Innovating for the Future

Cisco’s 3-Year Strategy

John Dominguez
Territory Business Manager
Andean Region

Customer Priorities

- Reimagine Applications
- Power Hybrid Work
- Transform Infrastructure
- Secure Enterprise

Our Strategy

Help customers connect, secure and automate to accelerate their digital agility in a cloud-first world

Cisco’s

Strategic Pillars

- Secure, Agile Networks
- Optimized Application Experiences
- Future of Work
- Internet for the Future
- End-to-End Security
- Capabilities at the Edge

Our Commitment

To drive the most trusted customer experience in the industry, through our innovation, choice and extraordinary people

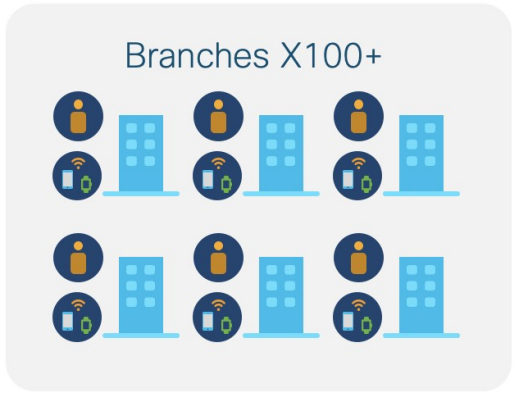
Arquitectura de Seguridad Empresarial

Miguel Torrez Zamora

Systems Architect

Andean Region

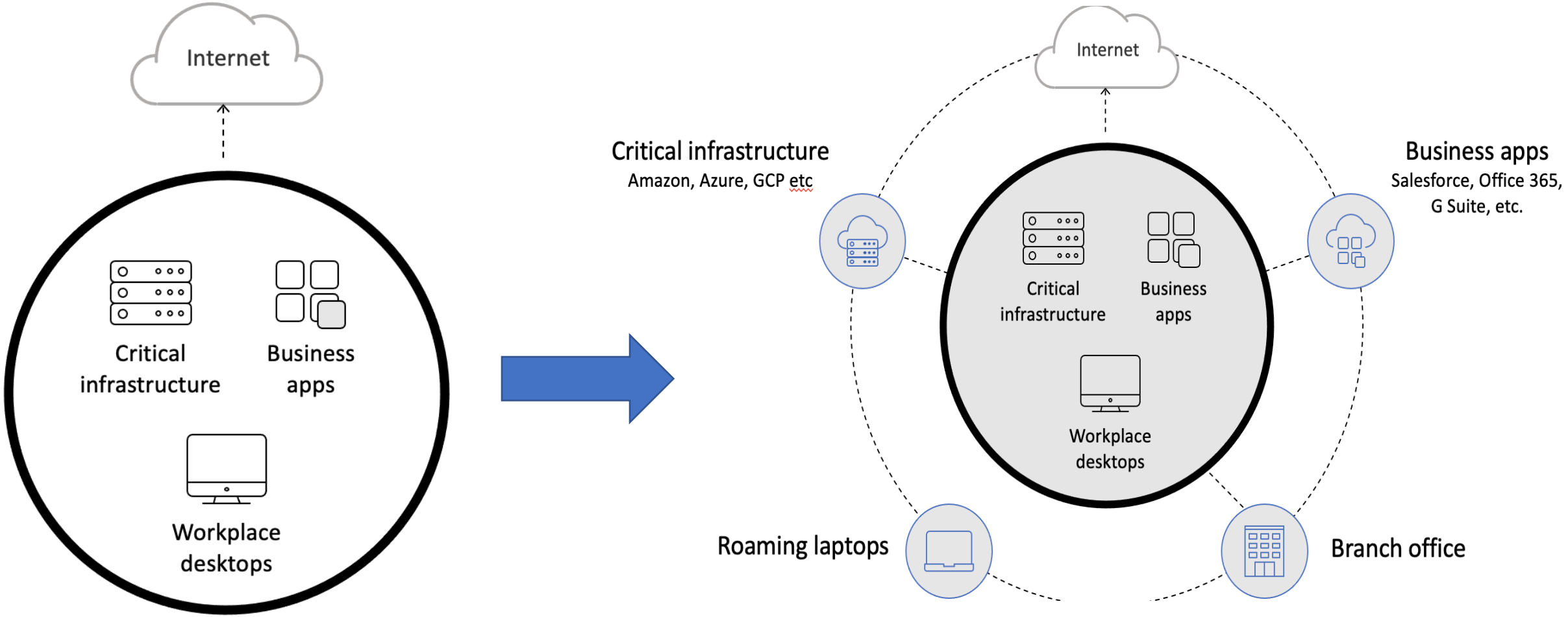
Entorno empresarial actual



- Explosión de dispositivos
- Fuerza de trabajo distribuida
- Uso de múltiples nubes

- Poca visibilidad
- Pocos expertos
- Poca integración

Entorno empresarial actual



Desafíos

TRANSFORMACION DIGITAL

Aprovechar los beneficios de la nube, la movilidad y el IoT.

