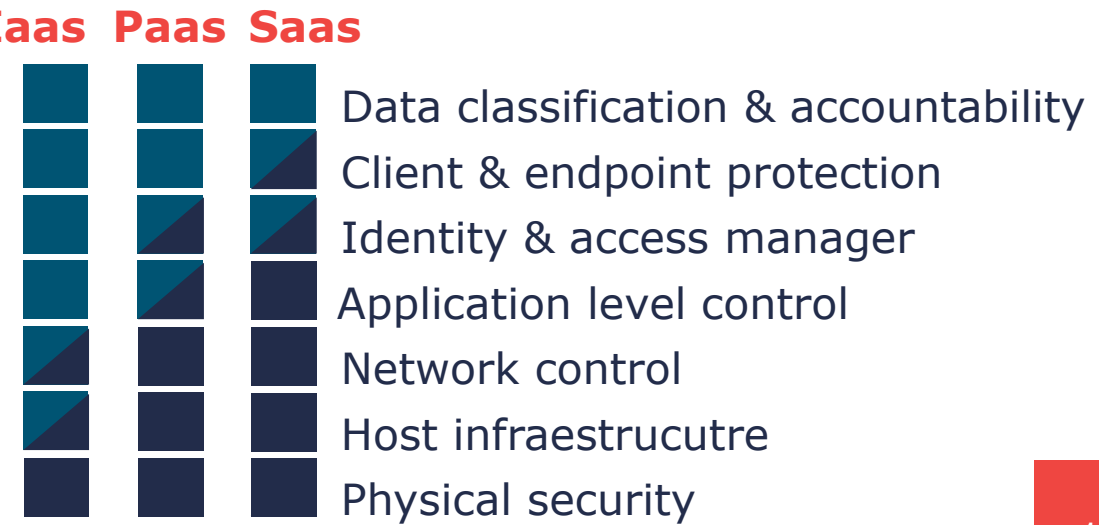
87% Permiten que sus empleados usen **dispositivos personales para acceder a las aplicaciones comerciales**.

97% De las empresas usan **servicios cloud**

Visibilidad
Control

CASB
CWPP
CSPM

Shared responsibility



Customer responsibility
Service provider responsibility

Aproximaciones Cloud

CASB – Cloud access security broker

- Visibilidad cloud
- Seguridad datos subimos nube
- Protección frente amenazas (account takeover)
- Cumplimiento normativo

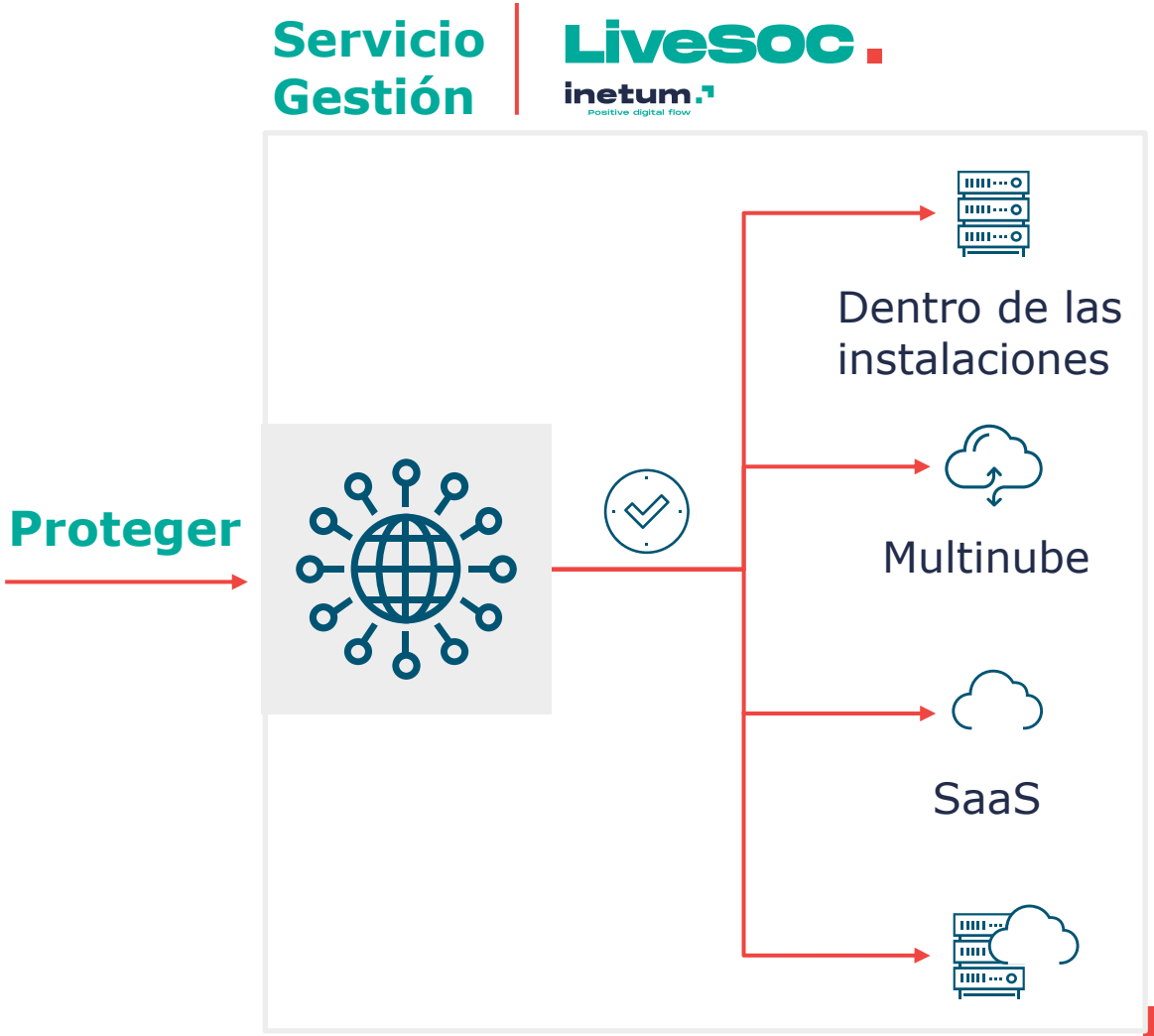
CWPP – Cloud workload protection platform