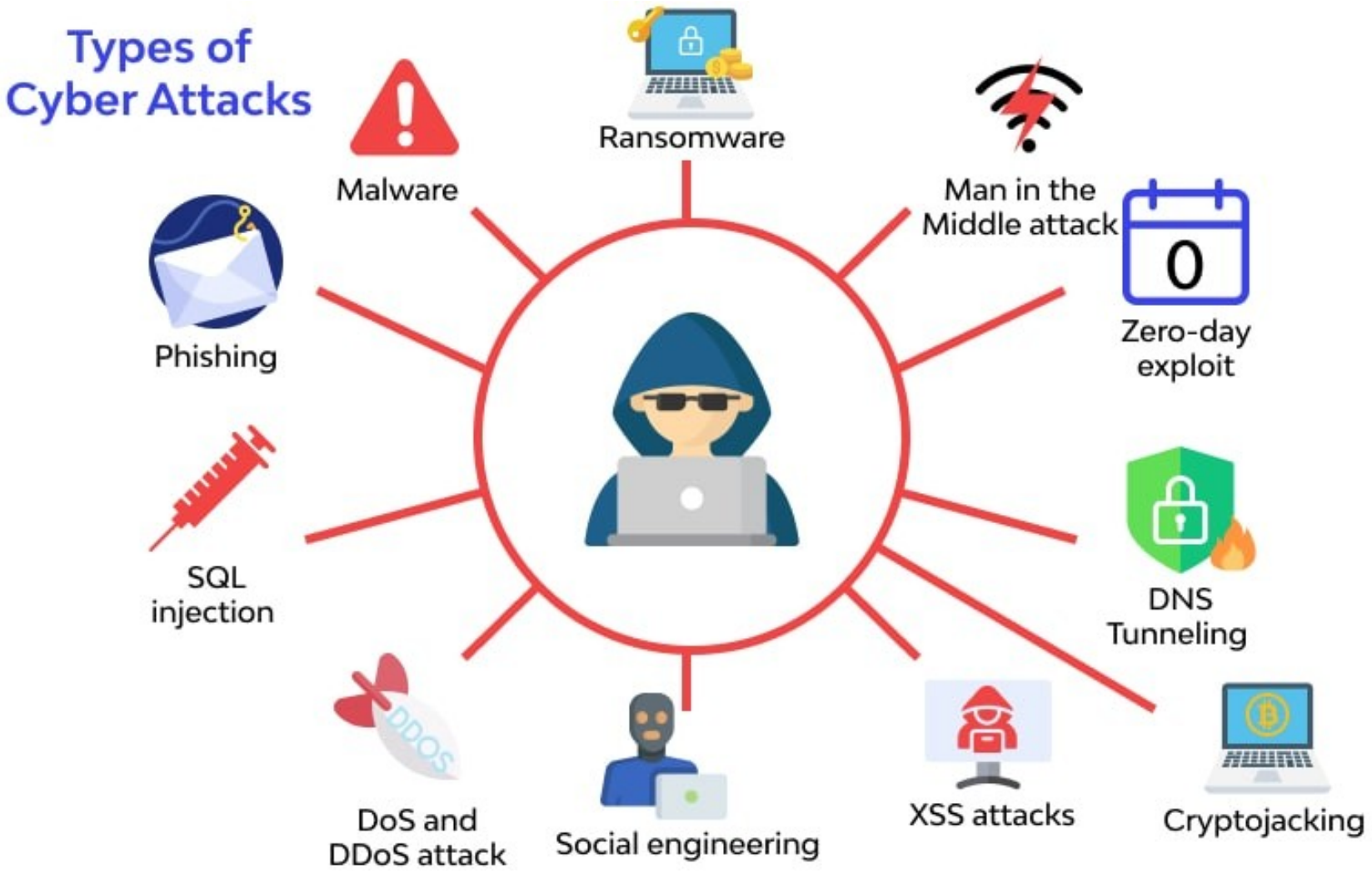
CANTIDAD DE AMENAZAS CRECIENTE

Proteger contra mas y nuevos vectores

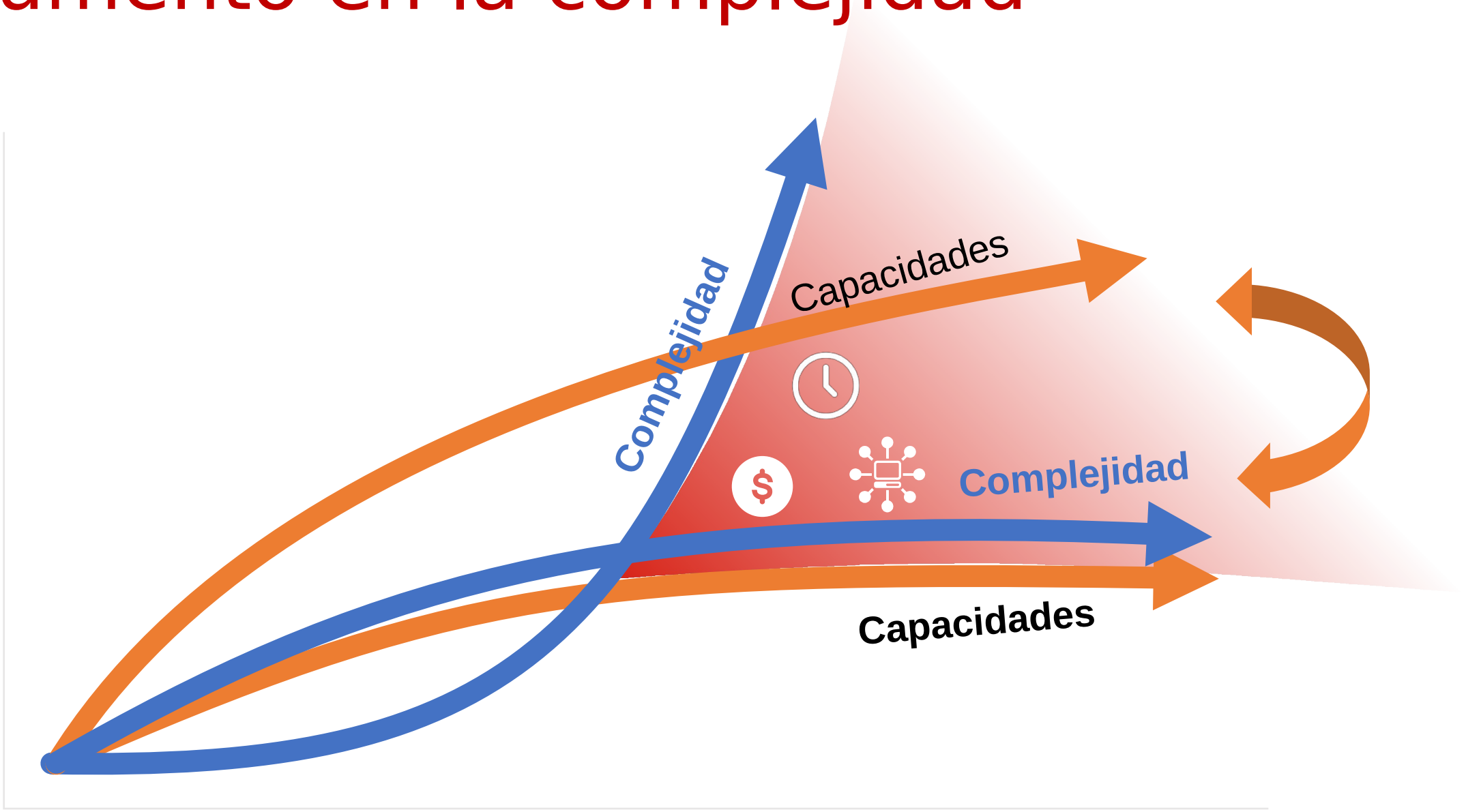
AUMENTO EN LA COMPLEJIDAD

Simplificar operaciones y reducir costos

Cantidad creciente de amenazas



Aumento en la complejidad



Transformación digital

En los últimos años:

¿Tiene un problema?

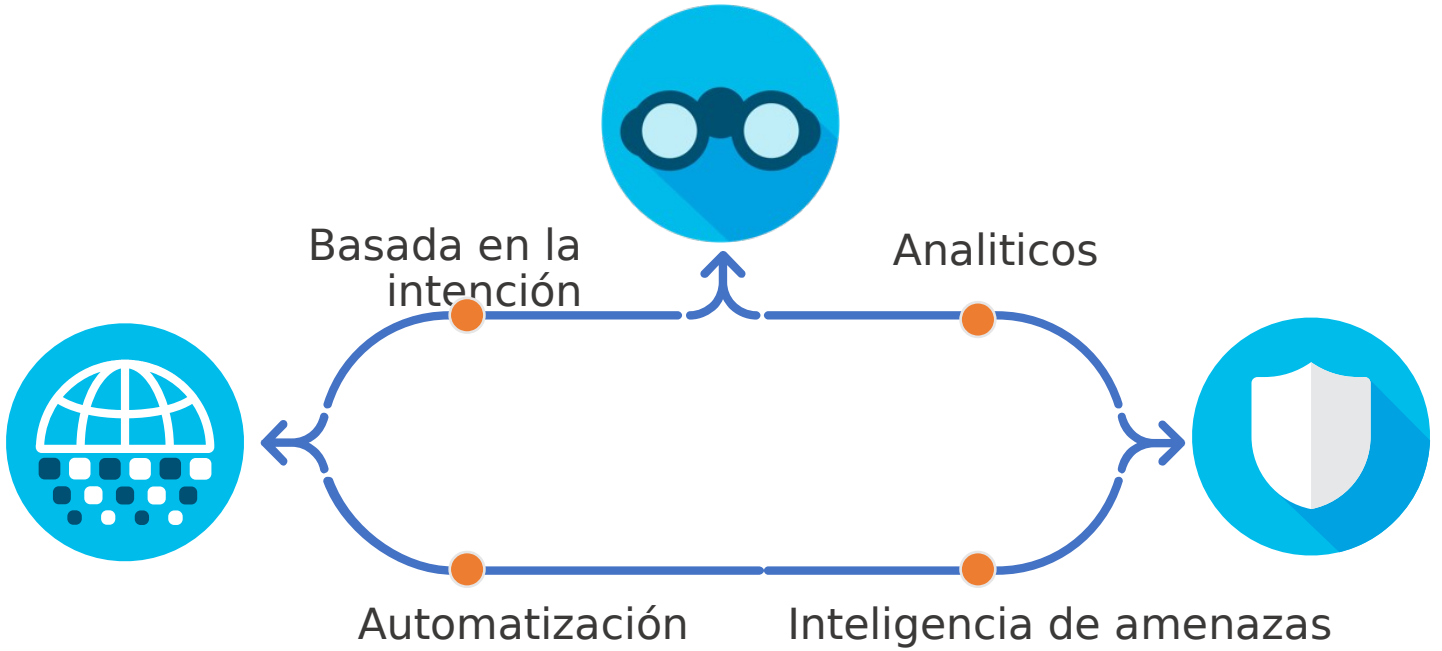
¿Que tan efectiva es nuestra política de seguridad?

¿Donde empezamos?

Se necesita una arquitectura de seguridad

Visibilidad

No puedo proteger lo que no puedo ver



Segmentación

Reducir el alcance del ataque

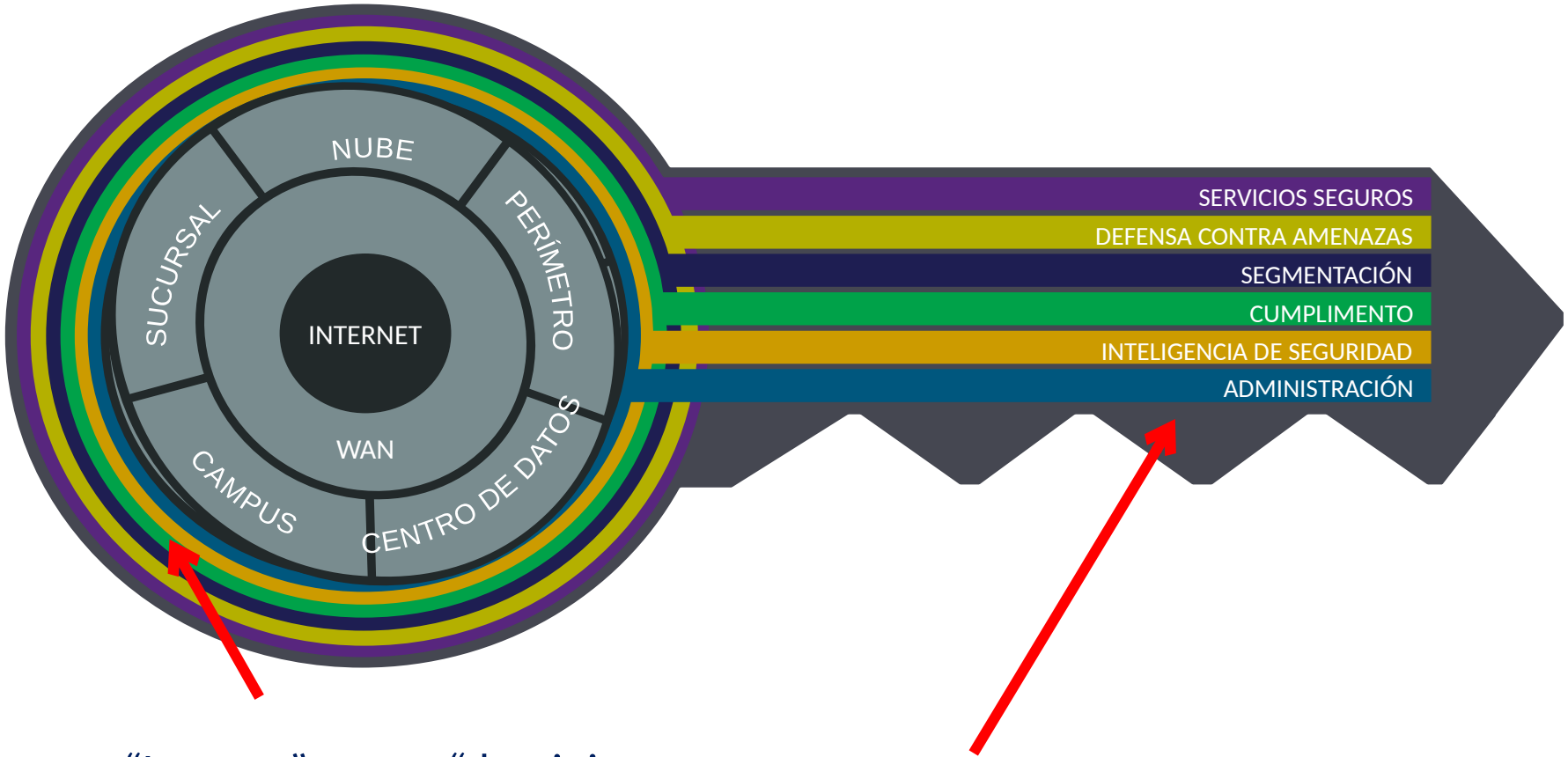
Protección

Detener los ataques

Metodología

1. Dividir la infraestructura – PIN
2. Categorizar los riesgos y amenazas.
3. Construir la solución de seguridad:
    1. Funciones
    2. Arquitectura
    3. Bajo nivel

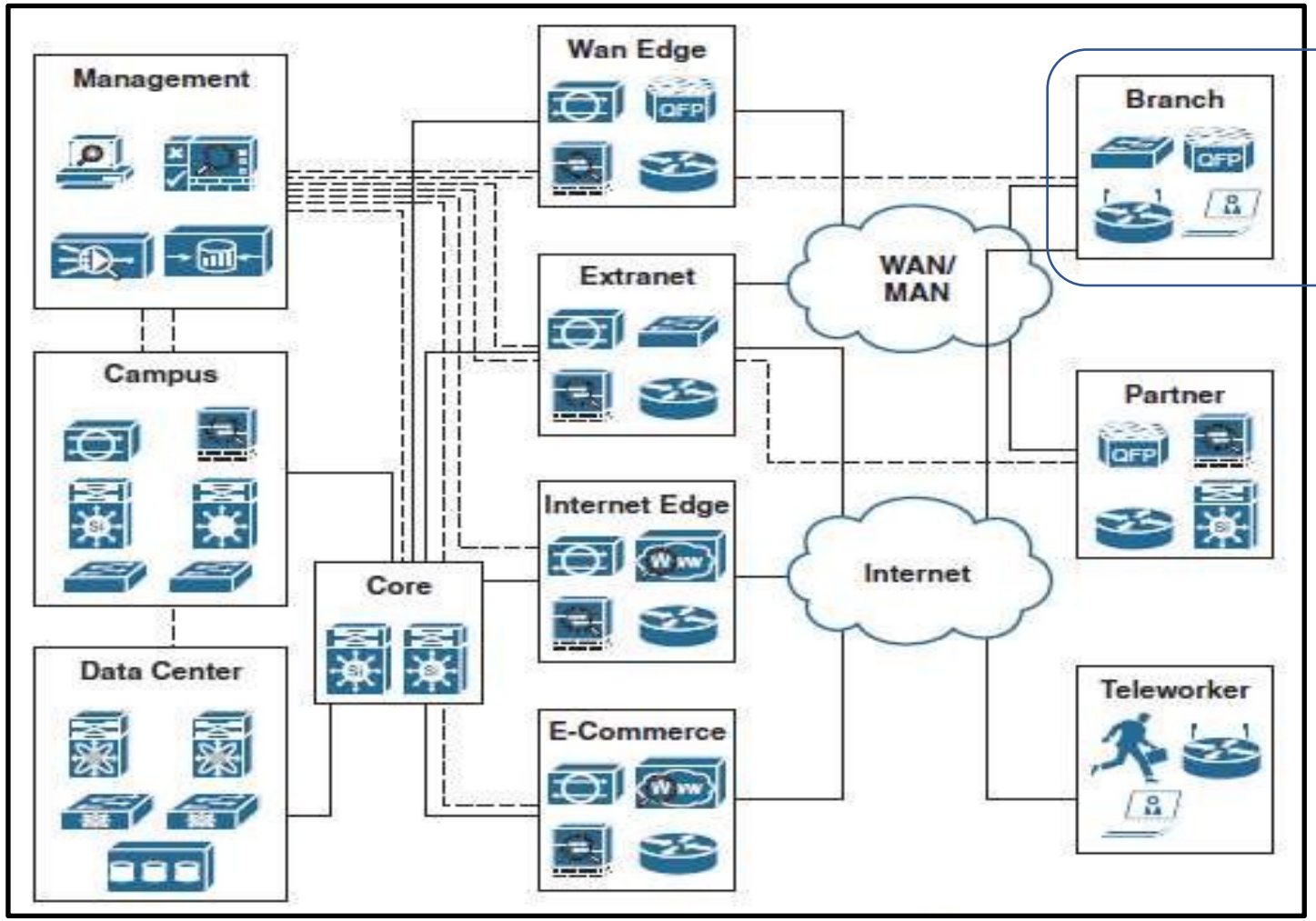
Enfoque de arquitectura no de producto



“Lugares” y “dominios seguros

Dividir la infraestructura

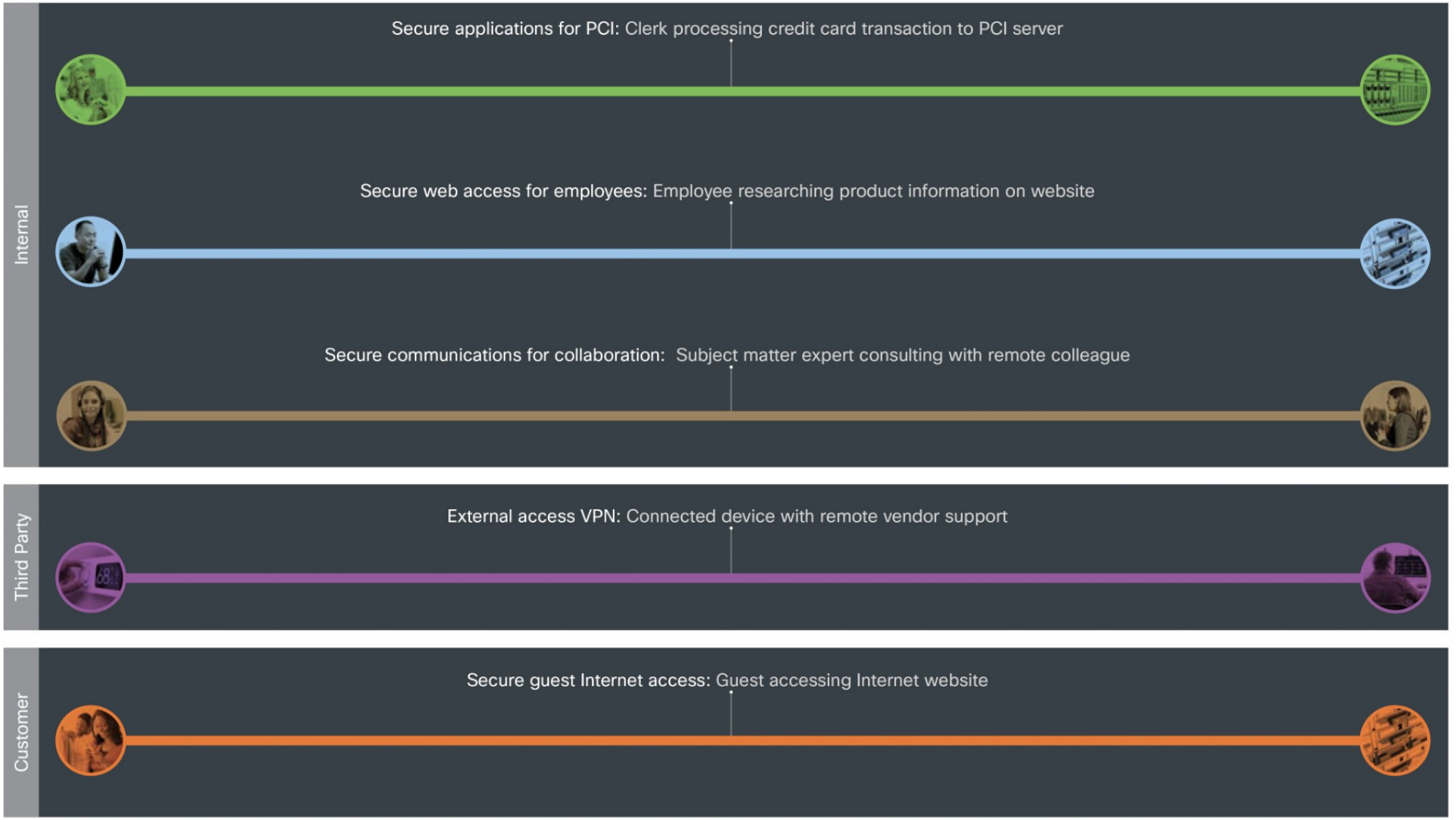
La estrategía de seguridad extremo a extremo



Ejemplo

Categorizar los riesgos

Identificar los flujos



Categorizar los riesgos

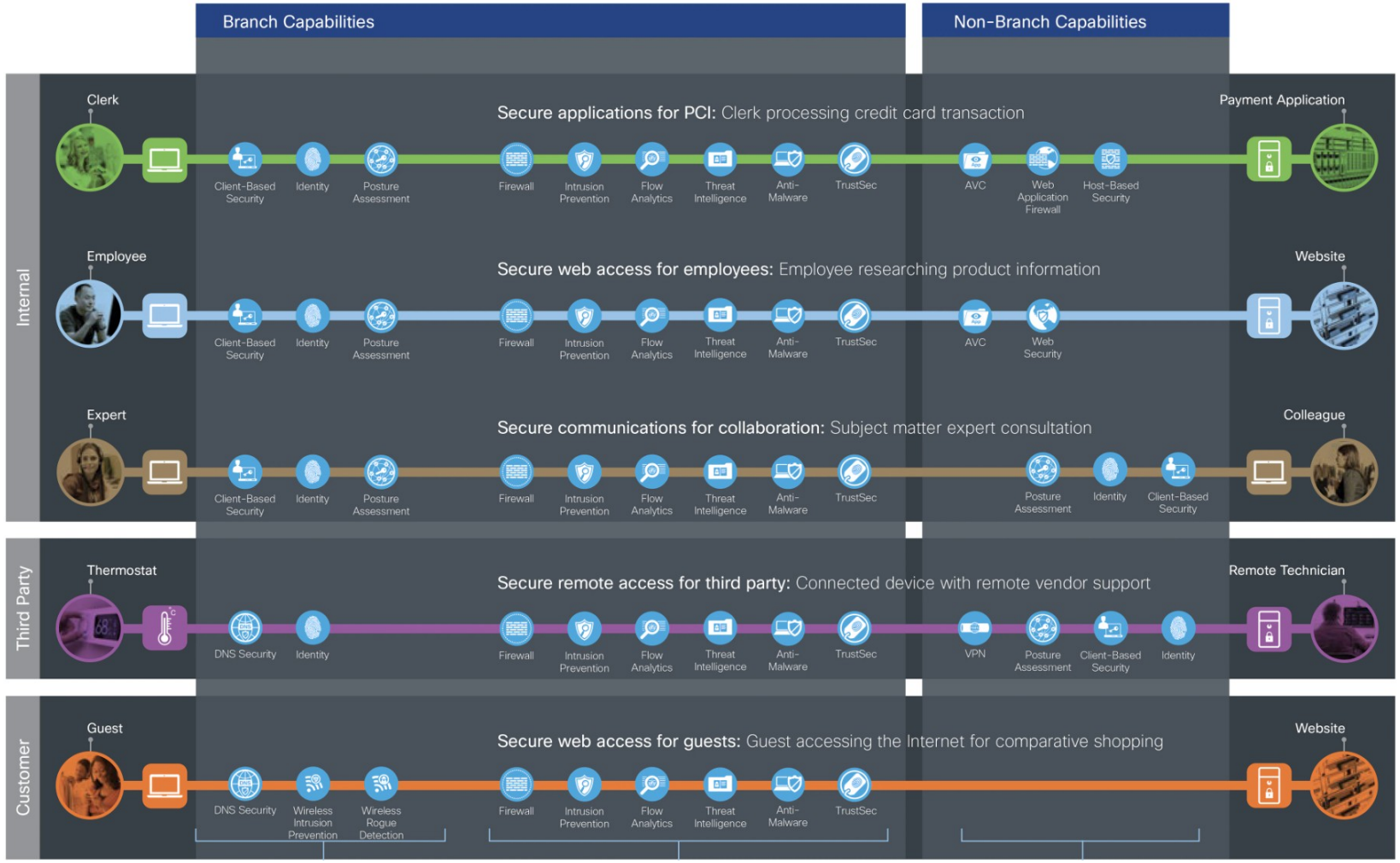
Identificar las amenazas

Categorizar los riesgos

Identificar el impacto

Categorizar los riesgos

Mapear con las capacidades requeridas



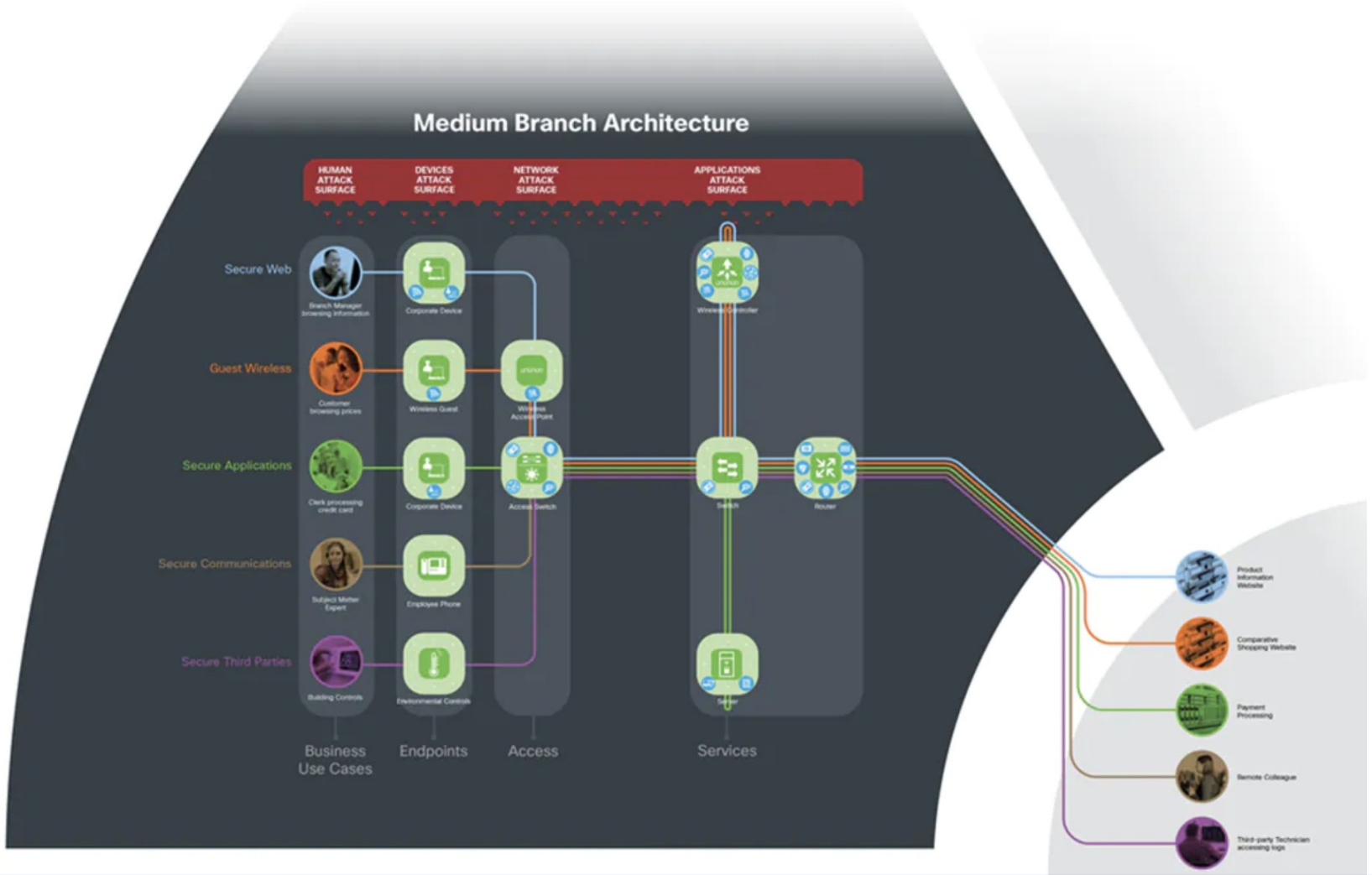
Categorizar los riesgos

Mapear con las capacidades requeridas

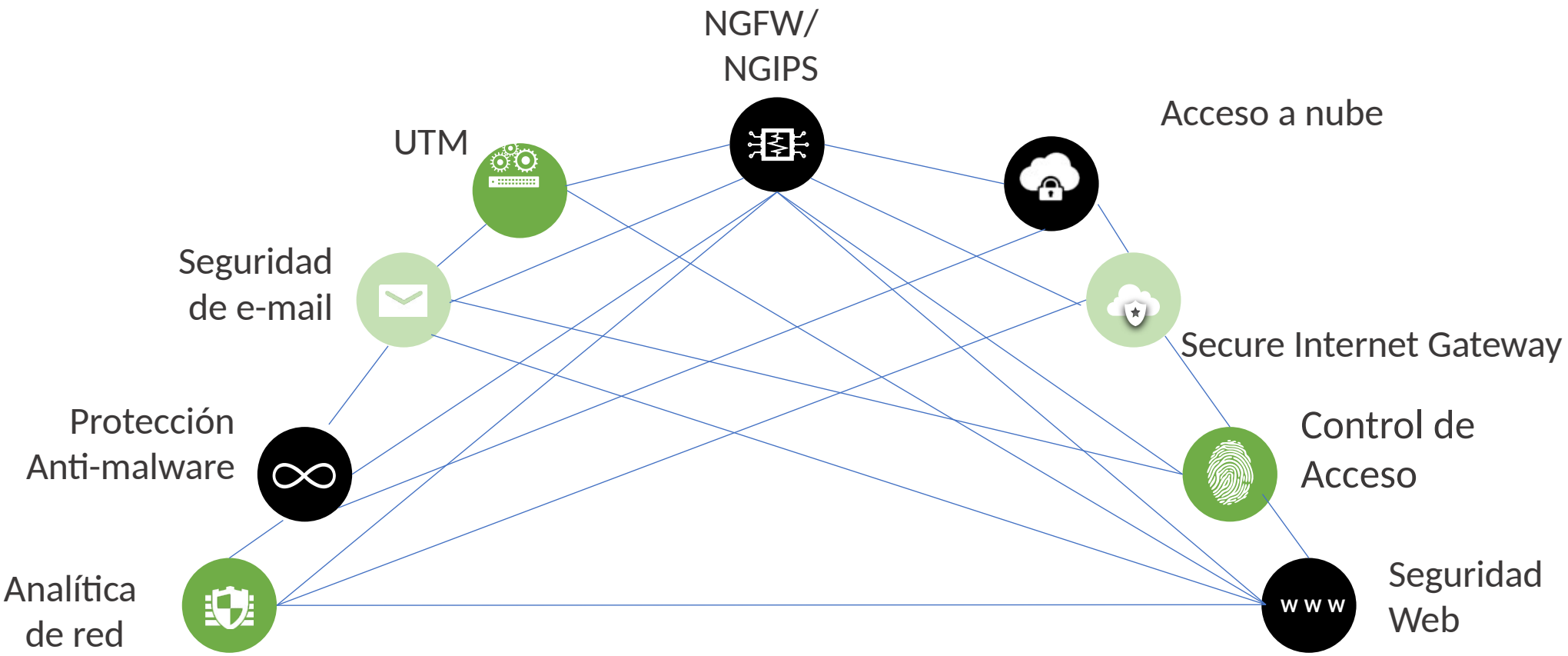
AMENAZA	CAPACIDAD
Atacantes accediendo a información restringida	Acceso basado en la identidad
Ataques de red desde usuarios externos	Segmentación
Ataques usando virus, gusanos, etc	Prevención de intrusiones
Distribución de malware entre cargas de trabajo	Anti-malware
Exfiltración de datos, amenazas encubiertas	Analítica de flujos
Redirección de sesiones a dominios maliciosos	Seguridad DNS
Explotar vulnerabilidades no parchadas	Evaluación de vulnarabilidades e inventario de cargas
	Evaluación de postura de seguridad

Construir la solución de seguridad

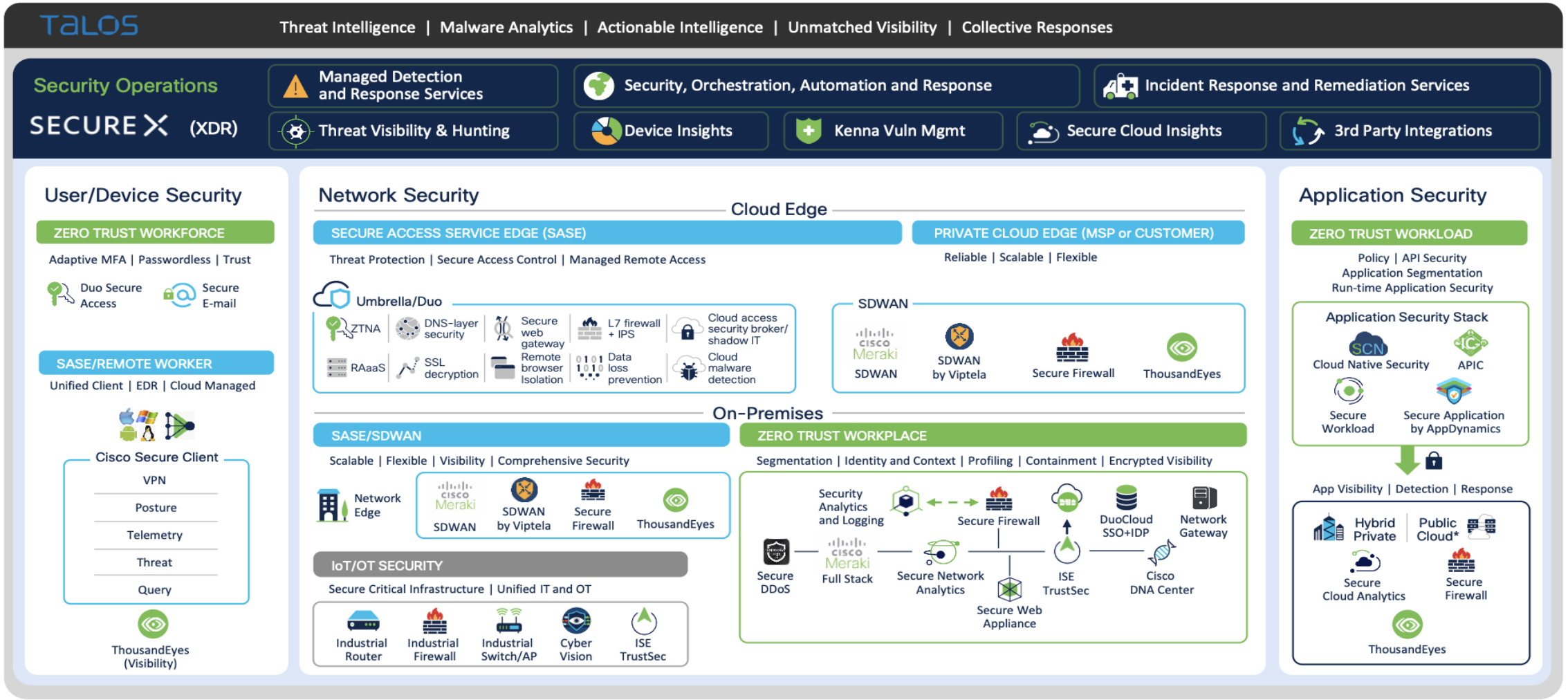
Diseño alto nivel



Arquitectura



Seguridad E2E
Portafolio



Gracias!