- Entornos virtuales
- Containers
- Cloud system software

CSPM – Cloud security posture manager

- Visibilidad tiempo real sobre seguridad, cumplimiento y vulnerabilidades cloud pública
- Guias remediación paso a paso
- Seguridad automatizada > garantizar cumplimiento continuo

Servicios B2C
(Escenario)



Cybersecurity & SOC

Aportación de Valor

LiveSOC
inetum
Positive digital flow

Seguridad 360 | **Certificación**

SOC Boutique | **Best PartnerShip**

McAfee · TREND MICRO · SOPHOS · Microsoft
FORCEPOINT · FORTINET · Check Point · proofpoint
splunk> · MICRO FOCUS · paloalto NETWORKS · Entrust Datacard
IBM · transmit SECURITY · gemalto · CROWDSTRIKE

Incident Response
- SIEM
- Incident Response
- SOAR

IAM
- General Users
- Privileged Users
- PKI
- Digital Signature

Endopoint Protect
- Antivirus, EDR
- MDM, BYOD
- Secure eMail
- CASB

Data Protect
- Data Leak Prevention
- Information Rights Mgmt
- CASB

Network Protect
- Firewalls, WAF, Anti Bot
- Proxy, NAC, IPS/IDS
- Cloud security
- Cloud Workload Protect

Vulnerabilities Management
- Vulnerability Management
- Hardening
- Virtual Patching

Sec Audit
- Ethical Hacking
- Red team & Blue team
- GDPR / ISOs
- ISMS

Digital Survelliance
- Identification & Alert
- Open Sources & "Dark" Web
- Correlation

ISO 2000 Government		ISO 27001 ISMS	
CMMI SW Development	**NATO** Security Clearance **NATO SECRET level**	**PMI** Project Management	**CEH™** Certified Ethical Hacker
CERT Carnege Mellon University	**CISSP** Certified Information Systems Security Professional	**CISA** Certified Information Systems Auditor	**CISM** Certified Information Security Manager

En progreso de certificación FIRST, CSIRT,TF-CSIRT, ISO22301, ENS Nivel Alto

Caso Éxito - GISS

Datos del Proyecto

- Migración + Soporte y Mantenimiento
- Duración: 2 años (3 meses implantación completa)
- Aprox 1,3M €

Alcance

- 36.000 Dispositivos (Windows, Linux, MAC)
- 37.000 Usuarios Correo
- 3.000 Usuarios Móviles
- 3.000 Usuarios Protección AD

Solución

- Protección Endpoint y servidores + EDR + Sandbox
- Protección correo Exchange Local + Sandbox
- Protección usuarios Navegación (IOS, Android, Windows)
- Protección Directorio Activo
- Navegación

Gerencia de Informática de la Seguridad Social

Caso de éxito: NIX

Junta de Andalucía

Servicios Troncales de Comunicaciones y Seguridad

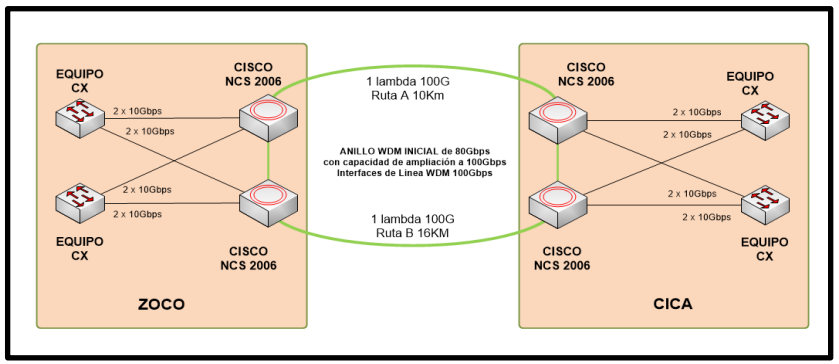
IMPORTE
9.516.571,68 € + IVA

NIX Avanzado	NIX BÁSICO	
4500 SEDES	+4500 Centros de enseñanza	1.600.000 Alumnos

Infoblox
FORTINET
FORCEPOINT
BROADCOM
allot

Transmisión
Conmutación

CISCO



ISO 27001 | ENS (AAP 6) | PILAR

inetum
Positive digital flow

Equipo especializado: **23 miembros**

- Firewalls PS/IDS
- Navegación Proxy
- Autenticación Unificada
- Gestión de Certificados
- Protección Avanzada
- WAF
- Protección DDoS
- Registro Unificado de Actividad
- Cifrado logs
- Monitorización
- Gestión de QoS
- Gestión especializada de routing
- Sandbox

inetum

Positive digital flow

inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND | POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA | CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI | COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE